साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम

यूनियन बैंक
ऑफ इंडिया
अच्छे लोग, अच्छा बैंक

Union Bank
of India
Good people to bank with

साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम

संपादक
राजेश कुमार

यूनियन बैंक ऑफ इंडिया
Union Bank of India

केंद्रीय कार्यालय, यूनियन बैंक भवन,
239, विधान भवन मार्ग, नरीमन पाइंट, मुंबई - 400 021

यूनियन बैंक ऑफ इंडिया Union Bank of India

राजभाषा कार्यान्वयन प्रभाग
मानव संसाधन विभाग
केंद्रीय कार्यालय, मुंबई - 400 021
फोन : 022 22896517 / 22896540

साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम

(आंतरिक परिचालन हेतु)

मुद्रक :
उचित ग्राफिक प्रिंटर्स प्रा. लि.
फोन 022-40336400

राजकिरण रै जी.
प्रबंध निदेशक एवं सी.ई.ओ.

यूनियन बैंक
ऑफ इंडिया

प्रिय यूनियनाइट्स,

मुझे यह जानकर हार्दिक प्रसन्नता हुई कि इस वर्ष हमारे बैंक द्वारा 'साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम' नामक पुस्तक का प्रकाशन किया जा रहा है. सुरक्षा का अर्थ जीवन में होने वाली संभावित हानि से बचाव की व्यवस्था है. आज तकनीक के इस युग ने विश्व को एक ग्लोबल विलेज बना दिया है. इंटरनेट ने जहां इस विश्व को ज्ञान के अपार भंडार एवं अनेकों प्रकार की सुविधाओं एवं जानकारियों से सुसज्जित किया है, वहीं साइबर क्राइम जैसी भयावह समस्या को भी जन्म दिया है, जिसमें हैकर्स द्वारा आए दिन विभिन्न संस्थाओं विशेषकर वित्तीय प्रतिष्ठानों के कंप्यूटर नेटवर्क पर सेंध लगाई जाती है, जिसका उद्देश्य उन्हें आर्थिक नुकसान पहुंचाना या उनसे जुड़े ग्राहकों के डाटा को चुराना या नष्ट करना है.

आज बैंकिंग में लगभग 70% लेनदेन डिजिटली किए जा रहे हैं, जिनमें इंटरनेट बैंकिंग एवं मोबाइल बैंकिंग अधिक प्रचलित माध्यम हैं. एक ओर बैंकिंग उद्योग में इन तकनीकों ने अपना नया महत्वपूर्ण स्थान बनाया है, वहीं इनके प्रयोग में तनिक भी लापरवाही से साइबर क्राइम का खतरा दिनोंदिन बढ़ता जा रहा है. इन खतरों से बचने के लिये साइबर सुरक्षा आज समय की मांग बन चुकी है.

जागरूकता ही सुरक्षा का आधार है एवं साइबर क्राइम से बचाव संबंधी जागरूकता प्रदान करने की दिशा में इस पुस्तक का प्रकाशन एक प्रशंसनीय प्रयास है. हर एक संस्था अपना डाटा एकत्रित कर उसे अपने सिस्टम, कंप्यूटर आदि अन्य उपकरणों में रखती है. 'साइबर सुरक्षा' ऐसे में सबसे महत्वपूर्ण आवश्यकता है क्योंकि ऐसा डाटा चोरी हो जाने से संस्था की प्रतिष्ठा पर तो आंच आती ही है, ग्राहक की भी निजी ज़िंदगी प्रभावित हो सकती है. नेशनल क्राइम रिकार्ड्स ब्यूरो की रिपोर्ट के अनुसार साइबर अपराध की दर वर्ष प्रति वर्ष बढ़ती ही जा रही है, इसलिए साइबर खतरों पर अंकुश लगाने के लिए अंतर्राष्ट्रीय स्तर पर भी कई प्रयास किए जा रहे हैं.

इस पुस्तक में लेखकों ने साइबर सुरक्षा से जुड़े विभिन्न विषयों पर अपने अनुभवों को साझा किया है. मुझे पूर्ण विश्वास है कि यह पुस्तक हमारे पाठकों एवं स्टाफ सदस्यों के लिए अत्यंत उपयोगी एवं ज्ञानवर्धक सिद्ध होगी. मैं इस पुस्तक के प्रकाशन से जुड़े सभी सदस्यों को हार्दिक शुभकामनाएं देता हूँ एवं उम्मीद करता हूँ कि इस तरह के महत्वपूर्ण विषयों पर प्रकाशन आगे भी जारी रहेगा.

हार्दिक शुभकामनाओं सहित,

राजकिरण रै जी

गोपाल सिंह गुसाईं
कार्यपालक निदेशक

यूनियन बैंक
ऑफ इंडिया

प्रिय साथियो,

सभी यूनियनाइट्स को शताब्दी वर्ष की हार्दिक शुभकामनाएं. राजभाषा के रूप में हिंदी को भारत के संविधान में शामिल हुए 70 वर्ष का समय बीत चुका है और सरकारी कामकाज में इसे प्रधानता प्रदान करने के हर संभव प्रयास अभी भी जारी हैं. मुझे प्रसन्नता है कि हमारा बैंक वर्ष प्रति वर्ष बैंकिंग जगत के महत्वपूर्ण, ज्वलंत एवं समीचीन विषयों पर ज्ञानवर्धक तथा उपयोगी जानकारी प्रदान करने के उद्देश्य से वर्ष 2008 से बैंकिंग के विभिन्न विषयों पर पुस्तक का प्रकाशन कर रहा है, जो जटिल विषयों को हिंदी में जानने की दिशा में मील का पत्थर साबित हुआ है. इसी श्रृंखला में हमारे बैंक द्वारा इस वर्ष 'साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम' पुस्तक का प्रकाशन किया जा रहा है, जो पुस्तक प्रकाशन की श्रृंखला में बैंक द्वारा प्रकाशित होने वाली 11वीं पुस्तक है. इस पुस्तक की विषय सामग्री का अवलोकन करने पर मुझे और भी प्रसन्नता है कि सामग्री का संकलन व प्रस्तुतीकरण अपने ही बैंक के अनुभवी स्टाफ सदस्यों द्वारा किया गया है.

डिजिटल इंडिया भारत सरकार की एक महत्वकांक्षी योजना है, लेकिन डिजिटल तकनीक के इस दौर में साइबर सुरक्षा एक बड़ी चिंता है. हम जैसे-जैसे नई तकनीक को अपना रहे हैं, उसमें सेंधमारी का खतरा उतना ही बढ़ रहा है. देश में साइबर सुरक्षा से जुड़ी चिंता गहराती जा रही है. इलेक्ट्रोनिक और सूचना प्रौद्योगिकी मंत्रालय के अनुसार देश में साइबर सुरक्षा एक बहुत बड़ी चुनौती है, जिस से किसी भी प्रकार का समझौता करना आर्थिक नुकसान का कारण बन सकता है, साथ ही इससे संस्था की छवि पर भी विपरीत प्रभाव पड़ता है.

8 नवंबर 2016 को नोटबंदी की घोषणा के उपरांत भारत में कैशलेस इकोनॉमी को बहुत बढ़ावा मिला है. डिजिटल वालेट का चलन बढ़ा है. भारत एक ऐसा देश है, जहां काफी लोग आज भी डिजिटल लेनदेन करने में स्वयं को असहज महसूस करते हैं. ऐसे में ग्राहकों को डिजिटल लेनदेन के प्रति जागरूक करना व उन्हें पूर्णतः सुरक्षित ऑनलाइन बैंकिंग प्लैटफ़ार्म उपलब्ध कराना हमारी जिम्मेदारी है. यदि ग्राहकों संबंधी डाटा की सुरक्षा के पुख्ता इंतजाम नहीं किए गए तो ऑनलाइन मौजूद सभी दस्तावेजों, बैंक की जानकारी और गोपनीयता में कभी भी सेंध लग सकती है.

इस पुस्तक में साइबर सुरक्षा और डिजिटल बैंकिंग के सभी विषयों पर विस्तार से प्रकाश डालने का प्रयास किया गया है. बदलते वक्त के इस दौर में समाज को प्रगति की ओर अग्रसर करने के लिए इन विषयों का ज्ञान होना सभी के लिए आवश्यक है. मुझे यकीन ही नहीं पूर्ण विश्वास है कि यह पुस्तक सुधी पाठकों और स्टाफ सदस्यों के लिए अत्यंत उपयोगी और ज्ञानवर्धक सिद्ध होगी. इस पुस्तक के प्रकाशन हेतु राजभाषा कार्यान्वयन प्रभाग का विशेष रूप से धन्यवाद करता हूं और उम्मीद करता हूं कि हमारा बैंक भविष्य में भी बैंकिंग संबंधी अन्य महत्वपूर्ण विषयों पर हिंदी में पुस्तकें प्रकाशित करने की इस परंपरा को कुशलतापूर्वक जारी रखेगा.

हार्दिक शुभकामनाओं सहित,

दिनेश कुमार गर्ग
कार्यपालक निदेशक

यूनियन बैंक
ऑफ इंडिया

प्रिय साथियो,

अत्यंत प्रसन्नता का विषय है कि गत वर्षों की भांति इस वर्ष भी हमारे बैंक द्वारा बैंकिंग विषयों पर पुस्तक प्रकाशन के अंतर्गत "साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम" नामक पुस्तक का प्रकाशन किया जा रहा है. मैं उन सभी स्टाफ़ सदस्यों को धन्यवाद देता हूँ, जिन्होंने इस पुस्तक के लिए लेख लिखे और प्रकाशन में अपना योगदान दिया है.

साइबर सुरक्षा और डिजिटल बैंकिंग एक सिक्के के दो पहलू हैं. साइबर सुरक्षा के बिना डिजिटल इंडिया - डिजिटल बैंकिंग की कल्पना असंभव है. आज जिस तरह से इंटरनेट का विस्तार हो रहा है, साइबर क्राइम भी उसी गति से बढ़ता जा रहा है. नेटवर्क कनेक्शन और इंटरनेट ने पूरी दुनिया को एक मुट्ठी में कैद कर लिया है जिसके कारण साइबर सुरक्षा का पूरा ध्यान रखना आवश्यक हो गया है.

निरंतर बदलती तकनीक की वजह से साइबर सुरक्षा काफी चुनौती भरा काम हो गया है. रेनसमवेयर, मालवेयर, सोशल इंजीनियरिंग और फिशिंग ये सभी ऐसे साइबर अपराध हैं, जिससे किसी भी कंप्यूटर या सिस्टम या मोबाइल को हैक कर बड़ी चालाकी से सभी डाटा चुराया जा सकता है. इस डाटा के कुछ भाग काफी महत्वपूर्ण भी होते हैं, जिसके चोरी हो जाने से किसी के जीवन पर बहुत ही गहरा प्रभाव पड़ता है. अधिकतर साइबर क्राइम डिजिटल बैंकिंग एवं इंटरनेट बैंकिंग में ही देखे गए हैं. पलक झपकते ही लाखों रुपए की धोखाधड़ी हो जाती है और लोग हाथ मलते रह जाते हैं. उस समय उनके सामने केवल लाचारी ही प्रकट होती है. अतः डाटा सुरक्षित रखने के लिए साइबर सुरक्षा तो आवश्यक है ही पर इसके साथ ही हमें अपने कार्यालयीन कार्यों के साथ ही साथ व्यक्तिगत रूप से, विशेषकर मोबाइल का प्रयोग करते समय स्वंय भी बहुत ही सावधानी बरतनी होगी.

"साइबर सुरक्षा एवं डिजिटल बैंकिंग" पुस्तक में साइबर क्राइम, साइबर सुरक्षा एवं डिजिटल बैंकिंग संबंधी विविध विषयों की गहन जानकारी प्रस्तुत की गई है, जिसका अध्ययन पाठकों के लिए अत्यंत ही उपयोगी साबित होगी. मैं आशा करता हूँ कि बैंकिंग एवं साइबर सुरक्षा से जुड़ी सम-सामयिक विषयों पर हिन्दी में पुस्तक प्रकाशन की यह परंपरा आगे भी इसी प्रकार भी जारी रहेगी और नए-नए विषयों पर पुस्तकों का प्रकाशन किया जाता रहेगा.

शुभकामनाओं के साथ,

मानस रंजन बिस्वाल
कार्यपालक निदेशक

यूनियन बैंक
ऑफ इंडिया

प्रिय साथियो,

मुझे इस बात की अत्यधिक प्रसन्नता है कि बैंक द्वारा हिन्दी पुस्तक प्रकाशन के क्रम में प्रत्येक वर्ष की भांति इस वर्ष भी "साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम" नामक पुस्तक प्रकाशित की जा रही है. इस पुस्तक में साइबर हमलों एवं उससे बचने के उपायों से संबंधित विभिन्न विषयों को समाहित किया गया है. साइबर सुरक्षा से अभिप्राय डिजिटल हैकरों से कम्प्यूटर, नेटवर्क, डाटा एवं प्रोग्राम की सुरक्षा करना है. ये हमले आमतौर पर हमारी संवेदनशील जानकरियों तक पहुंचने, बदलने अथवा उन्हें नष्ट करने के उद्देश्य से किए जाते हैं. इस बात से हम सभी सहमत हैं कि वित्तीय संस्थानों विशेषतः बैंकों में साइबर सुरक्षा अनिवार्य है और डिजिटलाइजेशन के इस दौर में साइबर अटैक से बचना हमारे लिए बेहद आवश्यक है.

तकनीक के विकास ने मनुष्य को इंटरनेट पर पूर्णरूपेण निर्भर बना दिया है और इंटरनेट ने दुनिया को एक मुठ्ठी में समेट लिया है. इंटरनेट पर लोगों की निर्भरता एवं तकनीक के बढ़ते विकास में साइबर हमलों से स्वयं को सुरक्षित रखना ही साइबर सुरक्षा है. जहां डिजिटलाइजेशन से लोगों की जीवन-शैली में काफी परिवर्तन आया है, वहीं इससे होने वाली समस्याओं का भी हमें सामना करना पड़ रहा है. जिस प्रकार साइबर अटैक की गति बढ़ती जा रही है, उसी प्रकार लोगों में इन हमलों से बचने के लिए अपने हार्डवेयर एवं सॉफ्टवेयर को साइबर हमलों से सुरक्षित रखने की आवश्यकता भी बढ़ती जा रही है.

साइबर अटैक से बचने के लिए हमें सुरक्षित एवं विश्वसनीय कार्यप्रणाली का उपयोग सुनिश्चित करने के साथ ही इंटरनेट सुरक्षा के मुद्दों पर एक सामान्य समझ विकसित करनी चाहिए. हमें सदैव इस बात का ध्यान रखना चाहिए कि इंटरनेट बैंकिंग या बैंकिंग लेनदेनों को करते समय कभी भी सार्वजनिक स्थानों पर उपलब्ध वाई-फाई का उपयोग न करें. इसके लिए अपने पर्सनल कम्प्यूटर या लैपटॉप का ही प्रयोग करें. पासवर्ड टाइप करने के बाद कंप्यूटर द्वारा पूछे जा रहे "ऑप्शन रिमेंबर पासवर्ड" या "कीप लॉगिन" पर क्लिक न करें. साइबर हैकरों द्वारा प्रयोग में लाए जा रहे नकली वेबसाइटों से बचने के लिए किसी अनजान व्यक्ति से प्राप्त ईमेल में दिए गए यूआरएल पर क्लिक कर उसे न खोलें.

मुझे प्रसन्नता है कि इस पुस्तक में डिजिटल बैंकिंग एवं उससे संबंधित सुरक्षा के विविध पहलुओं पर गंभीरता से विचार किया गया है, जो आपके लिए काफी उपयोगी सिद्ध होगी. मैं इस उत्कृष्ट कार्य से संबंधित सभी लेखकों एवं संपादक मण्डल की प्रसंशा करता हूँ एवं यह आशा व्यक्त करता हूँ कि सम-सामयिक विषयों पर पुस्तकों के प्रकाशन का यह कार्य भविष्य में भी जारी रहेगा.

हार्दिक शुभकामनाओं के साथ

मानस बिस्वाल

ब्रजेश्वर शर्मा
महा प्रबंधक (मा.सं.)

यूनियन बैंक
ऑफ इंडिया

प्रिय साथियो,

यह अत्यंत हर्ष का विषय है कि हमारा बैंक प्रति वर्ष बैंकिंग के ज्वलंत विषयों पर हिन्दी में लेख संकलित कर पुस्तक प्रकाशित कर रहा है. हमारे बैंक द्वारा वर्ष 2008 से शुरू हुई पुस्तक प्रकाशन की इस श्रृंखला में विभिन्न विषयों पर जैसे मानव संसाधन, संव्यवहार बैंकिंग, खुदरा बैंकिंग, ग्राहक सेवा, डिजिटल बैंकिंग, सुरक्षा, वित्तीय समावेशन तथा कृषि विकास जैसे महत्वपूर्ण विषयों पर उत्कृष्ट पुस्तकों का प्रकाशन किया गया है तथा इसी क्रम में इस वर्ष 'साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम' पुस्तक का प्रकाशन एक सराहनीय पहल है. साइबर सुरक्षा आज के युग में बैंक के साथ-साथ विश्व अर्थव्यवस्था की प्राथमिक आवश्यकता है.

बैंकों में इंटरनेट के बहुतायत प्रयोग से वर्तमान परिप्रेक्ष्य में सुरक्षा का महत्व और अधिक बढ़ गया है. वर्तमान समय में डिजिटल बैंकिंग कारोबार में लोगों की निर्भरता बढ़ती जा रही है. लोगों में हमेशा से यह धारणा रही है कि अपनी जमापूंजी को सुरक्षित रखने का सबसे उचित स्थान बैंक है, ऐसे में सुरक्षा की इस भावना को बरकरार रखना हम सभी बैंकरों का ग्राहकों के प्रति प्राथमिक उत्तरदायित्व बन गया है.

बदलते समय के साथ-साथ बैंकिंग की चुनौतियाँ भी बदल रही है तथा इस बदलती चुनौतियों में इंटरनेट बहुत हद तक शाखाओं में जाकर बैंकिंग लेनदेन करने की कठिनाइयों को आसान भी बना रहा है. एक तरफ जहां इंटरनेट हमारी मुश्किलों को आसान बना रहा है वहीं दूसरी तरफ यह हैकर्स को हमारी साइटों पर हमला करने का रास्ता भी बना रहा है. इस पुस्तक में प्रकाशित लेख हमे इंटरनेट पर मौजूद सभी सुविधाओं से अवगत तो कराते ही हैं, साथ ही साथ उसमें मौजूद खामियों तथा हैकर्स से बचने के रास्ते भी बताते हैं. हम सभी जानते हैं कि थोड़ी सी असावधानी बड़े से बड़े खतरे का निमंत्रण हो सकती है.

डिजिटल इंडिया के इस बढ़ते युग में आवश्यकता है संपूर्ण सुरक्षा की, जो सिर्फ कुछ लोगों तक सीमित न रहकर संपूर्ण समाज में व्याप्त हो. साइबर सुरक्षा वह पहलू है, जिसकी ज़िम्मेदारी प्रत्येक व्यक्ति को व्यक्तिगत रूप से लेनी होगी. ऐसी संपूर्ण सुरक्षा ही हमें हैकर्स के जाल से बचाकर, सफल डिजिटाइजेशन की ओर अग्रसर करेगी. इस पुस्तक में साइबर सुरक्षा एवं डिजिटल बैंकिंग से संबंधित महत्वपूर्ण विषयों पर उत्कृष्ट लेखों का संकलन किया गया है. मुझे पूर्ण विश्वास है कि यह पुस्तक पाठकों तथा स्टाफ सदस्यों के लिए अत्यंत उपयोगी साबित होगी. पुस्तक के सफल प्रकाशन के लिए मैं संपादक तथा सभी रचनाकारों को हार्दिक शुभकामनाएँ देता हूँ.

पुनः शुभकामनाओं सहित !

संपादक की कलम से

आज जब सम्पूर्ण विश्व पर विज्ञान का एकाधिकार हो चुका है, ऐसे समय में 'साइबर सुरक्षा एवं डिजिटल बैंकिंग के विविध आयाम' पुस्तक आप सभी के समक्ष प्रस्तुत करते हुए मुझे अपार हर्ष हो रहा है. इस पुस्तक के विषयों का चयन करते समय मेरे जहन में एक बात थी कि वर्तमान समय में मनुष्य इतना ज्यादा विज्ञान आश्रित हो गया है कि वह अपने भले-बुरे की परवाह किए बगैर तरह-तरह की सोशल साईटों पर अपना निजी विवरण फीड करता रहता है, इन घटनाओं को देखते हुए मेरे मन में यह बात उठी कि क्यूं न मैं कुछ ऐसे लेखों, विचारों और घटनाओं को आप सबके समक्ष लाऊं, जिससे पाठक यदि इन विषयों को संपूर्ण रूप से समझ कर अपनी रोजमर्रा की ज़िंदगी में ढाल लें, तो उनका हित अवश्य होगा. वो कहते हैं ना.....

सावधानी हटी, दुर्घटना घटी

अर्थात जो इंटरनेट आप को प्रत्येक विषय की जानकारी पलक झपकते दे सकता है, वही पलक झपकते ही आपकी जानकारी हैकर्स तक पहुंचा भी सकता है. आज एक तरफ सरकार डिजिटल इंडिया पर ज़ोर दे रही है, वहीं दूसरी तरफ साइबर सुरक्षा का खतरा भी बढ़ता जा रहा है. सेक्युरिटी लैंडस्केप एशिया-पेसफिक कंपनी ने वर्ष 2017 की अपनी रिपोर्ट में बताया है कि आने वाले समय में भारत दुनिया में फिशिंग, हैकिंग और ऑनलाइन ठगी के मामले में सबसे ज्यादा निशाने पर रहने वाला देश होगा, जाहिर है ऐसे में साइबर सुरक्षा को मजबूत करना सबसे बड़ी चुनौती है. जैसा कि हम सभी जानते हैं कि बैंकिंग के लिए फिशिंग कोई नई बात नहीं है. गाहे-बगाहे धोखाधड़ी की ऐसी घटनाएं सुनने में आती ही रहती हैं. इस पुस्तक में साइबर सुरक्षा से संबंधित पहलुओं पर बैंक के वरिष्ठ एवं अनुभवी स्टाफ सदस्यों द्वारा लिखे गए लेखों को समाहित किया गया है, जो आपके दैनिक एवं बैंकिंग जीवन में अपराधों की रोकथाम हेतु मार्गदर्शन करेंगे.

भारत में डिजिटाइजेशन का यह दौर अब थमने वाला नहीं है. जैसे-जैसे इसका प्रयोग बढ़ रहा है, वैसे-वैसे नई तकनीकें आती जा रही हैं. पाठकों को इन नई तकनीकों से अवगत कराना भी मैं आवश्यक समझता हूं, जिसे ध्यान में रखते हुए क्यू आर कोड, ब्लॉक चेन, ई-टेंडरिंग, ई-कामर्स, ई-मार्केट प्लेस, क्लाउड कंप्यूटिंग, इंटरनेट ऑफ थिंग्स, चैटबोट आदि जैसी नई तकनीकी विधाओं को इसमें विस्तार से शामिल किया गया है, जिससे आप इनके तकनीकी पहलुओं को और बारीकी से समझ सकें एवं उनका प्रयोग करते समय उनमें निहित सुरक्षा मानदंडों/जोखिमों का भी ध्यान रखें. आज आवश्यकता इस बात की भी है कि इन तकनीकों और इनसे जुड़े सुरक्षा मानकों/जोखिमों से ग्राहकों को भी जागरुक बनाया जाए, जिससे वे डिजिटल धोखाधड़ी से स्वयं को सुरक्षित रख सकें.

इस पुस्तक में साइबर सुरक्षा से संबंधित विभिन्न पहलुओं को बारीकी से समेटने का प्रयास किया गया है. मुझे विश्वास है कि साइबर सुरक्षा से संबंधित समस्याओं के समाधान में यह पुस्तक पाठकों की अपेक्षाओं पर खरी उतरेगी. इस पुस्तक की परिकल्पना को साकार करने के लिए मैं उच्च प्रबंधन से प्राप्त उनके मार्गदर्शन के प्रति कृतज्ञतापूर्ण आभार व्यक्त करता हूँ. मैं उन रचनाकारों का भी हृदय से आभार व्यक्त करता हूँ, जिन्होंने इस पुस्तक की परिकल्पना को साकार करने के लिए अपनी रचना के माध्यम से सहयोग प्रदान किया है. इसके साथ ही साथ, राजभाषा कार्यान्वयन प्रभाग की संपूर्ण टीम के प्रति मैं आभार व्यक्त करता हूँ, जिनके सक्रिय सहयोग के बिना यह कार्य संभव नहीं था. मैं आभार व्यक्त करता हूँ सहायक सेवाएँ विभाग की टीम का, जिन्होंने इस पुस्तक को मुद्रित कराने की जिम्मेदारी का बखूबी निर्वहन किया.

मुझे विश्वास है कि यह पुस्तक आपकी अपेक्षाओं पर खरी उतरेगी.

आपका

राजेश कुमार

यूनियन बैंक ऑफ इंडिया Union Bank of India

अनुक्रम

साइबर अपराध का वैश्विक बाज़ार

अनिल कुरील
उप महा प्रबंधक व मुख्य सूचना सुरक्षा अधिकारी
के. का. मुंबई

साइबर क्राइम, विश्व के प्रत्येक व्यक्ति, कंपनी और राष्ट्र के लिए सबसे बड़ा खतरा बनकर उभर रहा है और यह राष्ट्रों द्वारा लड़े जाने वाले सबसे बड़े युद्धों में से एक है. साइबर क्राइम का समाज पर प्रभाव वृहत संख्या में परिलक्षित होता है. साइबर सिक्योरिटी वेंचर्स ने भविष्यवाणी की है कि 2021 तक साइबर क्राइम की कीमत सालाना 6 ट्रिलियन डॉलर होगी, जो कि 2015 में अनुमानित 3 ट्रिलियन डॉलर की दो गुणी है. यह इतिहास में आर्थिक धन का सबसे बड़ा हस्तांतरण दर्शाती है, जो कि सभी प्रमुख गैरकानूनी ड्रग्स के वैश्विक व्यापार की तुलना में अधिक लाभदायक है.

साइबर हैकिंग कई स्तरों में बंटा हुआ है, ये विभिन्न प्रकार के हैकिंग के स्तर की विकराल अवस्था को दर्शाती है, ये स्तर निम्नलिखित हैं :

1. सरफेस वेब
2. डीप वेब
3. डार्क वेब

सरफेस वेब एक सामान्य वेब है, जो इंटरनेट प्रयोग करने वाले सभी उपयोगकर्ताओं को दिखता है, इसमें विभिन्न प्रकार के सर्च इंजन शामिल होते हैं, गूगल सरफेस वेब का सबसे बड़ा उदाहरण है. डीप वेब एक सेक्रेट वेब है, जो कि सामान्य इंटेरनेट उपयोगकर्ताओं को दृश्यमान नहीं होता है. सभी डीप वेब की निचली (अंतिम) सतह को डार्क वेब कहा जाता है, जिसमें साइबर अपराधी छुप रहते हैं. डार्क वेब का उपयोग गंभीर आपराधिक गतिविधियों को छुपाने और बढ़ावा देने के लिए किया जाता है. कुछ अनुमानों के अनुसार सरफेस

(Surface) वेब की तुलना में डीप (Deep) वेब का आकार 5,000 गुना बड़ा होता है. एक रिपोर्ट के अनुसार, डार्क वेब आज की तुलना में घातीय दर से बढ़ रहा है.

कुछ साइबर हमले, भविष्य के संभावित नुकसान का संकेत दे सकते हैं. याहू हैक ने हाल ही में पुनः गणना की, जिसमें पाया गया कि हैकिंग के दौरान 3 अरब उपयोगकर्ताओं के खाते प्रभावित हुए और 2017 में इक्विफैक्स उल्लंघन ने 143 मिलियन ग्राहकों को प्रभावित किया, जो कि अब तक की सबसे बड़ी सार्वजनिक रूप से प्रकट की गई हैक्स से अधिक है. 2017 में हुई वानाक्राई और नाटपेटिया साइबरटाक्स के साथ ये प्रमुख हैक्स न केवल बड़े पैमाने पर और पिछले हमलों की तुलना में अधिक जटिल हैं, परंतु आने वाले समय के संकेत हैं.

साइबर हमले का आकार एवं विस्तार

वर्ल्ड वाइड वेब का आविष्कार 1989 में हुआ था. पहली वेबसाइट 1991 में बनी थी. आज 1.2 अरब से अधिक वेबसाइटें हैं और 3.8 बिलियन इंटरनेट उपयोगकर्ता हैं (दुनिया की 7 बिलियन आबादी का 51%), जोकि 2015 में 2 बिलियन था. साइबर सिक्योरिटी वेंचर्स का अनुमान है कि 2022 तक 6 अरब इंटरनेट उपयोगकर्ता होंगे (अनुमानित विश्व जनसंख्या 8 अरब का 75%) और 2030 तक 7.5 अरब से अधिक इंटरनेट उपयोगकर्ता (अनुमानित विश्व आबादी का 90%). सड़क अपराध की तरह, जो ऐतिहासिक रूप से जनसंख्या वृद्धि के संबंध में बढ़ी है, हम साइबर क्राइम में समान विकास को देख रहे हैं. आने वाले समय में यह ना केवल अधिक परिष्कृत हथियार होगा, परंतु इसका विध्वनस्कारी प्रभाव मानव और डिजिटल संसाधनों दोनों पर पड़ेगा.

इंटेल के अनुसार, 'द बिग डाटा बैंग' एक आईओटी दुनिया है, जो कि 2006 में अनुमानित था कि 2 अरब स्मार्ट उपकरणों से बनेगी. अब अनुमानित है 2020 तक 200 बिलियन. गार्टनर का अनुमान है कि 2021 में दुनिया भर में आधे बिलियन पहनने योग्य उपकरणों को बेचा जाएगा, 2017 में ये लगभग 310 मिलियन था. पहनने योग्य उपकरणों में स्मार्टवॉच, हेड-माउंटेड डिस्प्ले, बॉडी-पहने कैमरे, ब्लूटूथ हेडसेट, फिटनेस मॉनीटर आदि शामिल हैं.

यह उम्मीद थी कि भविष्य में हमें पासवर्ड की जरुरत नहीं पड़ेगी क्योकि बॉयोमेट्रिक्स का उपयोग इसका सबसे और सुरक्षित समाधान है, परंतु 2017 की एक रिपोर्ट में पाया गया है कि 2020 तक दुनिया को वैश्विक स्तर पर 300 अरब पासवर्ड को सुरक्षित रखने की आवश्यकता होगी. इसका एक दूसरा कारण यह भी है कि जहां एक और बॉयोमेट्रिक्स तकनीक में विकास हो रहा है, वहीं साइबर हैकर उसे तोड़ने में भी सफल रहे हैं.

हर जगह स्वचालन की बढ़ती मांग के साथ प्रति वर्ष 111 अरब लाइनों का नया सॉफ्टवेयर कोड तैयार किया जा रहा है, जिसमें बड़ी संख्या में भेद्यताएं (Vulnerability) शामिल हैं, जिनका साइबर अपराधी द्वारा दुरूपयोग किया जा सकता है. दुनिया भर की सरकारें भी अपने सामरिक लक्ष्य के लिए साइबर अपराधियों की जाने-अनजाने मदद करती हैं.

यह अनुमान लगाया गया है कि 2020 तक 20 मिलियन से अधिक स्वचालित कारें, जो कि अंतर्निहित सॉफ्टवेयर-आधारित सुरक्षा तकनीक के साथ शिप करेंगी, जिनकी संख्या 2012 में केवल 2 प्रतिशत थी. उसकी तुलना में एक अनुमान के अनुसार 2020 तक 90 प्रतिशत कारें स्वचालित एवं ऑनलाइन होगीं.

सैकड़ों, हजारों और संभवतः लाखों लोगों को उनके वायरलेस कनेक्ट और डिजिटल निगरानी वाले इम्प्लांटेबल मेडिकल डिवाइसेज (आईएमडी) के माध्यम से हैक किया जा सकता है - जिसमें कार्डियोवर्टर डिफिब्रिलेटर (आईसीडी), पेसमेकर, गहरे मस्तिष्क न्यूरोस्टिम्युलेटर, इंसुलिन पंप, कान ट्यूब आदि शामिल हैं. एक चिंताजनक प्रवृत्ति उभर रही है, जहां इन उपकरणों का उपयोग कॉर्पोरेट को लक्ष्य करने और बड़ी आर्थिक हानि पहुचाने के लिये किया जा सकता है. सोनी और नेटफ्लिक्स साइबर हैक इस संभावनाओं के उदाहरण हैं, जो भविष्य में अधिक बार उद्धरित होंगे. इन संभावनाओं से इनकार नहीं किया जा सकता है कि कार, आईसीडी, पेसमेकर और अन्य उपकरण हत्यारों के मुख्य लक्ष्य हो सकते हैं, जो बिना किसी भी निशाने के डार्क वेब में संचालित होते हैं.

तकनीक, जो कृत्रिम बुद्धि (एआई), मशीन लर्निंग (एमएल), रोबोटिक प्रोसेस ऑटोमेशन (आरपीए), स्मार्ट और कनेक्टेड आईओटी और अन्य अभिनव प्रौद्योगिकी, जो अधिक जुड़ाव और स्वायत्त दुनिया के लिए आवश्यक है, न केवल कॉर्पोरेट, सरकार और नागरिकों की मदद करेगी, बल्कि यही प्रौद्योगिकी साइबर अपराधियों को भी समान रूप से मदद करेगी ताकि उनकी गतिविधियां बड़े पैमाने पर विस्तारित हो सकें.

आईटी विश्लेषकों के पूर्वानुमान के अनुसार साइबर क्राइम में नाटकीय वृद्धि, रैनसमवेयर के प्रसार, मालवेयर (Malware) का पीसी और लैपटॉप से स्मार्टफोन और मोबाइल उपकरणों की तरफ प्रसार, अरबों असुरक्षित आईओटी उपकरणों की तैनाती, सेवा के रूप में हैकिंग का आगमन और दुनिया भर में व्यवसायों, सरकारों, शैक्षणिक संस्थानों और उपभोक्ताओं पर किए जाने वाले अधिक परिष्कृत साइबर हमलों से बचाव के सीमित उपाय ही उपलब्ध हैं.

यू.एस. डिपार्टमेंट ऑफ जस्टिस (डीओजे) ने हाल ही में रैनसमवेयर को साइबर क्राइम के नए व्यवसाय मॉडल के रूप में वर्णित किया है. रैनसमवेयर एक वैश्विक घटना है. रैनसमवेयर - एक मैलवेयर है, जो कंप्यूटर को संक्रमित करता है और फ़ाइलों को एन्क्रिप्ट (encrypt) करता है. अक्सर हैकर्स को फिरौती का जब तक भुगतान नहीं किया जाता है, तब तक डाटा नष्ट करने की धमकी देते रहते हैं. रैनसमवेयर एक महामारी के स्तर तक पहुंच गया है और यह बड़ी तेजी से बढ़ रहा साइबर क्राइम है. हर 40 सेकंड में एक व्यवसाय रैनसमवेयर हमले का शिकार हो जाता है और यह भविष्यवाणी की गई है कि यह 2019 तक हर 14 सेकंड में बढ़ेगा.

एफबीआई का अनुमान है कि रैनसमवेयर हमलों के संबंध में कुल क्षति राशि का भुगतान सालाना $ 1 बिलियन तक पहुंच गया है और यह आसमान छू रहा है. 2017 में ग्लोबल रैनसमवेयर क्षति की लागत $ 5 बिलियन से अधिक होने की भविष्यवाणी की गई है, जो 2015 से 15 गुना अधिक है. रैनसमवेयर साइबर क्राइम की दुनिया में एक खेल परिवर्तक है और इसमें अपराधियों के हमलों को पूरी तरह से स्वचालित करने की क्षमता है. स्वचालित अपराध दुनिया भर के व्यवसायों और व्यक्तियों के लिए एक बहुत बड़ी चिंता का विषय है.ये इसके साथ-साथ अंतरराष्ट्रीय संगठित अपराध सिंडिकेट के मुनाफे को घातीय वृद्धि से बढ़ा रहा है.

सुरक्षा जागरूकता प्रशिक्षण

कंपनियां प्रौद्योगिकी और सेवाओं को खरीदने में बड़ा पैसा खर्च करती हैं. हालांकि नेटवर्क और सिस्टम की आधारभूत संरचना अभी भी पुरानी शैली की कमजोरियों के कारण कमजोर बनी रह सकती है. व्यक्तियों और संगठनों की रक्षा करने का सबसे अच्छा तरीका सुरक्षा जागरूकता प्रशिक्षण है. कर्मचारियों के लिए सुरक्षा जागरूकता प्रशिक्षण पर वैश्विक खर्च 2014 में करीब 1 अरब डॉलर से 2027 तक 10 अरब डॉलर तक पहुंचने की भविष्यवाणी की गई है.

साइबर हमलों के खिलाफ प्रशिक्षण, कर्मचारियों को साइबर हमले पहचानने और बचाव करने के लिए साइबर सुरक्षा उद्योग का सबसे कम खर्च वाला क्षेत्र है. हैकिंग

के इतिहास में स्मार्ट हैकर द्वारा सिस्टम में त्रुटियों को ढूंढते हुये अटैक करने जैसी कहानियों की कमी नहीं है, परंतु तथ्य यह है कि अधिकांश साइबर हमले एक साधारण ईमेल से शुरू होते हैं. 90% से अधिक सफल हैक्स और डाटा उल्लंघनों की शुरुआत फ़िशिंग से होती है, जहां पर उनके प्राप्तकर्ताओं को तैयार किए गए ईमेल में दिए गए लिंक को किसी अन्य व्यक्ति को अग्रेषित करने के लिए कहा जाता है. साइबर अपराध, उपयोगकर्ताओं और तकनीकी कर्मचारियों द्वारा की गई गलतियों के कारण सफल होते हैं और इसलिए उन्हें ही रक्षा की पहली पंक्ति के रूप में तैयार, सुशिक्षित और प्रमुख हथियार बनाना चाहिए.

सबसे अधिक साइबर क्राइम प्रभावित उद्योग, स्वास्थ्य देखभाल (Health care), निर्माण (Manufacturing), वित्तीय सेवाएं (Financial Services), सरकार (Government) और परिवहन (Transportation) हैं और आने वाले वर्षों में भी ऐसा ही रहने की भविष्यवाणी है.

उपभोक्ता साइबर खतरे से अधिक अनभिज्ञ नहीं हैं और कॉर्पोरेट एवं अन्य संगठनों की तरह उन्हें भी साइबर खतरों को पूरी तरह से समझने में कुछ और समय लगेगा. बढ़ते साइबर क्राइम के बावजूद, तकनीक दुनिया को एक अधिक सुरक्षित जगह बनाने का वादा करती है.

साइबर क्राइम एक प्राकृतिक विस्तार है, प्रौद्योगिकी के उन्नत उपयोग से इसे कम करने की अपेक्षा की जानी चाहिए. हमारे द्वारा इनका सामना करने के लिए जोखिमों और खतरों के प्रति यथार्थवादी दृष्टिकोण, संगठनों और उपभोक्ताओं को स्वयं की सुरक्षा के लिए बेहतर काम करने में मदद करेगा.

साइबर सुरक्षा के भौतिक आयाम एवं सुरक्षा संस्कृति

अमित माथुर
वरिष्ठ प्रबंधक
सीसो, के. का. मुंबई

आशुतोष सीरौठिया, सेना मेडल
मुख्य सुरक्षा अधिकारी
के. का. मुंबई

परिचय

किसी भी मर्मस्थल या मर्मबिन्दु की सुरक्षा को सुदृढ़ बनाने के लिए सुरक्षा प्रणाली विकसित करते समय कई तहें एक के बाद एक लगाई जाती हैं, ताकि अगर उसे भेदने का प्रयास किया जाए तो मर्मस्थल/बिन्दु पर सीधा आक्रमण न हो पाये और हमें स्थिति को संभालने हेतु थोड़ा समय मिल जाए. साइबर जगत में प्रायः यह देखा गया है कि भौतिक सुरक्षा को उतना महत्व नहीं दिया जाता जितना आवश्यक है और नतीजतन भौतिक सुरक्षा की यह अनदेखी गंभीर घटनाओं का कारण बनती है.

साइबर सुरक्षा भेद ने में भौतिक सुरक्षा की भूमिका

1. साइबर सुरक्षा को भेदने के प्रयास अहर्निश होते हैं. जो उस्ताद हैं, वे सुरक्षा प्रणालियों को भेदने की कला को भली-भांति जानते हैं और वे विश्व के किसी कोने में छुपे मर्मस्थल/बिन्दु पर अपने कंप्यूटर के द्वारा आक्रमण कर उसे तहस-नहस कर सकते हैं या उस संगठन की आर्थिक स्थिति को गंभीर क्षति पहुँचा सकते हैं, परंतु ऐसे महारथी बहुत कम होते हैं. बहुतायत संख्या उन छुटभइयों की ज्यादा है, जो तकनीकी रूप से इतने सशक्त नहीं होते कि सभी एंटीवायरस, फायरवाल्स, पासवर्ड व्यवस्था को भेद सकें, पर यदि वे आपके कंप्यूटर तक स्वयं पहुँच जाएँ, तो कहर बरसा सकते हैं. इसके लिए उन्हें भौतिक सुरक्षा की कमियों का लाभ उठाकर अंदर पहुँचना आवश्यक होता है. इस काम के लिए वे तरह-तरह के भेष - दूध/अखबार वाले से लेकर मजदूर, चपरासी, संदेशवाहक, डाकिया, कंप्यूटर सर्विस के नुमाइंदे या सूटेड-बूटेड कंपनी के नुमाइंदों के रूप में आते हैं तथा सुरक्षा व्यवस्था को टटोलते हैं और किसी भी चूक का फायदा उठा कर अपना काम कर जाते हैं. यह निम्न उदाहरण से स्पष्ट किया जा सकता है :-

श्रीमान X मेसर्स FZ में एक कर्मचारी है. मेसर्स FZ, ABC बैंक के साथ किसी गतिविधि में शामिल हैं. गतिविधि के दौरान श्री X कई बार लगातार बैंक में मिलने गए, जिससे सुरक्षा गार्ड एवं बैंक के अन्य कर्मचारी श्री X से भली-भांति परिचित हो गए थे. एक दिन श्री X बैंक की इमारत में गए, परंतु उन्होंने आगमन रजिस्टर में कोई भी प्रविष्टि नहीं की. बैंक के स्वागत डेस्क पर सभी आगन्तुकों की फोटो एवं अन्य डाटा कम्प्यूटर में रखा जाता हैं, परंतु फोटो हर बार अपडेट नहीं किया जाता. श्री X बैंक में नए नहीं थे, इसलिए उस वक्त न तो उनकी फोटो अपडेट की गयी और न ही डाटा एंट्री की गयी. श्री X ने एक कर्मचारी से उसके एक्सैस कार्ड को उपयोग करके की प्रार्थना की और टेलगेटिंग के जरिये मुख्य इमारत में प्रवेश कर गए.

कुछ समय बाद, श्री x बोर्ड रूम में गए, जहाँ कुछ संवेदनशील कागजात टेबल पर रखे हुए थे, उन्होंने कागज ले लिए. वे अपने साथ यूएसबी ड्राइव ले गए थे, जिसे उन्होंने एक महत्वपूर्ण कम्प्यूटर में लगा कर डाटा चुरा लिया. उस कम्प्यूटर को सर्वर का एक्सैस प्राप्त था और वह लॉक भी नहीं था एवं सर्वर का पासवर्ड दीवार पर ही लिखा हुआ था.

कुछ दिनों के बाद जब महत्वपूर्ण सूचनाएं लीक हो गई और बैंक को मीडिया से पता चला, तब जाँच शुरू की गई. श्री x को पकड़ा नहीं जा सका, क्योंकि उनके आगमन की कोई सूचना किसी भी रजिस्टर या सिस्टम में नहीं मिली. उनके उस दिन के आने की जानकारी आगंतुक मैनेजमेंट सिस्टम के कम्प्यूटर में स्वागत कक्ष में नहीं मिली. उन्हें आगंतुक एक्सैस कार्ड भी नहीं दिया गया था और उन्होंने टेलगेटिंग के जरिए बैंक के ही एक कर्मचारी के साथ प्रवेश किया था. अंत में, बैंक को पता चला कि आईपी बेस्ड कैमरा प्रणाली पहले ही हैक हो चुकी थी और कोई भी रिकॉर्डिंग दर्ज नहीं की गयी, अपितु कैमरा प्रणाली, रिकॉर्डिंग को कहीं और ही भेज रही थी और कैमरा प्रणाली का उपयोग एक बॉट कम्प्यूटर की तरह डीडॉस अटैक के लिए उपयोग किया जा रहा था, क्योंकि कैमरा प्रणाली साइबर सुरक्षा टीम के मानिटरिंग के दायरे में नहीं थी.

साइबर हैकेर्स के द्वारा भौतिक हमलों के उदाहरण :

खतरे किसी भी तरह से और किसी भी प्रकार से आ सकते हैं. हैकर और घुसपैठिये लगातार भौतिक सुरक्षा के बचाव की प्रणाली में कमजोरियां ढूंढते रहते हैं, जो उनकी जुर्म करने की संभावना को निम्नानुसार प्रबल करते हैं:

- महत्वपूर्ण सूचनाओं वाली आस्तियों को चुराने के लिए दरवाजे की लॉक प्रणाली को अपने अधिकार में करना.
- किसी की निगाह में आये बिना सूचना को चुराने के लिए वीडिओ रिकार्डिंग और मानिटरिंग को बंद कर देना.
- किसी जुर्म का साक्ष्य मिटाने के लिए सुरक्षा प्रबंधन प्रणाली के रिकॉर्ड्स मिटा देना.

सीसीटीवी एवं आईपी बेस्ड कैमरा प्रणाली के खतरे

कैमरा प्रणाली हमेशा से ही नेटवर्क में अलग-थलग रही है, इसलिए लोगों ने कभी भी उसे साइबर दुनिया से जोड़ कर नहीं देखा है परंतु आज के समय में कैमरा प्रणाली भी मुख्य नेटवर्क से ही जुड़ी हुई रहती है, जो कि सुरक्षा की दृष्टि से एक महत्वपूर्ण सर्वर एप्लिकेशन है.

- बैंक में अधिकतम नकदी का समय और उसे चुराने का समय जानने के लिए, सुरक्षा अधिकारी का मुख्य क्षेत्र में न होने की स्थिति पता करने के लिए सीसीटीवी कैमरे की निरंतर मानिटरिंग करना.
- भौतिक सुरक्षा प्रणाली को पूर्णतया बंद कर देना, जिससे कि सुरक्षा अधिकारी के पास मानिटरिंग करने के लिए कोई साधन न रहे.
- अलार्म प्रणाली को हैक करके गलत तरीके से बिना वजह के चालू करके, सुरक्षा अधिकारी को व्यस्त कर देना, जिससे कि मुख्य क्षेत्र बिना सुरक्षा अधिकारी के रह जाए.
- हाल ही में ये सूचना मिली है कि एक हैकर/ हमलावर किसी संगठन के वीडियो निगरानी प्रणाली को अपना निशाना बना रहे थे. जब डेकोय (हैकर्स को फसाने के लिए एक वास्तविक दिखने वाली नकली प्रणाली) ने चेतावनी भेजी, तो पता चला कि हैकर्स स्कैनिंग कर रहे थे, जिससे कि उन्हें पासवर्ड प्रणाली की सूचनाएं प्राप्त हो सके और वीडियो निगरानी प्रणाली को इंटरनेट में किसी और वेब पेज से संबोधित किया जा सके.
- सोचिए कि बोर्ड रूम में लगा एक वेब कैमरा, जो कि बोर्ड के सदस्यों की होने वाली बैठकों की गोपनीय एवं महत्वपूर्ण सूचनाएं कहीं और भेज रहा है या फिर कोई मालवेयर डाल कर कैमरा प्रणाली को बॉट की तरह डीडॉस (डिनायल ऑफ सर्विस) के हमले के लिए उपयोग में ले रहा हो. इस तरह से कोई व्यक्ति कुछ कैमरों से हमलवारों की एक पूरी फौज खड़ी कर सकता है.

- कैमरा जिस फायरवाल पोर्ट का प्रयोग करता है वह पोर्ट नंबर उसी नेटवर्क के अन्य हिस्सों में भी प्रयोग में लाया जा सकता है, इसलिए अगर वीडियो निगरानी प्रणाली हैक हो जाती है तो उस पोर्ट के जरिए अन्य हिस्सों से डाटा सेंटर या लेखा विभाग में भी पहुँचा जा सकता है.

2. भौतिक सुरक्षा में सेंध निम्नलिखित तरीकों से लगायी जा सकती है :-

i. **चोरी-छुपे देखना (SHOULDER SURFING) :** इस तरीके में व्यक्ति आपके पीछे खड़े होकर आपके पासवर्ड की किताब में लिखी जानकारी को या टाइप किए जा रहे पासवर्ड को देखकर नोट कर लेता है.

ii. **सामाजिक अभियांत्रिकी (SOCIAL ENGINEERING) :** इस तरीके में बजाए कंप्यूटर व्यवस्था को भेदने के ऐसे व्यक्ति, जो कंप्यूटर व्यवस्था को नियंत्रित कर रहे हैं, उन लोगों को ही वे साम, दाम, दंड या भेद की नीति अपना कर फंसा लेते हैं और अपना काम कर जाते हैं.

iii. **कूड़ाकर्कट गोताखोरी (DUMPSTER DIVING) :** इस तरीके में व्यक्ति किसी भी संगठन या व्यक्ति विशेष के कंप्यूटर कचरे (जैसे सी.पी.यू. या हार्ड डिस्क इत्यादि) की गहरी छान-बीन कर वांछित जानकारी निकाल लेते हैं और अपना काम कर जाते हैं.

3. कुछ परिभाषाएँ

i. **डाटा सेंटर :** एक ऐसी विशेष जगह, जहाँ किसी संगठन की सारी वेबसाइट्स सुरक्षित रखी जाती है तथा जहाँ से उस संगठन की डाटा सुविधाएँ दूसरी कंपनियों या संगठनों को मुहैय्या करायी जाती हैं. इस तरह के डाटा सेंटर में, नेटवर्क ऑपरेशन सेंटर (NOC) एक अतिसुरक्षित जगह पर चलाया जाता है. इसकी ऑटोमैटिक सिस्टम व्यवस्था 24X7 अनुपालना (परफॉर्मेंस) पर कंप्यूटर गतिविधि की निगरानी रखती है. वेब ट्रैफिक व नेटवर्क की ज़रा सी अनियमितता होने पर संकेत देकर बड़ी से बड़ी गलती होने से बचा जा सकता है.

ii. **भौतिक सुरक्षा :** ऐसी सुरक्षा व्यवस्था, जिसमें भौतिक बाधाएँ या नियंत्रण-प्रणाली की तहें लगाई जाती हैं, जिससे चूक होने से बचा जा सके या चूक हो जाने पर उसे जल्द से जल्द ठीक किया जा सके ताकि संगठन की संवेदनशील संपत्ति या सूचना खतरों से हमेशा सुरक्षित रहे. भौतिक सुरक्षा में निम्नलिखित का बहुत महत्व है :-

(अ) किसी भी परिसर, इमारत की जगह, उसमें लगे उपकरणों की जानकारी एवं उनमें प्रवेश अथवा पहुँच (access) की सुरक्षा.

(ब) सावधानियाँ एवं पद्धतियाँ, जो चोरी, लूटमार या व्यक्तियों द्वारा नियोजित किसी भी संकट/खतरे एवं प्राकृतिक आपदाओं (बाढ़, भूकंप इत्यादि) तथा अपघात (accident) के नुकसान से (जैसे कि बिजली शॉर्टसर्किट, अति गर्म वातावरण से आग लगना इत्यादि) बचाव करती हैं.

(स) घुसपैठियों से बचाव के लिए मजबूत भवन निर्माण, भरोसेमंद विद्युत पावर व्यवस्था तथा बैकअप, वातावरण पर नियंत्रण (जैसे ए.सी. इत्यादि से तापमान व्यवस्थित करना) एवं इमरजेंसी होने पर बचाव की पूरी तैयारी रखना.

(द) भौतिक सुरक्षा में निम्न बिंदु महत्वपूर्ण हैं :-

- आने जाने वाले व्यक्तियों एवं वाहनों की जाँच
- जाँच के तरीके एवं उपकरण
- वातावरण खतरों से सुरक्षा
- उपकरणों की सुरक्षा - उनकी चोरी, नुकसान, बदली या प्रतिलिपि होने से बचाव.

4. सुरक्षा की चेकलिस्ट

हर संगठन में सुरक्षा चेकलिस्ट दो भागों में बनाई जाती है - संपत्ति एवं लोग. संपत्ति में आते हैं भवन, उपकरण, कंप्यूटर हार्डवेयर, डाटा इत्यादि. लोगों के दो प्रकार के होते हैं - बाहरी व्यक्ति एवं हमारे लोग. हमारे लोगों में आते हैं अपने वेतनभोगी कर्मचारी, ग्राहक और ऐसे लोग, जिन्हें हमारे डाटा को हाथ लगाने की इजाज़त है. सफाई कर्मचारी, बाहरी संस्था से लिए गए गार्ड एवं सर्विस इंजीनियर्स बाहरी व्यक्तियों में गिने जाते हैं, जो कि संस्था के अपने वेतनभोगी कर्मचारी नहीं हैं. इन्हें हमारे डाटा से दूर रखा जाना चाहिए. संपत्ति की सुरक्षा जाँच हमेशा नियमित रूप से तथा एक-एक वस्तु को अच्छी तरह परख कर की जानी चाहिए. हर संपत्ति को वर्ष में कम से कम एक बार तो अवश्य जाँच की जानी चाहिए. जो महत्वपूर्ण संपत्तियाँ हैं उनकी जाँच महत्ता के अनुसार दैनिक, साप्ताहिक, मासिक या त्रैमासिक अंतराल पर की जानी चाहिए.

5. सुरक्षा खतरे

सुरक्षा को खतरा बाहरी एवं आंतरिक घटकों द्वारा हो सकता है तथा इस खतरे को अंजाम देने के तीन प्रशस्त रास्ते हैं :-

i. भौतिक पहुँच के द्वारा

ii. इंटरनेट द्वारा

iii. मोबाइल तथा अन्य उपकरणों द्वारा.

6. उपरोक्त तरीकों से संपत्ति, डाटा या डाटा सिस्टम को चुराया, गुमाया, बदली या बर्बाद किया जा सकता है. अतः सुरक्षा नीति में यह आवश्यक है कि सुरक्षा को पूर्णतः स्थापित (establish) करके उसे सदा ही कार्यान्वित (implement), परिचालित (operated), अनुश्रवित या अनुलक्षित (monitored), पुनरीक्षित (reviewed), अनुरक्षित (maintained) एवं उन्न्त (improved) रखा जाए.

परिसर की सुरक्षा

7. प्राकृतिक आपदा : किसी भी परिसर या इमारत के लिए ऐसी जगह का चयन किया जाना चाहिए, जहां पर प्राकृतिक आपदा का खतरा कम से कम हो. इलाके के अनुसार प्राकृतिक आपदा में बाढ़, भूकंप, सुनामी, जंगली-आग इत्यादि सभी को ध्यान में रखा जाना चाहिए.

8. मानवकृत आपदा : परिसर या भवन ऐसी जगह चुना जाए, जहाँ मानवकृत आपदाओं की संभावना न्यूनतम हो. मानवकृत आपदाओं में सम्मिलित हैं - दंगे-फसाद, आगजनी, बम हमला, वायुयान हमला (plane crash) आदि. अतः जहां तक संभव हो, संवेदनशील परिसर को विमानपत्तन (airports), जेल, मुक्तमार्ग (freeways), खेल परिसर या स्टेडियम, तेल-शोधक कारखाने, तेल-भंडारण परिसर, शोभायात्रा-मार्ग इत्यादि से दूर रखना चाहिए.

9. आधार संरचना (Infrastructure) : संवेदनशील जगहों पर विद्युत उपलब्धि 99.99% या उससे बेहतर होनी चाहिए. अतः इसे यदि दो विद्युत सब-स्टेशनों से जोड़ दिया जाए तथा जेनरेटर/यू.पी.एस. का सहारा दे दिया जाए, तो अच्छा है. इसी तरह पानी की मात्रा सुनिश्चित करने के लिए पानी के एक से ज्यादा कनेक्शन, बोरवेल, कुआँ और ओवरहेड एवं अंडरग्राउंड पानी की टंकियों पर निर्भर रहना बेहतर होगा.

10. **एकल-उद्देश्य (sole-purpose) परिसर :** कोई भी डाटा सेंटर का परिसर/भवन किसी अन्य दफ्तर या संस्था के साथ एक ही इमारत में नहीं होना चाहिए. डाटा सेंटर की इमारत एकल-उद्देश्य से रखी जानी चाहिए. यदि व्यय बचत को ध्यान में रखते हुए किसी इमारत/परिसर को साझा करना भी पड़े, तो डाटा सेंटर को सबसे ऊपर की मंजिलों पर, बीच में एक मंजिल खाली रखते हुए (या उसमें सुरक्षा के नुमाइंदे रखते हुए), बनाना चाहिए. डाटा सेंटर का प्रवेश द्वार ऐसी साझा इमारत/भवन में अलग ही हो, तो सर्वोत्तम है, अन्यथा डाटा सेंटर की लिफ्टों को अलग नामांकित कर अवांछित आगंतुकों को दूर रखा जा सकता है. यदि जमीनी तल पर इमारत/भवन साझा करना पड़ जाए तो बीच की दीवार को सीमेंट-गारे से अभेद्य बनाना चाहिए.

11. **परिसर परिधि (site perimeter) :** डाटा सेंटर की इमारत से कम से कम 20 फुट की दूरी पर चहुं ओर कंटीले तारों की परिधि-बाड़ या मजबूत दीवार होनी चाहिए. इस परिधि के हर प्रवेश बिन्दु पर गार्ड नियुक्त होने चाहिए. हर प्रवेश बिन्दु पर ऑटोमैटिक प्रमाणीकरण (authentication) यंत्र जैसे कि बैज रीडर (Badge Reader), फ्लैप बैरियर (Flap Barriers) या कार नंबर प्लेट रीडर लगे होने चाहिए. तारों की परिधि/दीवार को अच्छी तरह से रौशन रखना चाहिए ताकि किसी भी हरकत को दूर से पहचाना जा सके.

12. संवेदनशील भवन/इमारत से साधारण कारों का ड्राइव-वे एवं पार्किंग स्थल 25 मीटर या उससे अधिक दूरी पर होना चाहिए ताकि कार को बम धमाके से कम से कम नुकसान हो. वी आई पी कारें भी 25 मी. की दूरी पर जाँच के बाद ही इमारत के पास पहुँच पाएँ, ऐसी व्यवस्था आवश्यक है.

13. **विज्ञापन या मार्गदर्शक बोर्ड :** डाटा सेंटर के रास्ते की पहचान हो सके, ऐसा कोई भी विज्ञापन/बोर्ड या मार्गदर्शक चिह्न रास्तों पर नहीं लगाना चाहिए. देखा जाए, तो इमारत का नाम भी ऐसा हो, जिसमें डाटा या डिजिटल जैसे शब्दों का इस्तेमाल न हो, ताकि कोई भी अवांछित व्यक्ति इसकी नाम से पहचान न कर सके.

14. **निगरानी (surveillance) :** संवेदनशील इमारत की निगरानी निम्न तहों में लगाना चाहिए :-

    i. **पेट्रोलिंग :** गार्ड के पेट्रोलिंग के रास्ते एवं समय निश्चित किए जाने चाहिए. पेट्रोलिंग रात के समय बहुत कारगर हो सकती है.

ii. **सीसीटीवी कैमरे :** इमारत या परिसर के सभी रास्तों, दीवारों, पार्किंग स्थलों, बेसमेंट (भूतल), परिधि-बाड़ या दीवार, अंदरूनी कार या पैदल पथों को सीसीटीवी की निगरानी में रखा जाना चाहिए.

iii. **अलग पार्किंग स्थल :** डाटा सेंटर के अपने कर्मचारी, गार्ड, सफाई कर्मचारी इत्यादि को अलग पार्किंग दी जानी चाहिए तथा उनके पार्किंग परमिट अलग रंग के होने चाहिए. बाहरी सर्विस कंपनियों के कर्मचारी, आगंतुक (visitors) और वे सभी, जो मूल संस्था के वेतनभोगी न हों, उनकी पार्किंग अलग हो और उनके पार्किंग परमिट भिन्न रंग के हों. बिना परमिट के पार्किंग में मिली गाड़ियाँ' खींच कर (Tow-out) बाहर किसी स्थल पर रखने की व्यवस्था करना चाहिए.

15. **कंप्यूटर कक्ष की खिड़कियाँ :** भवन के कंप्यूटर कक्ष की खिड़कियाँ भवन की बाहरी दीवारों पर न हों यह आवश्यक है. ऐसी खिड़कियाँ वॉन एक विकिरण (Van Eck Radiation) से गोपनीय खबर हासिल करने का ज़रिया बन सकती हैं और HERF (High Energy Radio Frequency) गन अटैक का शिकार करने का माध्यम भी. HERF का धमाका इलेक्ट्रो मैगनेटिक (EM) विकिरण का एक ऐसा संकेंद्रित (concentrated) किरण पुंज होता है जो कि हार्ड डिस्क को पूरी तरह मिटा सकता है, कंप्यूटर को क्रैश कर सकता है एवं सिलिकॉन चिप्स को पूरी तरह फ्यूज़ (fuse) करके नष्ट कर सकता है. बाहरी दीवार की खिड़कियों से धूप भी अंदर आती है, जो कंप्यूटर कक्ष का तापमान बढ़ा कर वातानुकूलित वातावरण को प्रभावित कर बिजली का खर्च बढ़ाती है. किसी भी भवन/इमारत में कंप्यूटर और सर्वर कक्ष भवन के अंदरूनी हिस्सों में ही बनाए जाने चाहिए. अगर किन्हीं कारणों से कंप्यूटर कक्ष भवन की बाहरी तरफ बनाना ही पड़े, तो उसके सामने एक भौतिक बाधा (physical barrier) जैसे दीवार या कोई मोटे काँच या प्लाइवुड की आड़ बना देना चाहिए, जिससे छाया भी बनी रहे और बाहरी हमले से भी कुछ हद तक बचा जा सके.

16. **अंदर आने के रास्ते :** भवन/इमारत में अंदर आने के हर रास्ते पर, (चाहे वो आदमियों, गाड़ियों या किसी भी और चीज के आने-जाने का माध्यम हो, आवश्यकतानुसार दीवार के आर-पार ऑटोमैटिक प्रमाणीकरण (Authentication) यंत्र जैसे बैज रीडर, सिक्योरिटी बाधा जैसे बैरियर, मैनट्रैप (man-trap) और सिक्योरिटी कक्ष (kiosk) आदि होना चाहिए. हर रास्ते को CCTV से कवर करके हर आदमी/गाड़ी की पहचान करना आवश्यक है. जो बाहरी व्यक्ति, जैसे सर्विस इंजीनियर या सफाई कर्मचारी हों उन्हे फोटो पहचान पत्र के बदले में ही निश्चित

समय (3 घंटे या 6 घंटे) का बैज रीडर/पास दिया जाना चाहिए, जिसे वे वापस जाते समय जमा कराये तथा अपना फोटो पहचान पत्र ले जायँ. इमारत के अंदर एवं बाहर जाने वाले सामान को रजिस्टर में ठीक से दर्ज करके तथा CCTV की निगरानी के अंदर ही आने या जाने दिया जाए. रजिस्टर में किसने कब और कौन सा सामान किस आज्ञा पत्र के आधार पर बाहर ले जाया गया है या अंदर लाया गया है, उसका विस्तार से उल्लेख किया जाए.

कंप्यूटर कक्षः

17. **प्रवेश नियंत्रण :** दरवाजे पर ही प्रवेश निषेध या खाने पीने अथवा धूम्रपान की सख्त मनाही के निर्देश लिखे हों. दरवाजा स्वतः बंद होनेवाला हो और सिर्फ बैजरीडर या शारीरिक प्रमाणीकरण (जैसे अंगूठा या अंगुली रीडर या चेहरे की पहचान का यंत्र) की मदद से ही उसमें प्रवेश संभव हो. संवेदनशील कक्ष में फ्लैप-बैरियर लगाए जाएं ताकि पीछे से घुसने (tail-gating) की संभावना को रोका जा सके. दरवाजा अग्नि-रोधक बनावट का हो एवं हर कंप्यूटर कक्ष में पहले दरवाजे के बाद एक और दरवाजा हो, जिसमें काँच की बड़ी खिड़की हो ताकि आग लगने की सूरत में काँच के द्वारा अंदरूनी कक्ष को ठीक से देखकर ही अग्निशामक कर्मचारी उसमें प्रवेश करने की दिशा को निश्चित कर सकें.

18. **सर्वर या भवन की मरम्मत, रख रखाव वाले नुमाइंदों का प्रवेशः** इन व्यक्तियों को विशेष जांच एवं पहचान के बाद ही प्रवेश दिया जाए. छुट्टी के दिनों में यदि काम चल रहा हो तो वह कर्मचारियों की देख-रेख में ही हो अन्यथा इन व्यक्तियों को प्रवेश-पत्र/बैजरीडर/पास सर्वर या इमारत के लिए जवाबदार अधिकारी की आज्ञा एवं हस्ताक्षर से ही नियत समय के लिए प्रवेश दिया जाए.

19. **कंप्यूटर कक्ष में विशेष जरूरतें :** (i) हर कंप्यूटर कक्ष की निगरानी CCTV कैमरों से होना चाहिए. (ii) हर कक्ष में बैक-अप पावर, ए.सी एवं नेटवर्क की व्यवस्था आवश्यक है. (iii) कंप्यूटर कक्ष के निर्माण के समय केबल, तारों तथा हवा की आवा-जाही के लिए 1½ से 2 फुट का ताल-कक्ष (fab floor partition) बनाया जाना चाहिए, जिसमें तार व्यवस्थित हब से बिछाए जाने चाहिए. (iv) हर कक्ष ऊंची छत वाला हो तथा उसमें एयर-फिक्सर हों ताकि तापमान और हवा की गुणवत्ता को सुनिश्चित किया जा सके. (v) कक्ष का तापमान 12.5 C से 24 C के बीच में तथा आद्रता (humidity) 20 से 80 प्रतिशत के बीच रखी जाए तथा इसका रिकार्ड रखकर उसका विश्लेषण समय-समय पर किया जाए ताकि नुकसान न हो पाये.

आग से सुरक्षाः

20. हर कंप्यूटर कक्ष में हैलोजेन या ऐसे ही कक्ष को अग्नि-रोधक/शामक पदार्थों से भर देने वाले तंत्र ही लगाए जाएं. इसके अलावा हर कक्ष में अग्निशामक यंत्र भी दीवारों पर लगा हो. कंप्यूटर कक्ष में पानी के छिड़काव वाले संयंत्र न हों. बिजली को काट देने वाले इमेर्जन्सी एम् सी बी हर कक्ष में हों. कंप्यूटर कक्ष के बाहर कुछ रिस्पायरेटर मास्कस (respirator masks) भी हों ताकि धुएँ की स्थिति में इन्हें पहन कर प्रवेश किया जा सके और सुरक्षा सुनिश्चित की जा सके.

21. **सूचना सुरक्षा :** यदि संस्था में व्यवसायिक प्रतिस्पर्धा वाली कंपनियों के लोग एक साथ काम कर रहे हों तो उनके लिए अलग-अलग कंप्यूटर कक्ष दिये जाएं ताकि सूचना-सुरक्षा में कोई हादसा न हो. ऐसे कक्षों में ताला-चाबी का पुख्ता बंदोबस्त भी किया जाना चाहिए.

अन्य सुविधाएंः

22. **कूलिंग टावर्स :** कुछ रिजर्व कूलिंग टावर्स की व्यवस्था हमेशा रखी जाए ताकि वातानुकूलन हमेशा ठीक रहे. ऐसे कूलिंग टावर्स डाटा सेंटर की पार्किंग से हमेशा दूर रखे जाएं.

23. **पावर बैक अप :** संस्था में जनरेटर एवं यू.पी.एस की समुचित व्यवस्था आवश्यक है. जहां जनरेटर हों वहाँ पर कम से कम 48 घंटे का डीजल/पेट्रोल भी सुरक्षित करके अलग जगह पर रखा जाए. किसी भी संकट का सामना करने के लिए किसी पंप या सप्लायर से 7 से 10 दिन का डीजल/पेट्रोल स्टॉक करके रखने का अनुबंध भी किया जाना चाहिए तथा सौर ऊर्जा का उपयोग भी किया जाना चाहिए.

24. **कूड़ा कर्कट नियंत्रण :** सारे पेपर श्रेडर (shredder) के माध्यम से किसी पेपर नष्ट करने वाली कंपनी के द्वारा ही नष्ट किए जायें. सी.पी.यू/हार्ड डिस्क तथा अन्य कंप्यूटर कर्कट जहां भी नष्ट करने के लिए रखा जाए, वो जगह 24 X 7 CCTV कैमरे की निगरानी में हो.

25. **एन.ओ.सी (नेटवर्क ऑपरेशन सेंटर) :** हर एनओसी में पावर, आग, तापमान, मौसम एवं आद्रता की निगरानी के संयंत्र हमेशा होने चाहिए. वहाँ पर बाहरी संपर्क के लिए अतिरिक्त संचार व्यवस्था (Redundant Communication means) भी होना आवश्यक है. एनओसी 24 X 7 चालू रहना चाहिए तथा उसके लिए स्टाफ और उनकी बदली हमेशा लिखित रूप में जारी की जानी चाहिए. एनओसी में न्यूज चैनल देखने की व्यवस्था भी हो ताकि ऐसा कोई हादसा या घटनाचक्र, जो डाटा

सेंटर को नुकसान पहुंचा सकता हो, से बचाव की समुचित तैयारी एवं व्यवस्था की जा सके.

आपदा समुत्थान (Disaster Recovery)

26. हर डाटा सेंटर को संस्था की आपदा समुत्थान योजना में प्राथमिकता दी जानी चाहिए. डाटा सेंटर का बैक-अप जहां पर भी हो, वहाँ भी उपरोक्त सभी प्रावधान, सुविधाएं तथा सुरक्षा उपलब्ध करायी जाना चाहिए. बैक-अप डाटा सेंटर को समय-समय पर "ट्राई-रन" के तहत प्रयोग में लाया जाना चाहिए ताकि ऐन वक्त पर धोखा न हो.

27. **क्रॉस ट्रेनिंग :** डाटा सेंटर के कर्मचारी एक से ज्यादा विषयों में क्रॉस-ट्रेंड (cross-trained) होने चाहिए ताकि अगर कोई अचानक दुर्घटना का शिकार हो जाए या अनुपस्थित हो जाए तो उसका काम न रुके. इसी तरह मुख्य डाटा सेंटर एवं बैक-अप डाटा सेंटर के कर्मचारियों को भी अदला-बदली करके काम कराना चाहिए ताकि आपदा स्थिति में कोई भी कर्मचारी कहीं से भी काम कर सके.

स्टाफ की सुरक्षा शिक्षाः

28. हर कर्मचारी को समय-समय पर डाटा सेंटर के खतरों के विषय में ट्रेनिंग दी जानी चाहिए. उन्हें ऐसे घुसपैठिये जो खतरा हो सकते हैं, उनकी पहचान करने की ट्रेनिंग भी देना चाहिए, विशेष रूप से सामाजिक यान्त्रिकी (Social Engineering) के कुचक्र को पहचानने एवं उससे बचने के तरीके बताए जाने चाहिए. उन्हें अपने काम करने के वर्क-स्टेशन एवं लैप-टॉप इत्यादि को संस्था के अंदर एवं संस्था के बाहर कैसे सुरक्षित रखना है उसकी ट्रेनिंग भी दी जानी चाहिए.

29. हर कर्मचारी ने भौतिक सुरक्षा पॉलिसी पढ़ी है, यह सुनिश्चित करने के लिए उन्हें पॉलिसी पढ़वा कर उनसे हस्ताक्षर लेना चाहिए. यह हर वर्ष किया जाना चाहिए.

30. कुछ चुनिन्दा भरोसेमंद कर्मचारियों को टेलीकम्यूटिंग (telecommuting) का प्रशिक्षण भी दिया जाना चाहिए ताकि ऐसी स्थिति में जब डाटा सेंटर तक किसी परिस्थिति विशेष की वजह से पहुंचा ही न जा सके, दूर की किसी जगह में या घरों से ही डाटा सेंटर का काम किया जा सके. यह आवश्यक होगा कि ऐसे व्यक्ति इस भेद को दूसरों को कभी प्रकट न करें. ऐसी स्थिति की समय-समय पर प्रैक्टिस भी गुप्त रूप से की जानी चाहिए.

31. साइबर सुरक्षा संस्कृति

साइबर सुरक्षा संस्कृति (सीएससी) की अवधारणा साइबर सुरक्षा के बारे में लोगों के ज्ञान, मान्यताओं, धारणाओं, दृष्टिकोणों, विचार, मानदंड और मूल्य को संदर्भित करती है. साइबर सुरक्षा संस्कृति, साइबर सुरक्षा जागरूकता और सूचना सुरक्षा को कर्मचारियों के विचारों, अपने काम, आदतों, आचरण का एक अभिन्न अंग बनाने और उन्हें अपने दैनिक कार्यों में जोड़ने से संबंधित हैं.

अगर साइबर सुरक्षा एक संस्कृति के रूप में विकसित होगी तो कर्मचारी अपने दैनिक कार्यों के हर पहलू में सुरक्षा का ध्यान रखेंगे और उनसे कम से कम भूल होने की संभावना रहेगी, जिससे संगठन साइबर सुरक्षित संगठन बनने की ओर अग्रसर होगा.

संगठनों के भीतर सीएससी कार्यक्रमों की समझ और उत्थान दोनों को बढ़ावा देने में सहायता के लिए, संगठनात्मक विज्ञान, मनोविज्ञान, कानून और साइबर सुरक्षा सहित कई विषयों के समझ की आवश्यकता होती है.

एक मजबूत साइबर सुरक्षा संस्कृति का निर्माण करना एक मुश्त गतिविधि नहीं है, बल्कि ये लगातार चलने वाली और क्रमवत विकसित होने वाली प्रक्रिया है. यदि साइबर सुरक्षा संस्कृति को संगठन की संस्कृति में समाहित करना है तो संगठन के उच्च प्रबंधन की भागीदारी होना अत्यंत आवश्यक है, क्योंकि अगर उच्च प्रबंधन इस संस्कृति को अपने जीवन में और प्रतिदिन के कार्यों में उतारेंगे तभी अन्य कर्मचारी उनका अनुसरण करेंगे और अपनी आदतों को बदलेंगे.

किसी संगठन को साइबर सुसंस्कृत संगठन बनाने के लिए उन्हें कई तरह की गतिविधियां व्यापक स्तर पर करनी चाहिए जैसे कि फिशिंग ईमेल सिम्युलेशन एक्सर्साइज़, प्रतिदिन साइबर सुरक्षा पर कर्मचारियों को मोबाइल संदेश, ईमेल भेजना, साइबर सुरक्षा के समाचार भेजना, आए दिन मिलने वाले एलर्ट्स कर्मचारियों को बताना. कर्मचारियों को साइबर सुरक्षा का प्रशिक्षण देना, प्रश्नोत्तरी एवं जानकारी की प्रतियोगिता करवाना, साथ ही साथ जो कर्मचारी इन्हें अच्छे तरीके से अपने जीवन में उतारते और साइबर सुरक्षा के प्रति अच्छा कार्य करते है, उन्हें पुरस्कृत और सम्मानित करना, प्रशस्ति पत्र देना आदि, जिससे अन्य लोगों को प्रेरणा मिले.

एक संस्कृति तभी फल-फूल सकती है जब उसे लगातार पोषण मिले, क्योंकि एक संस्कृति तभी अपना अस्तित्व बना कर रख सकती है जब वह प्रभावी तौर पर लोगों द्वारा स्वीकारी जाए.

एक मजबूत साइबर सुरक्षा संस्कृति का निर्माण करके और उसे संगठन की मुख्य संस्कृति के साथ जोड़कर ही एक साइबर सुरक्षित संगठन का निर्माण संभव है.

यदि हम उपरोक्त भौतिक सुरक्षा आयामों की अनुपालना सुनिश्चित करें तो कोई ऐसी स्थिति शायद न हो जिसका सामना कर हम साइबर सुरक्षा को संस्था की सबसे सुरक्षित पद्धति न बना पायें. आवश्यक है कि सभी लोग एक टीम की तरह सोचें और "दुश्मन की तरह सोच" का अभ्यास करते रहे ताकि हम उनसे कई कदम आगे रहकर अपनी सुरक्षा सुदृढ़ कर सकें.

साइबर हमलों के वित्तीय एवं गैर वित्तीय प्रभाव

विजय जाधव
प्रबंधक
सीसो कार्यालय, के. का. मुंबई

के एम रेड्डी
सहायक महाप्रबंधक,
सीसो कार्यालय, के. का. मुंबई

व्यापार में उभरते रुझान के साथ बैंको का कार्य अब पूर्णतः डिजिटल प्रौद्योगिकी, इलेक्ट्रॉनिक डेटा और कंप्यूटर नेटवर्क पर निर्भर करता है जहां व्यक्तिगत और वित्तीय जानकारी से सम्बंधित सभी डेटा संग्रहित है. इन प्रवृत्तियों के साथ साथ, साइबर चोरी की रणनीति भी उन्नत हो रही है. साइबर क्राइम (Cyber Crime) आज की प्रमुख चुनौतियों में से एक है. हाल के वर्षों में प्रमुख साइबर अटैक (Cyber Attack) न सिर्फ वित्तीय नुकसानों का कारण बने हैं अपितु यह अत्यंत्य संवेदनशील जानकारियों के लीक होने का कारण भी बने हैं. ग्रुप-आईबी (Group-IB) विशेषज्ञों के मूल्यांकन के अनुसार, दुनिया के 99% साइबर क्राइम्स में पैसों की चोरी ही शामिल है. वर्ष 2017 में, बड़े पैमाने पर मालवेयर हमले हुए हैं जिसमें बड़ी कम्पनीज़ जैसे एमडीएलझेड़ (MDLZ), डीएलए पाईपर(DLA Piper), रोसनेफ्ट (Rosneft), एवराज़ (EVRAZ) इत्यादि और रूस में बैंकों, भारत और डेनमार्क में Maersk एवं कई अन्य देश साइबर अटैक का निशाना बने हैं. साइबर क्राइम के एक सबसेट के रूप में जानबूझकर किसी की पहचान की चोरी कर उससे किसी भी प्रकार का लाभ हासिल करना होता है. हाल के वर्षो में, पहचान की चोरी (Identity Theft) के कारण कई कंपनियों के ऑपरेशन्स एवं लाभप्रदता पर बहुत बुरा असर पड़ा है. वर्ष 2017 पहचान चोरों के लिए एक महान वर्ष था. Equifax वर्ष 2017 की सबसे बड़ी एवं ख़राब डाटा थेफ़्ट के साइबर क्राइम का शिकार हुई है. चुराया गया सभी डाटा, व्यक्ति की पहचान की चोरी (Identity Theft) के लिए इस्तेमाल किया जाता है. हालाँकि साइबर अटैक के विनाशकारी परिणामों ने कई व्यापारों को बुरी तरह प्रभावित किया है, एवं अभी इस तरफ और अधिक ध्यान देने की आवश्यकता है. पिछले कुछ वर्षों में, काफी संख्या में संगठित और विशेष समूह, मालवेयर (Malware) की सहायता से, इन वित्तीय संस्थानों को लूट रहे हैं. अन्य संगठनों की तरह, बैंक भी "मास मार्केट Mass Market" साइबर हमले का निशाना बने हैं.

साइबर जुर्म गैरकानूनी कृत्यों को संदर्भित करता है, जहां कंप्यूटर या तो एक

उपकरण है या लक्ष्य है या दोनों है. साइबर जुर्म एक अवैध कृत्य है, जिसे कार्यरूप देने में सूचना और संचार प्रौद्योगिकियों का उपयोग किया जाता है. सबूतों से पता चलता है कि बड़े संगठन जैसे बैंक, सरकारी एजेन्सियां, स्वास्थ्य संस्थान एवं बड़े कॉर्पोरेट्स जो कि अत्यधिक मूल्यवान डाटा रखते हैं, इनमें ज्यादा से ज्यादा साइबर अटैक होने की सम्भावना रहती है.

हमलावरों के प्रकार

हमलावर आम तौर पर तीन व्यापक श्रेणियों में विभाजित किये जा सकते हैं :

- आर्थिक रूप से प्रेरित हमलावर, जो इलेक्ट्रॉनिक रूप से चोरी या धोखाधड़ी का संचालन करने के लिए सिस्टम से समझौता करना चाहता है.
- जासूसी प्रेरित हमलावर, जो जानकारी चोरी करके तीसरी पार्टी को बेचने का इरादा रखता है.
- राजनीति प्रेरित हमलावर, जो एक समूह के भीतर साझा लक्ष्य को प्राप्त करने के लिए जानकारी या प्रणालियों से समझौता करने का इरादा रखता है.

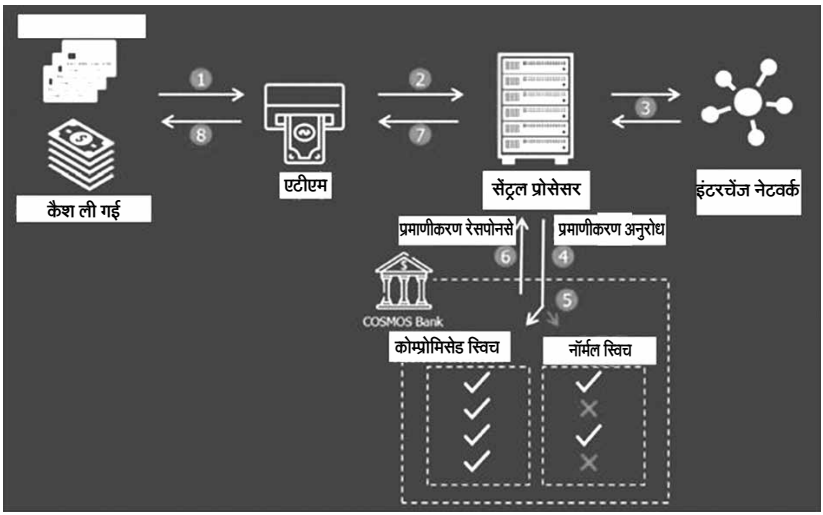
भिन्न प्रकार के कार्य साइबर क्राइम के अंतर्गत आते हैं.

अनधिकृत प्रवेश और हैकिंग	• किसी भी कंप्यूटर या कंप्यूटर नेटवर्क में बिना अनुमति के प्रवेश करने को unauthorized access या hacking कहा जाता है. अनधिकृत व्यक्ति द्वारा कंप्यूटर नेटवर्क में किया गया कोई भी कार्य इस अपराध की श्रेणी में आता है. जो व्यक्ति किसी नेटवर्क में अनधिकृत तरीके से प्रवेश करता है, उसे हैकर कहा जाता है. हैकर ऐसे प्रोग्राम बनाते हैं, जो वांछित नेटवर्क पर आक्रमण कर सकें. इस प्रकार की गतिविधियां साधारणयता वित्तीय अपराधों में बहुतायत होते हैं. जैसे • किसी बैंक के नेटवर्क में अनधिकृत तरीके से प्रवेश कर उनके खाताधारकों के अकाउंट से दूसरे अकाउंट में पैसे स्थानांतरित करना. • किसी व्यक्ति के क्रेडिट कार्ड की जानकारी चुरा कर उसका दुरूपयोग करना आदि. • किसी वेबसाइट के घटक अनधिकृत तरीके से बदलने की क्रिया को web हैकिंग कहा जाता है.

पहचान चुराना	जब साइबर अपराधी किसी व्यक्ति की पहचान से संबंधित विभिन्न जानकारियां जैसे - उसका नाम, आधार नं., मोबाइल नं., पता इत्यादि साइबर हमले के माध्यम से दुरुपयोग करने अथवा धोखा देने के उद्देश से चुराता है, तो उसे पहचान की चोरी कहा जाता है. इसका प्रचलन पहली बार वर्ष 1964 में हुआ, साईबर अपराधी किसी व्यक्ति की पहचान की चोरी कर, गुप्त रुप से उसके नाम का दुरुपयोग कर अर्थिक लाभ उठाने का प्रयत्न करता है. वर्ष 2017 में पहचान चोरी से संबंधित सबसे अधिक अपराध हुए. इसी वर्ष कंपनी सबसे बड़ी पहचान चोरी का शिकार हुई.
कंप्यूटर वायरस को फैलाना	जो प्रोग्राम किसी कंप्यूटर या कंप्यूटर नेटवर्क की अनुमति के बिना कंप्यूटर में प्रवेश कर लेते हैं, उन्हें कंप्यूटर वायरस की श्रेणी में डाला जाता है. साधारणता वायरस या वोर्म (Worm) का काम किसी अन्य के कंप्यूटर के डाटा को नष्ट करना है. इसलिए कोई व्यक्ति या संस्था किसी ऐसे प्रोग्राम को अनावश्यक रुप से फैलाते हैं तो उन्हें इस अपराध की श्रेणी में रखा जाता है. बहुत से बड़े नेटवर्क को यदि वायरस प्रभावित करें तब बहुत बड़ा नुकसान हो सकता है. उदाहरण के लिए किसी विमान सेवा के कंप्यूटर में वायरस ने डाटा को बदल दिया है तब कोई प्लेन दुर्घटनाग्रस्त हो सकता है. यद्यपि सभी बड़े कंप्यूटर नेटवर्क में वायरस से कंप्यूटर को बचाने की प्रणाली होती है. भारतीय आईटी एक्ट 2008 के सेक्शन 43 (C) एवं 43 (e) के अंतर्गत वायरस फैलाने के कार्य के लिए सजा का प्रावधान है.
Trojan उस प्रोग्राम को कहा जाता है जो दिखते तो उपयोगी हैं, लेकिन उनका कार्य कंप्यूटर नेटवर्क को नुकसान पहुंचाना होता है.	• साइबर क्राइम के कुछ अन्य उदाहरण हैं - • नेटवर्क का अनधिकृत तौर पर प्रयोग करना • कंप्यूटर तथा नेटवर्क का प्रयोग कर व्यक्तिगत (Private) तथा गुप्त (Confidential) सूचना प्राप्त करना • नेटवर्क तथा सूचना को नुकसान पहुंचाना • बड़ी संख्या में ई-मेल भेजना (E-Mail Bombing) • वायरस द्वारा कम्यूटर तथा डाटा को नुकसान पहुंचाना • इंटरनेट का उपयोग कर आर्थिक धोखाधड़ी (Financial Fraud) करना • इंटरनेट पर गैरकानूनी तथा असामाजिक तथ्यों तथा चित्रों को प्रदर्शित करना

पुणे के कॉस्मोस बैंक से हैकर्स ने उड़ाए 94 करोड़ रुपए, कस्टमर की निजी जानकारियां भी गायब

पुलिस में दर्ज कराई गई शिकायत के मुताबिक बैंक 2 बार शनिवार और रविवार को साइबर हमले का शिकार हुआ. शिकायत में कहा गया है कि पहला हमला 11 अगस्त को दोपहर 3 बजे से रात 10 बजे के बीच हुआ, जबकि 13 अगस्त को साइबर हमला सुबह साढ़े ग्यारह बजे के करीब हुआ. इसमें बैंक के गणेशखंड मार्ग स्थित मुख्यालय में काम प्रभावित हुआ. साइबर हमले के दौरान बैंक के मुख्यालय के सर्वर से हमलावरों ने ग्राहकों के वीज़ा और रुपे डेबिट कार्ड की जानकारियां भी उड़ा लीं. हैकर्स ने 12000 वीज़ा कार्ड ट्रांजैक्शन के माध्यम से 78 करोड़ रुपये हांगकांग समेत अन्य देशों के बैक खातों में भेज दिए.



विश्व में घटित साइबर अटैक की कुछ प्रमुख घटनायें :

2012 : न्यूयॉर्क टाइम्स के द्वारा साइबर अटैक पर दी गयी रिपोर्टः "बैंक ऑफ अमेरिका, जे पी मॉर्गन, सिटी ग्रुप, यू एस बैंक, वेल्स फारगो और पीएनसी के ग्राहक, जो अपने खाते नहीं देख पा रहे थे या ऑनलाइन बिल भुगतान की सुविधा का उपयोग नहीं कर पा रहे थे, काफी निराश एवं परेशान थे, क्योकि बैंक द्वारा उन्हें स्पष्ट रूप से क्या चल रहा है, बताया नहीं गया था. इसके अलावा, "सीईओ ब्रायन मोयनिहान ने विश्लेषकों को कहा कि बैंक ऑफ़ अमेरिका डाटा की सुरक्षा के लिए साइबर सिक्योरिटी पर प्रतिवर्ष कई सौ मिलियन डॉलर खर्च कर रहा है. हमलावरों का उद्देश्य आर्थिक फायदा अथवा डाटा

चोरी नहीं था, अपितु ग्राहकों को निराश एवं परेशान करना था, अंततः जिससे संस्था को आर्थिक नुकसान हो सके. सीएनएन CNN के द्वारा दी गई रिपोर्ट के अनुसार "DOS (डिनायल ऑफ़ सर्विसेज) एक प्रभावी परन्तु अपरिष्कृत शस्त्र है जिससे वास्तव में हैकिंग नहीं हुई है. किसी भी प्रकार का बैंक डाटा भी चोरी नहीं हुआ है एवं बैंक का एटीएम नेटवर्क भी अप्रभावी था एवं बराबर काम कर रहा था ". साइबर अटैक का सिर्फ एक ही उद्देश्य था, बैंक की पब्लिक फेसिंग वेबसाइट को थोड़े समय के लिए बंद करना.

2014 : यूएसए टुडे रिपोर्टः "संघीय अधिकारियों ने सोमवार को कंपनियों को चेतावनी दी है कि हैकर ने पिछले 12 महीनों में 500 मिलियन से अधिक वित्तीय रिकॉर्ड चोरी कर लिए हैं, जो कि एक बैंक ईमारत में घुसे बिना बैंक में घुसने के बराबर है.

2016 : सन 2017 में, "46 प्रमुख वित्तीय संस्थाओं को हैकर्स द्वारा डिस्ट्रिब्यूटेड डिनायल ऑफ़ सर्विसेज (DDOS) का शिकार बनाया गया था, जिसके तहत हैकर्स ने सैकड़ों कम्प्यूटर्स एवं सर्वर्स को रिमोट कंट्रोल करके इनके द्वारा वित्तीय संस्थाओं के सर्वर्स पर असीमित डाटा की बाढ़ भेज कर उन्हें जाम कर दिया था, जिसके कारण ये सर्वर्स वैध डाटा भी प्राप्त नहीं कर पा रहे थे."

बी सी कंपनी के अनुसार शिकार हुई कम्पनीज में बैंक ऑफ अमेरिका Bank of America, दि न्यू यार्क स्टॉक एक्सचेंज the New York Stock Exchange, कॅपिटल वन एण्ड आईएनजी Capital One and ING, तथा and पीएनसी बैंक्स PNC Banks इत्यादि के नाम थे. इसके बाद, एफबीआई और अमेरिका के सीक्रेट सर्विस एजेंटों ने एक आदमी को गिरफ्तार किया, जिसे अमेरिका के इतिहास में वित्तीय कंपनियों के सबसे बड़े साइबर हमले का आरोप लगाया गया. डाटा ब्रीच के कारण जेपी मार्गन JP Morgan कंपनी सबसे ज्यादा प्रभावित हुई थी जिसमें उसके 83 मिलियन से ज्यादा बैंक ग्राहकों का डाटा ब्रीच हुआ था.

यूरोप

2015 : "आरबीएस बैंकिंग समूह ने यह प्रकट किया कि उनकी ऑनलाइन सेवाओं पर एक साइबर हमला हुआ था जिसके कारण उनके ग्राहकों को मासिक बिलों के भुगतान करने के लिए करीब 1 घंटे तक लॉगिन के लिए संघर्ष करना पड़ा. नेस्डेक NASDAK कंपनी ने उल्लेख किया है कि वर्ष 2017 के उत्तरार्द्ध में उनके ऑनलाइन ट्रेडिंग पर कई साइबर अटैक हुए थे. नवीनतम डेटा उल्लंघन FXCM Inc, जो कि एक ऑनलाइन विदेशी मुद्रा व्यापार और संबंधित सेवा प्रदान करती है, ने सूचित किया था, 01 अक्तूबर को हैकर्स ने ग्राहकों की जानकारी अनधिकृत रूप से प्राप्त की और कुछ खातों में ऑनलाइन अंतरण भी किये. एक सूचना सुरक्षा कंपनी आईबी समूह ने एक ब्लॉग में प्रकाशित किया,"फरवरी

2015 में, पहली बार, एक ट्रोजन Corkow (Metel) ने एक स्टॉक एक्सचेंज ट्रेडिंग टर्मिनल का हैकिंग के द्वारा नियंत्रण प्राप्त किया और कई सौ मिलियन डॉलर की कुल मूल्य के आदेश रखे. सिर्फ 14 मिनट में हमलावरों ने असामान्य अस्थिरता पैदा की, जिस दौरान उन्होंने 55 रूबल्स में डॉलर्स खरीद कर 62 रूबल्स में बेच दिया. इस घटना की वजह से रुसी बैंकों को बहुत बड़ी हानि हुई. हालाँकि इसका फायदा हैकर्स को न होते हुए उस दौरान ट्रेडिंग करने वाले कई ग्राहकों को हुआ है. इस कंपनी ने इस बात पर प्रकाश डाला कि हैकर्स साइबर हमले (cyber attack) का उपयोग केवल वित्तीय हानि या सूचना उल्लंघन के लिए नहीं करते है बल्कि इसका उपयोग जासूसी और साइबर टेररिज़म (cyberterrorism) में भी किया जाता है. Corkow को Metel के रूप में भी जाना जाता है.

2016 : Crime Russia की एक रिपोर्ट के अनुसार "वर्ष 2017 में लर्क टीम Lurk Team के हैकर्स ने, इसी नाम से बने बैंकिंग ट्रोजन के द्वारा रशियन बैंक्स के खातों से राशि की चोरी की. इससे पहले कि रूस की आंतरिक मंत्री परिषद Interior Ministry और FSB कुछ समझ पाते या रोक पाते, 1.7 बिलियन रूबल्स (US $ 28.3 M) की चोरी हो गई. "Crime Russia ने Energo Bank के मामले में प्रकाश डाला, जहां Metel हैकर्स ने बैंकों को 244 मिलियन रूबल्स (US $ 28.3 M) का नुकसान पहुंचाया, Kaspersky ने एक ब्लॉग में लिखा है "किसी न किसी तरह से हैकर्स ने लगभग सभी बैंकों को 2.5 मिलियन से 10 मिलियन तक का नुकसान पहुंचाया है". "विशेषज्ञों का अनुमान है कि रूसी बैंकों में सबसे कम की चोरी $ 370,000 (25 मिलियन रूबल्स) है एवं सबसे अधिक की चोरी करीब $ 9 मिलियन (600 मिलियन रूबल्स) है.

2017 : HSBC, जो कि विश्व एवं यूरोप कि सबसे बड़ी बैंक है, भी वर्ष 2017 के प्रारम्भ में, साइबर अटैक का शिकार हुई थी. The Week Newsletter की एक रिपोर्ट के अनुसार "साइबर अटैक की वजह से HSBC Bank के ग्राहक एक माह में कम से कम दो बार ऑनलाइन बैंकिंग की सुविधा से वंचित रहे.

साइबर हमलों में संस्थाओं पर हैकर्स Hackers निम्न तरीके से प्रभावित करते हैं:

- प्रत्यक्ष हानि (वित्तीय)
- अप्रत्यक्ष हानि (गैर वित्तीय) - साइबर अपराधी हैकिंग के द्वारा दूर से ही डाटा का प्रशासन कर सकते हैं.
- वित्तीय नुकसान (झूठा लेनदेन करने से) कर सकते हैं.
- गोपनीय जानकारी चोरी कर सकते हैं और उनकी बिक्री कर सकते हैं, यहां तक कि वे इनका जासूसी या आतंकवाद के लिए उपयोग कर सकते हैं.

- संगठन पर हमला करके ग्राहकों को लक्षित/निशाना कर सकते हैं. ग्राहक को हताश कर सकते हैं.
- संगठन की सार्वजनिक छवि को नुकसान पहुंचा सकते हैं.

साइबर अपराधों से बचने के उपाय (Ways To Prevent Cyber Crime)

- लॉगिन आईडी तथा पासवर्ड सुरक्षित रखना तथा समय-समय पर इसे परिवर्तित करते रहना
- एन्टीवायरस साफ्टवेयर का प्रयोग करना
- फायर वाल का प्रयोग करना
- डाटा का बॅक-अप कॉपी रखना
- प्रॉक्सी सर्वर का प्रयोग करना
- डाटा को गुप्त कोड (इन्क्रिप्टेड फॉर्म) में बदलकर भेजना व प्राप्त करना

साइबर अपराध का रहस्यमयी संसार

के. के. यादव
प्रबंधक
क्षे. का. बेंगलूरु

प्रशांत विश्वकर्मा
सहायक प्रबंधक
क्षे. का. गोरखपुर

विकास खुराना
वरिष्ठ प्रबंधक
सीसो कार्यालय, के. का. मुंबई

सुप्रसिद्ध कार्टूनिस्ट पीटर स्टेनर ने 05 जुलाई, 1993 को न्यूयॉर्क पत्रिका में एक कार्टून बनाया था. इसमें दो कुत्ते कंप्यूटर पर बैठे हैं. वह कुत्ता जो कंप्यूटर पर काम कर रहा है, दूसरे से कहता है कि "On the Internet, nobody knows that you are a dog." अर्थात इंटरनेट पर कोई नहीं जानता कि कंप्यूटर चलाने वाला व्यक्ति कौन है.

साइबर के रहस्यमयी संसार की वास्तविकता दर्शाने हेतु यह कार्टून अपने आप में एक मील का पत्थर है. हम यह नहीं जानते कि सिलिकन की असंख्य उलझी लाइनों के मध्य आपसे कौन मुखातिब है. इन्हीं रहस्यों की दुनिया में साइबर अपराध पनप रहा है. तथापि यह भी सत्य है कि समाज के विकास में सूचना व साइबर तकनीकी अब तक के सबसे महत्वपूर्ण अविष्कार हैं.

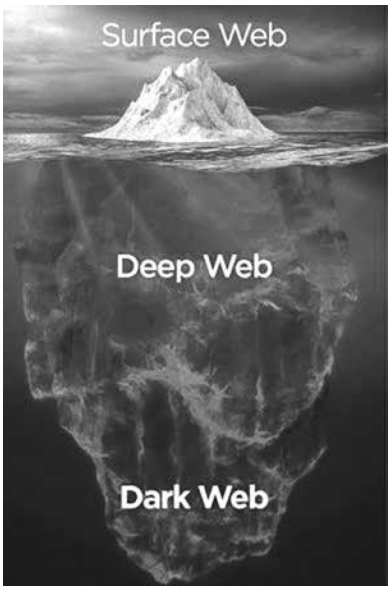
"On the Internet, nobody knows you're a dog."

वस्तुतः अपराध कानूनी नियमों के उल्लंघन करने की नकारात्मक प्रक्रिया है, जिसके परिणामस्वरूप सामाजिक मूल्यों का विनाश होता है. आज पृथ्वी, जल और आकाश तीनों क्षेत्रों में अपराधी पहुँच चुके हैं. "तू डाल-डाल, मैं पात-पात" की तर्ज पर सरकार द्वारा बनाए गए कानूनों का तोड़ अपराधी पहले ही निकाल लेते हैं. कम्प्यूटर के विकास के साथ-साथ सूचना एवं प्रौद्यागिकी का क्षेत्र भी अपराधियों की पहुँच से बाहर नहीं रहा है. इंटरनेट के रहस्यमयी जाल ने स्थितियों को ऐसा बदला कि अब चोरी दिन के प्रकाश में होने लगी है. आज हाथ में एक "माऊस" लेकर "की-बोर्ड" पर बैठा व्यक्ति जितना नुकसान पहुँचा सकता है, उतना शायद शक्तिशाली बम और तोप भी न पहुँचा पाए.

इंटरनेट ने आज हमें संचार एवं सूचनाओं व वस्तुओं के आदान-प्रदान के लिए एक समानांतर माध्यम दिया है. वैश्विक स्तर पर इंटरनेट को तेजी से अपनाने के परिणामस्वरूप, एक ओर हमारे जीवन में विभिन स्तरों पर समृद्धि आई है, वहीं दूसरी ओर इसने नयी-नयी चुनौतियों व जोखिमों को जन्म दिया है. बाज़ार एवं उपभोक्ताओं की आदतों व परस्परिक संबंधों में जहां डिजिटल व काल्पनिक दुनिया की वजह से बदलाव व उन्नति हो रही है, वहीं ये बदलाव नए साइबर अपराधों के लिए नए अवसर प्रदान कर रहे हैं. साइबर हमले, फ़िज़िकल हमलों की तरह सतही नहीं होते हैं, फिर भी साइबर हमले अत्यंत विध्वंसकारी हो सकते हैं क्योंकि आजकल सभी लोगों का जीवन कहीं न कहीं कंप्यूटर व इंटरनेट पर निर्भर है.

उदाहरण के तौर पर, पहले उद्यमों पर फ़िज़िकल आक्रमण होते थे, आज वही अटैक कम्प्यूटर व इंटरनेट के जरिये सस्ते व आसानी से न पकड़े जाने के भय से किए जाते हैं. साइबर अपराध का प्रभाव भी तुरंत होता है. अपराधियों का एक लक्ष्य यह होता है कि उसकी पहचान गोपनीय बनी रहे. यही एक माध्यम है, जिसके द्वारा वो उत्तरदायी रहे बिना कानून की पहुंच से दूर रह सकते हैं. वास्तविक दुनिया की तरह साइबर की दुनिया भी रहस्यों से भरी हुई है. साइबर अपराध में भी कई ऐसी विचित्र व अनोखी घटनाएं एवं अनसुलझे रहस्य हैं.

इंटरनेट की दुनिया में डार्कवेब या डार्कनेट सबसे बड़ा व डरावना रहस्य बना हुआ है, जो कि इंटरनेट पर एक छुपा हुआ क्षेत्र है, जिसमें लोग विभिन प्रकार के जघन्य आपराधिक गतिविधियों में लिप्त हैं.



डार्कनेट, साइबर अपराधों व साइबर आतंकवाद के लिए एक उपयुक्त स्थान है. डार्कनेट एक ऐसा नेटवर्क है, जिसे जानबूझकर इंटरनेट पर छुपाया गया है एवं इसे इसी तरह से डिज़ाइन किया गया है, जिससे कि अपराधी व उनकी पहचान गुप्त रह सके. डार्क वेब मानव तस्करी, अवैध अंगों की बिक्री, हथियारों की बिक्री, चाइल्ड पोर्नोग्राफी आदि जैसे जघन्य अपराधों में लिप्त है. डार्क नेट को विशेष तरह के टूल्स, सॉफ्टवेर ब्राउज़र (जैसे कि TOR ब्राउज़र) व अन्य प्रोटोकॉल की मदद से एक्सेस

किया जा सकता है. इन टूल्स व ब्राउज़र्स की मदद से ये अपराधी अपने आईपी एड्रैस एवं अपनी पहचान को इंटरनेट पर गुप्त रख सकते हैं. डार्कनेट की काल्पनिक संरचना अवैध कालाबाजारी के फलने-फूलने के लिए उपयुक्त स्थान है. ये एक ऑनलाइन बाज़ार है, जिसका उपयोग अपराधी अवैध वस्तुओं को खरीदने व बेचने के लिए एवं इसके द्वारा प्रदान की गयी गुमनामी का फायदा उठाने के लिए करते हैं और इन अवैध लेनदेनों के लिए अधिकतर डिजिटल करेंसी, जो कि यूज़र की पहचान छुपाने के लिए ही बनी है, का प्रयोग करते हैं, जिसका पता लगाना कानून प्रवर्तन एजेन्सीज के लिए भी बहुत मुश्किल है.

साइबर अपराध में कंप्यूटर, सर्वर और नेटवर्क सभी शामिल होते है. आमतौर पर डाटा कंप्यूटर या सर्वर में भंडारित रहता है और डाटा के आधार पर रिपोर्ट व सूचनाएं प्राप्त तथा संप्रेषित की जाती हैं. किसी भी कंप्यूटर का अपराधिक स्थान पर मिलना या कंप्यूटर से कोई अपराध करना कंप्यूटर अपराध कहलाता है. इस क्षेत्र में क्या-क्या अपराध हो सकते हैं, इसे जानना हम सब के लिए आवश्यक है. कोई भी आपराधिक कृत्य, जो कंप्यूटर अथवा संचार साधनों से जुड़ा है, साइबर अपराध की श्रेणी में आता है. उदाहरण के लिये कंप्यूटर के माध्यम से वित्तीय धोखाधड़ी, पहचान की चोरी, हैकिंग, अश्लील संदेश संप्रेषण, टेलीफोन तकनीक का दुरूपयोग, राष्ट्रविरोधी गतिविधियाँ, वायरस का फैलाव, कंपनी नीति के विरुद्ध गतिविधियों का संचालन, कंप्यूटर नेटवर्क पर आक्रमण, आंतरिक और गुप्त सूचनाओं की चोरी, बौध्दिक संपदा की चोरी, किसी की निजी जानकारी को प्राप्त कर उसका गलत इस्तमाल करना, किसी के कंप्यूटर से निजी जानकारी निकाल लेना या चोरी करना, उपलब्ध डाटा में फेर बदल करना, कंप्यूटर के किसी भाग की चोरी करना या नष्ट करना इत्यादि. इसके अतिरिक्त स्पैम ईमेल, हैकिंग, फिशिंग, वायरस डालना, दूसरों की जानकारी ऑनलाइन प्राप्त करना या किसी पर हर वक़्त नजर रखना आदि गतिविधियां व कार्यकलाप भी साइबर अपराध की श्रेणी में आते हैं.

विश्व में आज जितने भी साइबर अपराध होते हैं, वे सभी रिपोर्ट नहीं होते. शायद न लोगों को समझ में आता है कि उनसे कैसे निपटा जाय और न ही उन्हें विश्वास है कि इसका संतोषजनक हल निकल सकता है. सच यह भी है कि इस समय हमारे पास इस तरह के अपराधों की जांच करने के लिये न ही विशेषज्ञ हैं और न ही अपराध तय करने वाले सक्षम न्यायाधीश. लोग अक्सर साइबर अपराध यह सोंच कर करते हैं कि वे अज्ञात हो कर साइबर अपराध कर सकते हैं लेकिन यह पूरा सच नहीं है. अमूमन साइबर अपराध की गतिविधियां डाटा से जुड़ी होती हैं, अतः साइबर अपराधी अपने पीछे कोई न कोई इलेक्ट्रानिक साक्ष्य अवश्य छोड़ जाते हैं, चाहे वे कितने ही होशियार क्यों न हों. विश्वस्तर पर साइबर अपराधों की जांच के लिये "कंम्प्यूटर फोरेंसिक" का प्रयोग किया जा रहा है, जिसके माध्यम से आई.टी. और कंप्यूटर क्षेत्र के विशेषज्ञ इलेक्ट्रानिक साक्ष्यों

के आधार पर अपराधियों को पकड़ते हैं. यहाँ हम कुछ महत्वपूर्ण साइबर अपराध की चर्चा करते हैः

1) **स्पैम ईमेल (spam e-mail)** - हमारे ईमेल खाते में अनेक प्रकार के ईमेल आते हैं, जिसमें ऐसे ईमेल भी होते हैं, जो सिर्फ कंप्यूटर को न केवल नुकसान पहुंचाते हैं, बल्कि यूज़र का समय भी बर्बाद करते हैं.

स्पैम उस प्रकार के ईमेल को कहते हैं, जो बिना मांगे या बुलाये आता है, जिसमें प्रायः विज्ञापन भरे होते हैं. जब से ईमेल का विकास हुआ है, तब से स्पैम मेल एक समस्या बनी हुई है. स्पैम भेजने के लिए पते चैटरूम से, वेब साईट से या वायरस के प्रयोग से एकत्र किए जाते हैं.

2) **अप्राधकृत पहुंच एवं हैकिंग (unauthorised access and hacking)**

किसी भी कंप्यूटर या कंप्यूटर नेटवर्क में बिना अनुमति के प्रवेश करने को अनाधिकृत एक्सेस या हैकिंग कहा जाता है. अनधिकृत व्यक्ति द्वारा कंप्यूटर नेटवर्क में किया गया कोई भी कार्य इस अपराध की श्रेणी में आता है. जो व्यक्ति किसी नेटवर्क में अनधिकृत तरीके से प्रवेश करता है, उसे हैकर कहा जाता है. हैकर ऐसे प्रोग्राम बनाते हैं, जो वांछित नेटवर्क पर आक्रमण कर सके. इस प्रकार के कार्य साधारणतया वित्तीय अपराधों में बहुतायत में होते हैं. जैसे -

- किसी बैंक के नेटवर्क में अनधिकृत तरीके से प्रवेश कर उनके खाताधारकों के अकाउंट से दूसरे अकाउंट में पैसे स्थानांतरित करना.
- किसी व्यक्ति के क्रेडिट कार्ड की जानकारी चुरा कर उसका दुरूपयोग करना आदि.

किसी वेबसाइट को अनाधिकृत तरीके से बदलने की क्रिया को वेब हैकिंग कहा जाता है.

3) डाटा चोरी (data theft) -

किसी संस्था या व्यक्ति या कंप्यूटर नेटवर्क में अधिकृत व्यक्ति की अनुमति लिए बिना उसके कंप्यूटर के डाटा को कॉपी करना, उसे शेयर करना, डाटा चोरी के अपराध की श्रेणी में आता है. किसी अनाधिकृत व्यक्ति द्वारा किसी अन्य व्यक्ति या संस्था की अनुमति के बिना डाटा कॉपी करना गैरकानूनी माना जाता है. वर्तमान में बहुत से छोटे स्टोरेज डिवाइस जैसे पेन ड्राइव, मेमोरी कार्ड आदि आसानी से उपलब्ध हैं, इन डिवाइसें की सहायता से डाटा चुराना बहुत आसान हो गया है.

4) कंप्यूटर वायरस को फैलाना (Spreading virus or worms)

साधारणता वायरस या वोर्म प्रोग्राम का काम किसी अन्य के कंप्यूटर के डाटा को विकृत करना है. यदि कोई व्यक्ति या संस्था किसी ऐसे प्रोग्राम को अनावश्यक रुप से फैलाते हैं, तो उन्हें इस अपराध की श्रेणी में रखा जाता है. यदि बहुत बड़े नेटवर्क को वायरस प्रभावित कर देता है, तब बहुत बड़ा नुकसान हो सकता है. उदाहरण के लिए किसी विमान सेवा के कंप्यूटर में वायरस ने यदि डाटा बदल दिया है, तो प्लेन दुर्घटनाग्रस्त भी हो सकता है.

5) पहचान चुराना (Identity theft)

- किसी अन्य व्यक्ति की पहचान चुराकर कंप्यूटर नेटवर्क पर कार्य करना इस अपराध श्रेणी में आता है.
- कंप्यूटर नेटवर्क पर स्वयं की पहचान बचा कर स्वयं को दूसरे के नाम से प्रस्तुत करना, उसके नाम पर कोई घपला करना, बेवकूफ बनाना आईटी एक्ट के अंतर्गत अपराध है.
- इसके अतिरिक्त किसी अन्य व्यक्ति के पासवर्ड का प्रयोग करना, डिजिटल सिग्नेचर की नकल करना भी इस अपराध की श्रेणी में आते हैं.

- किसी अन्य के नाम का प्रयोग कर अवांछित लाभ लेना, धोखाधड़ी करना भी इस प्रकार के अपराध में आते हैं.

जिस व्यक्ति की पहचान चुराई गई है, उसे अनावश्यक रुप से कानूनी उलझनों का सामना करना पड़ता है और उसे बहुत बड़ा नुकसान भी हो सकता है. उदाहरण के लिए आपके बैंक अकाउंट को किसी अन्य व्यक्ति द्वारा आपकी पहचान चुराकर प्रयोग करना या आपकी पहचान चुरा कर दूसरी जगह धोखाधड़ी के लिए प्रयोग करना. इसलिए कंप्यूटर नेटवर्क पर अपने पासवर्ड व्यक्तिगत जानकारियां सार्वजनिक न करें.

6) **ट्रोजन एटैक (Trojan attack) :** Trojan उस प्रोग्राम को कहा जाता है जो दिखते तो उपयोगी हैं, लेकिन उनका कार्य कंप्यूटर नेटवर्क को नुकसान पहुंचाना होता है.

7) **फिशिंग (phishing) :** फ़िशिंग को आमतौर पर ईमेल स्पूफिंग द्वारा किया जाता है. इसमें सोशल साइट्स पर आपके पासवर्ड और आई डी हैक कर लिए जाते हैं. इसमें यूज़र को आकर्षक ईमेल भेजा जाता है. जैसे आपके बैंक के नाम से या आरबीआई के नाम से कोई मेल आपके पास आती है तो आप उस मेल में दिए गए लिंक को खोलते हैं. वस्तुतः वह लिंक उस बैंक की साईट न होकर फ्रॉड साईट का लिंक होता है. इसमें यदि आप अपने अकाउंट नंबर, अपना पासवर्ड और अन्य जानकरी डाल देते हैं, तो वह हैक हो जाती है और सीधे हैकर्स के पास चली जाती है, जिसका गलत इस्तमाल कर के आपके अकाउंट से पैसे निकाल सकते हैं.

ई-मेल में शामिल किसी भी लिंक को क्लिक करने से पहले वह सुरक्षित है या नहीं यह जरूर जांच लें.

8) **सॉफ्टवेयर पाइरेसी (software piracy)** - सॉफ्टवेयर की नकली कॉपी तैयार कर सस्ते दामों में बेचना भी साइबर अपराध के अन्तर्गत आता है. इससे साफ्टवेयर कम्पनियों को भारी नुकसान उठाना पड़ता है.

9) **साइबर बुलिंग (Cyber-bullying) :** Cyber-bullying का हिंदी में मतलब होता है साइबर-धमकी यानी इंटरनेट के माध्यम से गलत फोटो, गलत भाषा या झूठे

समाचार आदि का इस्तेमाल करते हुए किसी भी व्यक्ति को डराना, धमकाना, उसे टॉर्चर करना या उसे गलत दिशा में भटकाना, ये सब इसके अंतर्गत आता है.

यह एक अपराध है, जिसके लिए कानून में सजा का भी प्रावधान है. इसकी चपेट में ज्यादातर बच्चे आते हैं, जिससे उनकी जिन्दगी पर बहुत ही बुरा असर पड़ता है. इसमें किसी बच्चे को गन्दी फोटो, भाषा या किसी गेम के जरिए डराकर, धमाका कर या बहलाकर गलत काम करवाए जाते हैं. इससे बच्चों के दिमाग पर बहुत ही ज्यादा नकारात्मक प्रभाव पड़ता है और वे इस चीज से इतने डरे हुए होते हैं कि उन्हें समझ नहीं आता कि वे क्या करें, जिसके कारण वे अपने माता-पिता को भी ये बात नहीं बता पाते हैं और जाने-अनजाने बताए गए गलत रास्ते पर चलने लगते हैं. आगे चलकर उनके दिमाग पर इतना बुरा प्रभाव पड़ जाता है कि कई बार वे अपनी जान तक दे देते हैं. इसका उदाहरण आपने कुछ ही समय पहले देखा होगा कि एक ब्लू व्हेल (Blue Whale) नाम के गेम ने किस तरह से कई बच्चों को अपने जाल में फंसाया और आखिर में उनकी जान ले ली.

10) **फर्जी बैंक कॉल (fraud bank call) :** आपको जाली ईमेल, मैसेज या फोन कॉल प्राप्त हो, जो आपकी बैंक से आई हुई लगे, जिसमें आपसे पूछा जाये कि आपके एटीएम नंबर और पासवर्ड की आवश्यकता है और यदि आपके द्वारा यह जानकारी नहीं दी गयी तो आपका खाता बन्द कर दिया जायेगा या इस लिंक पर सूचना दें. याद रखें किसी भी बैंक द्वारा ऐसी जानकारी कभी भी इस तरह से नहीं मांगी जाती है और भूलकर भी अपनी इस प्रकार की जानकारी किसी को भी इन्टरनेट या फोनकॉल या मैसेज के माध्यम से न बताएं.

11) **सोशल नेटवर्किंग साइटों पर अफवाह फैलाना (Spreading rumors on social networking sites) :** बहुत से लोग सोशल नेटवर्किंग साइटों पर सामाजिक, वैचारिक, धार्मिक और राजनैतिक अफवाह फैलाने का काम करते हैं लेकिन यूज़र्स उनके इरादे समझ नहीं पाते हैं और जाने-अनजाने में ऐसे लिंक्स को शेयर करते रहते हैं. यह भी साइबर अपराध और साइबर-आतंकवाद की श्रेणी में आता है.

12) **स्मर्फ़ हमला (smurf attack) :** यह हमला पीड़ित नेटवर्क पर बड़ी मात्रा में यातायात उत्पन्न करता है, जिससे नेटवर्क क्रैश हो जाता है व वास्तविक यूज़र को जरूरी एप्लिकेशन का एक्सेस नहीं मिल पाता है.

13) **अनजाने में होता साइबर अपराध :** आज इंटरनेट का प्रयोग करने वाला लगभग हर शख्स अनजाने में कोई न कोई साइबर अपराध अवश्य करता है. यह भी हो सकता है कि ये कानूनी अपराध न हो, पर नैतिक अपराध तो है ही. आप कोई

चित्र, लेख या वीडियो इंटरनेट से कॉपी-पेस्ट करते समय जरा भी नहीं झिझकते. परंतु क्या आपको पता है कि इंटरनेट पर ऐसे तमाम काम साइबर अपराध के तहत आते है.

14) **कॉपीराइट सामग्री की चोरी :** हर क्रिएटिव चीज बनाने वाले के पास एक खास हक होता है, जो उसे अपनी सामग्री को गैरकानूनी ढ़ंग से नकल किए जाने के खिलाफ सुरक्षा देता है. इसे कॉपीराइट कहते हैं. कॉपीराइट लेने की एक कानूनी प्रक्रिया है, लेकिन अगर ऐसा नहीं भी करते, तो भी अपनी रचना पर आपका ही हक है. इसी तरह अगर आप किसी और की फोटो उसकी लिखित मंजूरी के बिना अपने फेसबुक प्रोफाइल पर पोस्ट करते हैं, गूगल इमेज या दूसरी इमेज होस्टिंग वेबसाइटों से ले उसे अपने ब्लॉग, सोशल नेटवर्किंग, वेबसाइट या पत्र-पत्रिका में इस्तेमाल करते हैं तो यह भी साइबर अपराध की श्रेणी में आता है.

15) **चाइल्ड पॉर्नोग्राफी :** अगर आप जाने या अनजाने अपने इंटरनेट कनेक्शन के जरिये चाइल्ड पॉर्नोग्राफी अर्थात् अश्लील चित्र, साहित्य, वीडियो, लेख आदि देखते हैं, तो वह साइबर अपराध है. आपने ऐसी किसी सामग्री को अपने किसी दोस्त को फॉरवर्ड कर दिया, तो आप एक और साइबर अपराध कर चुके हैं. इसके अतिरिक्त 18 साल से कम उम्र वालों से संबंधित अश्लील सामग्री देखना, इंटरनेट से भेजना और सहेजना भी साइबर अपराध है.

16) **प्रतीक चिह्नों, ट्रेडमार्क आदि की चोरी :** इंटरनेट पर लोगो, आइकंस, प्रतीक चिह्नों, ट्रेडमार्क वगैरह की चोरी भी आम है. अच्छा सा लोगो दिखाई दिया और आपने उसे कॉपी कर इस्तेमाल कर लिया या किसी डिजाइनर की सेवा ली, जिसने झटपट इंटरनेट से किसी कंपनी का अच्छा सा लोगो इस्तेमाल कर आपका विजिटिंग कार्ड, ब्रोशर और लेटरहेड तैयार कर दिया. ऐसा करके आपने न सिर्फ कॉपीराइट का उल्लंघन किया बल्कि ऑनलाइन ट्रेडमार्क के उल्लंघन मामले में आपको दोषी भी करार दिया जा सकता है.

17) **वाई-फाई का दुरुपयोग :** जुलाई, 2008 में अहमदाबाद बम विस्फोटों के बाद उनकी जिम्मेदारी लेते हुए आतंकवादियों ने जांच एजेंसी को ईमेल भेजा. जांच एजेंसियों ने पता लगाया कि यह ईमेल नवी मुंबई के एक फ्लैट में लगे वायरलेस इंटरनेट कनेक्शन के जरिये आया है. इस फ्लैट में मल्टिनैशनल कंपनी में काम करने वाला अमेरिकी नागरिक केनेथ हैवुड रहता था. दरअसल, हैवुड के वाई-फाई कनेक्शन में कोई सिक्युरिटी सेटिंग नहीं लगाई गई थी, जिसके कारण उसके

आस-पास से गुजरता कोई भी शख्स हैवुड के कनेक्शन का इस्तेमाल कर सकता था. आतंकवादियों ने यही किया और हैवुड आतंकियों से सांठ-गांठ के मामले में गिरफ्तार होते-होते बचा. अगर कोई अपराधी आपके इंटरनेट कनेक्शन का इस्तेमाल करते हुए साइबर अपराध करता है, तो पुलिस उसे भले ही न ढूंढ पाए, पर आप तक जरूर पहुंच जाएगी और इसके नतीजे आपको भुगतने होंगे.

18) **किसी का अकाउंट खोलना :** कुछ लोग अपने दोस्तों और साथियों के ईमेल अकाउंट, फेसबुक वगैरह का पासवर्ड ढूंढने की कोशिश करते हैं और कभी-कभी सफल भी हो जाते हैं. हो सकता है, आप महज मौज-मस्ती या मजाक के लिए ऐसा कर रहे हों, लेकिन अगर आप किसी का पासवर्ड हासिल करने के बाद उसके खाते में लॉग-इन करते हैं तो आप साइबर अपराध कर रहे हैं.

19) **गूगल क्लिक फ्रॉड :** इंटरनेट पर कई बार विज्ञापनों को क्लिक किए जाने की संख्या के आधार पर भुगतान की व्यवस्था होती है. जैसे दस क्लिक यानी दो डॉलर या करीब 150 रुपये. ऐसे में कुछ लोग खुद ही अपने ब्लॉगों पर लगे विज्ञापनों को क्लिक करते रहते हैं या फिर कुछ दूसरे लोगों के साथ गठजोड़ कर लेते हैं. शायद उन्हें पता नहीं कि इंटरनेट पर ऐसे फर्जी क्लिक की निगरानी रखी जा सकती है. यह एक बड़ा आर्थिक अपराध है और पता लगने पर आपका विज्ञापन तो बंद होगा ही साथ में भारी-भरकम जुर्माना या दूसरी सजा भी मिल सकती है.

20) **बैंडविड्थ की चोरी :** कुछ लोग अपनी वेबसाइट पर दूसरी जगहों से लिए गए भारी-भरकम ग्राफिक फाइलें डालने के लिए शॉर्टकट अपनाते हैं. वे फाइलों को अपनी वेबसाइट पर सीधे नहीं डालते बल्कि ऑरिजनल वेबसाइट से ही उन्हें लिंक कर देते हैं. होता यह है कि वीडियो या चित्र दिखता तो आपकी वेबसाइट पर है, लेकिन असल में वह अपनी ऑरिजनल वेबसाइट पर ही लगा रहता है. यहां आप दो तरह के साइबर अपराध कर रहे हैं. पहला कॉपीराइट संबंधी और दूसरा बैंडविड्थ की चोरी का. बैंडविड्थ की चोरी को ऐसे समझ सकते हैं. हर वेबसाइट को डाटा डाउनलोड का एक खास कोटा मिला होता है और इस सीमा से बाहर जाने पर उसके संचालक को अलग से पैसे का भुगतान करना होता है. जब आप किसी और की साइट पर मौजूद भारी-भरकम वीडियो को लिंक करके अपनी साइट पर देखते हैं तो आपकी साइट पर आने वाले हर विजिटर के लिए वह वीडियो ओरिजनल साइट से डाउनलोड होता है. डाउनलोड की इस प्रक्रिया में उसकी बैंडविड्थ खर्च होती है, जबकि आप अपनी बैंडविड्थ बचा लेते हैं. यह किसी अनजान व्यक्ति की जेब काटने जैसा है.

21) **साइबर स्क्वैटिंग :** किसी मशहूर ब्रैंड, कंपनी, संगठन, इंसान आदि के नाम से जुड़ा डोमेन नेम अनधिकृत रूप से अपने नाम से बुक करवा लेना भी साइबर अपराध है.

22) **ऑनलाइन मानहानि :** अपने ब्लॉग, वेबसाइट, सोशल नेटवर्किंग ठिकाने या दूसरे इंटरनेट ठिकाने पर किसी के बारे में अपमानजनक या अश्लील टिप्पणी करना साइबर अपराध है.

23) **वेबसाइट, डोमेन नेम पर कब्जा :** भारत में अनेकों वेब डेवलपमेंट कंपनियां ऐसा करने की दोषी पाई गई हैं. अपने ग्राहकों के लिए डोमेन नेम बुक कराते, वेब होस्टिंग स्पेस लेते और इंटरनेट सेवा मुहैया कराते समय वे उनका सबसे खास यूज़रनेम और पासवर्ड अपने कब्जे में रख लेते हैं और फिर उस के दम पर ग्राहकों को ब्लैकमेल करते हैं.

24) **डिज़ाइन की चोरी :** किसी वेबसाइट, ब्लॉग, ई-बुक आदि की बिना मंजूरी हूबहू नकल कर लेना, किसी की टेम्प्लेट को अनधिकृत रूप से इस्तेमाल करना भी साइबर अपराध है.

25) **साइबर जासूसी :** इसे एडवेयर या स्पाईवेयर भी कहा जाता है. यह आपके कंप्यूटर में कभी आपकी अनुमति से और कभी बिना अनुमति के स्थापित हो जाते हैं. यह आपकी व्यक्तिगत गतिविधियों की सूचना एकत्र कर अन्य को देते हैं.

26) **साइबर स्टॉकिंग :** किसी का पीछा करना, तंग करना, इस हद तक घूरना कि दूसरा व्यक्ति खीज जाये या डर जाय. यही काम जब इंटरनेट पर हो तो साइबर स्टॉकिंग कहलाता है.

कुछ और साइबर अपराध

इनके अतिरिक्त भारत की एकता, अखंडता, सुरक्षा या संप्रभुता को भंग करने या इसके निवासियों को आतंकित करने के लिए कोई व्यक्ति यदिः

*किसी अधिकृत व्यक्ति को कंप्यूटर के इस्तेमाल से रोकता है या रोकने का कारण बनता है,

*बिना अधिकार के या अपने अधिकार का अतिक्रमण कर जबरन किसी कंप्यूटर के इस्तेमाल की कोशिश करता है,

*कंप्यूटर में वायरस जैसी कोई ऐसी चीज डालता है या डालने की कोशिश करता है, जिससे लोगों की जान को खतरा पैदा होने की आशंका हो या संपत्ति के नुकसान का ख़तरा हो या जीवन के लिए आवश्यक सेवाओं में जानबूझ कर खलल डालने की कोशिश हो या धारा 70 के तहत संवेदनशील जानकारियों पर बुरा असर पड़ने की आशंका हो, या

*अनाधिकार या अधिकारों का अतिक्रमण करते हुए जानबूझ कर किसी कंप्यूटर से ऐसी सूचनाएं हासिल करने में कामयाब होता है जो देश की सुरक्षा या अन्य देशों के साथ उसके संबंधों के नज़रिए से संवेदनशील है या कोई भी गोपनीय सूचना इस इरादे के साथ हासिल करता है, जिससे भारत की सुरक्षा, एकता, अखंडता एवं संप्रभुता, सार्वजनिक जीवन या नैतिकता पर बुरा असर पड़ता हो या ऐसा होने की आशंका हो, देश की अदालतों की अवमानना अथवा मानहानि होती हो या ऐसा होने की आशंका हो, किसी अपराध को बढ़ावा मिलता हो या इसकी आशंका हो, किसी विदेशी राष्ट्र अथवा व्यक्तियों के समूह अथवा किसी अन्य को ऐसी सूचना से फायदा पहुंचता हो, तो उसे साइबर आतंकवाद का आरोपी माना जा सकता है.

साइबर अपराध किस तरह काम करता है?

आज साइबर अपराध के लिए साइबर अपराधी अनेकों टेक्निकल हमले करते हैं और हमेशा नए-नए तरीके खोजते रहते है, जैसेः

- यह सिस्टम और नेटवर्क को बंद करने के लिए डीडीओएस नामक तकनीक इस्तेमाल कर नेटवर्क प्रोटोकॉल पर हमला करते हैं. इस तरह के हमले ज़्यादातर वाइरस हमलों से सिस्टम को नुकसान पहुँचाने के लिए किये जाते हैं. यह हमले कई बार लोगों को किसी और मुश्किल में फँसाकर कुछ और अपराध करने के लिए भी किये जाते हैं.
- सिस्टम और नेटवर्क को मालवेएर की मदद से संक्रमित कर सिस्टम को खराब कर देना या सिस्टम में रखे सॉफ्टवेयर या डाटा को खराब कर देना.
- फिशिंग कैम्पेन में फर्जी मेल द्वारा लोगों को बेवकूफ बनाया जाता है जिससे कि वे दिये गए एटेचमेंट को डाउनलोड करें और या फिर दी गयी लिंक पर क्लिक करें जिससे सिस्टम में वाइरस फैल जाए और उस सिस्टम से वह वाइरस उनकी कंपनी के नेटवर्क में तक पहुंच जाए.
- कई बार क्रेडेंशियल हमला भी किया जाता है, जिसमें उपयोगकर्ता के निजी अकाउंट के आईडी और पासवर्ड जान लिए जाते हैं और फिर उसका सारा पैसा अपराधी अपने अकाउंट में डाल लेता है. कई बार कुछ सॉफ्टवेयरों की भी मदद ली जाती है, जिससे किसी व्यक्ति का निजी अकाउंट हैक कर उसकी सारी पूंजी हड़प ली जाती है.

साइबर अपराध का प्रभाव

किसी कंपनी या बैंक के डाटा को चुरा लेने से न केवल वितीय (आर्थिक) नुकसान हो

सकता है बल्कि साथ ही उस कंपनी या बैंक के प्रति ग्राहक का विश्वास भी समाप्त हो जाता है. ग्राहक के संवेदनशील डाटा के नुकसान के परिणामस्वरूप उन कंपनियों को दंड और जुर्माना भी हो सकता है, जो अपने ग्राहकों के डाटा की सुरक्षा में विफल रहे हैं. डाटा उल्लंघन पर मुकदमा भी चलाया जा सकता है.

स्मार्ट बनें व इस मकड़जाल से बचें:

आज सबसे बड़ी चिंता यह है कि नई तकनीक आधारित उत्पादों और सेवाओं को आम तौर पर जल्दबाज़ी में आरंभ किया जाता है. ऐसे में केवल उत्पादों व सेवाओं की कार्यप्रणाली पर गौर किया जाता है और उसकी सुरक्षा कमजोरियों पर विचार नहीं हो पाता है. आज निर्माता शायद ही 3 डी प्रिंटर, खिलौने, गेम्स, ड्रोन्स, रोबोट या किसी अन्य इंटरनेट से जुड़े उपकरणों के तेजी से बढ़ते इंटरनेट की चीज़ों (Internet of thingh) से संबंधित साइबर अपराध के अवसरों पर ध्यान देते हैं. साइबर विशेषज्ञ बताते हैं कि पिछले दिनों साइबर अपराधियों द्वारा बेहद आक्रामक मैलवेयर उपकरण "कारबैनक" का प्रयोग किया गया, जो चिंतित करता है. इस प्रकार के साइबर हथियार पहले वित्तीय संस्थानों को लक्षित कर प्रयोग होते थे, परंतु अब इसे व्यापक रूप से इस्तेमाल किया जा रहा है. मैलवेयर और अधिक परिष्कृत हो रहा है. आज वित्तीय संस्थानों के बीच और अधिक समावेशी सहयोग की जरूरत है ताकि साइबर आपराधिक संगठनों का एकजुट होकर सामना किया जा सके.

भारत में साइबर अपराध के वर्तमान रुझान

साइबर अपराध के मामले में, ऑनलाइन खर्च किए जाने वाले समय के अनुरूप बड़ी संख्या में अपराध की संभावनाएं बढ़ रही हैं. ऑनलाइन सेवाओं जैसे बैंकिंग, खरीदारी और फ़ाइल साझाकरण का उपयोग उपयोगकर्ताओं को फ़िशिंग हमलों या धोखाधड़ी के लिए प्रोन बनाता है. भारत में रिपोर्ट किए गए प्रमुख साइबर अपराध जैसे वेब सेवाओं एवं वेबसाइटों की हैकिंग, कंप्यूटर वायरस और वोर्म्स, पोर्नोग्राफी, साइबर स्क्वाटिंग, साइबर स्टॉकिंग, कार्ड क्लोनिंग और फ़िशिंग हैं, जिनका उल्लेख विस्तार से ऊपर किया जा चुका है. वर्तमान और पूर्व कर्मचारियों द्वारा लगभग 69 प्रतिशत सूचना चोरी की जाती है और हैकर्स द्वारा 31 प्रतिशत. 29 अप्रैल, 2013 को सिमेंटेक (अमेरिकी ग्लोबल कंप्यूटर सिक्योरिटी सॉफ्टवेयर कॉरपोरेशन) इंटरनेट सुरक्षा खतरे की रिपोर्ट (वॉल्यूम 18) के अनुसार, भारत ने बॉट संक्रमण में 280 प्रतिशत की वृद्धि पायी गयी है. लगभग 280 मिलियन प्रति दिन स्पैम या जंक मेल की दुनिया में भारत का उच्चतम अनुपात है. भारत के घरेलू पीसी मालिक साइबर हमलों के लिए सबसे लक्षित क्षेत्र हैं एवं मुंबई और दिल्ली साइबर अपराध के लिए शीर्ष दो शहरों के रूप में उभर रहे हैं.

साइबर अपराध की रोकथाम के लिए सर्वोत्तम अभ्यास के लिए निम्नलिखित सुरक्षा दिशानिर्देशों और अच्छे प्रथाओं का पालन किया जा सकता हैः

- **कंप्यूटर अपडेट करके :** साइबर हमलों से बचने के लिए, नियमित रूप से कंप्यूटर और ऑपरेटिंग सिस्टम के एंटीवायरस को अपडेट करें. वैसे तो कंप्यूटर को अद्यतित रखने से उपयोगकर्ता को सभी हमलों से सुरक्षित नहीं किया जा सकता परंतु यह हैकर्स को कंप्यूटर तक पहुंचने के मार्ग को कठिन अवश्य बनाता है.

- **मजबूत पासवर्ड चुनकर :** पासवर्ड इंटरनेट की ऑनलाइन चाभी है. पासवर्ड का चयन करने में कम से कम आठ अक्षरों, संख्याओं और प्रतीकों के संयोजन का उपयोग करें उदाहरण के लिए (# $ % ! ? आदि). नाम, शहर के नाम आदि का प्रयोग न करें. पासवर्ड को सुरक्षित स्थान पर रखें और प्रत्येक ऑनलाइन साइट या एप्लिकेशन के लिए समान पासवर्ड का उपयोग न करें. पासवर्ड को नियमित रूप से कम से कम हर 90 दिनों में बदलें.

- **सुरक्षा सॉफ़्टवेयर के साथ कंप्यूटर की सुरक्षा करके :** सुरक्षा सॉफ़्टवेयर में आमतौर पर फ़ायरवॉल और एंटीवायरस प्रोग्राम शामिल होते हैं. फ़ायरवॉल नियंत्रित करता है कि कौन कंप्यूटर और कंप्यूटर के साथ ऑनलाइन संचार कर सकता है. एंटीवायरस सॉफ़्टवेयर सभी ऑनलाइन गतिविधियों पर नज़र रखता है और कंप्यूटर को वायरस, वोर्म्स, ट्रोजन हॉर्स और अन्य प्रकार के दुर्भावनापूर्ण प्रोग्राम से बचाता है. एंटीवायरस और एंटीस्पायवेयर सॉफ़्टवेयर को स्वयं अपडेट करने के लिए कनफ़िगर किया जाना चाहिए और इसे हर बार इंटरनेट से कनेक्ट करना चाहिए.

- **व्यक्तिगत जानकारी सुरक्षित रूप से ऑनलाइन :** फ़िशिंग संदेश अक्सर यह बताएंगे कि खाता खोलने, सुरक्षा अपडेट करने या जल्दी से कोई कार्य करने के लिए लिंक पर क्लिक करें. उन्हें जवाब मत दें. व्यक्तिगत जानकारी मांगने वाले ईमेल संदेशों का जवाब न दें. किसी वेबसाइट पर जाकर, ईमेल या तत्काल के भीतर किसी लिंक का पालन करने के बजाय सीधे URL पर URL टाइप करें. ऑनलाइन ऑफ़र जो बहुत अच्छे लगते हैं, जैसे - मुफ्त सॉफ्टवेयर या सेवा के लिए पूछने वाले आपके व्यवहार को ट्रैक करते हैं और अवांछित विज्ञापन प्रदर्शित करते हैं. मुफ्त में गाने या सॉफ्टवेर डाउनलोड करते समय सावधान रहें. नियमित रूप से बैंक और क्रेडिट कार्ड विवरणों की समीक्षा करें. नियमित रूप से बैंक और क्रेडिट कार्ड की जांच करें.

- **सोशल-मीडिया सुरक्षित हो :** सुनिश्चित करें कि सोशल नेटवर्किंग प्रोफाइल (जैसे फेसबुक, ट्विटर इत्यादि) पर मौजूद जानकारी Privacy - Private setting पर सेट है. इसमें भी सावधानी बरतने की जरूरत है कि कौन सी जानकारी ऑनलाइन जरूरी है, अतः कम से कम जानकारी पोस्ट करें.
- **सुरक्षित वायरलेस नेटवर्क :** घर पर वाई-फाई (वायरलेस) नेटवर्क यदि ठीक से मजबूत पासवर्ड द्वारा सुरक्षित नहीं किये गये हैं तो ये घुसपैठ के लिए आसान हैं. डिफ़ॉल्ट सेटिंग्स की समीक्षा करें और संशोधित करें. सार्वजनिक वाईफाई स्पॉट का उपयोग करने से बचें.

साइबर अपराध एक ऐसा क्षेत्र है, जहाँ अनुभवी पेशेवरों की कमी है जिसका फायदा साइबर अपराधी उठा रहे हैं. भारत में पुलिस तंत्र में भी बाह्य पेशेवरों को बुला कर तंत्र को ट्रेनिंग देने की आवश्यकता है. आलम तो ये है कि सरकारी वेबसाइट भी हैक कर ली जा रही है एवं अपराधी अपने आप को छुपा ले जाते हैं. हाल में ही अपराधियों ने तो पुलिस के सीयूजी मोबाइल पर ही वीओआईपी कॉल करके धमकियां देना प्रारम्भ कर दिया है. अतः आज जरूरत है कि जानकार लोग अपराध की रोकथाम के लिए पुलिस तंत्र को फीडबैक दें ताकि पुलिस तंत्र उन फीड बैक के आधार पर समाज को इस रहस्यमयी दुनिया के अपराधों से सुरक्षित बनाए.

हमें स्मरण रखना चाहिए कि साइबरस्पेस हमारी एक साझा विरासत है, जिसे हमने बढ़ती प्रौद्योगिकी के लाभ के द्वारा अपने जीवन काल में पाया है. गुरुदेव रवींद्र नाथ टैगोर के सुप्रसिध्द शब्दों की आज के संदर्भ में पुर्नरचना कर हम कह सकते हैं कि "जहाँ साइबरस्पेस भय या अपराध से मुक्त है और सिर ऊँचा रखा जाता है, जहां ज्ञान निःशुल्क प्राप्त है, जहां अथक प्रयास विस्तृत पूर्णता के लिये भुजाएँ फैला कर खड़ा है,..... स्वतंत्रता के साइबर स्वर्ग में, हे मेरे पिता, हमारी मानवता जागृत हो."

एथिकल हैकिंग - सुरक्षा उपायों के लिए बढ़ती चुनौती

गौरव बिष्ट
प्रबंधक
सीसो कार्यालय, के. का. मुंबई

शंकर रूपानी
मुख्य प्रबंधक
सीसो कार्यालय, के. का. मुंबई

इंटरनेट और नेटवर्किंग क्षमताओं पर हमारी बढ़ती निर्भरता का विशेष महत्व है. इंटरनेट ने उन क्षेत्रों की विस्तृत श्रृंखला में असीमित अवसर प्रदान किए हैं, जो विगत में असंभव थे. इंटरनेट के माध्यम से ही आज हम विश्व में उपलब्ध सूचनाओं के विशाल भंडार तक पहुंचने में सक्षम हैं.

इंटरनेट और नेटवर्किंग में क्षमताओं के सकारात्मक पहलुओं के साथ कुछ अप्रिय पहलू भी मौजूद हैं. कई वर्षों से विभिन्न प्रकार के अपराध होते आ रहे हैं, इंटरनेट और सूचना प्रौद्योगिकी ने अपराध को आपके घरों और व्यवसायों में, अकल्पनीय तरीकों से पहुंचाया है. आज के अपराधियों के पास गतिविधियों का संचालन करने के लिए एक नया मंच है. दुनिया क्लाउड की तरफ बढ़ रही है, जहां वर्च्युलाइजेशन और आईटी आउटसोर्सिंग का प्रमुख स्थान है. इस संक्रमण ने जिस प्रकार से खतरों के स्तर में वृद्धि की है, उसी प्रकार एथिकल हैकर्स की मांग में भी वृद्धि हुई है. क्लाउड कंप्यूटिंग के आगमन के बाद से सुरक्षा एक प्रमुख चिंता बन गयी है. सुरक्षा को नुकसान पहुंचाए बिना क्लाउड और वर्च्युलाइजेशन के उपयोगों का लाभ उठाने के लिए, कंपनियों को एथिकल हैकर्स की सेवाओं का उपयोग करना पड़ेगा. चूंकि आजकल सभी जानकारी ऑनलाइन उपलब्ध है, बड़ी संख्या में उपयोगकर्ता इसका उपयोग कर रहे हैं, उनमें से कुछ ज्ञान प्राप्त करने के लिए इस जानकारी का उपयोग करते हैं और कुछ इसका उपयोग यह जानने के लिए करते हैं कि वेबसाइटों या डाटाबेस के डाटा को कैसे नुकसान पहुंचाया जा सकता है.

सिस्टम या कंप्यूटर नेटवर्क में कमजोरियों को एथिकल तरीके से जानने का तरीका एथिकल हैकिंग कहलाता है. यह किसी भी नेटवर्क के एथिकल यानि कि नैतिक तरीके से हैकिंग की प्रक्रिया का वर्णन करने का एक तरीका है. असल में हैकर के लिए हमारे दिमाग में सामान्य धारणा बन गई है कि वह बुरा, आपराधिक और अनैतिक होगा. असल में कुछ हैकर्स ने कुछ संगठनों को बहुत बुरी तरह से क्षति पहुंचायी है जैसे कि उन्होंने किन्हीं संगठनों के ग्राहकों की बहुत महत्वपूर्ण जानकारी चुरा ली या फिर कुछ सरकारी संगठनों की सामाजिक सुरक्षा संख्या (सोशल सेक्युरिटी नंबर) और अन्य संवेदनशील एवं गोपनीय जानकारियां चुराकर बहुत नुकसान पहुंचाया. यही वजह है कि हैकरों की छवि कुछ अच्छी नहीं है. ऐसी स्थितियों से बचने के लिए कई संगठनों ने अपने सिस्टम और कंप्यूटर नेटवर्क पर ट्रैक रखने के लिए कई एथिकल हैकरों को काम पर लगा रखा है. एथिकल हैकर्स वर्तमान प्रणाली में कमजोरियों को दूर करने के लिए काम करते हैं.

एथिकल अथवा "नैतिक हैकिंग" शब्द हमेशा से विवादास्पद रहा है. बहुत से लोग इस शब्द के अस्तित्व पर सवाल करते हैं क्योंकि दो शब्द 'नैतिक' और 'हैकिंग' स्वयं विरोधाभासी हैं. हैकिंग एक अनधिकृत घुसपैठ है, जो एक नकारात्मक अर्थ है और ऐसा करने के लिए इसे कभी नैतिक नहीं माना जाता है, इसलिए इस शब्द पर हमेशा चर्चा होती रहती है. नैतिक हैकिंग को प्रवेश परीक्षण, घुसपैठ परीक्षण या 'रेड टीमिंग' के रूप में भी जाना जाता है लेकिन यह केवल प्रवेश परीक्षण तक ही सीमित नहीं है. यदि हैकिंग आक्रामक है तो नैतिक हैकिंग रक्षात्मक.

एथिकल हैकिंग वह शब्द है, जिसका प्रयोग पेशेवरों द्वारा सिस्टम को अधिक सुरक्षित बनाने के लिए किया जाता है. एक व्यक्ति को एथिकल हैकर के रूप में बुलाया जाएगा, जो सिस्टम की सुरक्षा को नष्ट नहीं करेगा बल्कि वह हैकर के दृष्टिकोण से सिस्टम की सुरक्षा का ख्याल रखेगा. वह व्यक्ति, जो इन सभी प्रयासों को कर रहा है, उसे एथिकल हैकर या व्हाइट हैट हैकर के रूप में जाना जाता है. जहां तक सूचना प्रौद्योगिकी का संबंध है, एथिकल हैकिंग में हमें सिस्टम की सुरक्षा सुनिश्चित करनी होती है.

सर्वर और आईपी श्रेणियों के बारे में जानकारी एकत्र करना सफल हैकिंग का पहला कदम है. पेनिट्रेशन टेस्टिंग, हैकर्स को नेटवर्क और उसकी कमजोरियों का

अवलोकन करने हेतु सक्षम बनाती है. हैकिंग का सबसे महत्वपूर्ण हिस्सा, हैकिंग करने के बाद कोई निशान न छोड़ना है. अगर एथिकल हैकिंग सही तरीके से नहीं की जाती है, तो हमलावर एथिकल हैकर द्वारा पहले से संग्रहीत जानकारी प्राप्त कर सकता है. इन विधियों का उपयोग हैकर्स और क्रैकर्स दोनों द्वारा किया जाता है, अंतर केवल उनके इरादे में ही होता है. क्रैकर्स संवेदनशील जानकारी तक पहुंचने के लिए काम करते हैं, जबकि एथिकल हैकर्स नेटवर्क में त्रुटियों को सुधारने और इसकी सुरक्षा में सुधार करने के लिए हैकिंग करते हैं.

एथिकल हैकर कर्मचारियों से संबंधित सभी जानकारी और व्यक्तिगत डाटा चुरा सकता है. वह गलत डाटा भी बना सकता है. एथिकल हैकर कंपनी में आईटी में सुरक्षा व्यक्ति के रूप में है, लेकिन हम कभी नहीं जान पाएंगे कि वह वास्तव में क्या कर सकता है. वह वायरस कोड लिख सकता है या वायरस कोड को कंपनी के सर्वर में प्रवेश करने की इजाजत दे सकता है. कभी-कभी एथिकल हैकर्स को कुछ वायरस के तथ्य और प्रभाव का एहसास नहीं हो पाता. एथिकल हैकर को कंपनी का अंदरूनी कर्मचारी होने के नाते कंपनी के सभी गोपनीय डाटा तक पहुंचने के सभी अधिकार प्राप्त हैं. यह वास्तव में एथिकल हैकर्स के असली इरादों पर निर्भर करता है कि वे अपनी नौकरी किस उद्देश्य से करते हैं.

बैंक उनके प्रमुख लक्ष्य हैं, इसलिए वे हमेशा गंभीर साइबर खतरों के तहत रहते हैं. बैंकों के अलावा, अन्य संगठन, मध्यम या बड़े साइबर हमलों के अधीन रहते हैं. पिछले साल एडोब सिस्टम्स ने 2.9 मिलियन ग्राहकों के डाटा हैक का सामना किया था. सभी परिदृश्यों को ट्रैक करना एथिकल हैकर के लिए वास्तव में एक बड़ी समस्या है. एथिकल हैकर को किसी भी संगठन की प्रणाली में कमजोरियों की जांच करने के लिए एक सम्मानजनक नौकरी दी जाती है. कुछ दिनों के बाद कुछ जानकारी हैक की जाती है तो उस संगठन के लिए कौन जिम्मेदार है? सुरक्षा और अन्य मामलों में कमजोरियों की जांच के लिए एक एथिकल हैकर लिया जाता है. किसी सुरक्षा प्रक्रिया को डिजाइन करना या परीक्षण में शामिल होना, प्रक्रिया या आवेदन को पूरी तरह से समझना आवश्यक है. एथिकल हैकर देखता है कि अपराधियों द्वारा उपयोग की जाने वाली तकनीकों के साथ और कितनी जानकारी उपलब्ध है. इस तरह के परीक्षण सिस्टम को नियंत्रित करने वाले कानूनों और संविदात्मक दायित्वों का उल्लंघन कर सकते हैं. कानूनी और संविदात्मक जोखिमों की सराहना करते हुए, कई प्रबंधकों ने विकास परीक्षण के लिए लाइव डाटा के

उपयोग को प्रतिबंधित करना शुरू कर दिया है. एथिकल हैकिंग के दौरान लाइव डाटा के उपयोग को रोकना - तर्कसंगत रूप से सुरक्षा परीक्षण या एथिकल हैकिंग पर लागू होता है. नैतिक हैकर को लाइव वातावरण का परीक्षण करना चाहिए, जिसमें लाइव डाटा शामिल है.

कुछ हैकर्स तर्क देते हैं कि वे अपराधी नहीं हैं, बल्कि कार्यकर्ता हैं. अन्य लोग कहेंगे कि वे प्रौद्योगिकी के बारे में सोचने के तरीके में विद्रोही हैं.

विभिन्न प्रकार के हमले

1. ऑपरेटिंग सिस्टम अटैक
2. मिसकंफिगरेशन अटैक
3. एप्लीकेशन लेवल अटैक

- शुरुआत में सोशल नेटवर्किंग साइट ट्विटर ने एक हैकिंग दुर्घटना का सामना किया, जहां 55,000 से अधिक ट्विटर उपयोगकर्ताओं के नाम और पासवर्ड हैक किए गए थे.
- नवीनतम तरीकों में एक वायरलेस इंसुलिन पंप को हैक करना शामिल है, जिसके द्वारा मधुमेह शरीर में हार्मोन को बांटा जाता था.
- नकदी मशीनों में हैकिंग के उदाहरणों को सबसे अच्छी तरह से जाना जाता है. हाल ही में, एक रूसी आदमी पर केलिहोस बॉटनेट का संचालन करने का आरोप लगाया गया था, अंत में अमेरिकी संघीय अदालत में उसे दोषी ठहराया गया.
- सुरक्षा शोधकर्ताओं ने पासवर्ड, एन्क्रिप्शन कुंजी और अधिकांश आधुनिक कंप्यूटरों पर संग्रहीत अन्य संवेदनशील जानकारी चोरी करने के लिए एक नया हमला किया है, यहां तक कि पूर्ण डिस्क एन्क्रिप्शन को भी अपना शिकार बनाया है. यह हमला बूट अटैक का एक नया बदला हुआ रूप है, जो कंप्यूटर बंद होने के बाद रैम में संक्षेप में बनी रहती है.
- साइबर हमलों के खिलाफ अपनी कारों की ड्राइविंग सिस्टम की सुरक्षा के लिए उचित सुरक्षा उपायों के बावजूद, सुरक्षा शोधकर्ताओं की एक टीम ने दो सेकंड से भी कम समय में टेस्ला मॉडल एस लक्ज़री सेडान को हैक करने का एक तरीका खोजा.

- ब्रिटिश एयरवेज, जो खुद को विश्व की पसंदीदा एयरलाइन के रूप में बताती है, ने एक डाटा उल्लंघन की पुष्टि की है, जिसने 380,000 ग्राहकों के व्यक्तिगत विवरण और क्रेडिट कार्ड नंबरों का खुलासा किया.
- माइक्रोसॉफ्ट ने सितंबर 2018 में अपने नवीनतम मासिक पैच अपडेट को जारी किया, जिसमें कुल 61 सुरक्षा भेद्यताएं थीं, जिनमें से 17 को महत्वपूर्ण के रूप में रेट किया गया है.

हालांकि, इस तरह से प्रयास किया जाना चाहिए कि किस डाटा का खुलासा किया गया है, कौन सी तकनीकों को नियोजित किया जाएगा, लागू कानूनी दायित्वों की पहचान और परीक्षणों का संचालन कौन करेगा और परिणामों के साथ क्या किया जाएगा. पर्याप्त मात्रा में विश्लेषण और तैयारी के साथ, सूचना सुरक्षा कार्यक्रम के मिशन को संरक्षित करते समय, परीक्षण की प्रभावकारिता को किए बिना जोखिमों को संबोधित किया जा सकता है. सूचना सुरक्षा और कानूनी कार्य एक ऐसी प्रक्रिया बनाने के लिए मिलकर काम कर सकते हैं, जो संगठन के लिए सबसे प्रभावी है.

मानव मस्तिष्क बहुत शक्तिशाली उपकरण है और वास्तव में इस पर कोई नियंत्रण नहीं है. अच्छे या बुरे इरादे के बावजूद, हैकर सिस्टम को पाने के लिए हमेशा कुछ रास्ता तलाशते रहेंगे. भविष्य में हैकर्स और एथिकल हैकर्स के कार्यों को करने के तरीके अलग-अलग होंगे. उन्हें दिए गए कार्यों के अनुसार उन्हें अलग किया जाएगा. किसी भी एथिकल हैकर को हैकर के रूप में नहीं माना जाएगा.

सुरक्षा सॉफ्टवेयर कंपनी सिमेंटेक के मुताबिक भारत उन देशों में तीसरे स्थान पर आता है, जिन्हें साइबर अटैक के खतरों का सबसे अधिक सामना करना पड़ रहा है. लक्षित हमलों के मामले में भी भारत दूसरे स्थान पर रहा. इस को ध्यान में रखते हुए, मौजूदा कानूनी परिदृश्य में एथिकल हैकिंग की आवश्यकता और महत्व को अनदेखा करना सही नहीं होगा.

फिशिंग ई-मेल - सबसे खतरनाक साइबर खतरा

मिलिंद अलकरी
मुख्य प्रबंधक,
सीसो कार्यालय, के. का. मुंबई

फिशिंग का इतिहास

फिशिंग का पहली बार उपयोग 1990 के दशक में, अमेरिका में हैकर्स एवं पायरेटेड सॉफ्टवेयर उपयोग करने वाले लोगों ने अमेरिका ऑनलाइन (AOL) के कस्टमर्स का पासवर्ड, कार्ड नंबर, इत्यादि चुराने के लिए किया था, जिन्हें वारेज़ कम्युनिटी (Warez Community) के नाम से जाना जाता था. इस हेतु हैकर्स ने AOHell नामक सॉफ्टवेयर का उपयोग किया था. अमेरिका ऑन लाइन(AOL) उस वक़्त की अमेरिका की सबसे प्रमुख इंटरनेट सेवा प्रदान करने वाली कंपनी थी. इंटरनेट रिकॉर्ड के मुताबिक, "फिशिंग" शब्द का पहली बार इस्तेमाल **2 जनवरी, 1996** को AOHell सॉफ्टवेयर में किया गया था.

फिशिंग शब्द की वर्तनी (स्पेलिंग) में "**एफ**" के स्थान पर "**पीएच**" के उपयोग का एक कारण है. शुरुआती हैकर्स में से कुछ को फ्रेक्स (Phreaks) के रूप में जाना जाता था. प्रेकिंग (Phreaking) दूरसंचार प्रणालियों में हैकिंग की कार्रवाई, खासकर मुफ्त कॉल प्राप्त करने के लिए एवं दूरसंचार प्रणालियों की खोज, प्रयोग और अध्ययन को संदर्भित करता है. Phreaks और Hackers हमेशा निकटता से जुड़े रहे. इन भूमिगत समुदायों के साथ फ़िशिंग घोटालों को जोड़ने के लिए "**पीएच**" **(Ph)** वर्तनी का उपयोग किया गया था एवं इस प्रकार फिशिंग (Phishing) शब्द अस्तित्व में आया.

फिशिंग क्या हैं ?

जिस प्रकार मछली पकडने के लिये कॉटे में चारा लगाकर पानी में डाला जाता है और चारा खाने के लालच या धोखे में आकर मछली कॉटें में फंस जाती है, ठीक उसी प्रकार फिशिंग भी हैकर्स (Hackers) द्वारा इन्टरनेट पर नकली वेबसाइट (Fake Website) या ई-मेल (E-mail) के माध्यम से इन्टरनेट यूजर्स के साथ की गयी धोखेबाजी

(Scams) को कहते हैं, जिसमें वह आपकी निजी जानकारी (Personal Information) को धोखेबाजी(scams)से चुरा लेते हैं और फिर उसका गलत उपयोग करते हैं.

फ़िशिंग के माध्यम से हैकर्स (Hackers) आपको नकली ई-मेल या संदेश भेजते हैं, जो किसी प्रतिष्ठित कम्पनी, आपके बैंक, आपकी क्रेडिट कार्ड कम्पनी, ऑनलाइन शॉपिंग की तरह मिलते-जुलते होते हैं और उनके द्वारा प्रेषित किये गए ही प्रतीत होते हैं. अगर आप सतर्क नहीं हैं तो आप इनके झॉसे में आ सकते हैं. इन नकली ईमेल (Fake e-mail) या संदेश का उद्देश्य, आपकी PII यानी पर्सनल आइडेंटिफाइएबल इन्फ़ॉर्मेशन (Personal Identifiable Information) को चुराना अथवा आपके कम्प्यूटर पर मेलिसियस मैलवेयर स्थापित करना होता है. PII के अन्तर्गत आपकी निम्नलिखित निजी जानकारियॉ आती है जैसे -

1. आपका नाम
2. आपकी ई-मेल यूज़र आई.डी.
3. आपका पासवर्ड
4. आपका मोबाइल नम्बर या फोन नम्बर
5. आपका पता
6. आपका बैंक खाता नम्बर
7. आपका एटीएम कार्ड, डेबिट कार्ड तथा क्रेडिट कार्ड नम्बर
8. आपका एटीएम कार्ड, डेबिट कार्ड तथा क्रेडिट कार्ड आदि का वेलिडेशन कोड
9. आपकी जन्मतिथि
10. आपका आधार नंबर, पैन नंबर, इत्यादि

फिशिंग टेक्निक अब हैकर्स का अत्यधिक लोकप्रिय शस्त्र बन गया है क्योंकि इसके द्वारा वे कम्प्यूटर्स/नेटवर्क सिस्टम की प्रबल सुरक्षा को तोड़ने की जटिल प्रक्रिया में उलझने के बजाय, आसानी से टार्गेटेड कर्मचारियों (end users) के कंप्यूटर तक पहुंच सकते हैं, जहाँ से उनके द्वारा आसानी से संगठनों पर साइबर अटैक किया जा सकता है.

आज के समय में फ़िशिंग एक प्रमुख चिंता का विषय बन गया है. यह न केवल इसलिए कि फ़िशिंग घटनाओं की संख्या बड़ी मात्रा में बढ़ रही है, बल्कि इसलिए भी कि अब हमलों के तरीके अत्यधिक परिष्कृत (sophisticated) हो रहे हैं, जिससे ई-मेल प्राप्तकर्ता को इन्हें पहचानना और अधिक कठिन हो गया है.

निम्नलिखित कुछ नवीनतम आंकड़े फिशिंग ई-मेल के खतरों की सीमा और कौन सी रणनीति हमलावरों में सबसे लोकप्रिय है, दर्शाते हैंः

1. वर्ष 2017 में दुनिया के 76% संगठनों ने फिशिंग हमलों का अनुभव किया था.
2. वर्ष 2017 के अंत तक, प्रत्येक ई-मेल रेसिपिएंट को हैकर्स द्वारा प्रति माह औसतन 16 फिशिंग ई-मेल प्रेषित किये गए थे.
3. ई-मेल अभी भी मैलवेयर डिलीवरी के लिए हैकर्स का नं 1 पसंदीदा साधन है. हैकर्स द्वारा 92.4 % मेलिसियस मैलवेयर की डिलीवरी फिशिंग ई-मेल के द्वारा ही की गई.
4. वर्ष 2015 में दुनिया की एक प्रमुख एंटी वायरस कंपनी मैकेफी (Mcafee) ने एक सर्वेक्षण में पाया कि 97% उपभोक्ता फ़िशिंग ईमेल की सही पहचान करने में असमर्थ थे.
5. आजकल फिशिंग ई-मेल के द्वारा मैलवेयर वितरित करने के लिए हैकेर्स नकली चालान के अटैचमेंट का सबसे ज्यादा उपयोग कर रहे हैं.

फिशिंग के कुछ प्रमुख प्रकार निम्नानुसार हैं : -

1. स्पीयर फिशिंग (Spear Phishing)

यह फिशिंग तकनीक हैकर्स में काफी लोकप्रिय है. लगभग 90 प्रतिशत हमले इस तकनीक के द्वारा ही किये जाते हैं. इसमें हेकर्स द्वारा पहले पूर्व निर्धारित कंपनी या व्यक्तियों की व्यक्तिगत जानकारियों/सूचनाओं को एकत्र किया जाता है एवं तत्पश्चात् संगठन के कई कर्मचारियों (employees) को एक साथ फिशिंग ई-मेल प्रेषित किया जाता है.

2. व्हेल फिशिंग (Whale Phishing)

Whaling attacks/Phishing एक प्रकार के स्पीयर फिशिंग अटैक होते हैं, जिसमें विशेष रूप से बड़ी रकम चोरी करने के उद्देश्य से किसी संगठन (Organisation) के वरिष्ठ अधिकारियों को टार्गेट किया जाता है. ई-मेल में मैसेजेस अधिक रियल लगने के लिए, इस प्रकार के फिशिंग ई-मेल में टार्गेट/विक्टिम के बारे में डिटेल इनफॉर्मेशन होती है. टार्गेट से संबंधित विशिष्ट जानकारी का उपयोग करने से हमला सफल होने की संभावना बढ़ जाती है.

3. क्लोन फिशिंग (Clone Phishing)

क्लोन फ़िशिंग एक प्रकार का फ़िशिंग हमला है, जिसके द्वारा पूर्व में वितरित एक वैध ई-मेल, जिसमें एक अनुलग्नक (attachment) अथवा लिंक होता है, उसे मेल प्राप्तकर्ता (mail recipient) के उसी पते (address) पर लगभग एकसमान (identical) या क्लोन ईमेल बनाकर पुनः प्रेषित करने के लिए उपयोग किया जाता है. ईमेल के अंदर अनुलग्नक (attachment) अथवा लिंक को एक मेलिसियस अनुलग्नक अथवा लिंक से बदल दिया जाता है. क्लोन ई-मेल मूल प्रेषक के ईमेल पते से भेजा गया ही प्रतीत होता है एवं इस प्रकार मेल प्राप्तकर्ता को धोखा दिया जाता है. यह तकनीक पहले से संक्रमित मशीन या ईमेल धारक, जिस पर साइबर अपराधियों ने पहले से हमला किया है, के ई-मेल खाते के द्वारा की जाती है.

4. फार्मिंग फिशिंग (Pharming Attack)

Pharming Attacks एक प्रकार का फ़िशिंग है जो DNS कैश पोइज़निंग पर निर्भर करता है ताकि यूजर्स को किसी वैध साइट से एक जाली (Fraud) वेबसाइट पर अनुप्रेषित (Redirect) किया जा सके और इस फ्रॉड साइट पर लॉग-इन करने का प्रयास करने पर उनके लॉगिन क्रेडेंशियल्स की चोरी की जा सके.

5. एसएमएस फिशिंग (SMS Phishing) :

एसएमएस फिशिंग के द्वारा पीडितों को बैंक अकाउंट क्रेडेंशियल्स का खुलासा करने अथवा मैलवेयर इंस्टॉल करने के लिए, हेकर द्वारा टेक्स्ट मैसेजिंग (Text Message) का उपयोग किया जाता है.

फ़िशिंग कैसे कार्य करता हैः

- फ़िशिंग के द्वारा ग्राहकों की व्यक्तिगत पहचान संबंधी डाटा एवं खातों संबंधी वित्तीय जानकारियां चुराने के लिए सोशल इंजीनियरिंग और तकनीकी छल दोनों का प्रयोग किया जाता है.
- ग्राहक को एक फर्जी ई-मेल प्रेषित किया जाता है, जिसमें सेन्डर का ई-मेल एड्रेस सही/वैध प्रतीत होता है.
- ई-मेल के द्वारा ग्राहक/टारगेट को एक अटैचमेंट डाउनलोड करने के लिए कहा जाता है, जिसके माध्यम से हैकर द्वारा उसके कंप्यूटर पर मेलिसियस मैलवेयर डाउनलोड किया जा सके अथवा, ई-मेल के द्वारा ग्राहक/इ-मेल प्राप्तकर्ता को प्रेषित एक हाइपरलिंक पर क्लिक करने के लिए कहा जाता है.

- हाइपर लिंक पर क्लिक करते ही वह ग्राहक को एक फर्जी वेब साइट (Fraud Website) पर ले जाता है, जो वास्तविक साइट के समान दिखती है.
- प्रायः ऐसी ई-मेल बताये गये निर्देशों की अनुपालन करने पर इनाम देने का वादा भी करती है अथवा न मानने पर किसी प्रकार की पेनाल्टी लगाने की चेतावनी भी देती है.
- ग्राहक को अपनी व्यक्तिगत जानकारी जैसे कि पासवर्ड, क्रेडिट कार्ड और बैंक खाता संख्या आदि को अद्यतन करने के लिए कहा जाता है.
- ग्राहक विश्वास में आकर अपनी व्यक्तिगत जानकारियां दे देता है और ''सबमिट'' बटन पर क्लिक करता है, जो सीधे हैकर के कमांड एंड कण्ट्रोल कंप्यूटर (C&C) पर सुरक्षित (save) हो जाती है, जिसका हैकर बाद में गलत कार्य के लिए उपयोग करता है.
- Submit बटन पर क्लिक करने के पश्चात ग्राहक/ई-मेल प्राप्तकर्ता को error page दिखाई देता है. इस प्रकार ग्राहक/ई-मेल प्राप्तकर्ता फ़िशिंग का शिकार हो जाता है.

फिशिंग से सम्बंधित - क्या करें:

- हमेशा एड्रेस बार में सही यूआरएल (URL) टाइप कर साईट को लॉग-ऑन करें.
- अपना यूजर आईडी एवं पासवर्ड केवल अधिकृत लॉगिन (Login) पृष्ठ पर ही उपयोग करें.
- अपना यूजर आईडी एवं पासवर्ड प्रविष्ट करने से पूर्व कृपया सुनिश्चित कर लें कि Login Page का URL **'https://'** से प्रारम्भ हो रहा है, **'http://'** से नहीं होना चाहिए. यहां **'एस' (स)** से आशय है सुरक्षित (Secured) तथा यह दर्शाता है कि वेब पेज में एंक्रिप्शन (encryption) का प्रयोग हो रहा है.
- कृपया ब्राउसर एवं वेरीसाइन प्रमाण पत्र के दाईं ओर नीचे लॉक का चिन्ह भी अवश्य देखें.
- अपनी व्यक्तिगत जानकारी फोन या इंटरनेट पर केवल तभी दें जब कॉल या सैशन आपने प्रारम्भ किया हो अथवा सहकर्मी को आप पूरी तरह से जानते हों.

फिशिंग से सम्बंधित - क्या न करें:

- किसी अंजान स्तोत्र से प्राप्त ई-मेल में संलग्न लिंक पर क्लिक न करें. यह किसी हैकर द्वारा Melicious code या फिशिंग हमले का प्रयास हो सकता है.

- Pop-Up window के रूप में आए पेज पर किसी भी प्रकार की जानकारी प्रविष्ट न करें.
- कभी भी अपना पासवर्ड फोन पर अथवा ई-मेल पर न बताएं.
- हमेशा ध्यान रखिये कि आपके फाइनेंशियल क्रेडेंटियल्स जैसे पासवर्ड, पिन, ओटीपी, क्रेडिट कार्ड की जानकारी, आधार कार्ड नंबर, इत्यादि अत्यंत गोपनीय हैं एवं बैंक कभी भी ये जानकारी किसी भी प्रकार/माध्यम से नहीं मांगते हैं.

साइबर सुरक्षा जागरूकता प्रशिक्षण (Cyber Security Awareness Training) :

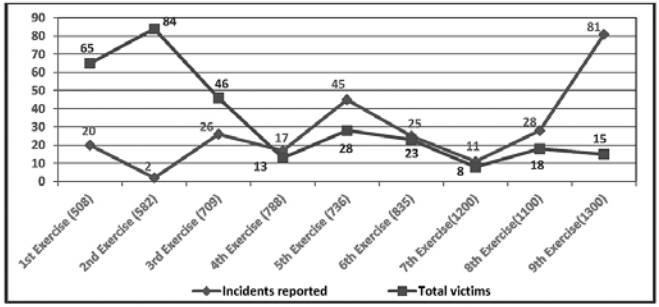
फिशिंग ई-मेल के घातक हमले से बचने के लिए और इन पर अंकुश लगाने के लिए किसी भी संगठन के लिए अपने कर्मचारियों को साइबर सुरक्षा जागरूकता प्रशिक्षण (Cyber Security Awareness Training) देना अत्यंत आवश्यक है. सभी संगठनों की साइबर सुरक्षा (Cyber Security) उनके अपने कर्मचारियों की साइबर सुरक्षा जागरूकता में निहित है एवं फिशिंग ई-मेल के हमले को पहचानने की उनकी क्षमता पर काफी हद तक निर्भर करती है. अपने कर्मचारियों को साइबर सुरक्षा जागरूकता प्रशिक्षण प्रदान करना संगठन को साइबर हमलों से सुरक्षा प्रदान करने में एक महत्वपूर्ण कड़ी साबित हो सकता है.

नकली फिशिंग ई-मेल का अभ्यास (Phishing E-mail Simulation Exercise) :

इसी तथ्य को ध्यान में रखते हुए, यूनियन बैंक ऑफ़ इंडिया के मुख्य सूचना सुरक्षा अधिकारी, (Chief Information Security Officer, CISO) ऑफिस द्वारा हमारे बैंक के समस्त कर्मचारियों एवं अधिकारियों के लिए साइबर सुरक्षा जागरूकता हेतु लगातार विभिन्न स्तर पर प्रशिक्षण दिए जा रहे हैं. उसमें भी, खास तौर पर, बैंक के कर्मचारियों द्वारा फिशिंग ई-मेल की पहचान आसानी से की जा सके, इसके लिए प्रति माह फिशिंग ई-मेल सिमुलेशन एक्सरसाइज (Phishing E-mail Simulation Exercise) की जाती है. प्रत्येक सिमुलेशन एक्सरसाइज के दौरान, बैंक के करीब 1000 कर्मचारियों/अधिकारियों को उनके बैंक के कार्यालयीन (official) ई-मेल पते पर फिशिंग ई-मेल प्रेषित किये जाते हैं एवं इस पर उनके द्वारा लिए गए एक्शन का अध्ययन कर तदनुसार उन्हें सूचित/आगाह किया जाता है.

वर्ष 2017-18 के दौरान CISO ऑफिस द्वारा अब तक 9 फिशिंग एक्सरसाइज सम्पादित की जा चुकी है एवं करीब 8000 स्टाफ को सिमुलेटेड फिशिंग इ-मेल प्रेषित किये जा चुके हैं. अब तक किये गए फिशिंग इ-मेल अभ्यास से सम्बंधित संक्षिप्त जानकारी निम्नानुसार ग्राफ में दर्शाई गई है :--

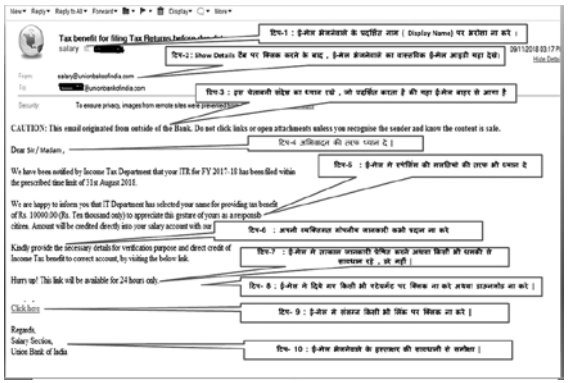
फिशिंग एक्सरसाइज़ परिणाम



- **रिपोर्ट किए गए मामले (Incidents reported) :** वे स्टाफ, जिन्होंने फिशिंग ई-मेल को सफलतापूर्वक पहचान लिया एवं CISO कार्यालय को सूचित किया
- **कुल प्रभावित स्टाफ (total victims) :** वे स्टाफ, जो फिशिंग ई-मेल अभ्यास के शिकार हुए.

फिशिंग ई-मेल को पहचानने के कुछ महत्वपूर्ण टिप्स : -

सभी स्टाफ सदस्यों के अवलोकनार्थ, माह सितम्बर 2018 में आयोजित 9th फिशिंग एक्सरसाइज के दौरान कुछ रैनडमली (randomly) चुने हुए कर्मचारियों को भेजे गए फिशिंग ई-मेल की प्रति निम्न चित्र में दर्शाई गई है एवं इस फिशिंग ई-मेल को पहचानने के टिप्स भी निम्न चित्र में दर्शाये गए हैं :



टिप 1 एवं 2 : ई-मेल भेजने वाले के प्रदर्शित नाम (Display name) पर भरोसा न करे. भेजने वाले का वास्तविक ईमेल एड्रेस जानने के लिए, ईमेल-शो डिटेल्स टैब (Show Details Tab) पर क्लिक करें, जो ईमेल पेज के टॉप राइट हैंड कार्नर पर होता है.

टिप 3 : उपरोक्त चेतावनी संदेश का ध्यान रखें, जो यह प्रदर्शित करता है कि उक्त ई-मेल यूनियन बैंक के बाहर से आया है. अतः यदि आप प्रेषक को नहीं जानते हैं एवं मेल की वैधता सुनिश्चित नहीं कर पाते हैं, तो इस स्थिति में मेल के साथ संलग्न किसी भी लिंक अथवा अटैचमेंट को क्लिक अथवा डाउनलोड न करें.

टिप 4 : अभिवादन की तरफ ध्यान दें. साधारणतया वैध व्यावसायिक संदेशों में अक्सर आपके पहले और अंतिम नाम के साथ व्यक्तिगत अभिवादन का उपयोग किया जाता है.

टिप 5 : ई-मेल में स्पेलिंग (Spelling) की गलतियों की तरफ ध्यान दें. साधारणतया फिशिंग ईमेल में स्पेलिंग की गलतियां पायी जाती हैं.

टिप 6 : बैंक और अधिकतर कंपनियां कभी भी ईमेल के माध्यम से व्यक्तिगत जानकारी नहीं माँगते. अपनी व्यक्तिगत जानकारी कभी भी न दें.

टिप 7 : फिशिंग ई-मेल में तत्काल जानकारी देने के लिए डराने वाली या धमकी देने वाली भाषा एक सामान्य फ़िशिंग रणनीति है. इससे डरें नहीं. ईमेल में दी गई इस प्रकार की पंक्तियों से सावधान रहें, जो दावा करते हैं कि 'आपका खाता निलंबित कर दिया गया है' अथवा 'आपके खाते में अनाधिकृत लॉग इन प्रयास किया गया था' आदि.

टिप 8 एवं 9 : ईमेल के द्वारा वायरस और मैलवेयर ग्रसित अनुलग्नक प्रेषिक करना एक सामान्य फिशिंग रणनीति है. ये मैलीशियस अनुलग्नक आपके कंप्यूटर एवं फाइलों को नुकसान पहुंचा सकते हैं, आपकी जानकारी के बिना चुपचाप आपके पासवर्ड को चुरा सकते हैं या आपके कंप्यूटर पर की जा रही सभी गतिविधियों की जासूसी भी कर सकते हैं. इस प्रकार प्राप्त ईमेल, जिनके प्राप्त होने की आपको कोई उम्मीद ही न थी, के साथ भेजे गए लिंक्स/अनुलग्नकों को न तो खोलें और न ही डाउनलोड करें.

टिप 10 : हस्ताक्षरकर्ता के बारे में पर्याप्त जानकारी न होना अथवा उनका संपर्क न होना फिशिंग ईमेल की मुख्य पहचान है. वैध इमेल प्रेषक अपना संपर्क विवरण अवश्य प्रदान करते हैं.

तुरंत सूचित करें : -

बैंक में कार्य करते वक्त, यदि आप के मेल बॉक्स में कोई फिशिंग अथवा संदेहास्पद ई-मेल आता है तो तुरंत निम्नलिखित कार्रवाई करेः--

1. इस प्रकार के ई-मेल्स को किसी को फॉरवर्ड न करें.
2. इस ई-मेल से किसी भी प्रकार का अटैचमेंट अपने कंप्यूटर पर डाउनलोड न करें.
3. ई-मेल में एम्बेडेड किसी भी इंटरनेट लिंक पर क्लिक न करें.

4. ई-मेल का स्क्रीन प्रिंट लें एवं इस ई-मेल को अपने कंप्यूटर से तुरंत डिलीट कर दें.

5. यह ई-मेल प्रिंट स्क्रीन CISO Office/DIT को निम्नलिखित ई-इमेल्स पर प्रेषित करें :-

   1) antiphishing.ciso@unionbankofindia.com

   2) antivirusteam@unionbankofindia.com

   3) Itsecurityteam.ubi@unionbankofindia.com

   साथ ही अपने कंप्यूटर पर यह भी सुनिश्चित करें कि : --

   1) नवीनतम सिग्नेचर के साथ एंटी वायरस इन्सटाल्ड होना चाहिये.

   2) ऑपरेटिंग सिस्टम के सभी पैचेस इन्सटाल्ड होने चाहिये.

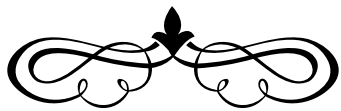
   3) पेन ड्राइव डीएक्टिवेट होना चाहिये.

   4) अन्यथा तुरंत आपके RCC अधिकारियों से संपर्क करें एवं उपरोक्त 3 बिंदु सुनिश्चित करें.

सभी स्टाफ सदस्यों से निवेदन है कि अपने ई-मेल को पढ़ते समय उपरोक्त सावधानियों का अवश्य ध्यान रखें एवं अपने बैंक को साइबर सेफ बनाये रखने में अपना अमूल्य योगदान प्रदान करें.

याद रखें, साइबर सिक्योरिटी हम सभी की साझा जिम्मेदारी है.

आइये हम सब मिलकर अपने बैंक को साइबर सुरक्षित बनाएं.



हमारा कंप्यूटर सिस्टम जोखिम में है, इसका पता कैसे लगाएं

सतीश कप्पाला
प्रबंधक
सीसो कार्यालय, के. का. मुंबई

गौरव बिष्ट
प्रबंधक
सीसो कार्यालय, के. का. मुंबई

हाल के वर्षों में साइबर सुरक्षा एक चिंता का विषय बन गया है. अधिकांश लोग ईमेल और सोशल मीडिया जैसे साधनों का प्रयोग करते हैं और अपने बैंकिंग लेनदेन और खरीदारी का भुगतान करने के लिए ऑनलाइन साधनों का प्रयोग करते हैं. फलस्वरूप, आपका सभी डाटा डिजिटल हो जाता है और डिजिटलीकरण में व्याप्त समस्त जोखिम भी इससे जुड़ जाते हैं.

साइबर सुरक्षा या कंप्यूटर सुरक्षा का अर्थ कंप्यूटर सिस्टम में निहित जानकारी को चोरी से रोकने और उन्हें नुकसान होने से बचाना है. आपके कंप्यूटर की सुरक्षा के साथ-साथ कई अलग-अलग तरीकों से एक हैकर आपके डाटा को चुरा लेने या आपके कंप्यूटर को संक्रमित करने का प्रयास कर सकता है. यह लंबे समय तक या ज्ञात अवधि तक चालू रह सकता है.

इन खतरों के प्रति आपकी संवेदनशीलता को कम करने के लिए विभिन्न प्रकार के खतरों की सूची यहां दी गई है :

1. कमजोरियाँ

कंप्यूटर या सुरक्षा कॉन्फ़िगरेशन समुचित न होने पर इसमें आसानी से सेंध लगाई जा सकती है. हैकर कमजोरियों का फायदा उठाते हैं, जिसके परिणामस्वरूप कंप्यूटर या उसके डाटा को संभावित नुकसान होता है.

आपको कैसे मालूम हो?

कंपनियां कमजोरियों की घोषणा करती हैं क्योंकि उन्हें खोजा जाता है और

सॉफ्टवेयर और सुरक्षा "पैच" के साथ उन्हें ठीक भी किया जाता है.

क्या करें?

- सॉफ्टवेयर और सुरक्षा पैच अद्यतित रखें.
- अपने ऑपरेटिंग सिस्टम, इंटरनेट ब्राउज़र और सुरक्षा सॉफ्टवेयर के लिए सुरक्षा सेटिंग्स कॉन्फ़िगर करें.
- बैंक में ऑनलाइन व्यवहार के लिए उन्नतशील व्यक्तिगत सुरक्षा नीतियां उन्नतशील करनी चाहिए और कर्मचारियों को ऑनलाइन सुरक्षा को बढ़ावा देने के लिए घोषित नीतियों को अपनाना सुनिश्चित करना चाहिए.
- भेद्यता को लक्षित करने वाले खतरों को अवरुद्ध करने के लिए नॉर्टन इंटरनेट सुरक्षा जैसे एक सक्रिय सुरक्षा समाधान का प्रयोग करना चाहिए.

2. स्पाइवेयर

स्पाइवेयर वेबसाइटों, ईमेलसंदेशों, त्वरित संदेश और प्रत्यक्ष फ़ाइल साझाकरण से यह डाउनलोड हो जाता है. इसके अतिरिक्त, कोई उपयोगकर्ता सॉफ़्टवेयर प्रोग्राम से अंतिम उपयोगकर्ता लाइसेंस अनुबंध स्वीकार कर अनजाने में स्पाइवेयर प्राप्त कर सकता है.

आपको कैसे मालूम हो?

स्पाइवेयर अक्सर उपयोगकर्ता को सिस्टम पर सक्रिय रूप से छुप कर या अपनी उपस्थिति अज्ञात रखकर सक्रिय रहने का प्रयास करता है.

क्या करें?

सॉफ्टवेयर और सुरक्षा पैच अद्यतित रखें. अपने ऑपरेटिंग सिस्टम, इंटरनेट ब्राउज़र और सुरक्षा सॉफ्टवेयर के लिए सुरक्षा सेटिंग्स कॉन्फ़िगर करें. बैंक में ऑनलाइन व्यवहार के लिए उन्नतशील व्यक्तिगत सुरक्षा नीतियां विकसित करनी चाहिए और कर्मचारियों को ऑनलाइन सुरक्षा को बढ़ावा देने के लिए घोषित नीतियों को अपनाना सुनिश्चित करना चाहिए.

3. स्पैम

ईमेल स्पैम जंक मेल का इलेक्ट्रॉनिक संस्करण है. इसमें अनचाहे संदेशों, अनचाहे विज्ञापन, बड़ी संख्या में प्राप्तकर्ताओं को भेजना शामिल है. स्पैम एक गंभीर सुरक्षा चिंता है क्योंकि इसका उपयोग भारी मात्रा में एक साथ ईमेल वितरित कर ईमेल

प्राप्तकर्ता की संवेदनशील व्यक्तिगत जानकारी प्राप्त करने के लिए किया जाता है. ऐसे स्पैम ईमेल में ट्रोजन हॉर्स, वायरस, स्पाइवेयर और लक्षित हमले शामिल हो सकते हैं.

आपको कैसे मालूम हो?

जिन संदेशों में TO या CC फ़ील्ड में आपका ईमेल पता शामिल नहीं है, वे स्पैम के सामान्य रूप हैं. कुछ स्पैम में अनुचित सामग्री या अनुचित सामग्री वाले वेब साइटों के लिंक हो सकते हैं. साथ ही, कुछ स्पैम में छुपा पाठ शामिल हो सकता है, जो केवल सामग्री को हाइलाइट करते समय दिखाई देता है.

क्या करें?

- स्पैम फ़िल्टरिंग/अवरुद्ध सॉफ्टवेयर स्थापित करें.
- अगर आपको संदेह है कि कोई ईमेल स्पैम है, तो जवाब न दें - बस इसे मिटा दें.
- अपने ईमेल के पूर्वावलोकन फलक को अक्षम करने और सादे पाठ में ईमेल पढ़ने पर विचार करें.
- उन सभी लोगों से प्राप्त संदेशों को तत्काल अस्वीकृत करें, जो आपकी सूची में नहीं हैं.
- यूआरएल लिंक पर क्लिक न करें, जब तक कि वह एक ज्ञात स्रोत से न हो और अपेक्षित न हो.
- सॉफ्टवेयर और सुरक्षा पैच अद्यतित रखें.

4. मैलवेयर

मैलवेयर दुर्भावनापूर्ण कोड की एक श्रेणी है, जिसमें वायरस और ट्रोजन हॉर्स शामिल हैं. ईमेल और तत्काल संदेशों के माध्यम से भेजे गए वायरस, वेब साइट्स से ट्रोजन हॉर्स और पीयर-टू-पीयर कनेक्शन से डाउनलोड वायरस से संक्रमित फ़ाइलें इसमें शामिल होती हैं. मैलवेयर अपनी प्रविष्टि को शांत और आसान बनाने वाले सिस्टम पर मौजूदा भेद्यता का भी फायदा उठाने का प्रयास करेगा.

आपको कैसे मालूम हो?

मैलवेयर सक्रिय रूप से छुपकर या उपयोगकर्ता के ज्ञात प्रणाली पर अपनी उपस्थिति न दर्ज कराते हुए अनजान रहकर काम करता है. ऐसा हो सकता है कि

आपका सिस्टम पहले की तुलना में धीमी गति से कार्य कर रहा हो.

क्या करें

- केवल विश्वसनीय स्रोतों से आने वाले ईमेल या आईएम अनुलग्नक खोलें.
- ईमेल खोलने से पहले यह सुनिश्चित करें कि अनुलग्नक एक प्रतिष्ठित इंटरनेट सुरक्षा सॉफ्टवेयर द्वारा स्कैन है.
- किसी ऐसे व्यक्ति द्वारा भेजे गए वेब लिंक पर क्लिक न करें, जिसे आप नहीं जानते हैं.
- अगर आपकी बडी (Buddy) सूची में कोई व्यक्ति अजीब संदेश, फाइल या वेब साइट लिंक भेज रहा है, तो अपने आईएम सत्र को समाप्त कर दें.
- अपने सिस्टम में स्थानांतरित करने से पहले सभी फ़ाइलों को एक प्रतिष्ठित इंटरनेट सुरक्षा कार्यक्रम के साथ स्कैन करें.
- केवल ज्ञात स्रोतों से फ़ाइलों को स्थानांतरित करें.
- सभी अनचाहे आउटबाउंड संदेशों को अवरुद्ध करने के लिए एक प्रतिष्ठित इंटरनेट सुरक्षा कार्यक्रम का उपयोग करें.
- सुरक्षा पैच अद्यतित रखें.

5. फिशिंग

फ़िशिंग एक स्पैम, दुर्भावनापूर्ण वेबसाइट्स, ईमेल संदेश और तत्काल संदेशों का उपयोग लोगों की संवेदनशील जानकारी, जैसे बैंक और क्रेडिट कार्ड की जानकारी या व्यक्तिगत खातों तक पहुंचने के लिए भेजे जाते हैं.

आपको कैसे मालूम हो?

फ़िशिंग घोटालों की पहचान करने के चार तरीके हैंः फिशर्स, वैध कंपनियां होने का नाटक करते हुए, व्यक्तिगत जानकारी देने का अनुरोध करने और प्राप्तकर्ताओं को दुर्भावनापूर्ण वेबसाइटों के माध्यम से प्रतिक्रिया देने के लिए ईमेल का उपयोग कर सकते हैं. वे यह भी दावा कर सकते हैं कि प्राप्तकर्ताओं को अपने कंप्यूटर पर दुर्भावनापूर्ण प्रोग्राम डाउनलोड करने के लिए त्वरित कार्रवाई करने की आवश्यकता है. फिशर्स भावनात्मक भाषा का उपयोग करते हैं. फिशसाइटें वैधसाइटों की तरह ही दिखती हैं, क्योंकि अपराधी वास्तविक साइटों से कॉपीराइट की गई छवियों का उपयोग करते हैं.

ईमेल या त्वरित संदेशों के माध्यम से गोपनीय जानकारी के लिए अनुरोध वैध नहीं हैं. संक्रमित प्रोग्राम या अनुलग्नक को खोलने और चलाने के बाद हो सकता है कि आप तुरंत अपने कंप्यूटर पर प्रभावों को न देख सकें. यहां कुछ संकेत दिए गए हैं जो इंगित कर सकते हैं कि आपका कंप्यूटर संक्रमित हो गया है. आपका कंप्यूटर सामान्य से अधिक धीमे चलता है. आपका कंप्यूटर प्रतिक्रिया देना बंद कर देता है या अक्सर लॉक हो जाता है. आपका कंप्यूटर हर कुछ मिनट पर रिस्पांड करना बंद कर देता है और फिर से शुरू होता है. आपका कंप्यूटर अपने आप पुनः प्रारंभ (Restart) होता है और फिर सामान्य रूप से चलने में विफल रहता है. आप असामान्य त्रुटि संदेश देखते हैं. आप विकृत मेनू और संवाद बॉक्स देखते हैं.

क्या करें

अगर आपको लगता है कि आपको फ़िशिंग ईमेल प्राप्त हुआ है और लिंक पर क्लिक करने या प्रोग्राम डाउनलोड करने की लालच दी गयी है और चिंतित हैं कि आपके कंप्यूटर पर कुछ प्रकार का दुर्भावनापूर्ण प्रोग्राम इंस्टॉल हो सकता है, तो यहां कुछ सावधानियां निम्नलिखित हैं, जिनकी आप जांच कर लें :

- क्या आपका वायरस स्कैन चल रहा है?
- क्या आपका एंटीवायरस एक सप्ताह के अंदर अद्यतित किया गया है
- क्या आपने पूर्ण डिस्क/मेमोरी वायरस स्कैन किया था.
- क्या आप एंटी-स्पाइवेयर प्रोग्राम जैसे एडवेयर और/या स्पाइबॉट एसडी चला रहे हैं?
- एक बार जब आप अपना स्कैन चलाते हैं और सकारात्मक परिणाम प्राप्त करते हैं या प्रोग्राम हटाते हैं, तो सुनिश्चित करें कि आपके ऑनलाइन खाते सुरक्षित हैं.
- अपने खाते का पासवर्ड बदल दें.
- सुनिश्चित करें कि आपने अपने फ़िशिंग फ़िल्टर को सक्षम किया है, जो विंडोज इंटरनेट एक्सप्लोरर 7 की सुविधा है. अपने द्वारा उठाए जा सकने वाले अन्य चरणों को जानने के लिए अपने एडमिन या एंटी-स्पाइवेयर/ वायरस विक्रेता से संपर्क करें.

कंप्यूटर सुरक्षा कंप्यूटिंग सिस्टम और उनके घटकों की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित करने का प्रयास करती है. कंप्यूटिंग सिस्टम के तीन प्रमुख

भाग हमलों के अधीन हैंः हार्डवेयर, सॉफ्टवेयर और डाटा. ये तीन और उनमें से संचार, कंप्यूटर सुरक्षा भेद्यता के लिए अतिसंवेदनशील हैं.

काउंटर मेजर्स और नियंत्रण डाटा, कार्यक्रम, सिस्टम, भौतिक उपकरण, संचारलिंक, पर्यावरण और कर्मियों पर लागू किया जा सकता है. कभी-कभी एक भेद्यता को कवर करने के लिए कई नियंत्रणों की आवश्यकता होती है, लेकिन कभी-कभी एक नियंत्रण कई समस्याओं को एक साथ संबोधित करता है.

निष्कर्ष यह है कि साइबर अपराध एक बड़ा अपराध है. भविष्य में प्रौद्योगिकी, इंटरनेट और वैश्वीकरण के रूप में साइबर अपराध की संभावना बढ़ेगी. इसलिए प्रत्येक व्यक्ति को इन प्रकार की गतिविधियों से अवगत होना चाहिए. बैंकिंग, व्यापार, भुगतान बिल आदि जैसी ऑनलाइन गतिविधियों के दौरान हमें बहुत सावधान रहना होगा. हमें यह सुनिश्चित कर लेना चाहिए कि हमारे कंप्यूटर या इंटरनेट से संबंधित सभी डिवाइस में इंटरनेट सुरक्षा है और उचित रूप से एंटी-वायरस सॉफ़्टवेयर का उपयोग किया जा रहा है. हमें अपनी निजी जानकारी पिन, सोशल सिक्योरिटी नंबर, क्रेडिट कार्ड की जानकारी, खाता संख्या या ईमेल के माध्यम से कोई भी संवेदनशील व्यक्तिगत जानकारी सार्वजनिक रूप से प्रकट नहीं करना चाहिए. हैकर कभी-कभी ईमेल सर्वर देखते हैं और ईमेल को अवरुद्ध कर सकते हैं. प्रत्येक वर्ष कितना नुकसान हैकर्स के कारण होता है, इसका अनुमान लगाना मुश्किल है.

संदर्भ

https://hi.wikipedia.org/wiki/

http://www.informit.com

बैंकों द्वारा ग्राहकों के डाटा को सुरक्षित करने हेतु उपाय

उर्वशी टंडन
सहायक प्रबंधक
सीसो कार्यालय, के. का. मुंबई

बैंकों के पास ग्राहकों से संबन्धित कई जानकरियाँ उपलब्ध होती हैं, जो किसी प्रकार का खाता खोलने या लोन देते समय ग्राहकों द्वारा प्रदान की जाती हैं. ग्राहकों की व्यक्तिगत जानकारी जैसे ग्राहक का नाम, पता, व्यवसाय, मोबाइल नंबर, पैन नंबर, आधार नंबर आदि केवाईसी (अपने कस्टमर को जानें) के तहत ग्राहक की पहचान के लिए बैंकों को प्रदान करना आवश्यक है. इसके अलावा, खाते से संबन्धित जानकारी जैसे खाते का बैलेन्स, खाते के लेनदेन की जानकारी भी बैंकों के पास उपलब्ध होती है, जो ग्राहक के अलावा किसी को नहीं दी जा सकती. क्रेडिट कार्ड, डेबिट कार्ड से संबन्धित जानकारी जैसे कार्ड नंबर, सीवीवी नंबर आदि ऐसी जानकरियाँ हैं, जिसके किन्ही गलत हाथों में चले जाने पर ग्राहक को वित्तीय नुकसान उठाना पड़ सकता है.

इन सभी जानकारियों को सुरक्षित रखना बैंक की ज़िम्मेदारी है. ग्राहकों को यह विश्वास होना चाहिए कि उनकी जानकारी बैंक के पास सुरक्षित रहेगी और इसका कोई गलत इस्तेमाल नहीं होगा. इसका इस्तेमाल केवल बैंक द्वारा सीमित अवसरों पर किया जाएगा व किसी अन्य व्यक्ति या संस्थान के साथ इसे साझा नहीं किया जाएगा. ऑनलाइन धोखाधड़ी, साइबर क्राइम और पहचान की चोरी के मामले में हाल में हुई तेज़ वृद्धि ने उपभोक्ता को सशंकित कर रखा है. ग्राहकों की निजता के लिए बैंक प्रतिबद्ध है. अगर किसी तरह से ये जानकारी बाहर जाती है और इसके गलत इस्तेमाल से ग्राहक को निजी या आर्थिक तौर पर नुकसान उठाना पड़ता है तो इससे बैंक के व्यवसाय के

साथ-साथ बैंक की साख पर भी गलत प्रभाव पड़ता है. यहाँ तक कि इस का क़ानूनी या अनुपालन प्रभाव भी हो सकता है. इसलिए बैंकों के लिए यह ज़रूरी है कि ग्राहकों में यह विश्वास लाएँ कि उनकी जानकारी बैंक के पास सुरक्षित रहेगी.

आज के डिजिटल युग में जहां ग्राहकों को अधिक सुविधाजनक बैंकिंग प्रदान की जा रही है, वहीं तकनीक के गलत इस्तेमाल से साइबर अपराधी कई तरीकों से डाटा चोरी करने की कोशिश करते रहते हैं. ग्राहक इंटरनेट बैंकिंग, मोबाइल बैंकिंग के माध्यम से अपने खाते को कभी भी कहीं भी एक्सैस कर सकता है, क्रेडिट एवं डेबिट कार्ड के माध्यम से भुगतान कर सकता है. इन सबकी जानकारी ऑनलाइन उपलब्ध होने के कारण इनका दुरुपयोग होने की आशंका बढ़ जाती है और इससे बचने के लिए बैंकों को इसकी सुरक्षा के लिए ठोस इंतजाम करने होंगे.

ग्राहक के डाटा को सुरक्षित रखने के लिए बैंकों को निम्नलिखित उपाय अपनाने चाहिए-

i) **भौतिक सुरक्षा** - सर्वर कक्ष भौतिक सुरक्षा का केंद्र है और उस कक्ष में सर्वर, स्विच, रूटर, केबल्स एवं अन्य उपकरणों तक भौतिक पहुँच वाला कोई भी व्यक्ति सुरक्षा को भारी नुकसान पहुँचा सकता है. सर्वर कक्ष में केवल अधिकृत व्यक्ति ही प्रवेश कर सके, इसके लिए सख्त उपाय मौजूद होने चाहिए. सर्वर कक्ष में ताले का प्रयोग, भीतर जाने के लिए नियंत्रण कार्ड, बायोमेट्रिक एक्सैस सिस्टम का प्रयोग आदि होना चाहिए. घुसपैठ का पता लगाने हेतु सेन्सर, गर्मी सेन्सर, धुआं डिटेक्टर, निगरानी कैमरों का इस्तेमाल किया जाना चाहिए. सुरक्षा सुनिश्चित करने के लिए आपदा निवारण नीतियों और प्रक्रियाओं का नियमित आधार पर परीक्षण किया जाना चाहिए.

ii) **प्रभावी एंड पॉइंट सुरक्षा का इस्तेमाल** - किसी भी डिवाइस जैसे मोबाइल डिवाइस, लैपटाप, डेस्कटॉप को नेटवर्क के भीतर लाने के लिए या नेटवर्क के भीतर के संसाधन का उपयोग शुरु करने से पहले ही निश्चित मानकों का पालन करना ज़रूरी है. इसके लिए प्रभावी एंड पॉइंट सुरक्षा का इस्तेमाल करना चाहिए. इससे यह सुनिश्चित होगा कि कोई भी अनधिकृत बाहरी व्यक्ति डिवाइस नेटवर्क के भीतर किसी संसाधन को एक्सैस नहीं कर पाएगा.

iii) **केवल अधिकृत सॉफ्टवेर का इस्तेमाल करना** - केवल उन्ही सॉफ्टवेयर को इन्स्टाल करने की अनुमति होनी चाहिए, जो कि बैंक द्वारा अधिकृत हों. अनधिकृत अथवा पायरेटेड सॉफ्टवेयर के इस्तेमाल से सिस्टम को खतरा हो सकता है. इसके इस्तेमाल से विभिन्न वायरस एवं मालवेयर सिस्टम में प्रवेश करके डाटा को क्षति पहुंचा सकते हैं. बैंक के पास स्वीकृत सॉफ्टवेयर लाइसेन्स की सूची होनी

चाहिये एवं किसी भी अनधिकृत सॉफ्टवेयर के इस्तेमाल पर रोक लगाई जानी चाहिए.

iv) **एंटीवायरस पैच इन्स्टाल एवं अपडेट करना** - एंटीवायरस का उपयोग वायरस खोजने एवं उसे नष्ट करने के लिए किया जाता है. पैच एक सॉफ्टवेयर कोड है, जो कि कम्प्यूटर प्रोग्राम की खामियों को दूर करने के लिए बनाया जाता है. एंटीवाइरस एवं पैच का इस्तेमाल सुनिश्चित किया जाना चाहिए एवं समय-समय पर इसे अपडेट करते रहना चाहिए.

v) **फायरवॉल इन्स्टाल करना** - फायरवॉल एक नेटवर्क सिस्टम है, जो कि आने-जाने वाले नेटवर्क ट्रैफिक पर निगरानी रखता है एवं उसे नियंत्रित रखता है. फायरवॉल पहले से निर्धारित नियमों पर काम करता है और इसके मुताबिक यह तय करता है कि किस ट्रैफिक को अंदर आने देना है ओर किसे रोकना है. फायरवॉल आमतौर पर एक विश्वसनीय आंतरिक नेटवर्क और अविश्वसनीय बाहरी नेटवर्क के बीच बाधा स्थापित करता है.

vi) **एंक्रिप्शन तकनीक का इस्तेमाल** - प्लेन डाटा को हैक करना अपेक्षाकृत आसान है. एंक्रिप्शन वह तकनीक है, जिसमें डाटा को एक कुंजी की मदद से सांकेतिक शब्दों में परिवर्तित (एंकोड) किया जाता है एवं उसे केवल वही व्यक्ति एक्सैस कर सकता है, जिसे इसकी कुंजी की जानकारी हो. इस प्रकार डाटा सुरक्षित रहता है. डाटा को स्टोर करने एवं ट्रान्सफर करने के लिए एंक्रिप्शन तकनीक का ही इस्तेमाल करना चाहिए. पासवर्ड को स्टोर करने के लिए भी इस तकनीक का इस्तेमाल करना चाहिए. हमेशा प्रभावी व नवीनतम एंक्रिप्शन तकनीक का इस्तेमाल किया जाना चाहिये और इसे हमेशा अपडेट करते रहना चाहिये.

vii) **ई-मेल गेटवे का इस्तेमाल** - सुरक्षित ई-मेल सिस्टम का इस्तेमाल करना चाहिए ताकि नेटवर्क के अंदर कोई भी जाली मेल, संक्रमित फ़ाइल या लिंक प्रवेश न कर सके. ऐसे मेल को गेटवे पर ही ब्लॉक किया जाना चाहिए जो कि स्पैम की श्रेणी में आते हैं. जैसे कि मार्केटिंग मेल या ऐसे मेल, जिनमें एक्सिक्युटेबल फ़ाइल अटैच हो आदि. ऐसी फ़ाइल के साथ मालवेयर फ़ाइल संलग्न हो सकती है.

viii) **यूएसबी एक्सैस एवं इंटरनेट एक्सैस का नियंत्रण :** अनधिकृत डाटा एक्सैस रोकने के लिए यूज़र के सिस्टम पर यूएसबी एक्सैस एवं इंटरनेट एक्सैस को नियंत्रित रखना चाहिए. किसी भी अंजान यूएसबी को कम्प्यूटर में नहीं लगाना चाहिए. इसे पासवर्ड से सुरक्षित करना चाहिए. इंटरनेट का इस्तेमाल करते समय हमेशा सुरक्षित साइट ब्राउज़ करना चाहिए.

ix) **पासवर्ड पॉलिसी का निर्माण** - बैंकों द्वारा कर्मचारियों के लिए पासवर्ड पॉलिसी का निर्माण करना चाहिए. इसके तहत पासवर्ड की लंबाई, पासवर्ड की जटिलता के न्यूनतम मानक तय किए जाने चाहिए.

x) **डाटा एक्सैस नियंत्रित करना :** पहले अपने सिस्टम को पूर्ण प्रमाणित करना चाहिए यानि आंतरिक रूप से जांचना कि किस की डाटा व जानकारी तक पहुँच है, क्या हर किसी के पास मास्टर डाटा तक पहुँच और नियंत्रण है. बैंक में ग्राहकों के डाटा के एक्सैस का अधिकार केवल उन्ही लोगों तक सीमित होना चाहिए, जिन्हें इस पर काम करने की आवश्यकता हो. डाटा को एक्सैस करने की अनुमति विभिन्न स्तरों पर नियंत्रित की जानी चाहिए जैसे कि डाटा को देख पाना, डाटा में कुछ बदलाव कर पाना एवं डाटा को डिलीट करने की अनुमति केवल उन्ही लोगों को होनी चाहिए, जिनको यह कार्य सुपुर्द किया गया है एवं जो इसके लिए जिम्मेदार हैं. इसके लिए पूर्व अनुमति ली जानी चाहिए एवं सत्यापन के उपरांत ही डाटा एक्सैस किए जाने की सुविधा होनी चाहिए. इस प्रकार कोई भी अनधिकृत व्यक्ति डाटा को एक्सैस नहीं कर पाएगा.

xi) **वेबसाइट सुरक्षा सुनिश्चित करें :** बैंक की वेबसाइट की सुरक्षा के लिए महत्वपूर्ण उपायों को अपनाना चाहिए जैसे कि 2 फैक्टर प्रमाणीकरण (2FA) और एसएसएल (SSL) प्रमाणपत्र. दो कारक प्रमाणीकरण एक सुरक्षा प्रक्रिया है, जिसमें वैध उपयोगकर्ता को पहचान के दो साधन आमतौर पर उपयोगकर्ता नाम - पासवर्ड कॉम्बो और सुरक्षा कोड प्रदान करने की आवश्यकता होती है. इस द्वि-चरणीय प्रक्रिया से हैकर्स सामान्यतया किसी भी जानकारी को क्रैक करने में सक्षम नहीं हो पाते. इसके अलावा एसएसएल प्रमाणपत्र उपयोगकर्ताओं की पहचान को प्रमाणित करता है और स्टोर और पारागमन के दौरान डाटा को एन्क्रिप्ट करता है और अंत में उपयोगकर्ता सिस्टम और वेबसाइट के बीच सुरक्षित कनेक्टिविटी स्थापित करता है.

xii) **वेंडर मैनेजमेंट :** आउटसोर्स वेंडर से कांट्रैक्ट के समय डाटा सुरक्षा के नियम बताए जाने चाहिए. वेंडर का ड्यू डिलिजेंस करना चाहिए. किसी भी तरह के डाटा के एक्सैस का अधिकार बैंक द्वारा नियंत्रित किया जाना चाहिए और इसे बैंक के बाहर ले जाने या सेव करने पर पाबन्दी होनी चाहिए.

xiii) **निरंतर निगरानी एवं विश्लेषण :** सर्वर, अंतबिन्दु, डाटाबेस, वेबसाइट एवं अन्य प्रणालियों पर गतिविधि की निगरानी एवं विश्लेषण के लिए सुरक्षा संचालन केंद्र (SOC) की स्थापना होनी चाहिए. यह एक ऐसी सुरक्षा टीम है, जो 24/7 साइबर सुरक्षा घटनाओं का पता लगाने, विश्लेषण करने एवं प्रतिक्रिया देने का काम करती

है. कोई असंगत गतिविधि, सुरक्षा घटना या समझौते का संकेत हो सकती है. इसकी निरंतर निगरानी से साइबर हमले से बचाव हो सकता है.

xiv) **कर्मचारियों को शिक्षित करना :** बैंक में सुरक्षा की संस्कृति बनाना आवश्यक है. कर्मचारियों को संभावित जोखिम, डाटा की जानकारी को लगातार सुरक्षित रखने और डाटा उल्लंघन के मामले में क्या करना है, ये जानने की आवश्यकता है. इसके लिए समय-समय पर कर्मचारियों को ट्रेनिंग दी जानी चाहिए एवं मेल, सर्कुलर्स इत्यादि की सहायता से कर्मचारियों को जागरूक करना चाहिए. उन्हें निम्नलिखित नियमों का पालन करने के लिए कहना चहिए -

- **जटिल पासवर्ड का उपयोग** - पासवर्ड जटिल होना चाहिए ताकि इसका कोई अन्य व्यक्ति अंदाज़ा न लगा सके. पासवर्ड की लंबाई बहुत कम नहीं होनी चाहिए. पासवर्ड अक्षरों, अंकों एवं विशेष वर्णों का मिश्रण होना चाहिए एवं इसमें नाम, जन्मतिथि जैसी जानकारी शामिल नहीं होनी चाहिए क्योंकि इनका आसानी से अंदाज़ा लगाया जा सकता है. पासवर्ड कभी किसी के भी साथ साझा नहीं करना चाहिए.
- **सिस्टम लॉक करना** - अपनी डेस्क छोड़ने से पहले हमेशा अपने सिस्टम को लॉक करना चाहिए.
- **किसी जानकारी को नष्ट करने का सही तरीका** - किसी भी संभावित सुरक्षा उल्लंघन से बचने के लिए कागज़ के दस्तावेजों को पेपर श्रेडर में नष्ट करना चाहिए.
- **डेस्क साफ रखना** - किसी भी जानकारी को किसी और हाथों में आने से बचने के लिए हमेशा अपनी डेस्क से दस्तावेजों को काम होने पर हटाकर अलमारी या दराज में ताला लगाकर रखना चहिए.
- **ई-मेल के इस्तेमाल में सावधानी** - कर्मचारियों को सही मेल व फिशिंग मेल में फर्क करने के लिए शिक्षित करना चाहिए. साइबर अपराधी ई-मेल द्वारा ऐसी फाइल या लिंक भेजते हैं, जिससे सिस्टम में मालवेयर प्रवेश कर सकता है और ये डाटा की चोरी या फाइल को नुकसान पहुंचा सकते हैं.

xv) **ग्राहक को शिक्षित करना :** ग्राहक को शिक्षित करना भी आवश्यक है कि वह अपना एटीएम कार्ड/डेबिट कार्ड/क्रेडिट कार्ड नंबर, ओटीपी, पिन नंबर, सीवीवी नंबर किसी के साथ साझा न करें. बैंक ग्राहक को यह जानकारी एसएमएस द्वारा, वेबसाइट पर प्रकाशित करके अथवा अन्य किसी माध्यम से दे सकता है. ग्राहक को मोबाइल नंबर पंजीकृत करने को प्रेरित करना चाहिए ताकि उसके पास खाते

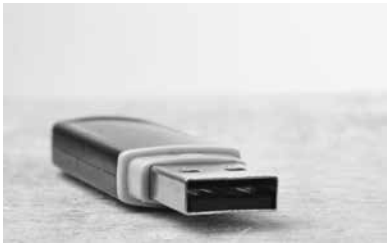
में किसी भी लेन-देन की सूचना आती रहे. ग्राहक को इंटरनेट बैंकिंग, मोबाइल बैंकिंग इस्तेमाल करते समय भी सतर्कता बरतने को कहना चाहिए. हमेशा सुरक्षित (https) साइट का उपयोग करना चाहिए. किसी भी फ़र्ज़ी फ़ोन अथवा ई-मेल का जवाब नहीं देना चहिए.

उपरोक्त सभी उपाय अपना कर ग्राहक का डाटा एवं विश्वास दोनों सुरक्षित रखे जा सकते हैं एवं कई असुविधाओं से बचा जा सकता है.

यूएसबी प्रयोग के सही तरीके

शानमथी कुमार
सहायक प्रबंधक
सीसो कार्यालय, के. का. मुंबई

के एम रेड्डी
सहायक महाप्रबंधक
सीसो कार्यालय, के. का. मुंबई



जब साइबर सुरक्षा की बात आती है, तो यह कोई रहस्य नहीं है कि किसी भी संगठन का मानव पहलू इसका सबसे कमजोर लिंक है. फ़िशिंग ईमेल से पीड़ित होने से लेकर पासवर्ड साझा करने तक का सफर, ये चुनौतियां मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) कार्यालय के लिए दुःस्वप्न है. आखिरकार, किसी संगठन के कर्मचारियों द्वारा बनाए गए नेटवर्क सुरक्षा में त्रुटि को एक साधारण सॉफ़्टवेयर पैच से प्लग नहीं किया जा सकता है. कर्मचारियों को प्रशिक्षित करने के प्रयासों के बावजूद, कर्मचारियों का शोषण अभी भी हैकर्स के लिए सबसे आसान मार्ग है खासकर जब यूएसबी आधारित सुरक्षा की बात आती है.

आप एक बार अवश्य ध्यान दें कि सेलफोन, टैबलेट, कीबोर्ड, माऊस, जैसे कितने डिवाइस यूएसबी पोर्ट के माध्यम से कनेक्ट करते हैं. अक्सर हम अपने डिवाइस को यूएसबी पोर्ट में प्लग करने के बाद के संभावित जोखिमों पर विचार किए बिना ही प्लग कर देते हैं, जबकि आपका यूएसबी आपके डिवाइस को चार्ज करने या डाटा ट्रान्सफर का एक तेज़, सुविधाजनक तरीका हो सकता है. यह आपके नेटवर्क पर मालवेयर स्थानांतरित करने और डाटा चोरी करने का एक प्रमुख तरीका भी हो सकता है.

स्टोरेज, वायरलेस या ब्लूटूथ क्षमताओं वाले किसी भी डिवाइस से सिस्टम में संक्रमण हो सकता है. वास्तविक जोखिम आवश्यक रूप से संक्रमण नहीं है, बल्कि यह है कि यूएसबी का उपयोग किस काम के लिए किया जा रहा है. चूंकि यूएसबी निर्माता अपने उपकरणों में फर्मवेयर की रक्षा नहीं करते हैं, इसलिए मालवेयर फर्मवेयर को ओवरराइट करने और रोजमर्रा के उपकरणों पर नियंत्रण रखने की क्षमता रखता है और

बहुत से अलग तरह के डिवाइस एक ही कनेक्शन में प्लग किए जा सकते हैं, एक प्रकार के डिवाइस को पुनः प्रोग्राम किया जा सकता है और उपयोगकर्ता के बिना जानकारी के किसी संक्रमित डिवाइस में बदला जा सकता है.

यूएसबी स्टोरेज डिवाइस अलग-अलग कंप्यूटर के बीच डाटा स्थानांतरित करने का सुविधाजनक माध्यम है. आप इसे यूएसबी पोर्ट में प्लग कर सकते हैं, अपना डाटा कॉपी कर सकते हैं और इसे हटा सकते हैं. दुर्भाग्यवश यह पोर्टेबिलिटी, सुविधा और लोकप्रियता आपकी जानकारी के लिए विभिन्न खतरों को साथ लाती है-

- **मालवेयर संक्रमण :** यूएसबी स्टोरेज उपकरणों के माध्यम से मालवेयर फैलता है. कोई जानबूझकर आपकी गतिविधियों, फ़ाइलों, सिस्टम और नेटवर्क पर निगाह रखने के लिए मालवेयर के साथ यूएसबी स्टोरेज डिवाइस दे सकता है. स्वचालित रूप से autorun.exe का उपयोग कर यूएसबी स्टोरेज डिवाइस के माध्यम से मालवेयर एक डिवाइस से दूसरे डिवाइस में फैलाया जा सकता है. उदाहरण के लिएः कन्फिकर वॉर्म, निराकरणीय उपकरणों और ड्राइव जैसे मेमोरी स्टिक्स, एमपी 3 प्लेयर्स और डिजिटल कैमरे के माध्यम से फैलता है. स्टक्सनेट वॉर्म यूएसबी ड्राइव के माध्यम से फैले वर्ष के उच्च प्रोफ़ाइल खतरों में से एक था. इसके अलावा 30 प्रतिशत नए वॉर्म विशेष रूप से कंप्यूटर से जुड़े यूएसबी स्टोरेज उपकरणों के माध्यम से फैलाने के लिए डिज़ाइन किए गए हैं.
- **अनधिकृत उपयोग :** कोई डाटा चोरी करने के लिए आपके यूएसबी डिवाइस को चुरा सकता है
- **बैटिंग :** कोई जानबूझकर मालवेयर रहित यूएसबी डिवाइस आपके डेस्क या जगह पर छोड़ सकता है

यूएसबी का समर्थन करने वाले उपकरणों के प्रकार

- कार्ड रीडर
- मोबाइल फोन
- पीडीए
- डिजिटल कैमरा
- डिजिटल ऑडियो प्लेयर
- पोर्टेबल मीडिया प्लेयर
- पोर्टेबल फ्लैश मेमोरी डिवाइस

बैकडोर बंद करें

2016 में, इलिनोइस विश्वविद्यालय के शोधकर्ताओं ने परिसर के चारो ओर 300 गैर-यूएसबी ड्राइव छोड़े और ट्रैक किया कि आगे क्या हुआ. 98% गिराए गए ड्राइव कर्मचारियों और छात्रों द्वारा समान रूप से उठाए गए थे और कम से कम आधे ड्राइव कंप्यूटर पर प्लग-इन फ़ाइलों तक पहुंचने के लिए प्लग किए गए थे. यद्यपि अध्ययन दो साल पहले आयोजित किया गया था, लेकिन इसका परिणाम 2018 में असामान्य नहीं है और यह एक सुरक्षा बैकडोर है जो दुनियाभर के कई नेटवर्कों के लिए अभी भी खुला है. कारण स्पष्ट है - व्यावहारिकता. इसमें कोई संदेह नहीं है कि यूएसबी डिवाइस मशीनों के बीच फ़ाइलों को स्थानांतरित करने का सबसे आसान तरीका है.

शून्य-ट्रस्ट - जिसका अर्थ है कि किसी भी व्यक्ति या डिवाइस पर स्वाभाविक रूप से भरोसा नहीं किया जा सकता है - यह दृष्टिकोण संगठनों में तेजी से बढ़ रहा है, और यही वजह है कि संगठन में यूएसबी उपकरणों का उपयोग बंद किया जा रहा है. तो क्या ऐसा संभव नहीं है कि इस तरह से फ्लैश ड्राइव का उपयोग न करके संगठन पूरी तरह से यूएसबी पोर्ट से दूर रह सकते हैं? यूएसबी पोर्ट स्टोरेज उपकरणों के उपयोग को सुविधाजनक बनाने के अलावा कई उद्देश्यों को पूरा करते हैं. इससे पहले कि वे अंतिम उपयोगकर्ता टर्मिनल पर पूरी तरह से अक्षम हो जाएं और सुरक्षा के हित में आईटी परिदृश्य से हटा दिए जाएं, इससे निपटने के लिए और चुनौतियां हैं.

5 तरीके, जिससे यूएसबी स्टिक सुरक्षा जोखिम हो सकता है-

आपकी यूएसबी स्टिक जितनी उपयोगी है उतनी ही जोखिमदायक भी साबित हो सकती है.

1. **यूएसबी स्टिक गुम हो जाना**

शायद यूएसबी फ्लैश डिवाइस से संबंधित सबसे बड़ा सुरक्षा जोखिम है डिवाइस का खो जाना. यदि आपके

पास पासवर्ड सुरक्षित यूएसबी है, या यह एन्क्रिप्टेड है तो अगर आप इसे खो देते हैं तो आपको अत्यधिक चिंतित नहीं होना चाहिए. मान लीजिए आपके पास कहीं और डाटा का बैकअप है, तो आपको कोई नुकसान नहीं होगा. यह खगोलीय रूप से असंभव है कि कोई भी एन्क्रिप्शन तोड़ने में सक्षम होगा (निश्चित रूप से आधुनिक, व्यावसायिक रूप से उपलब्ध हार्डवेयर का उपयोग करके). इसलिए आपका डिवाइस खोने के बावजूद आपका डाटा सुरक्षित है. लेकिन पासवर्ड सुरक्षा के बिना एक यूएसबी फ्लैश डिवाइस खोना पूरी तरह से अलग मामला है. संग्रहित डाटा के महत्व के आधार पर हम यहां प्रमुख सुरक्षा मुद्दों की बात कर रहे हैं. बेशक, अगर यह सिर्फ आपका पुनरुत्थान है, तो आप अत्यधिक चिंतित नहीं हो सकते हैं; दूसरी तरफ, ये बहुत ही व्यक्तिगत दस्तावेज हो सकते हैं, खासकर अगर यह मसौदे में हैं.

मान लें कि आप अपने नियोक्ता के लिए यूएसबी स्टिक पर संवेदनशील डाटा ले रहे हैं. डिवाइस को खोने के परिणामस्वरूप यह एक सुरक्षा घटना घोषित की जा सकती है. इसकी आंतरिक जांच, शायद एक झगड़ा - या यहां तक कि आपके रोजगार पर प्रश्नचिन्ह भी लगा सकते हैं.

यूएसबी स्टिक खोने से बचने का सरल तरीका यह सुनिश्चित करना है कि यह डाटा आपके पास व्यक्तिगत रूप से संग्रहीत हो. इसे ऐसे रखा जाना चाहिए जहां इसे क्षतिग्रस्त न किया जा सके.

2. यूएसबी फ्लैश ड्राइव प्राप्त करना

"मुफ्त सामान!" आप शायद यह सोच रहे हैं, और हाँ, संभावित रूप से यह सही है. दुर्भाग्य से, आपके कंप्यूटर पर मालवेयर लोड करने में आपको बेवकूफ़ बनाने के लिए एक मुफ़्त यूएसबी फ्लैश ड्राइव का उपयोग किया जा सकता है.

एक अध्ययन से पता चला है कि लगभग 50 प्रतिशत लोग जो यूएसबी फ्लैश डिवाइस पाते हैं, उन्हें बिना किसी सावधानी के अपने कंप्यूटर में लगा लेते हैं. सुरक्षा विशेषज्ञों को एक यूएसबी फ्लैश ड्राइव की सामग्री की जांच करनी चाहिए. सैंडबॉक्सिंग और विशेष सुरक्षा सॉफ़्टवेयर के साथ सुरक्षित पीसी का उपयोग करना चाहिए, न कि अपने लैपटॉप का.

यदि आप कभी एक अंजान यूएसबी ड्राइव पाते हैं तो ऐसी गलती न करें. आस-पास एक यादृच्छिक यूएसबी ड्राइव ढूंढना आपकी जिज्ञासा पैदा कर सकता है, लेकिन इससे पहले कि आप कुछ भी गलत करें, अपने आप को ऐसा करने से ना रोकें. यह एक गलती आपके लिए बहुत दर्द और अफसोस का कारण बन सकती है.

जबकि कुछ एंटी-वायरस सॉफ़्टवेयर ऑटोरन मालवेयर को आपके पीसी को यूएसबी फ्लैश डिवाइस से संक्रमित करने से बचा सकता है, लेकिन यह तब नहीं हो सकता है जब आपका सिस्टम अद्यतित न हो. इसलिए, यदि आपको एक यूएसबी फ्लैश ड्राइव मिलती है, तो इसे अकेला छोड़ दें, या इसे बिन में रखें. लेकिन इसे प्लग न करें.

3. दोस्त को यूएसबी देना

शायद आपको अभी एक नया यूएसबी फ्लैश डिवाइस प्राप्त हुआ है और आपने फैसला किया है कि आपकी पुरानी यूएसबी स्टिक अब आपके काम की नहीं है. यदि ऐसा है, तो आप इसे बेचने या किसी को देने के बारे में सोच रहे होंगे.

आपको डाटा सुरक्षा के बारे में सोचना चाहिए. क्या आपने डिस्क की अपनी सामग्री हटा दी है? यदि हां, तो डाटा सुरक्षित रूप से हटा दिया गया था? चाहे आप किसी मित्र या अजनबी को डिवाइस दे रहे हों, आपको निश्चित रूप से सामग्री को पूरी तरह से हटाने के लिए समय लेना चाहिए.

4. यूएसबी-विशिष्ट मालवेयर

कुछ मानक ट्रोजन और वॉर्म ऑटो-रनिंग हो सकते हैं और इन्हें आपके पीसी पर सुरक्षा सॉफ़्टवेयर के न होने पर सफलता का एक अच्छा स्तर प्राप्त होगा.

5. अपने यूएसबी स्टिक को जानें

आपके यूएसबी फ्लैश डिवाइस का सुरक्षित भंडारण महत्वपूर्ण है, लेकिन यह केवल एक मान्यता है. अक्सर यूएसबी स्टिक को अलग करना बहुत मुश्किल होता है. जब तक उन्हें विशेष रूप से विचित्र तरह से डिजाइन (लेगो, लकड़ी, आदि) नहीं दिया जाता है, उन्हें आसानी से मिटाना आसान होता है. स्टिकी लेबल लागू करना एक विकल्प है, लेकिन आप उनके लिए विशिष्ट भंडारण क्षेत्र का उपयोग भी कर सकते हैं. अपने व्यक्तिगत ड्राइव को उन ड्राइव से अलग रखें, जिन्हें आप काम के लिए उपयोग करते हैं और किसी अन्य व्यक्ति को सौंपने से पहले हमेशा ड्राइव की सामग्री जांचें.

डेटा लीकआउट वीआईए यूएसबी स्टोरेज कैसे बंद करें?

- यूएसबी स्टोरेज उपकरणों के उपयोग को सीमित करने के लिए एक अच्छी सुरक्षा नीति तैयार करें और अपनाएं.
- कर्मचारियों की निगरानी करें कि वे क्या कॉपी कर रहे हैं.
- अपनी जानकारी को सुरक्षित करने के लिए प्रमाणीकरण और लेखांकन लागू करें.

जब आप डिवाइस खो देते हैं तो क्या करें?

- अगर आपने यूएसबी ड्राइव के अंदर कोई व्यक्तिगत या संवेदनशील जानकारी संग्रहीत की है जैसे पासवर्ड आदि, तो किसी भी खाते के निर्माण के दौरान सुरक्षा प्रश्नों और उत्तरों के साथ तुरंत सभी पासवर्ड बदल दें. संभावना है कि हैकर चोरी ड्राइव के डाटा का उपयोग करके आपका ऑनलाइन खाता लॉगऑन की जानकारी प्राप्त कर सकता है.
- यह भी सुनिश्चित करें कि खोए गए डाटा के खिलाफ सभी सुरक्षा उपाय किए गए हैं.

डिवाइस चोरी को कैसे रोकें?

- हमेशा कुंजी श्रृंखला में टैग करके भौतिक रूप से ड्राइव को सुरक्षित करें.
- कभी भी अपने ड्राइव को कहीं भी न छोड़ें.
- बिना एन्क्रिप्शन के संवेदनशील जानकारी कभी भी न रखें.

जोखिम बनाम रिवार्ड

यह व्यापक रूप से स्वीकार किया जाता है कि हैकर्स अधिक से अधिक परिष्कृत हो रहे हैं. हालांकि, इसका मतलब यह नहीं है कि वे निम्न स्तर के नेटवर्क घुसपैठ के प्रयास नहीं करेंगे, जैसे यूएसबी फ्लैश ड्राइव के साथ बैटिंग. 2016 में बीएसआई (सूचना सुरक्षा के लिए जर्मन कार्यालय) द्वारा पहचाने गए 10 प्रमुख साइबर खतरों में से, यूएसबी उपकरणों का उपयोग दूसरे स्थान पर है.

दुर्भाग्यवश, जब एंटरप्राइज़ सुरक्षा की बात आती है तो कर्मचारी हमेशा से आसान लक्ष्य रहे हैं. यह तार्किक है, कि संगठन कर्मचारियों की लापरवाही के परिणामस्वरूप होने वाली क्षति को कम करने की कोशिश कर रहा हैं. यूएसबी पोर्ट को अक्षम करना हमले को कम करने का सरल उपाय है. यह आवश्यक है कि विक्रेता और उद्यम समाधान खोजने के लिए मिलकर काम करें जो उत्पादकता को प्रभावित किए बिना हर सुरक्षा बैकडोर से हैकर्स को लॉक कर दें.

यूएसबी स्टोरेज डिवाइस का उपयोग करते समय अपनी जानकारी को सुरक्षित रखने के लिए नीचे कुछ युक्तियां दी गई हैं-

यूएसबी स्टोरेज उपकरणों के सुरक्षित उपयोग के लिए क्या करें और क्या न करें

क्या करें:

- पहली बार उपयोग के लिए ड्राइव को हमेशा लो फ़ारमैट करें
- हमेशा ड्राइव को सुरक्षित रूप से सिस्टम से हटाएँ
- एक्सेस करने से पहले नवीनतम एंटीवायरस के साथ हमेशा यूएसबी डिस्क स्कैन करें
- अपने यूएसबी डिवाइस को पासवर्ड से सुरक्षित रखें
- डिवाइस पर फ़ाइलों/फ़ोल्डरों को एन्क्रिप्ट करें
- अपने यूएसबी में डाटा तक पहुंचने या कॉपी करने के लिए यूएसबी सुरक्षा उत्पादों का उपयोग करें
- मॉनीटर करें कि किस डेटा की प्रतिलिपि बनाई जा रही है
- अनधिकृत यूएसबी को कनेक्ट करने से अवरुद्ध करें
- अनुपालन आवश्यकताओं और संगठन की आवश्यकताओं को पूरा करने के लिए डिवाइस को सुविधाओं और सही स्तर के एन्क्रिप्शन के साथ चुनें

क्या न करें:

- अज्ञात सदस्यों से किसी भी प्रचार यूएसबी डिवाइस को स्वीकार न करें
- कार्यालय/शाखा कंप्यूटर के साथ व्यक्तिगत यूएसबी का कभी भी उपयोग न करें
- जब तक आप ऐसा करने के लिए अधिकृत नहीं होते हैं, तब तक यूएसबी पर किसी भी ग्राहक और लेनदेन डेटा की प्रतिलिपि न लें

यूएसबी के रूप में मोबाइल के सुरक्षित उपयोग के लिए क्या करें और क्या न करें

कंप्यूटर से कनेक्ट होने पर मोबाइल फोन यूएसबी मेमोरी डिवाइस के रूप में इस्तेमाल किया जा सकता है. कंप्यूटर से कनेक्ट करने के लिए मोबाइल फोन के साथ एक यूएसबी केबल प्रदान किया जाता है.

क्या करें:

- जब एक मोबाइल फोन किसी व्यक्तिगत कंप्यूटर से कनेक्ट करते हैं, तो एक अद्यतन एंटीवायरस का उपयोग कर बाहरी फोन मेमोरी और मेमोरी कार्ड को स्कैन करें
- अपने फोन और बाहरी मेमोरी कार्ड का नियमित बैकअप लें क्योंकि यदि सिस्टम क्रैश या मालवेयर प्रवेश जैसी कोई घटना होती है, तो कम से कम आपका डाटा सुरक्षित रहे.
- कंप्यूटर से डाटा को मोबाइल में स्थानांतरित करने से पहले, डाटा को सभी अपडेट के साथ नवीनतम एंटीवायरस के साथ स्कैन किया जाना चाहिए
- दूर जाने से पहले अपने कंप्यूटर से यूएसबी कनेक्शन को हटाना याद रखें

क्या न करें:

- अपने मोबाइल को कार्यालय कंप्यूटर से कभी कनेक्ट न करें.

वेब ब्राउज़र का सुरक्षित उपयोग

नाज़िया सिद्दीकी
सहायक प्रबंधक
सीसो कार्यालय, केंद्रीय कार्यालय, मुंबई

वैश्विक कंप्यूटर नेटवर्क (WWW) हमें विभिन्न संचार और जानकारियों को आदान-प्रदान करने की सुविधा प्रदान करता है. वेब ब्राउज़र एक प्रोग्राम है, जो हमें इन्टरनेट के उपयोग से वेब साइट तक पहुंचाता है.

इंटरनेट ब्राउज़र का मुख्य उद्देश्य उपयोगकर्ता के उपकरण में जानकरियां प्रदर्शित करना है. यह प्रक्रिया उपयोगकर्ता द्वारा यूआरएल लिखने से शुरू होती है, जो शुरू होता है http या https से, जो भी संचार ब्राउज़र और वेब सर्वर के बीच में होता है वह अधिक सुरक्षा और गोपनीयता के लिए **एन्क्रिप्टेड** होता है. एक अन्य यूआरएल (URL) उपसर्ग फाइल है, जिसका उपयोग स्थानीय फाइलों को प्रदर्शित करने के लिए किया जाता है, जो पहले से ही उपयोगकर्ता के सिस्टम पर मौजूद है. वेबसाइट में आमतौर पर हाईपरलिंक होते हैं, जो अन्य साइटों और संसाधनों को ढूंढने में मदद करते हैं. प्रत्येक लिंक में एक यूआरएल शामिल होता है और जब इस पर क्लिक किया जाता है, तो ब्राऊजर, नेविगेट कर एक नये संसाधन की ओर ले जाता है. सभी प्रमुख ब्राउज़र, उपयोगकर्ता के कई पन्नों को एक ही समय में खोलने की सुविधा देते हैं या तो अलग-अलग ब्राउज़र विंडो में या अलग-अलग टैब एक ही विंडो में.

कुछ प्रमुख वेब ब्राउज़र के नाम हैं, गूगल, क्रोम, फायरफॉक्स, इंटरनेट एक्सप्लोरर, ओपेरा, सफारी आदि. हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल (HTTP) वेब की आम भाषा है और सभी ब्राउजरों द्वारा समर्थित है. कई ब्राउज़र सेक्योर सॉकेट लेयर (SSL) इस्तेमाल करते हैं. SSL एक विशेष प्रोटोकॉल है, जो खरीदने और बेचने में और लेन-देन के काम में सुरक्षा देता है. वेब का उपयोग करके ऑनलाइन बिल भुगतान, शॉपिंग, भुगतान सेवाओं, इंटरनेट बैंकिंग और मोबाइल बैंकिंग की सुविधा का उपयोग किया जा सकता है. प्रत्येक नागरिक के लिए महत्वपूर्ण है कि वह इंटरनेट का उपयोग सुरक्षित रूप से करे. आज इंटरनेट पर विभिन्न प्रकार के साइबर अपराध और धोखाधड़ी होते हैं. यहां तक कि बहुत बार बड़ी कंपनियों, बैंकों सरकारी बेबसाइटों की जानकारियां लीक हुई हैं. इंटरनेट सुरक्षा का महत्व ऑनलाइन लेनदेन और डिजिटल पर्स का उपयोग

करते समय और अधिक हो जाता है. विशेष रूप से बच्चों, किशोरों, कंप्यूटर की कम समझ रखने वाले लोगों के साथ अधिक धोखा हो रहा है.

इंटरनेट सुरक्षा का महत्व ऑनलाइन बैंकिंग सेवाओं और ख़रीदारी करते समय अधिक है. कदाचित सम्मानित साइटों में स्पाइवेयर जाल शामिल किए जा सकते हैं या फिशिंग साइट्स आपको लुभाके, आपको गुमराह कर सकती हैं और जरूरी डाटा भी हासिल कर सकती हैं. जब भी आप अपना वेब ब्राउज़र खोलकर ब्राउजिंग शुरू करते हैं तब आप एक साइट पर जाते हैं और अनजाने में ही स्पाइवेयर जाल में फंस सकते हैं, जैसे कोई पॉप-अप पर क्लिक करके. कभी-कभी बस एक वेब पेज या एक HTML ईमेल खोलने पर इन्स्टालेशन शुरू कर देता है. स्पाइवेयर हमारी जानकारी के बिना मशीन पर चालू हो जाता है अतः यह हमारी व्यक्तिगत जानकारी हासिल कर हमें एक बड़ी चुनौती दे सकता है. अपने कंप्यूटर की सुरक्षा करने और स्पाइवेयर से बचने के लिए कुछ इंटरनेट सुरक्षा युक्तियां इस्तेमाल की जानी चाहिए. सबसे पहले संदिग्ध वेबसाइटों से बचें. सॉफ्टवेयर केवल भरोसेमंद साइटों से ही डाउनलोड करें.

यदि आप अनिश्चित हैं, तो इसे डाउन लोड या फिक्स न करें. फाइल शेयरिंग साइटों और torrenting से बचने हेतु, ब्लॉग पोस्ट पर उनकी समीक्षा देख लें, क्योंकि इसमें आपके कंप्यूटर से समझौता करने की क्षमता है. इन फाइलों में हो सकता है कि फिल्म, सॉफ्टवेयर या कुछ वाणिज्यिक कॉपीराइट मूल्य की फाइलें हों. मालवेयर एक ऐसा सॉफ्टवेयर है, जो किसी भी व्यक्ति को किसी दूसरे के कंप्यूटर में आसानी से नियंत्रण हासिल करने में मदद करता है. जैसे ही अपडेट आए शीघ्र ही अपने ऑपरेटिंग सिस्टम और सॉफ्टवेयर अद्यतन करें. कुछ कार्यक्रम बिना अनुमति के आटोमैटिक ही अद्यतन करते हैं, लेकिन कई ऑपरेटिंग सिस्टम और आवेदन (अप्लीकेशन) पहले पूछते हैं. कई लोग कभी इसे अद्यतन नहीं करते हैं. यह एक समस्या है. जब हैकर्स को पता चलता है कि वहां सुरक्षा भेद्यता है तो वे इसका लाभ उठाने की कोशिश करने लगते हैं. जितना ज्यादा वक्त आप अद्यतन करने में लगाते हैं, उतना अधिक जोखिम बढ़ता है. अपने ब्राउजर की सुरक्षा सेटिंग्स बढ़ाएं, वे एक्सटेंशन का समर्थन करते हैं, जिससे आप अपने ब्राउजर में, ऑपरेशन के तरीकों को भिन्न तरीके से इस्तेमाल कर सकते हैं. किसी भी कंपनी के विश्वसनीय यूआरएल का इस्तेमाल अपने ब्राउजर के पता पट्टी में फिर से टाइप कर करें, इससे आप ईमेल में आए लिंक को बाय पास कर सकते हैं. खरीदारी के लिए सम्मानित साइटों का उपयोग करें. ज़्यादातर ब्रांड जैसेः ई-कामर्स साइटों अमेज़न के पास अच्छी सुरक्षा प्रणालियां हैं, जो अगर कुछ गलत हो जाता है तो पैसे वापस कर देते हैं. स्कैमर्स (scammers) से बचने के लिए रेटिंग और ग्राहक की समीक्षा की जांच करें. कोई भी ख़रीदारी करने से अपने घर और व्यापार के उपकरणों में पहले सबसे अच्छी सुरक्षा वाले सॉफ्टवेयर उत्पादों का इस्तेमाल सुनिश्चित करें.

एंटीवायरस सुरक्षा और फायरवॉल का उपयोग करें. एंटीस्पाईवेयर (antispyware) सॉफ्टवेयर संरक्षण का इस्तेमाल करें और सदा अपनी स्क्रीन लॉक रखें. इंटरनेट लापरवाही के लिए एक खतरनाक जगह हो सकती है. किसी भी गलत वेबसाइट पर जाने से आपका कंप्यूटर दुर्भावनापूर्ण सॉफ्टवेयर से संक्रमित हो सकता है, जो आपके डाटा की चोरी करके आपसे फिरौती की मांग कर सकता है.

सामाजिक रूप से हैकर्स द्वारा ब्राउज़र में इस्तेमाल किए जाने वाले दो सबसे आसान तरीके हैं **इंजीनियर मालवेयर और फिशिंग** और लगभग एक तिहाई इंटरनेट उपयोगकर्ता, इंजीनियर, मालवेयर का शिकार हुए हैं. धोखे कई तरह से दिए जा सकते हैं. उदाहरण के लिए, संक्रमित वेबसाइट के लिंक्स. इसका इस्तेमाल करते समय ये आपके मशीनों में दुर्भावनापूर्ण सॉफ्टवेयर डाल सकते हैं. इस तरह के सॉफ्टवेयर आपके विवेक से समझौता कर सकते हैं या हार्डवेयर को नुकसान पहुंचा सकते हैं या संवेदनशील जानकारी की चोरी कर सकते हैं. रैनसमवेअर (Ransomware) इसी तरह से वितरित किया जाता है. मैलवेयर के इस फार्म की वृद्धि पिछले 12 महीनों में हुई है. यह एक संक्रमित कंप्यूटर पर डाटा को **एन्क्रिप्ट** करके फिरौती की मांग करते हैं. फिशिंग का इस्तेमाल संवेदनशील डेटा पाने के लिए किया जाता है. उदाहरण के लिए, आपको बैंक से अपने खाते में यूज़र नेम और पासवर्ड का उपयोग करने के लिए ईमेल प्राप्त होता है, केवल फर्क इतना है कि यह ईमेल बैंक से नहीं है, बल्कि हैकर्स ने किया है और अगले ही पल बैंक खाता खाली हो जाता है. प्रमुख ब्राउजर, इंजीनियरिंग मालवेयर और फिशिंग के खिलाफ सुरक्षा देते हैं. हालांकि दूसरों की तुलना में, कुछ वेब ब्राउज़र अधिक सुरक्षा देते हैं जैसे कि माइक्रोसॉफ्ट एज़ में एक प्रौद्योगिकी है, स्मार्ट स्क्रीन यूआरएल और अप्लीकेशन रेपूटेशन फिल्टरिंग, जो किसी भी यूआरएल (URL) को डाउनलोड की अनुमति देने से पहले उसे इंस्टाल करती है. यदि वेबसाइट की प्रतिष्ठा समुचित नहीं है तो एक चेतावनी मिलेगी. आप भी ब्राउजर अधिक सुरक्षित बना सकते हैं, उदाहरण के लिए, उसके सेटिंग्स मेनू में जाकर आप ब्राउजर की ऑटो फिल सुविधाओं को बंद कर सकते हैं, जो स्वचालित रूप से पासवर्ड के साथ फार्म भरता है और हैंकिंग में सहायता करता है. दूसरी तरफ, फॉर्म को मैनुअल भरना, एक बोझ हो सकता है. कुकीज़ को बंद रखके आप अपनी गोपनीयता को बढ़ा सकते हैं, लेकिन इसके कारण बहुत सी वेबसाइट को आप इस्तेमाल नहीं कर पाएंगें, क्योंकि उसमें कुकीज़ सक्षम है. एक विकल्प का प्रयोग निश्चित रूप से करना चाहिए और वह है ब्लॉक पॉप-अप विंडों, जो अनचाहे विज्ञापनों को न दिखने में मदद करता है.

फिशिंग ईमेल कभी भी आपके नाम पर नहीं आता है और वो किसी अंजान व्यक्ति से आता है, जो हमारी व्यक्तिगत जानकारी हासिल करने की कोशिश में रहता है. साइट विश्वसनीय है कि नहीं यह पहचान करने का एक तरीका है कि उसकी वर्तनी या व्याकरण की गलतियों को पहचानें. एक अन्य तरीका है कि आपके ब्राऊजर के एड्रेस

बार में, हरे रंग के ताले के संकेत का रहना. इसका यह मतलब होता है कि आपके और साइट के बीच की जानकारी एन्क्रिप्टेड है.

एक अच्छा **पासवर्ड प्रबंधक** चुनना सुरक्षित सर्फिंग के लिए लगभग आवश्यक हो गया है. विशेष रूप से ब्राउजर में पासवर्ड याद रखें और रूपों को भरने के विकल्प बंद करने के बाद. यह आपको हर वेबसाइट के लिए अनूठा और सुरक्षित पासवर्ड बनाने की अनुमति देता है. पासवर्ड को बनाना भी कम थका देने वाला नहीं है. आपका यह काम भी, पासवर्ड मैनेजर ऑटोमेट कर सकता है. बस आपको पासवर्ड मैनेजर को एक सुरक्षित पासवर्ड बनाने को कहना है और चुटकी बजाते ही आपका काम हो जाएगा. वीपीएन सेवा आपके कनेक्शन में, डेटा एन्क्रिप्ट कर, आपके कनेक्शन को सुरक्षित करती है और आपके डेटा को हाइड करके आपके प्राइवेसी का भी ध्यान रखती है. यह सेवा खास तौर पर तब लाभदायक साबित होती हैं, जब आप असुरक्षित वाईफ़ाई से कनेक्टेड होते हैं. ऐसे में यह आपकी आइडेंटिटी छुपा देती है. कोई भी आपके ऑनलाइन मूवमेंट ट्रैक नहीं कर सकता फिर चाहे वो आपकी सरकार ही क्यों न हो.

जब भी संभव हो आपको दो फैक्टर **आथेंटिकेशन** का प्रयोग करना है. जैसेकि बैंक आपको ओटीपी (वन टाइम पासवर्ड) या ईमेल भेजेगा. पर यह दो टाइम पासवर्ड ऑटोमैटिक नहीं है. आपको अपना सेल फोन नंबर अपने बैंक में देना होगा, तभी आपकी यह सेवा चालू होगी. गूगल और फेसबुक के लिए आप अपने डेटा को बैक-अप कर सकते हैं, जो आपके लिए किसी आपातकालीन परिस्थिति में लाभदायक होगा. जैसे कि आप अपने कंप्यूटर से किसी एक्सटर्नल हार्ड डिस्क, यूएसबी से कनेक्ट होने वाले एक्सटर्नल डिस्क में यह बैकअप ले जाते हैं. आजकल तो ज्यादातर लोग क्लाउड बैकअप का इस्तेमाल कर रहे हैं. क्लाउड बैक-अप्स एक सुरक्षित तरीका है, जिससे आप अपने डेटा को इंटरनेट की सहायता से ट्रांसफर कर सकते हैं जैसे कि ड्रॉपबॉक्स सेवा. बढ़ते इंटरनेट और सोशल मीडिया उपयोग के कारण, साइबर सुरक्षा पहले के मुक़ाबले और भी जरूरी हो गयी है. बढ़ते साइबर जुर्म जैसे डेटा थेफ्ट, फ़िशिंग और कई अन्य साइबर अपराधों के कारण ग्राहक को और भी सावधान रहने की आवश्यकता है. इंटरनेट की दुनिया में विभिन्न प्रकार के जोखिम और कमजोरियां होती हैं. हमें इस बात का ध्यान रखना चाहिए क्योंकि गैर-कानूनी एक्टिविटी साइबर अपराध भी बन सकता है. सभी ग्राहकों को, किसी भी ऑनलाइन मीडिया को इंटरनेट से कनेक्ट करने से पहले इन बातों का ध्यान रखना चाहिए, किसी और ग्राहक से कोई इन्फार्मेशन शेयर करने से पहले भी दो बार सोच लेना चाहिए.

इंटरनेट बैंकिंग बनाम साइबर सुरक्षा

सुनील कुमार वर्मा
सहायक प्रबंधक
जूनागढ़ शाखा

बी पी शर्मा
मुख्य प्रबंधक
स्टाफ प्रशिक्षण केंद्र भोपाल

इंटरनेट बैंकिंग से बैंकिंग उद्योग में एक व्यापक बदलाव आया है. इसके चलते, बैंकिंग अब केवल शाखाओं तक सीमित नहीं रह गयी है और न ही ग्राहकों को आज शाखा में जाने की आवश्यकता ही रह गयी है. ग्राहक को कहीं पैसा भेजने या खाते का विवरण आदि मंगवाने के लिए शाखा से संपर्क करने की आवश्यकता नहीं है. वह अपने खाते की, किसी भी तरह की पूछताछ एवं विवरणिका, नेट बैंकिंग से अपने कंप्यूटर अथवा मोबाइल अथवा टैब से प्राप्त कर सकता है. कई विकसित देशों में, "नेटबैंकिंग" एक विशेष सेवा नहीं, बल्कि सामान्य एवं आवश्यक बैंकिंग सेवा मानी जाने लगी है और यह बैंकिंग सेवाएं प्रदान करने का **सस्ता साधन** भी है. इंटरनेट बैंकिंग के चलते पहले शाखा में किये जाने वाले लगभग सारे कार्य इंटरनेट बैंकिंग के माध्यम से आसानी से घर बैठे अथवा अपनी सुविधा से, कहीं भी और कभी भी कर पाना संभव हो जाता है, फिर भी इंटनरेट बैंकिंग संबंधी कुछ विशेषताओं को यहाँ जान लेना आवश्यक होगा.

इंटरनेट बैंकिंग की विशेषताएं

इंटरनेट बैंकिंग एक साधन है, जिससे ग्राहक अपने बैंक खातों में किसी भी स्थान से इंटरनेट के माध्यम से अपने समस्त लेन-देन कर सकता है, बिलों का भुगतान कर सकता है, मियादी जमाएं बना सकता है, उन्हें बंद भी कर सकता है. इसके साथ ही खाते का विवरण प्राप्त करना, दूसरे बैंक खातों में अंतरण करना, मोबाइल रिचार्ज करना, पीपीएफ एवं एनपीएस खातों में धन अंतरण करना, विभिन्न सरकारी योजनाओं हेतु आवेदन करना, आईपीओ हेतु आवेदन करना, म्युचुअल फंड में निवेश एवं एसआईपी करना आदि कई सुविधाओं का लाभ भी इंटरनेट बैंकिंग उपयोगकर्ता को प्राप्त है. यह जानना बहुत रोचक है कि इंटरनेट बैंकिंग के माध्यम से, बैंकिंग उद्योग द्वारा करोड़ों रुपये का व्यय एवं मानव संसाधन प्रति वर्ष बचाया जाता है.

प्रति व्यक्ति प्रति संव्यवहार पर आने वाली लागत में इंटरनेट बैंकिंग एवं डिजिटल सुविधाओं के विकास से बहुत तेजी आई है और भविष्य में, इंटरनेट उपयोगकर्ताओं की संख्या में वृद्धि होने की स्थिति में, यह लागत और भी कम हो जाएगी. ऐसे में, देश के समस्त बैंक खातों को इंटरनेट बैंकिंग से जोड़ना संभव हो जाएगा. जन धन योजना के अंतर्गत खोले गये खाते भी इंटरनेट बैंकिंग से जुड़ जाएंगें. ऐसे में बैंकिंग सुविधाओं का व्यापक आधार पर विस्तार किया जा सकेगा.

इंटरनेट बैंकिंग द्वारा दी जाने वाली सुविधाएं : इंटरनेट बैंकिंग वर्तमान समय में सभी बैंकों (सरकारी व निजी) द्वारा दी जाने वाली एक बहुत ही लाभप्रद सुविधा है. इंटरनेट बैंकिंग द्वारा सामान्यतः निम्नलिखित सेवाएं ग्राहकों को प्रदान की जाती हैं :

- किसी भी व्यक्ति तथा किसी भी बैंक खाते से धन का ट्रान्सफर.
- सरकारी योजनाएं जैसे पीपीएफ़, एसएसए, सुकन्या समृद्धि योजना, अटल पेंशन योजना आदि के लिए ऑनलाइन आवेदन.
- इनकम टैक्स भुगतान एवं टीडीएस की जानकारी.
- आधार लिंक, मोबाइल बैंकिंग पंजीकरण, प्रधानमंत्री बीमा योजना, ऑनलाइन एफ़डी बनाना तथा एफ़डी बंद करना जैसी सुविधाएं इंटरनेट बैंकिंग पर उपलब्ध हैं.
- आईपीओ में आवेदन.
- ऑनलाइन शॉपिंग करते समय भुगतान.
- ऋण खातों की अद्यतन जानकारी.
- मोबाइल रिचार्ज, बिजली बिल, टेलीफोन बिल आदि जैसी रोजमर्रा की जरुरतों से संबंधित बिल का भुगतान आदि.

इसके अलावा भी बैंकों द्वारा कई अन्य सुविधाएं इंटरनेट बैंकिंग के माध्यम से ग्राहकों को प्रदान की जाती हैं.

क्या इंटरनेट बैंकिंग सुरक्षित है?

इंटरनेट बैंकिंग का प्रयोग करने वाले के मन में अक्सर यह खयाल आता है कि क्या इंटरनेट बैंकिंग सुरक्षित है? तो इसका जवाब है "हां".इंटरनेट बैंकिंग पूरी तरह से सुरक्षित है, बस आज के मौजूदा दौर में, जहां साइबर क्राइम की घटनाएं दिन-प्रतिदिन बढ़ती जा रही हैं, हमें थोड़ी सावधानी बरतने की आवश्यकता होती है. इसके लिए, हमें निम्नलिखित कुछ महत्वपूर्ण सावधानियों पर ध्यान रखना चाहिए.

1 अपने यूज़र नेम व पासवर्ड को गुप्त रखना चाहिए और किसी को भी इसकी जानकारी नहीं देनी चाहिए.

2 फोन पर प्राप्त ओटीपी या उससे संबंधित अन्य कोई जानकारी किसी को नहीं देनी चाहिए.

3 यहां यह कहना उल्लेखनीय है कि बैंक आपके खाते से जुड़ी कोई भी जानकारी टेलीफोन अथवा मोबाइल पर नहीं मांगता है. यह ध्यान रखें कि किसी भी व्यक्ति, चाहे बातचीत से वह बैंक का कर्मचारी ही क्यों न प्रतीत होता हो, कोई व्यक्तिगत जानकारी नहीं प्रदान करनी चाहिए.

साइबर सुरक्षा

कहा यह जाता है कि जितनी अधिक सुविधा होती है, उससे जुड़े हुए खतरे भी उतने ही अधिक हो जाते हैं. ऐसे में, इंटरनेट बैंकिंग से जुड़ी हुई कई सुरक्षा संबंधी कठिनाइयाँ व चुनौतियाँ भी हैं. इलेक्ट्रानिक बैंकिंग के इतने अधिक लाभ होते हुए भी सुरक्षा का मुद्दा महत्वपूर्ण है, इसलिए बैंकों को सुरक्षित लेन-देन की प्रणाली अपनानी पड़ेगी, जिससे ग्राहकों का विश्वास बढ़े और उन्हें अच्छी से अच्छी सुविधा प्रदान की जा सके. इंटरनेट बैंकिंग काफी सुविधाजनक है लेकिन साइबर संबंधी कुछ समस्याएं भी हैं, जिसकी वजह से कुछ ग्राहक इसके उपयोग में हिचकिचाते हैं. इसमें भी दो राय नहीं कि आनलाइन बैंकिंग लेन-देन को निशाना बनाने वाले एप्लिकेशन और धोखाधड़ी वाले संदेशों की संख्या में लगातार वृद्धि हो रही है, जो बैंकिंग उद्योग के लिए न केवल चिंता का विषय है बल्कि इससे निजात पाना उनके समक्ष एक बड़ी चुनौती है.

इंटरनेट बैंकिंग में सुरक्षा की चुनौतियाँ

ग्राहक के विषय में महत्वपूर्ण सूचना, जो गोपनीय रहनी चाहिए, उसे अनधिकृत व्यक्ति को खुलासा करने से वित्तीय संस्थान को गंभीर हानि उठानी पड़ सकती है. कोई भी एक सुरक्षा उपाय या उपकरण सार्वजनिक नेटवर्क प्रणाली को सुरक्षित नहीं कर सकता और लेन-देन में सुरक्षा की समस्या की वजह से क्लाइंट एवं सर्वर के बीच में असुरक्षित डाटा का आदान-प्रदान हो जाता है. नेटवर्क प्रणाली की समस्या संचार तंत्र और कंप्यूटर में निहित है. इसलिए आज सुरक्षा के मुख्य बिंदु सेशन लेयर प्रोटोकॉल और एंड टू एंड कम्प्यूटिंग की कमियों पर ज़ोर दिया जा रहा है क्योंकि अभी भी ट्रस्टेड चैनल उपलब्ध नहीं हैं.

ई बैंकिंग में आक्रमण एवं जोखिम निम्नानुसार हैं:

सोशल इंजीनियरिंग-

इसमें किसी भी तरह के कंप्यूटर सिस्टम की जानकारी आवश्यक नहीं है. हमलाकर्ता द्वारा ग्राहक सेवा अधिकारी या सिस्टम एडमिनिस्ट्रेटर बनकर ग्राहक से संवेदनशील जानकारी प्राप्त करने की कोशिश को सोशल इंजीनियरिंग कहा जाता है. इससे उपयोगकर्ता के व्यक्तिगत खातों में लेन-देन किया जा सकता है.

ई मेल बम :

यह एक परेशान करने वाला हथियार है. ई-मेल बम हजारों संदेशों की एक श्रृंखला है, जो मेल बॉक्स में भेजी जाती है. हमलावर का उद्देश्य मेल बॉक्स को जंक मेल से भरने का रहता है.

पोर्ट स्कैनर :

इसमें आक्रमणकारी कम्प्यूटर के ऐंट्री पाइंट में पोर्ट स्कैनर लगाकर सूचनाओं की चोरी करते हैं. यह एक साफ्टवेयर के माध्यम से किया जाता है, जो कि मशीन या राउटर के संकेत या संदेश को रिकार्ड करके हार्डवेयर एवं साफ्टवेयर से गोपनीय सूचनाएं एकत्रित करता है, जिससे सिस्टम पर आक्रमण की योजना बनाई जा सकती है.

पैकेट स्निफर्स :

यह उपयोगकर्ता के कम्प्यूटर और वेब सर्वर के कनेक्शन में, पैकेट को पहचानकर क्रेडिट कार्ड, पासवर्ड अथवा अन्य सूचनाओं का डाटा एकत्र कर लेता है. पैकेट स्निफर का पता लगाना मुश्किल रहता है क्योंकि ये नेटवर्क ट्राफिक पर कब्जा करके सूचना निकालते हैं, लेकिन डाटा के प्रवाह को नहीं छेड़ते हैं. **सेक्योर सॉकेट लेयर कनेक्शन, पैकेट स्निफर** के आक्रमण से बचने के लिए सबसे अच्छा तरीका है.

पासवर्ड की चोरी :

इसका व्यापक अर्थ में प्रयोग पासवर्ड को इलेक्ट्रानिक आधार पर चुराने तथा अन्य तरीकों से उसकी जानकारी हासिल करने से है. पासवर्ड चोरी का सबसे "कुख्यात" तरीका है ब्रूट फोर्स प्रयास. इसमें किसी व्यक्ति के यूजर नेम एवं पासवर्ड की हजारों सामान्य शब्द, नाम, शब्द समूह आदि से तब तक खोज करते हैं जब तक सही संयोजन न मिल जाए. "ब्रूट फोर्स" ऐसे सिस्टम से लाभ उठाता है, जिसमें सशक्त पासवर्ड की जरूरत नहीं होती है. पासवर्ड चोरी की अन्य तकनीक है हैश टेबल. इसमें पासवर्ड फाइल को डीकोड करके सिस्टम में उपलब्ध यूजर नेम एवं पासवर्ड की सूची निकाली जाती है.

ट्रोज़न :

इंटरनेट बैंकिंग में ट्रोज़न सॉफ्टवेयर को सुरक्षा के लिए सबसे अधिक नुकसानदेह माना जाता है क्योंकि ये गुप्त तरीके से जुड़कर गोपनीय सूचना बाहर भेजते हैं. ट्रोज़न का उपयोग विभिन्न क्लाइंट सर्वर, डाटाबेस सिस्टम से डाटा फिल्टर करने के काम में आता है. ट्रोज़न ई-मेल संदेश, डाटा संचार या किसी भी अन्य माध्यम से अनधिकृत रुप से इंस्टाल किया जा सकता है.

डिनायल ऑफ सर्विस अटैक :

यह वाइरस सर्वर को ओवरलोड कर देता है, जिससे वह अनुपयोगी हो जाता है. इसमें सर्वर बार-बार ऐसा कार्य करने के लिए कहता है, जिसमें अधिक डाटा का उपयोग हो. इस वायरस का उपयोग एक प्रतिस्पर्धी दूसरे ई-कामर्स की साइट पर आक्रमण करने के काम आता है और उस साइट के सुरक्षा उपायों को निष्क्रिय कर देता है. एक बार सर्वर डाउन होने पर यह डाटा बेस और यूज़र सिस्टम में सेंध लगाता है.

सर्वर बग्स :

यह अधिकांशतः समयबद्ध तरीके से पैच न डालने से संबंधित है, जिससे हमलाकर्ता को मौका मिल जाता है, जो ई-बैंकिंग वेबसाइट के लिए खतरा है. कुछ "सिस्टम एडमिनिस्ट्रेटर" नये अपडेट डालने में सुस्ती दिखाते हैं, जिससे आक्रमणकारी को हमला करने का समय मिल जाता है. विश्व में हजारों वेब सर्वर ऐसे हैं, जिनमें समय से पैच नहीं डाला जाता है.

होल्स :

होल एक तरह की हार्डवेयर, सॉफ्टवेयर या नीतिगत खराबी है, जिससे हमलावर को सिस्टम में अनधिकृत प्रवेश का मौका मिल जाता है. होल्स राउटर, क्लाइंट और सर्वर सॉफ्टवेयर, ऑपरेटिंग सिस्टम और फ़ायरवॉल में हो सकते हैं.

सुपर यूज़र एक्सप्लाइट

यह हमलावार को सिस्टम का नियंत्रण दे देते हैं, जैसे वह खुद उसके एडमिनिस्ट्रेटर हों. ये ऐसी स्क्रिप्ट का उपयोग करते हैं, जो डाटा में हेरफेर करते हैं तथा पूरे सिस्टम को अपने नियंत्रण में ले लेते हैं. यह डिनायल ऑफ सर्विस अटैक जैसा ही है.

बैंकों द्वारा अपनाए जाने वाले सुरक्षा उपाय :

1. **ऑथेंटिकेशन तकनीक :** यह उपयोगकर्ता की पहचान सत्यापित करता है. जैसे पासवर्ड, पिन के अतिरिक्त निम्न ऑथेंटिकेशन के साधन हैं.

   - **टोकन** - एक छोटा हस्तचालित कार्ड मशीन जैसा है, जिससे पासवर्ड बनाते हैं, टोकन को जागृत करने के लिए पिन आवश्यक है.
   - **स्मार्ट कार्ड** - यह क्रेडिट कार्ड जैसा है, जिसमें चिप होती है, चिप में प्रोसेसर, ऑपरेटिंग सिस्टम, रोम और रेम शामिल है. यह एक बार में उपयोग हेतु पासवर्ड उत्पन्न करती है, इसके लिए स्मार्ट कार्ड रीडर आवश्यक है.
   - **बायो मैट्रिक्स** - व्यक्ति की पहचान भौतिक लक्षण, जैसे ऊँगली के निशान, हथेली, आँख की पुतली से की जाती है.

2. **फ़ायरवॉल :** आन्तरिक नेटवर्क और बाहरी दुनिया के बीच, रक्षक का कार्य फ़ायरवॉल करती है अन्यथा आन्तरिक नेटवर्क खुल जायेगा. फ़ायरवॉल अंदर आने वाले और बाहर जाने वाले, पैकेट डाटा का परीक्षण करती है कि उसे नेटवर्क में अनुमति प्रदान कर सकते हैं कि नहीं.

   - **पैकेट फ़िल्टरिंग राऊटर** - यह फ़ायरवॉल का सरल रूप है, जो आन्तरिक नेटवर्क और आन्तरिक गेटवे को जोड़ता है.
   - **प्रॉक्सी सर्वर्स** - प्रॉक्सी सर्वर, नेटवर्क में आने और जानेवाले डाटा को, विशिष्ट प्रॉक्सी प्रोग्राम कार्यान्वित कर नियंत्रित करता है.

2. **क्रिप्टोग्राफ़ी :** ऐसी प्रक्रिया है, जिससे एक संदेश को 'की' (चाबी) के माध्यम से, इस तरह से प्रस्तुत करना कि उसका विषय पता न चले, को क्रिप्टोग्राफ़ी या कोडीकरण कहते हैं. पुनः मूल सन्देश को प्रस्तुत करने को, डिकोडीकरण कहते हैं. इसमें दो 'की' का उपयोग होता है, प्राइवेट 'की' और पब्लिक 'की'.

3. **डिजिटल हस्ताक्षर और प्रमाणीकरण :**

   - **डिजिटल हस्ताक्षर**, 'की' के माध्यम से प्रेषक की पहचान को प्रमाणित करते हैं.
   - **डिजिटल प्रमाणपत्र** से प्रमाणीकरण, अनधिकृत सन्देश को अस्वीकार करना, डाटा की गोपनीयता और क्रिप्टोग्राफी 'की' मैनेजमेंट, आदि मुद्दों का समाधान किया जाता है.

- **सिक्योर सोकेट लेयर (SSL)** - टी सी पी के उपयोग से, एंड टू एंड भरोसेमंद और सुरक्षित सेवा प्रदान की जा सकती है. सर्वर पासवर्ड /पिन/ डिजिटल प्रमाणपत्र से क्लाइंट को प्रमाणित करते हैं. एक बार क्लाइंट और सर्वर द्वारा एक दूसरे को प्रमाणित करने के बाद, सन्देश का कोडीकरण करते हैं.

5. **पब्लिक 'की' (key) संरचना (PKI) :** गोपनीयता, प्रमाणीकरण, डिजिटल हस्ताक्षर तथा सम्पूर्णता प्रदान करने में पब्लिक 'की' महत्वपूर्ण है. दो तरह की 'की' उपयोग करते हैं. पब्लिक ' की'जो सबको ज्ञात रहती है और प्राइवेट 'की' जो केवल मालिक के पास रहती है. सन्देश के जनक की पहचान, प्राइवेट 'की' के मालिक से खोजी जा सकती है.

6. **टूल्स :** टूल्स नेटवर्क सिस्टम और उपयोगकर्ता के अनुश्रवण एवं नियंत्रण बहुत उपयोगी हैं. कुछ टूल्स हैं स्कैनर, स्निफर, लॉगिंग(IDS) और ऑडिट टूल्स NIDS.

   - स्कैनर टी सी पी/आई पी सुरक्षा की जांच करता है और नेटवर्क में, निहित किसी भी कमजोरी को दर्शाता है
   - स्निफर नेटवर्क पैकेट, ट्रैफिक के धीमे चलने या अन्य समस्या का पता लगाता है.
   - घुसपैठ पकड़ उपकरण (IDS)- यह उपकरण, ऐसी घुसपैठ (लॉगिंग) के प्रयास या खतरे का पता लगाता है, जो अनधिकृत प्रवेश कर सिस्टम को अस्थिर और अनुपयोगी बनाता है.
   - नेटवर्क आधारित घुसपैठ पकड़ उपकरण (NIDS)- यह नेटवर्क ट्रैफिक में, संदिग्ध गतिविधियों के तरीके को देखकर, हमले का पता लगाता है.

7. **भौतिक सुरक्षा :** भौतिक सुरक्षा के बिना सूचना सुरक्षा, सॉफ्टवेयर सुरक्षा, उपयोगकर्ता पहुंच सुरक्षा और नेटवर्क सुरक्षा मुश्किल है. इसमें मजबूत भवन निर्माण, आकस्मिक आपदा प्रबंधन, सुचारू विद्युत आपूर्ति, तापमान नियंत्रण और अनधिकृत प्रवेश नियंत्रण शामिल है.

ग्राहक द्वारा अपनाने वाले सुरक्षा उपाय :

- सशक्त पासवर्ड रखना और नियमित रूप से बदलना
- सार्वजनिक कंप्यूटर का उपयोग न करना
- पासवर्ड/पिन/गोपनीय सूचना किसी से साझा न करना

- अपने खाते की नियमित जाँच करना
- खाते के एस एम एस अलर्ट देखना
- लाइसेंसी एंटी वायरस सॉफ्टवेयर का उपयोग करना
- इन्टरनेट बैंकिंग का https/यूआरएल उपयोग करना
- उपयोग के बाद कंप्यूटर का नेट कनेक्शन विच्छेद करना

आधुनिक बैंकिंग में, ऐसे हमलों से सुरक्षा के लिए, सबसे अच्छा रास्ता है साइबर शिक्षा, व्यक्तिगत फायरवाल, सेक्योर साकेट लेयर और सर्वर फायरवाल.

एक बहु स्तरीय ढाँचा, जिसमें फायरवाल फिल्टरिंग राउटर, कोडिकरण और डिजिटल प्रमाणीकरण ग्राहक की सूचना की किसी भी अनधिकृत पहुंच से सुरक्षा को सुनिश्चित करता है. कम से कम, दो फैक्टर ऑथेंटिकेशन को लागू किया जाना चाहिए. पहला ऑथेंटिकेशन कारक पासवर्ड हो सकता है, दूसरा कारक ओटीपी हो सकता है. हॉलाकि बेहतर सुरक्षा के लिए, तीन कारक ऑथेंटिकेशन प्रक्रिया अपनानी चाहिए. तीसरा कारक बायोमेट्रिक का उपयोग है.

अपनी व्यक्तिगत सूचनाओं जैसेः भ्रमण किये जाने के स्थान, खरीदी गयी वस्तुएं इत्यादि को सोशल मीडिया पर व्यक्त करने से बचना चाहिए क्योंकि हैकर तथा क्रैकर इसी ताक में रहते हैं कि कोई कमजोर पासवर्ड वाला व्यक्ति अपनी जानकारी को लीक करे और वे उसे पकड़ कर अपना गोरखधंधा चलाएं.

डिजिटल होती हुई दुनिया में साइबर अपराध एक गंभीर समस्या है. हैकरों द्वारा उन्हीं कंप्यूटरों में सेंध लगाई जाती है, जिनका सुरक्षा नेटवर्क कमजोर होता है. अतः तकनीक को उन्नत करते रहना हमारी प्राथिकमता होनी चाहिए, इसलिए इंटरनेट बैंकिंग या दूसरे डिजिटल उत्पादों का प्रयोग जागरूक होकर करना चाहिए तथा असामाजिक तत्व या फ़ेक लिंक से बचना चाहिए. इसलिए साइबर सुरक्षा का आर्थिक भार भी उतना ही महतवपूर्ण है जितना कि इसका तकनीकी पक्ष.

इंटरनेट के उपयोग में वृद्धि के परिणाम स्वरूप, इलेक्ट्रानिक कामर्स तेजी से उभरा है और ई-व्यवसाय में काफी संभावनाएं बढ़ी हैं. इंटरनेट चैनल से, संचार माध्यम से, बैंकिंग उद्योग को बहुत लाभ हुआ है, जो ग्राहक को कई तरह की सुविधाएं प्रदान कर रहा है. आज ग्राहक बैंक खाते के साथ-साथ कहीं से भी बिना समय सीमा के कभी भी वित्तीय लेन-देन कर सकता है. यह माना जाता है कि सूचना तकनीक और सुरक्षा उपायों में सकारात्मक बदलाव लाना संभव है. इस हेतु नैतिक, सांविधिक एवं सुरक्षा आयामों जैसे विषयों पर नियमित प्रशिक्षण की आवश्यकता है.

शोध अध्ययन में पाया गया है कि सूचना सुरक्षा और ग्राहक की निजता में सबसे बड़ी समस्या सुरक्षा नियंत्रण की कमी है. दूसरी समस्या, ग्राहक के गोपनीय सूचना के दुरुपयोग और पहचान संबंधी जानकारी की चोरी है. वर्तमान तकनीक से एक सुरक्षित वेबसाइट की डिजाइन संभव है, लेकिन यह बैंक पर निर्भर करता है कि वह सुरक्षा के खतरों के मामले में कितना अग्र सक्रिय और कितना प्रतिक्रियाशील है और ग्राहक पर निर्भर है कि वह आनलाइन लेन-देन और पासवर्ड सुरक्षा के मामले में कितना सजग है.

सन्दर्भ : इन्टरनेट से उपलब्ध बैंक एवं अन्य साईट से उद्धरित.

जितना अधिक आटोमेशन, उतना अधिक जोखिम

अमित प्रकाश
वरिष्ठ प्रबंधक
क्षे. म. प्र. का. रांची

मुकेश कुमार सिन्हा
मुख्य प्रबंधक
सीसो कार्यालय, के. का. मुंबई

आटोमेशन (स्वचालन) धीरे-धीरे सभी क्षेत्रों में कदम जमा चुका है. आटोमेशन से ना सिर्फ काम जल्दी होता है, बल्कि त्रुटि विहीन भी होता है. इससे कार्य दक्षता बढ़ती है और उत्पादन मूल्य में भी कमी आती है. आटोमेशन के कई फायदे हैं और यही वजह है कि आटोमेशन का इस्तेमाल हर क्षेत्र में हो रहा है. आज हम कंप्यूटर और मोबाइल पर बस अंगुली घुमा कर ऑनलाइन आग्रह कर देते हैं और जरूरत की सामग्री हमारे पास न्यूनतम समय में उपलब्ध हो जाती है. अपने दैनिक जीवन की कई जरूरतें आज हम घर बैठे ही किसी भी समय पूर्ण कर लेते हैं, चाहे वो एक खाते से दूसरे खाते में पैसे अंतरित करना या बिजली बिल का भुगतान करना हो या टिकट बुक करना या खाना ऑर्डर करना हो या मेडिकल का बिल भरना या फिर कोई जानकारी प्राप्त करना हो.

हर सिक्के के दो पहलू होते हैं. आटोमेशन के भी दो पहलू हैं यथा फायदे एवं नुकसान. आटोमेशन जहाँ एक ओर इतनी सारी सुविधाएं साथ लेकर आया है, वहीं दूसरी ओर कई जोखिम भी इसके साथ जुड़ी हुई हैं. आज आटोमेशन स्वयं साइबर संकट से चारों ओर से घिरा हुआ है, जिसके कारण बैंकिंग, वित्तीय सेवाएं एवं बीमा कारोबारी अपने और अपने ग्राहकों के डाटा और अन्य जानकारियों को सुरक्षित रखने के लिए निरंतर प्रयासरत हैं.

बैंकिंग एक सेवा उद्योग है. यदि हम अपने आप को ग्राहक की मांग के अनुसार ढाल पाने में असमर्थ होते हैं, तो यह हमारे अस्तित्व के लिए चुनौती होगा. प्रौद्योगिकी के विस्तार के साथ-साथ ग्राहकों की मांग भी दिन प्रति दिन बढ़ती जा रही है. इसलिए बैंकों ने लोगों के सामने कई विकल्प प्रस्तुत किए हैं यथा - मोबाइल बैंकिंग, इंटरनेट बैंकिंग, एटीएम, पॉस मशीन, क्रेडिट कार्ड, डेबिट कार्ड इत्यादि जिनके निम्नलिखित फायदे हैं - 24*7 उपलब्धता, समय की बचत, त्वरित सुविधा, सीमा रहित बैंकिंग इत्यादि. हर कार्य

के साथ कुछ न कुछ खर्चे जुड़े होते हैं. बैंकों में आटोमेशन से खर्चों में कमी आई है एवं कारोबार और ग्राहक आधार बढ़ाने में मदद मिली है. साथ ही ग्राहक सेवा की गुणवत्ता में भी काफी सुधार हुआ है.

पहले जब एटीएम की शुरुआत नहीं हुई थी, तब तक ग्राहकों की निर्भरता पूरी तरह से बैंक शाखा पर थी. आटोमेशन का मुख्य अर्थ है मानव के कम से कम हस्तक्षेप से मशीन द्वारा अधिक से अधिक कार्य को सफलता पूर्वक संपन्न करना. यहीं से जोखिम की भी शुरुआत हुई. जैसे-जैसे मानव का टेक्नोलोजी की ओर रुख होता गया, लोगों की निर्भरता मशीन पर बढ़ती गयी. मशीन आखिर मशीन है, वो सिर्फ उसे दिए गए आदेशों की भाषा समझती है न कि मानवीय दृष्टिकोण.

डिजिटल भुगतान में भारी वृद्धि और नकद रहित अर्थव्यवस्था की ओर बढ़ते कदम ने वित्तीय साइबर सुरक्षा को मजबूत करने की आवश्यकता पर ध्यान केंद्रित किया है. बैंक और वित्तीय संस्थान साइबर हमलों और ऑनलाइन धोखाधड़ी के विभिन्न तरीकों के प्रति बेहद कमजोर हैं. सबसे ज्यादा वित्तीय ट्रोजन संक्रमण वाले देशों की वरीयता सूची में भारत पिछले तीन वर्षों से लगातार अपनी बढ़त बना रहा है, जो गंभीर चिंता का विषय है. कम से कम चालीस प्रतिशत बैंकिंग, वित्तीय सेवाओं और बीमा कारोबार पर न्यूनतम एक बार हमला अवश्य किया गया है. पिछले तीन वर्षों में क्रेडिट और डेबिट कार्ड धोखाधड़ी के मामलों में छह गुना वृद्धि हुई है. कोर बैंकिंग के अलावा, ई-बैंकिंग, एटीएम और खुदरा बैंकिंग जैसी अतिरिक्त सेवाएं साइबर क्राइम का निरंतर शिकार हो रही हैं. वर्ष 2017 में करीब 60-65% मोबाइल धोखाधड़ी बढ़ी, जो विशेष रूप से खतरनाक है, क्योंकि आज मोबाइल उपकरणों पर 40-45% वित्तीय लेनदेन किए जा रहे हैं.

भारतीय बैंकिंग परिदृश्य ने पिछले कुछ सालों से कई बड़े पैमाने पर साइबर हमलों को देखा है. जून 2016 में भारतीय बैंकों की स्विफ्ट प्रणाली को निशाना बनाया गया. अक्टूबर 2016 में, देश में अब तक का सबसे बड़ा डाटा उल्लंघन हुआ, जिसमें विभिन्न बैंकों के 32 लाख डेबिट कार्ड पर साइबर मैलवेयर हमले किए गए. बैंकों को साइबर सुरक्षा न केवल घरेलू घटनाओं पर बल्कि विश्व भर में घट रही ऐसी घटनाओं को ध्यान में रखते हुए करनी है. उदाहरण के लिए, सुरक्षा उपायों पर अपने बुलेटिन में, भारतीय रिज़र्व बैंक ने कार्बानक गिरोह का संदर्भ दिया है, जिसने रूस और यूक्रेन में बैंक की आंतरिक प्रणाली को लगभग 1 अरब डॉलर नुकसान पहुंचाने का लक्ष्य रखा है.

साइबर खतरों की सूची में आम तौर पर निम्नलिखित शामिल हैंः उन्नत निरंतर धमकी (एडवांस्ड पेरसिस्टेंट थ्रेयट्स), फिशिंग, ट्रोजन, बॉटनेट्स, रैनसमवेयर, वितरित डेनॉयल ऑफ सर्विस (डीडीओएस), वाइपर हमले, बौद्धिक संपदा चोरी (इंटेलेक्चुवल

प्रॉपर्टि थेफ्ट), पैसे की चोरी, डाटा मेनिपुलेशन, डाटा विनाश, स्पाइवेयर / मैलवेयर, मैन इन द मिडल (एमआईटीएम), अप्रतिबंधित सॉफ्टवेयर, इत्यादि.

साइबर अपराध को अंजाम देने वाले एक ही झटके में किसी के खाते से एक ही बार में उपलब्ध सभी धनराशि को कहीं स्थानांतरित कर खाताधारकों और बैंकों तथा वित्तीय संस्थानों को भारी आर्थिक नुकसान पहुंचा सकते हैं. सबसे बड़ी क्षति तब पहुँचती है, जब साइबर अपराध को अंजाम देने वाले करोडों की धनराशि को वित्तीय संस्थानों से निकाल कर रफू चक्कर हो जाते हैं.

हमारे समाज मे विभिन्न प्रकार के लोग रहते हैं. कुछ लोग अपने ज्ञान का उपयोग गलत ढंग से करते हैं एवं उसके चलते आम आदमी को कठिनाइयों का सामना करना पड़ता है. त्वरित ढंग से पैसे हस्तांतरण के लिए हम विभिन्न माध्यमों का उपयोग करते हैं और उन्ही माध्यमों से छेड़छाड़ कर आम आदमी को चपत लगाई जाती है. जैसे-जैसे आटोमेशन बढ़ता जा रहा है, वैसे-वैसे जोखिम भी बढ़ता जा रहा है, क्योंकि इसमें दोनों स्तर पर यथा ग्राहक एवं बैंक द्वारा मशीन का उपयोग किया जा रहा है. आज कल जोखिम बढ़ाने वाली एवं तकनीकी स्तर पर धोखाधड़ी के लिए उपयोग में ली जाने वाली प्रक्रिया निम्नलिखित हैः-

एटीएम पर हमला, फिशिंग, स्कीमिंग, क्लोनिंग, वाइरस, फर्जी ई-मेल लिंक, फर्जी फोन काल्स इत्यादि अधिक प्रचलित हैं, जिनके माध्यम से ग्राहक ठगी के शिकार हो रहे हैं.

कृत्रिम समझ (Artificial Intelligence), एक ऐसी तकनीक है, जिसके माध्यम से कंप्यूटर को मानव बुद्धि की नकल करने में सक्षम बनाया जाता है. इसके कई सकारात्मक उपयोग होते हैं. लेकिन आज कल इसका उपयोग मशीनों और उनके कंप्यूटर नेटवर्क पर हमला करने के लिए भी किया जा रहा है. ड्रोन और स्वायत्त वाहनों को एआई का उपयोग करके हैक किया जा सकता है और हथियारों में बदला जा सकता है. पारंपरिक साइबर सुरक्षा प्रक्रियाओं को यह पता भी नहीं चलेगा कि स्मार्ट मशीनों द्वारा किए गए नए हमलों का सामना कैसे किया जाए.

वह दिन दूर नहीं, जब मशीनें स्वयं हमला करेंगी. आने वाले समय में अपने आप से सीखने वाले कंप्यूटर प्रोग्राम की अवधारणा बढ़ रही है और तेजी से परिष्कृत भी हो रही है. यह विचार ही अपने आप में डरावना है. यह चीजों पर हमला करना सीख रहा है, जो और भी भयावह है.

कृत्रिम समझ को एक और तकनीक बज़्जवर्ड (buzzword) के रूप में जाना जाता है, लेकिन इसका पहले से ही रोजाना एल्गोरिदमिक प्रक्रियाओं के माध्यम से उपयोग

किया जा रहा है, जिसे मशीन लर्निंग के रूप में जाना जाता है. मशीन लर्निंग अनुप्रयोगों को कंप्यूटर पर एक निश्चित कार्य को पूरा करने के लिए तथा प्रशिक्षित करने के लिए डिज़ाइन किया गया है. मशीनों को अनिवार्य रूप से कई बाधाओं को पार कर उस कार्य को पूरा करने के लिए सिखाया जाता है. इस तरह की तकनीक कई फायदे जैसे बेहतर कंप्यूटिंग और कई कार्यों को स्वचालन प्रदान करने का वादा करती है, लेकिन इससे विशेषज्ञ चिंतित भी हैं.

तकनीकी जानकार और शोधकर्ता ऐसी तकनीक के खतरे से सावधानी बरतने की सलाह दे रहे हैं. ये मूलभूत रूप से साइबर सुरक्षा का बेहतर प्रयोग करने की सलाह देते हैं, जो ग्राहकों और सरकारों/निगमों के कंप्यूटर और डाटा को हैकर्स से सुरक्षित रखता है. इस तरह की तकनीक कई फायदे प्रदान करने का वादा करती है, जैसे कि कई कार्यों का आटोमेशन, जो वर्षों में, मानव हस्तक्षेप के बिना संचालित होना संभव है, लेकिन इससे विशेषज्ञ चिंतित भी हैं. इस तरह के हमले, जो आज विज्ञान कथाओं की तरह लगते हैं, अगले कुछ वर्षों में वास्तविकता बन सकते हैं.

कृत्रिम समझ (एआई) और मशीन लर्निंग हर उद्योग में बाधा डालने के लिए तैयार है और इससे रोबोटिक्स अलग नहीं है. रोबोटिक्स और एआई या मशीन लर्निंग का शक्तिशाली संयोजन पूरी तरह से नई आटोमेशन संभावनाओं का दरवाजा खोल रहा है.

वर्तमान में, कृत्रिम समझ और मशीन लर्निंग को सीमित तरीकों से लागू किया जा रहा है और औद्योगिक रोबोट सिस्टम की क्षमताओं को बढ़ाया जा रहा है.

चुनौतियांः

वित्तीय संस्थान को सेवाएं प्रदान करने के लिए अन्य सिस्टम के साथ अपने सिस्टम को एकीकृत करना आवश्यक है, इसके बिना बैंक पूरी तरह से ग्राहक को वित्तीय सेवाएं प्रदान करने में सक्षम नहीं होगा. इस एकीकरण प्रक्रिया के कारण बैंक के बुनियादी ढांचे का जोखिम भी बढ़ जाता है. चूंकि ऑनलाइन भुगतान प्रणालियों की पूरी प्रक्रिया कई चरणों में पूरी की जाती है और डाटा कई स्थानों पर संग्रहीत होता है, इसलिए साइबर उल्लंघन के खतरे की संभावना में वृद्धि हुई है, जिसे ध्यान में रखते हुए बैंकों के लिए डाटा की गोपनीयता और अखंडता को बनाए रखना बेहद चुनौतीपूर्ण है.

तकनीकी समाधानः

साइबर अपराध पर काबू पाने के लिए वित्तीय संस्थानों को निम्न तकनीकी समाधानों को मजबूत सुरक्षा प्रदान करना चाहिए :

1. महत्वपूर्ण संपत्तियों से जुड़े जोखिम की पहचान

2. सबसे प्रभावी तकनीक के साथ संरक्षण
3. घटना और अलर्ट की निगरानी के लिए उन्नत जांच तंत्र
4. घटना के प्रति प्रतिक्रिया, प्रभावी वृद्धि तंत्र, नियामकों को रिपोर्टिंग
5. बिना किसी समझौते के गोपनीयता, अखंडता बनाए रखना

निर्णय समर्थन प्रणाली (Decision Support System - DSS) एक सूचना प्रणाली है, जो व्यवसाय या संगठनात्मक निर्णय लेने की गतिविधियों का समर्थन करती है. डीएसएस एक संगठन के तौर पर सामान्यतः मध्य और उच्च प्रबंधन के प्रबंधकीय कौशल, संचालन और नियोजन स्तर की सेवा करता है और उनकी समस्याओं के बारे में निर्णय लेने में उन्हें मदद करता है. आईबीएम सुरक्षा एक स्मार्ट प्रकार की साइबर सुरक्षा के लिए कृत्रिम समझ का इस्तेमाल कर रही है.

निष्कर्ष

साइबर सुरक्षा से संबंधित मानकों का व्यापक अनुपालन सुनिश्चित करने के लिए नियमित लेखा परीक्षा के साथ साइबर सुरक्षा फ्रेमवर्क को सख्ती से लागू किया जाना चाहिए. वित्तीय संस्थानों में साइबर सुरक्षा को प्राथमिकता दी जानी चाहिए. साइबर सुरक्षा के समाधान को इस प्रकार डिजाइन करना चाहिए कि वास्तविक समय में साइबर हमलों को पहचान कर उसे रोका जा सके. विशेषज्ञों का यह भी सुझाव है कि वित्तीय संस्थानों को पूरी तरह से सुरक्षित रखने के लिए डिजिटलीकरण के साथ आगे बढ़ने का सबसे प्रभावी तरीका क्रिप्टो-मुद्राओं और ब्लॉक चेन श्रृंखला प्रौद्योगिकी को अपनाना है. इसके अलावा, नकदी रहित अर्थव्यवस्था में बढ़ते सुरक्षा जोखिमों का सामना करने के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 एक पूर्ण और परिपक्व उपाय है. साथ ही उपभोक्ताओं को शिक्षित और जागरूक करना भी अति आवश्यक है.

जब एक पूरी तरह से स्वचालित प्रणाली में इन सुरक्षा उपायों को नहीं रखा जाता है और संवेदनशील जानकारी किसी भी अन्य डाटा के समान व्यवहार करती है, तो वह संगठन जुर्माना और कानूनी कार्रवाई के अधीन हो सकता है. इस जानकारी को सुरक्षित रखने के लिए एक तरीका होना चाहिए और संभावित मुद्दों से आगे बढ़ने के लिए मानव कर्मचारियों को प्रक्रिया के साथ ही काम करने की अनुमति होनी चाहिए.

डाटा उल्लंघनों और व्यक्तिगत डाटा का दुरुपयोग सभी संगठनों के लिए एक भारी समस्या है, साथ हीं विभिन्न प्रक्रियाओं के सम्पूर्ण स्वचालन की स्थिति में आवश्यकतानुसार हस्तक्षेप करना मुश्किल हो जाता है. इसके बजाए आवश्यक प्रक्रियायों का आटोमेशन करके, अपना ध्यान सुरक्षा पर केंद्रित करें. इसके साथ ही साथ साइबर आक्रमण की चेतावनी के लिए भी आटोमेशन आवश्यक है.

आटोमेशन एक अच्छे अंत का साधन है, न कि खुद का अंत.

आज इन सभी कारणों से अवगत होकर अन्य कारणों की खोज से ज्यादा आवश्यक है कि हम कैसे खुद को विभिन्न प्रकार की धोखाधड़ी से और बेहतर तरीके से बचें. प्रौद्योगिकी समस्याओं के साथ-साथ समाधान भी लेकर आती है. आज के जमाने में हम पूरी तरह आटोमेशन पर निर्भर हो गए हैं, इसलिए यह आवश्यक है कि प्रौद्योगिकी हमें सुरक्षा भी प्रदान करे. क्योंकि

"**मानव ने मशीन का निर्माण किया है न कि मशीन ने मानव का**"

आज के आटोमेशन युग में भी हम अपने जोखिम को थोड़ी सावधानी बरत कर कम कर सकते हैं. अतः आवश्यक है कि हम रोज कुछ ऐसी नई जानकारियां ग्रहण करते रहें एवं उससे स्वयं को अद्यतन रख कर, अपने सभी जानने वालों को ऐसे हमलों से एवं उनसे बचने के तरीकों से अवगत कराते रहें. सतर्क रहें एवं विकल्पों के लिए सदैव अपने आपको तैयार रखें.

अंत में हम यह कह सकते हैं कि आटोमेशन ने तकनीक को जो मुकाम और स्वीकार्यता दिलाई है, उसके साथ-साथ जोखिम में भी बढ़ोतरी हुई है, जिसे हम सतर्क रह कर ही कम कर सकते हैं.

इंटरनेट वरदान या अभिशाप

ध्रुव गुप्ता
प्रबंधक
क्षे. का. दिल्ली (दक्षिण)

दीप्ति आज़ाद
प्रबंधक
मॉडल टाउन, करनाल शाखा

आज शाम मेरा आंखों के डॉक्टर के पास एपॉइंटमेंट था. कुछ दिनों से मुझे ऑफिस में कम्प्यूटर पर काम करने पर सरदर्द की शिकायत हो रही थी. मैंने अपना ऑफिस का काम जल्दी से निपटाया और 5 बजकर 15 मिनट पर ऑफिस से निकल कर रिक्शा पकड़कर डॉक्टर की क्लीनिक में पहुंच गयी. मेरा 5 वां नंबर था और डॉक्टर साहब अभी आए नहीं थे. मैंने देखा मुझसे पहले एक लगभग 3-4 साल की छोटी बच्ची मोटे लेंस का नज़र का चश्मा लगाए, आई-पैड लेकर यूट्यूब पर कुछ कार्टून विडियो देख रही थी. पास ही बैठी उसकी माँ अपने फोन के वाट्स एप्प पर किसी से बड़ी तन्मयता से चैटिंग कर रही थी. इतनी कम उम्र में उस बच्ची को नज़र का चश्मा लगाए देखना मुझे मन ही मन कचोट रहा था. मैं खुद को रोक नहीं पायी, मैं उस बच्ची के पास गयी और उससे उसका नाम पूछा. 'एंजेल'. .. जितना सुंदर नाम था उतनी ही सुंदर उसकी मुस्कुराहट थी. बातों ही बातों में मैंने उससे चश्मा लगाने का कारण तथा इतनी कम उम्र में यूट्यूब प्रयोग करने के सारे राज जान लिए. एंजेल ने मुझे बताया कि उसकी माँ के पास उससे बात करने की कभी फुर्सत ही नहीं रहती तथा दिन रात उसकी माँ फोन में व्यस्त रहती है. मुझे अपना बचपन याद आ रहा था, जब मेरी माँ अपने हाथों से मुझे खाना खिलाया करती थी तथा पूरे दिन मेरे साथ खेलती थी. एंजेल की बातें सुन कर मुझे लगा जैसे फोन तथा इंटरनेट आने के बाद हमारे पास अपनों के लिए भी समय नहीं बचा है. एक अदृश्य सी दीवार हमारे रिश्तों के मध्य इंटरनेट तथा सोशल मीडिया के रूप में मौजूद है. क्या इंटरनेट के आने से हम अपनी भारतीय परंपराओं से दूर होते जा रहे हैं तथा हमारे रिश्तों में दूरियाँ बढ़ रही है. मेरा मन उदास होने लगा था तथा मैं इस सोच में डूब गयी कि क्या इंटरनेट हमारे जीवन में एक अभिशाप बन गया है.

विज्ञान ने इस कदर तरक्की कर ली है कि कुछ समय पहले असंभव सा लगने वाला ख्वाब आज सच प्रतीत हो रहा है. आज बच्चे से लेकर वृद्ध तक के पास मोबाइल फोन है तथा महानगरों से लेकर सुदूर गांवों तक मोबाइल नेटवर्क की पहुंच है. फोन

अब स्मार्ट हो चुका है तथा हर किसी के मोबाइल में इंटरनेट उपलब्ध है. हमारे जीवन में इंटरनेट की उपयोगिता को वरदान या अभिशाप के रूप में देखें, तो एक तरफ जहां इसके बहुत सारे फायदे हैं, वही बहुत से नुकसान भी हैं. इंटरनेट के बारे में यह कहना बिलकुल भी गलत नहीं है कि आधुनिक युग में जिस दौर में हम खड़े हैं वहाँ जीवन की परिकल्पना इंटरनेट के बिना करना शायद संभव नहीं है. एक पल के लिए यह सोचना भी कि एटीएम, इंटरनेट बैंकिंग आदि छोड़ कर हमें बैंक लाइन में घंटो खड़े हो कर कैश निकालना पड़े, वाट्सएप्प त्याग कर वापस डाकिया और अंतर्देशीय पत्र की दुनिया में जाना पड़े, फिर से अपने पसंदीदा टीवी शो देखने के लिए इंतेजार करना पड़े या ट्रेन का टिकिट लेने के लिए घंटों लाइन में लगना पड़े. सोचते हुए भी पसीना टपकने लगता है. यह तो समझ आ रहा है कि इंटरनेट को वरदान की श्रेणी में न रखना तार्किक नहीं होगा पर सवाल यह है फिर इंटरनेट अभिशाप कैसे हो गया. मुझे लगता है इंटरनेट अभिशाप नहीं है, इंटरनेट का गलत प्रयोग या इंटरनेट की लत अभिशाप है.

इंटरनेट क्या है? इंटरनेट एक ऐसी सुविधा है, जिसने विश्व भर के सभी कम्प्यूटरों एवं अन्य डिवाइसेस जैसे मोबाइल, फोन आदि को नेटवर्क के माध्यम से आपस में जोड़ दिया है. इस नेटवर्क में निजी, सार्वजनिक, शिक्षा, व्यवसायिक आदि सहित दुनिया के सभी क्षेत्र शामिल हैं, जो इलेक्ट्रानिक, वायरलेस और आप्टिकल नेटवर्किंग प्रौद्योगिकियों के माध्यम से आपस में जुड़े हैं.

इंटरनेट में सूचना संसाधनों और सेवाओं की एक विस्तृत श्रृंखला है. 1950 के दशक में अमरीकी डिफेंस के आरपानेट नामक एक छोटे से प्रोजेक्ट से शुरू हुई यह सुविधा 1990 में पहली बार वित्तीय रूप में आई और 2000 के दशक के अंत तक इसकी जड़ें जिंदगी के लगभग हर पहलू में प्रवेश कर गईं. इंटरनेट इस तेजी से वृद्धि करेगा और दुनिया को आपस में इस कदर जोड़ देगा शायद इसकी कल्पना किसी ने भी नहीं की होगी.

इन दिनों युवाओं के बीच एक मुहावरा खासा लोकप्रिय है 'कर लो दुनिया मुट्ठी में'. वास्तव में मोबाइल और इंटरनेट के प्रयोग से आधी दुनिया मुट्ठी में आ गयी है, सिर्फ एक क्लिक या यूं कहें एक टच से इंटरनेट की तमाम सुविधाओं के लाभ हम उठा सकते हैं. इंटरनेट की वजह से ही ऑनलाइन संचार बहुत ही सरल और आसान हो गया है. पुराने समय में संचार का माध्यम पत्र होता था और डाकिये का इंतजार थका देने वाला होता था. लेकिन अब, कुछ सोशल नेटवर्किंग साइट को खोलने के लिये हमें सिर्फ इंटरनेट से जुड़ने की जरुरत है, जहां हम अपनों के बीच 24 घंटे ऑनलाइन बिता सकते हैं. जी-मेल, याहू आदि अकांउट के द्वारा पल में ही संदेश भेजा जा सकता है.

मेट्रो, रेलवे, व्यापारिक उद्योग, दुकान, स्कूल, कॉलेज, शिक्षण संस्थान, एनजीओ,

विश्वविद्यालय, कार्यालयों (सरकारी तथा गैर-सरकारी) आदि में हर डाटा को कंप्यूरीकृत करके बड़े स्तर पर कागज और कागजी कार्यों से बचा जा सकता है. ये शिक्षा, यात्रा, और व्यापार में बहुत उपयोगी है. इसके द्वारा ऑनलाइन पब्लिक लाइब्रेरी, टेक्स्टबुक, तथा संबंद्ध विषयों तक पहुँच आसान हुई है. वो चाहे इंटरनेट के प्रयोग से गठित हुई आधुनिक बैंकिंग सुविधाएं हों या पढ़ाई के लिए ऑनलाइन क्लासेस, सभी ने जिंदगी को बेहद आसान बना दिया है.

आधुनिक समय में लोग बस एक क्लिक से अपने यात्रा टिकट की बुकिंग कर सकते हैं साथ ही एक सॉफ्ट कॉपी अपने मोबाईल फोन में भी रख सकते हैं. इंटरनेट की दुनिया में, किसी एक को ये जरुरी नहीं कि लंबी दूरी तय करके वो अपने किसी व्यापारिक मुलाकात या किसी और काम के लिये यात्रा करे. कोई भी विडियो कॉनफ्रेंसिंग, कॉलिंग, स्काईप या दूसरे तरीकों से अपनी जगह पर रह कर ही बैठक का हिस्सा बन सकता है. इंटरनेट हमें कई तरीकों से फायदा पहुँचाता है जैसे ऑनलाइन स्कूल, कॉलेज, या विश्वविद्यालयों में दाखिला दिलाने में, व्यापारिक और बैंकिंग लेन-देन में, शिक्षकों और कर्मचारियों की नियुक्ति में, ड्राइविंग लाइसेंस आवेदन करने में, बिल जमा करने आदि में मदद करता है.

इंटरनेट वरदान है, जो हमारे जीवन को बेहतर बना रहा है या एक अभिशाप है, जिसके कारण हमारे जीवन पर नकारात्मक प्रभाव पड़ रहा है? एक अनोखे दृष्टिकोण से आकलन किया जाए तो इसकी तुलना एक छोटे बच्चे के आइस-क्रीम खाने से की जा सकती है. गर्मी के मौसम में स्वाद और ठंडक तो मिलती है परंतु तबीयत खराब होने पर या सर्दी के मौसम में हमें नुकसान पहुँचा सकती है या फिर ये कहा जाए कि हर चीज़ को औसत के नियम के तहत देखा जाना चाहिए. हर सिक्के के दो पहलू होते है, दोनों तरफ हीं रोशनी डालने पर ही सही आकलन किया जा सकता है.

एक वरदान के रूप में :

इंटरनेट के माध्यम से ई-कॉमर्स ई-व्यवसाय से व्यापार का संचालन किया जा रहा है. न केवल खरीदना और बेचना, बल्कि ग्राहकों के लिये सेवाएं और व्यापार के भागीदारों के साथ सहयोग भी इसमें शामिल है. कई प्रकार के व्यापारों के लिए इंटरनेट नए अवसर प्रदान करता है. वर्तमान में इंटरनेट से व्यवसायों में बड़े पैमाने पर विश्वव्यापी परिवर्तन हो रहे हैं. आज ग्राहक कहीं से भी, सफर करते हुए या घर बैठे, अपनी ज़रूरत के समान की खरीददारी कर सकता है. बिना अतिरिक्त समय लगाए और बिना लंबी कतरों में लगे कोई भी इंटरनेट के माध्यम से आसानी से सामान खरीद सकता है. ज़रूरत का ही नहीं बल्कि शॉपिंग का सामान जैसे कपड़े, इलेक्ट्रॉनिक्स, खाना भी घर पर ही उपलब्ध है.

रिसर्च के क्षेत्र में इंटरनेट का एक महत्वपूर्ण योगदान है. इंटरनेट ज्ञान का एक महासागर है, जिस पर किसी भी विषय में तुरंत और सरलता से वृहद जानकारी प्राप्त की सकती है. आज के आधुनिक युग में क्रिएटिव आइडियास देश या विदेश में बैठे व्यक्ति से इंटरनेट के माध्यम से शेअर किए जाते हैं, जिससे दुनिया में ज्ञान का संवर्धन हो रहा है. हर विषय के संदर्भ में हजारों पन्नों में जानकारी उपलब्ध है, जो रिसर्च के लिए इस्तेमाल की जा सकती है. घर बैठे ही देश और विदेश में बसे लोगों के आर्टिक्ल्स भी पढ़े जा सकते हैं और उनसे सीधे बात भी की जा सकती है.

पढ़ाई के संदर्भ में आज विद्यार्थियों को इंटरनेट की मदद से उनकी रूचि के अनुसार किसी भी विषय में पढ़ने का अवसर प्रदान हो रहा है. पहले जो विषय कुछ क्षेत्रों तक ही सीमित था या जिनके शिक्षक आसानी से उपलब्ध नहीं थे, वो विषय भी इंटरनेट की मदद से अब सभी छात्रों की पहुंच में हैं. आज का विद्यार्थी सिर्फ स्कूल या लाइब्रेरी में उपलब्ध किताबों तक ही सीमित नहीं है, बल्कि इंटरनेट के कारण आज पूरी दुनिया का ज्ञान उसकी पहुंच में है. एक ही विषय के बारे में अलग-अलग वेबसाइट्स पर अलग-अलग जानकारी उपलब्ध है, जिसका विभिन्न दृष्टिकोणों से अध्ययन किया जा सकता है. एक रिसर्च के अनुसार अगर बच्चों को आडिओ-विज़ुअल वीडियो की सहायता से पढ़ाया जाए तो उनकी स्मरण शक्ति बेहतर होती है, वो ज्यादा लंबे समय तक पाठ को स्मरण रख सकते हैं और बेहतर परिणाम ला सकते हैं. आडिओ-विज़ुअल पाठ बच्चों के लिए ज्यादा रूचि वाले भी होते हैं, क्योंकि ये मनोरंजक तरीके से पढ़ने में सहायता करते हैं. इंटरनेट हर दिन नई जानकारी जोड़ता है और बच्चों के लिए नए विकल्प प्रदान करता है. किंडल का प्रयोग करके हम सफर में भी बिना किताबें उठाए हुए किसी भी किताब को पढ़ सकते हैं. इंटरनेट के ज़रिए हम एक साथ हजारों किताबों को अपने पास रख सकते हैं.

सोशल मीडिया की मानव संबंध को बनाए रखने में एक अहम भूमिका है. आज के युग में हम सब अपनी जिंदगी में अति व्यस्त हैं और पूरी तरह से काम के दवाब में हैं, ऐसे में इंटरनेट पर उपलब्ध सोशल नेटवर्किंग साइट्स हमें रिश्ते बनाए रखने में मदद करती है. बचपन के मित्रों से भी हम सोशल नेटवर्किंग साइट्स के ज़रिए संपर्क में रह सकते हैं और उनके जीवन में होने वाली गति-विधियों से परिचित रहते हैं. इस तरह दूर रह कर भी हम उनके जीवन का हिस्सा बन पाते हैं. आज बड़ी संख्या में छात्र पढ़ाई करने के लिए विदेश जा रहे हैं, जिससे वे अपने परिवार से दूर रहते हैं, ऐसे में इंटरनेट इन दूर बैठे परिवार के सदस्यों को एक दूसरे से जोड़े रखने में अत्यंत सहायक है. स्काइप या फेसबुक के जरिये हम विडियो चैट करके सात समंदर पार होने पर भी परिवार जनों को देख कर उनसे बात कर सकते हैं. ये फासला सिर्फ इंटरनेट से ही कम कर पाना संभव हुआ है.

आजकल लोग देश-विदेश में घूमने जाने से पहले ही इंटरनेट के जरिये किसी भी देश व उसकी विभिन्नताओं के बारे में जानकारी प्राप्त कर सकते हैं. वहाँ के तौर-तरीके, खान-पान, रहन-सहन और संस्कृति की जानकारी प्राप्त कर लेते हैं. कौन से क्षेत्र पर्यटन की दृष्टि से महत्वपूर्ण हैं, वहां की क्या विशेषताए हैं आदि. इंटरनेट की मदद से टिकट एवं होटल बुकिंग सहित सारा इंतज़ाम घर बैठे ही बड़ी सरलता से हो जाता है, जिससे हमारी यात्रा सुखद और आसान हो जाती है.

बैंकिंग के संदर्भ में भी इंटरनेट ने क्रांतिकारी परिवर्तन किए हैं. आज हम बैंकिंग सेवाएं इंटरनेट के प्रयोग से बड़ी सरलता से ग्राहकों तक पहुंचा रहे हैं. इसकी मदद से बैंकिंग के क्षेत्र को एक नया आयाम मिला है. आज हम बिना किसी बैंक शाखा में गए घर बैठे ही, अपने ज्यादातर बैंकिंग कार्य खुद ही कर सकते हैं. हम अपने खाते का शेष जान सकते हैं, कोई नई फ़िक्स्ड डिपॉज़िट बना सकते हैं और देश-विदेश में किसी को भी कभी भी पैसे भेज सकते हैं. शेयर मार्केट में भी एस्बा से पैसे निवेश कर सकते हैं. एटीएम मशीन का प्रयोग भी इंटरनेट के जरिये ही किया जाता है और केवल एटीएम मशीन ही नहीं, कैश रीसाइकलर, चेक डिपॉज़िट मशीन इत्यादि भी इंटरनेट के माध्यम से ही उपयोग में लायी जाती है. इंटरनेट बैंकिंग की वजह से आज ग्राहकों को बैंकों में लंबी कतारों में नहीं लगना पड़ता, बल्कि वे घर बैठे ही आराम से इन सेवाओं का लाभ उठा रहे हैं. मोबाइल फोन पर भी इंटरनेट के ज़रिए मोबाइल एप का प्रयोग करके हम बैंकिंग की सेवाओं का लाभ उठा सकते हैं.

इंटरनेट पर घर बैठे ही विभिन्न बैंकों, जीवन बीमा कंपनियों, सामान्य बीमा कंपनियों आदि द्वारा दी जाने वाली सेवाओं की तुलना कर सकते हैं और सर्वश्रेष्ठ चुन सकते हैं. नए उत्पाद का आरंभ होने पर या किसी नई योजना के अपडेट के बारे में एक साथ सब ग्राहकों को सूचित भी कर सकते हैं.

भारत सरकार द्वारा डिजिटल इंडिया को बनाने का एक जोरदार प्रयास चल रहा है, जिसके चलते भारत सरकार ने कई नए अभियान शुरू किए हैं, जिसमें बैंकों ने बढ़-चढ़ कर भाग लिया है और लाखों ग्राहकों तक डिजिटल इंडिया की सेवाओं को पहुंचाने में अपना योगदान दिया है. ऐसी ही कुछ योजनाओं में शामिल है यूनाइटेड पेमेंट इंटरफ़ेस एवं भारत इंटरफ़ेस फॉर मनी, जो कि नेशनल पेमेंट्स कार्पोरेशन ऑफ इंडिया ने स्थापित किए हैं.

ये सभी सुविधाएं देश के सामान्य जन से संबंधित हैं. इंटरनेट के माध्यम से इनका लाभ उठाते हुए हम इसे वरदान के रूप में ही मानते हैं.

इंटरनेट अभिशाप के रुप में :

किसी सिक्के के समान इन्टरनेट के भी दो पहलू है. एक सकारात्मक तो दूसरा नकारात्मक. इन दिनों इंटरनेट एवं उसके विस्तार के साथ उत्पन्न हुई समस्याओं की ओर पूरे देश का ध्यान आकर्षित हुआ है. सवाल अनेक हैं. विज्ञान के इस इंटरनेट रूपी चमत्कार ने हमारे आस-पास की छोटी-छोटी चीजों को भी परिवर्तित कर दिया है. कल तक जिस समाज के परिवारों में माता-पिता, भाई-बहन के पास आपस में बात करने का समय होता था, आज वही समाज अपने सदस्यों की ओर टकटकी लगाए देख रहा है कि कोई तो हेागा, जो कहकहों और मुस्कुराहटों के उस दौर को वापस लायेगा. वर्तमान तेज रफ्तार जीवन में सामाजिक रिश्तों का तेजी से ह्रास हुआ है. आज इंटरनेट तथा सोशल मीडिया क्रांति के परिणामस्वरूप प्रत्येक व्यक्ति एक संदेश छोड़कर अपने सामाजिक दायित्वों से हाथ खींच रहा है. किंतु यथार्थ के धरातल पर देखा जाये तो इंटरनेट अनेक समस्याओं की जड़ है. सोशल नेटवर्किंग साइट्स की मदद से महत्वपूर्ण एवं कई बार आपत्तिजनक तथा कई बार भड़काने और दंगा फैलाने वाली सूचनाओं का आदान-प्रदान होता है. सच्चे किस्सों तथा ज्ञानवर्धक तथ्यों के साथ-साथ विचारोत्तेजक एवं अश्लील तस्वीरों का आदान-प्रदान भी इंटरनेट के माध्यम से किया जा रहा है. अवयस्क मस्तिष्क में इंटरनेट की अच्छी-बुरी बातें और अश्लील तस्वीरों का नकारात्मक प्रभाव पड़ रहा है, जो उनके अवचेतन मस्तिष्क में तूफान को जन्म दे रहा है.

इंटरनेट के जरिए नौजवानों पर बहुत बुरा असर पड़ा है क्योंकि अगर इंटरनेट का उपयोग हम जरूरत पड़ने पर ही करें तो अच्छा है लेकिन ज्यादातर लोग ऐसे हैं, जिन्हें इंटरनेट की लत लग चुकी है. वह दिन-रात इंटरनेट का उपयोग करते रहते हैं और जो समय कैरियर बनाने का होता है, उस समय को बर्बाद कर देते हैं और अपनी जिंदगी बर्बाद कर रहे हैं. उनका ध्यान किसी भी वस्तु पर पूर्ण तरीके से नहीं रहता, जिसके कारण वो विचलित भी महसूस करते हैं. इंटरनेट एडिक्शन डिसऑर्डर इंटरनेट का सबसे बड़ा दुष्प्रभाव है, जिससे कि लोग ये समझते हैं कि वो हर समय इंटरनेट पर हैं, भले ही वो इंटरनेट का प्रयोग न भी कर रहे हों. यह बीमारी ज्यादातर बच्चों में देखी गई है. इंटरनेट के अधिक प्रयोग से होने वाली इस तरह की बीमारियों पर बड़े स्तर पर शोध चल रहा है.

इंटरनेट की वजह से अपराध जगत का दायरा भी बढ़ा है. आज कई साइटों पर बम बनाने से लेकर आतंकवादी संगठन से जुड़ने तक की जानकारी उपलब्ध है. इंटरनेट की वजह से बहुत सारे अपराध भी बढ़े हैं. लोग अपराध करने में भी इंटरनेट का उपयोग करते हैं. वह इंटरनेट से कोई भी उपयोगी जानकारी हासिल कर उसका गलत तरह से उपयोग करते हैं, जिससे कुछ लोगों को बहुत नुकसान उठाना पड़ता है.

लोग आजकल अपनी छोटी से छोटी बात भी सोशल नेटवर्किंग साइट्स पर शेयर करते हैं, जिनमें वे जानकारियां भी शामिल होती हैं, जो उन्हें अपने तक ही सीमित रखनी

चाहिए. जैसे अगर आप उनसे यह शेयर करते हैं कि आप सपरिवार बाहर घूमने जा रहे हैं, तो यह चोरों को आमंत्रण देना है. आप ऐसी जानकारी यदि शेयर करना ही चाहते हैं, तो उसे यात्रा की समाप्ति के उपरांत घर लौटकर आने के बाद शेयर करें.

दूसरे, सोशल मीडिया पर ये देखना कि आपके परिवार जन या आपके मित्र घूमने जा रहे है और आप अपनी रोज़मर्रा के जीवन में व्यस्त हैं, तो ये बात आपको डिप्रेस कर सकती है. आप खुद की ज़िंदगी की तुलना दूसरों से करने लगते हैं कि आप घूमने नहीं जा पा रहे है और आपका जीवन उतना खुशहाल नहीं है, जितना कि आपके करीबी लोगों का है. यह तुलना एक खतरनाक समस्या है. हम सोशल नेटवर्किंग पर एक वर्चुअल दुनिया में जीने लगते हैं, जहा हजारों दोस्त हैं पर वास्तविक दुनिया से हमारा नाता छूटने लगता है.

खेल कूद भी आजकल इंटरनेट पर हो रहा है, बच्चे घर बैठ कर ऑनलाइन दोस्तों के साथ खेलते हैं. वर्चुअल गेम्स के कारणवश कमरे में बंद खेल खेलते हैं, जिससे उनका शारीरिक और मानसिक विकास अवरुद्ध हो रहा है और वो लाइफ स्टाइल संबंधित बीमारियों का शिकार हो रहे हैं.

ई-कॉमर्स से सस्ता मिलने पर ऐसा सामान खरीद लेते हैं, जिसकी आवश्यकता नहीं होती. ई-कॉमर्स कुछ बड़ी कंपनियों के हाथ में है, जिसकी वजह से छोटे व्यापारियों का रोजगार कम हो गया है. देश का विकास तभी होगा जब हर छोटे व्यक्ति को कमाने का मौका मिलेगा.

सूचना-संचार के क्षेत्र में कंप्यूटर और इंटरनेट विज्ञान के क्रांतिकारी आविष्कार माने जाते हैं. आज का समाज जितना सूचनाओं पर निर्भर है, उतना ही ज्यादा सूचनाओं के ग्रहण और प्रसार के लिए उसे इंटरनेट और कंप्यूटर की आवश्यकता है. इसमें कोई संशय नहीं है कि इंटरनेट क्रान्ति हमारे लिए एक वरदान सिद्ध हुआ है परंतु इसे अभिशाप बनने से रोकने के लिए हमें इसके प्रयोग तथा प्रयोग करने के तरीके के बीच एक संतुलन बनाने की ज़रूरत है. यहां यह ध्यान रखने की ज़रूरत है कि इंटरनेट की लत हमें समाज, अपने परिवार तथा अपनी संस्कृति से दूर न ले जाये. समाज का हर व्यक्ति अगर अपना दायित्व समझ कर इंटरनेट का उपयोग देश और समाज हित में करेगा, तो इंटरनेट को अभिशाप बनने से रोका जा सकता है. आज स्थिति ऐसी आ गई है कि इंटरनेट के बिना सामाजिक एवं आर्थिक क्षेत्र में एक कदम भी चलना संभव नही है. सामान्यतः अन्त में अच्छाई की ही जीत होती है, इसलिए समाज द्वारा इंटरनेट के जिम्मेदाराना प्रयोग से निश्चित है कि बुराई नष्ट हो जायेगी.

इंट्रानेट बनाम इंटरनेट

राहुल कुमार
सहायक प्रबंधक (राभा)
क्षे.का. कोझिकोड

आज के आधुनिक युग के बदलते प्रारूप में विज्ञान की गति और भी तेज हो गई है. विज्ञान के दो बहुमूल्य उत्पाद इंट्रानेट और इंटरनेट आज के बदलते परिदृश्य की नवीन झलकियाँ तैयार कर रहे हैं. वास्तव में इंट्रानेट और इंटरनेट आज के आधुनिक युग के बुनियादी आधार बनकर उभरे हैं. एक तरफ इंट्रानेट जहां सीमित क्षेत्रों को अपने दायरे में लाने में सक्षम है, वहीं दूसरी ओर इंटरनेट बहुत बड़े क्षेत्र का प्रतिनिधित्व कर रहा है. वास्तव में इंट्रानेट और इंटरनेट दोनों एक ही सिक्के के दो पहलू हैं. दोनों ही सर्वर के माध्यम से सेवाएं उपलब्ध कराते हैं. ध्यान से देखा जाए तो हम पाते हैं कि

"इंटरनेट और इंट्रानेट दोनों का है एक सूत्र
रिश्तों में देखें तो एक पिता और दूसरा पुत्र"

इंट्रानेट क्या है ?

वास्तव में इंट्रानेट कम्प्यूटरों का निजी नेटवर्क है, जो इंटरनेट प्रोटोकॉल तकनीक का उपयोग करता है. इंट्रानेट के माध्यम से किसी संस्था द्वारा आवश्यक सूचनाएं सुरक्षित रूप से अपने कर्मचारियों के बीच आदान-प्रदान की जा सकती हैं. इंट्रानेट एक स्वतंत्र इकाई नहीं है बल्कि यह एक ऐसा सॉफ्टवेयर है, जो इंटरनेट प्रोटोकॉल के माध्यम से एक ही संगठनों या संस्थाओं के बीच एक कड़ी उपलब्ध कराती है, जिससे सभी कंप्यूटर नेटवर्क आपस में जुड़े रहते हैं. यही कारण है कि इंट्रानेट को नेटवर्क बिट्वीन ऑर्गनाइज़ेशन या 'इंटरनल लिंक ऑफ ऑर्गनाइज़ेशन' से जुड़ा सॉफ्टवेयर भी कहते हैं. इंट्रानेट सॉफ्टवेयर के मुख्य दो पोर्टल होते हैंः-

(क) इंट्रानेट पोर्टल
(ख) एंटरप्राइज़ पोर्टल

(क) इंट्रानेट पोर्टल : इंट्रानेट पोर्टल किसी संस्था के आंतरिक कामकाज को संयोजित करने के साथ-साथ ऑर्गनाइज़ेशन एंटरप्राइज़ इन्फॉर्मेशन को एक से दूसरे कंप्यूटर तक पहुंचाने के लिए भी कार्य करता है.

(ख) एंटरप्राइज़ पोर्टल : एंटरप्राइज़ पोर्टल वह पोर्टल है, जिसके माध्यम से कोई संस्थान विशेष अपनी सूचनाओं को बाहर भेजता है. इसमें एक सेक्योर यूनिसेफ एक्सेस पॉइंट होता है, जिसे वेब आधारित इंट्राफेस भी कहते हैं. सामान्यतः एंटरप्राइज़ पोर्टल संस्थान के डाटा कॉपी से भी जुड़ा रहता है, जिससे संस्थान विशेष की सूचना को कॉपी व पेस्ट न किया जा सके. यह सूचना को एक जगह से दूसरे जगह स्थानांतरित करता है यही कारण है कि इसे एंटरप्राइज़ इन्फॉर्मेशन पोर्टल (ईपीआई) के नाम से भी जाना जाता है.

*** इंट्रानेट के लाभ :** आज के दौर में विभिन्न निजी संस्थानों में शत-प्रतिशत कार्य इंट्रानेट के माध्यम से हो रहा है और काफी सक्रियता और विश्वनीयता के साथ सूचनाओं का आदान-प्रदान सुचारू रूप से हो रहा है. इंट्रानेट बहुत बड़े या छोटे से छोटे संस्थान की सूचनाओं की कड़ी बनकर उभरा है. ध्यान से देखा जाए तो पता चलता है कि सूचनाओं के जाल को संस्थाओं के अंदर प्रेषित कर संस्थाओं के विकास और गोपनीयता के क्षेत्र में ऊर्ध्व गति प्रदान कर रही है इसके निम्न लाभ हैं:-

- यह कर्मचारियों के बेहतर जुड़ाव में संयोजक का कार्य करता है.
- यह बेहतर संचार व्यवस्था प्रदान करता है.
- यह आपस में सुव्यवस्थित सहयोग प्रदान करता है.
- यह सूचना और प्रबंधन का कार्य करता है.
- यह प्रोजेक्ट (परियोजना) प्रबंधन को गोपनीय बनाए रखकर संस्था के विकास में अनुकूल वातावरण तैयार करता है.
- यह प्रक्रिया समेकन (प्रोसैस कोंसोलिडेसन) का कार्य करता है.
- यह मानव संसाधन प्रबंधन प्रक्रिया को सरल बनाता है.

इंटरनेट क्या है ?

कंप्यूटर और टेलीकम्यूनिकेशन के समन्वय से जिस सूचना प्रौद्धोगिकी का विकास हुआ है उसे इंटरनेट के नाम से जाना जाता है. दूसरे शब्दों में हम कह सकते हैं कि "सूचना और अन्य इलेक्ट्रानिक संसाधनों को साझा करने के लिए विभिन्न संचार माध्यमों से आपस में जुड़े कम्प्यूटरों एवं अन्य इलेक्ट्रोनिक उपकरणों का समूह, कम्प्यूटर नेटवर्क कहलाता है और इन्हीं कम्प्यूटर नेटवर्कों का विश्वस्तरीय नेटवर्क इंटरनेट है." आज लगभग सभी लोग इंटरनेट सेवाओं के माध्यम से जुड़े हुए हैं. इस इंटरनेट तकनीक का जन्म एकाएक नहीं हुआ, बल्कि कई दशकों से गुजरते हुए इसका परिष्कृत रूप आज हमारे सामने है. इस इंटरनेट प्रणाली का जन्म अमेरिका में शीत युद्ध के गर्भ से हुआ था. सन 1960 के दशक में सोवियत संघ के परमाणु आक्रमण से चिंतित अमेरिकी सरकार ने एक ऐसी व्यवस्था की संरचना की, जिससे अमेरिकी शक्ति किसी एक जगह पर केन्द्रित न रहे. अमेरिका के विकेन्द्रित इंटरनेट नेटवर्क से यह उम्मीद थी कि वह किसी भी आक्रमण से बचा रहेगा. इस नेटवर्क द्वारा कम्प्यूटर शक्ति से संबंधित सभी सूचनाओं को संग्रहित रखा जा सकेगा. सत्तर(70) के दशक में अमेरिका की उन्नत रक्षा अनुसंधान परियोजना एजेंसी ने अपने प्रयास में सफलता प्राप्त की और इस नेटवर्क का उदय हुआ. अमेरिकी सूचना संसाधनों के संरक्षण और आपस में सूचना को साझा करने के उद्देश्य से पहली बार कुछ कम्प्यूटरों के एक नेटवर्क "आरपानेट (ARPANET) की स्थापना की गयी. इससे कम्प्यूटर के बीच बहु संयोजित पैकेज नेटवर्क में सूचनाओं का आदान-प्रदान संभव हो सका. यही अंतर चेटिंग परियोजना परिष्कृत होकर 'इंटरनेट' के नाम से जानी जाती है. 2000 दशक के अंत तक इसकी सेवाओं और प्रोद्योगिकी को रोज़मर्रा की ज़िंदगी के लगभग हर पहलू में शामिल कर लिया गया.

इंटरनेट की भूमिका : इंटरनेट के माध्यम से पूरे विश्व और भारत को एक नई दिशा मिली है. घर के किसी एक कोने से होकर विश्व पटल पर आज इंटरनेट की क्यारियां फैली हुई हैं और उससे आज का मानव समाज सफलता के शिखरों पर अपना पांव फैलाने में कामयाब हो पाया है. आज विश्व का हर एक कोना इंटरनेट के आईने में अपनी सूरत संवार रहा है. **अमेरिकी लेखक डेव बैरी** ने कहा है कि **"टेलीफोन व मोबाइल के आविष्कार के बाद मानव संचार के इतिहास में इंटरनेट सबसे महत्वपूर्ण एकल विकास है."**

भारत में इंटरनेट की शुरुआत भारत संचार निगम लिमिटेड (बीएसएनएल) ने वर्ष 1965 में किया था. अब तो धड़ल्ले की तरह इसका प्रयोग सभी दूरसंचार कंपनियाँ (एयरटेल, रिलायंस, वोडाफोन, आइडिया) कर रही हैं. आज 4G जियो के समीकरण ने इंटरनेट को विकास की दिशा में और अधिक परिष्कृत और समृद्ध किया है. आज विश्व

के कुल 7 अरब से अधिक लोगों में से लगभग 3 अरब लोग इंटरनेट से जुड़े हुए हैं. विश्व में चीन और अमेरिका के बाद इंटरनेट का प्रयोग करने वाले सर्वाधिक लोग भारत में ही हैं. हमारे देश में लगभग 35 करोड़ से ज्यादा लोग इंटरनेट से जुड़े हुए हैं.

आज जीवन की मूलभूत आवश्यकताओं से लेकर विदेश जाने तक के टिकट, किचन के सामानों से लेकर किताबों का ऑर्डर, व्यापार को बढ़ाने के लिए विज्ञापन, स्वास्थ्य, कानून, शिक्षा आदि सभी क्षेत्रों में इंटरनेट अपना पांव पसार रहा है. यहाँ तक कि अब आप चुनाव में अपना मतदान भी इंटरनेट के माध्यम से कर सकते हैं. शिक्षा के क्षेत्र में इंटरनेट वरदान साबित हुआ है. आज विश्व के एक छोर से दूसरे छोर तक के पुस्तकालय इंटरनेट सेवा से जुड़े हुए हैं, किताबों की ऑनलाइन शॉपिंग तथा ऑनलाइन किताबों की इमेज ने शिक्षा जगत में क्रांति ला दी है. इंटरनेट के इन उपयोगों को देखते हुए अमेरिकिन लेखक पाल्स लिखते हैं कि "**इंटरनेट दुनिया का सबसे बड़ा पुस्तकालय है, मानो जहां सभी पुस्तकें खुली पड़ी हों.**" ध्यान से देखा जाए तो पता चलता है कि "**इंटरनेट वह जिन्न है, जो आपके आदेशों का पालन करने को हमेशा तैयार रहता है.**"

इंट्रानेट और इंटरनेट में मूलभूत अंतर

आज के गतिशील युग में इंट्रानेट और इंटरनेट दोंनों ही अहम भूमिका निभा रहे हैं. सूचनाओं के आदान-प्रदान से देश की गतिविधियों में दोनों की अपनी महत्वपूर्ण भूमिका है. सूचनाओं के समुचित मापदण्डों के कारण सूचना तंत्र में क्रांति सी आ गई है किन्तु ध्यान से देखें तो पता चलता है कि कार्य क्षेत्र के स्तर पर कुछ अंतर हैः-

- इंट्रानेट मुख्य रूप से लोकल एरिया नेटवर्क (LAN) से जुड़ा होता है जबकि इंटरनेट नेटवर्कों का नेटवर्क है. इसमें विभिन्न प्रकार के नेटवर्क (LAN, MAN, WAN) को मिलाकर एक नेटवर्क तैयार किया जाता है.
- इंट्रानेट में सर्वर की संख्या सीमित होती है, जबकि इंटरनेट पर हजारों सर्वर कार्य करते हैं.
- इंट्रानेट किसी संस्था या कॉर्पोरेट विशेष के आंतरिक कामकाज के लिए प्रयोग किया जाता है, जबकि इंटरनेट बाह्य स्तर पर सभी के लिए समान रूप से कार्य करता है.
- इंट्रानेट में डाटा की सुरक्षा सुनिश्चित होती है, जबकि इंट्रानेट की तुलना में इंटरनेट में डाटा की सुरक्षा कम रहती है.
- इंट्रानेट में सीमित व्यक्तियों को ही प्रवेश मिलता है, जबकि इंटरनेट में कोई भी व्यक्ति अपनी मर्जी से कहीं भी नेटवर्क का प्रयोग कर सकता है.

- इंट्रानेट में मेल सर्वर व सूचनाओं का प्रयोग निजी न्यूज़ ग्रुप बनाने में किया जाता है जबकि इंटरनेट में मेल सर्वर तथा सूचनाओं का प्रयोग सार्वजनिक रुप से किया जाता है.
- इंट्रानेट की साइट को इंटरनेट साइट की सहायता के बिना नहीं बनाया जा सकता है, जबकि इंटरनेट की वैश्विक साइट को सीधे तौर पर बना सकते हैं.
- इंट्रानेट पर किसी साइट को अपलोड करने के लिए वेब स्पेस की आवश्यकता नहीं होती है, बल्कि उसमें प्रयोग होने वाले सर्वर से ही काम किया जाता है, जबकि इंटरनेट पर किसी साइट को चलाने के लिए पहले इस साइट पर अपलोड करने के लिए वेब स्पेस की आवश्यकता होती है. इसके लिए अलग सर्वर की सेवाएं ली जाती हैं.
- इंट्रानेट पर किसी न किसी का मालिकाना हक़ होता है जबकि इंटरनेट पर किसी का मालिकाना हक़ नहीं होता है.
- इंट्रानेट एक प्राइवेट नेटवर्क है, जबकि इंटरनेट एक सार्वजनिक नेटवर्क है.

इंट्रानेट और इंटरनेट का तुलनात्मक विश्लेषण, सीमाएं और संभावनाएं : आज इंट्रानेट और इंटरनेट विश्व पटल पर अपनी छाप छोड़ रहे हैं. अधिकाधिक कार्य इंटरनेट और इंट्रानेट के माध्यम से किया जा रहा है. किन्तु ध्यान से देखेँ तो पता चलता है कि इंट्रानेट का प्रयोग अपने किसी निजी संस्थान में सूचनाओं के आदान-प्रदान के लिए किया जाता है. पूरा संस्थान केवल एक सर्वर से जुड़ा हुआ होता है. इंट्रानेट से आप विशेष समय, विशेष स्थान, विशेष सर्वर से ही जुड़ सकते हैं, जो इसकी सबसे बड़ी सीमा है. यदि इंट्रानेट का फैलाव विशेष समय स्थान से उन्मुक्त होकर कर्मचारी विशेष की व्यक्तिगत डिवाइस से जुड़ जाता तो निश्चित रुप से इसका विकास होता. वहीं इंटरनेट अपने विस्तारण क्षमता के कारण पूरे विश्व को जोड़े रखता है.

यह कहना कोई अतिशयोक्ति नहीं होगी कि "**आज का युग इंटरनेट का युग बन चुका है**" जहाँ एक ओर इंटरनेट सभी सुख-सुविधाओं का साधन बना हुआ है, वहीं दूसरी ओर इंटरनेट मानवता के बदलते दृश्य से भी परिचित करवा रहा है. आज इंटरनेट के माध्यम से कई बड़ी घटनाओं को अंजाम दिया जा रहा है. इंटरनेट के माध्यम से अश्लील तस्वीरें धड़ल्ले से पोस्ट की जा रही हैं. साइबर अपराधों की घटनाएं दिन प्रतिदिन बढ़ती जा रही हैं. कई आतंकवादी संघटन और देशविरोधी लोग साइबर क्षमता बढ़ाने में लगे हैं, क्योंकि वे भलीभाँति जानते हैं कि इंटरनेट के द्वारा किए गए हमले का कोई प्रमाण नहीं होता है. स्थिति यह आ गई है कि इंटरनेट का प्रयोग कर व्यक्ति की व्यक्तिगत पहचान तक चुराई जा रही है, जिससे जन-जीवन मानसिक त्रासदी के खतरे से गुजर रहा है. सरकार को चाहिए कि इंटरनेट से संबंधित एक ठोस कानून बनाए और उसे क्रियान्वित

करें. ज्यादा आवश्यकता कानून को लागू करने की है क्योंकि भारत सरकार ने इंटरनेट के कारण होने वाले अपराध को रोकने के लिए अक्टूबर, 2000 में सूचना प्रोद्योगिकी एक्ट बनाया है, किन्तु यह मात्र दस्तावेजी पोशाक ही पहनकर रह गया है. आज भी लोग बड़ी चालाकी से इंटरनेट का प्रयोग अपने अनुसार कर रहे हैं. सरकार को चाहिए किः-

- इंटरनेट उपयोगकर्ता की एक व्यक्तिगत पहचान हो, जो आधार कार्ड से लिंक हो, तभी वो किसी साइट पर लॉग हो सके.
- एक ठोस कानून बनाकर एक समूह का गठन करें, जो नियमित रूप से इसकी देखरेख करे. कुछ गलत पाए जाने पर सूचना प्रौद्योगिकी एक्ट, 2000 के तहत ठोस कार्यवाही करे.

इंट्रानेट और इंटरनेट को व्यावहरिकता के पटल पर देखें तो पता चलता है कि इंटरनेट का सहारा लेकर बना इंट्रानेट, इंटरनेट से सुरक्षा के स्तर पर कहीं ज्यादा उन्नत है किन्तु उतना ही संकीर्ण भी है. अतः एक ओर जहां इंट्रानेट में क्षेत्र और समय के स्तर पर वहीं दूसरी ओर इंटरनेट में सुरक्षा के स्तर पर सुधार की काफी संभावनाएं हैं. हम कह सकते हैं किः-

"नवगांतकारी सोच के लिए बदलता हुआ अपना देश है,
इंट्रानेट और इंटरनेट को परिष्कृत करने की संभावनाएं अभी शेष हैं."

संदर्भः-

1. इंटरनेट
2. इंट्रानेट

सिम स्वैप धोखाधड़ी

विनीत भारद्वाज
प्रबन्धक
क्षे. का. रीवा

सिम स्वैप धोखाधड़ी क्या है?

आज के दौर को, यदि मोबाइल फोन का दौर कहा जाए तो कोई अतिशयोक्ति न होगी. आज मनुष्य की आवश्यकता का लगभग हर कार्य, मोबाइल फोन पर कुछ एक क्लिक करने से हो जाता है. आज लगभग हर व्यक्ति के पास एक मोबाइल फोन अवश्य है. भारतीय दूरसंचार विनियामक प्राधिकरण की दिनांक 18 जुलाई 2018 की रिपोर्ट के अनुसार भारत में मई 2018 के अंत तक 131.10 करोड़ की जनसंख्या के सापेक्ष मोबाइल फोन की संख्या 118.34 करोड़ है अर्थात औसतन 86.89% जनसंख्या के पास मोबाइल फोन है.

पिछले कुछ वर्षों से, हमारे देश में, डिजिटल इंडिया का नारा ज़ोरों से दिया जा रहा है. एक तरफ सरकार, डिजिटल इंडिया अभियान के तहत कैशलेस अर्थव्यवस्था को बढ़ावा दे रही है, वहीं हैकर डिजिटल भुगतान की, खामियों का फायदा उठाकर नए-नए तरीकों से लोगों के बैंक खातों में सेंध लगा रहे हैं. ऑनलाइन भुगतान व इंटरनेट बैंकिंग के कई लाभ हैं परंतु इस कैशलेस अर्थव्यवस्था ने ऑनलाइन अपराध करनेवाले हैकरों के लिए आप के साथ आर्थिक धोखाधड़ी करने के कई रास्ते खोल दिये हैं. वैसे तो बैंक अकाउंट को कई तरीकों से हैक किया जा सकता है, लेकिन आजकल जो प्रणाली सर्वाधिक प्रचलन में हैं, वह है सिम स्वैप धोखाधड़ी. "सिम स्वैप" इन दिनों सबसे बड़े साइबर अपराध के तौर पर सामने आया है. इसके सबसे बड़े शिकार हैं स्मार्टफोन उपयोगकर्ता. हमारे देश में सिम स्वैप धोखाधड़ी के मामले लगातार बढ़ते जा रहे हैं.

सिम (SIM) का अर्थ है "सब्स्क्रायबर इन्सट्रक्शन मॉड्यूल" अर्थात वह कार्ड, जिसमें पंजीकृत उपयोगकर्ता का डाटा संचयित (स्टोर) होता है. सिम स्वैप धोखाधड़ी में सिम का इस्तेमाल होता है अर्थात आपके पास जो सिम (मोबाइल नंबर) है, वह अचानक बंद हो जाता है. असल में होता यह है कि सिम स्वैप धोखाधड़ी के अंतर्गत अगर आपके

पास कोई सिम कार्ड है, जो आपके बैंक खाते से जुड़ा हुआ है, तो साइबर अपराधी, जिन्हें हैकर कहा जाता है, आपके बैंक खाते में सेंध लगाने हेतु मोबाइल सेवा प्रदाता के पास जाकर उसी नंबर का नया सिम कार्ड निकलवा लेते हैं. बैंक खाते में धोखाधड़ी के शिकार व्यक्ति के मन में अक्सर यह सवाल उठता है कि हैकरों को उनका डुप्लीकेट सिम कैसे मिल जाता है? साइबर अपराध विशेषज्ञों के अनुसार, हैकर ज़्यादातर सोशल मीडिया के जरिए आपकी व्यक्तिगत जानकारियां जुटाते हैं. उन्हीं जानकारियों के आधार पर एक फर्जी पहचान पत्र तैयार करते हैं, जिसकी मदद से डुप्लीकेट सिम जारी करा लिया जाता है. अमूमन सिम कार्ड देने से पहले, टेलीकॉम कंपनियों के स्टोर पर आवेदक और दस्तावेजों का अच्छे से मिलान नहीं किया जाता है. हैकर इस बात का फायदा उठाते हैं. कई बार टेलीकॉम कंपनी के स्टोर पर कार्यरत किसी कर्मचारी की मदद से भी डुप्लीकेट सिम मिल जाता है. इसके अलावा, आपके नाम से जो भी सिम है, उस सिम को हैकर स्वैप कर लेते हैं. फिर स्वैप किए गए सिम को, क्लोन करके उसका नकली (डुप्लीकेट सिम) बना लिया जाता है. इसके पश्चात हैकर बैंक से आने वाले ओटीपी मैसेज का इस्तेमाल कर कुछ ही मिनटों में आपके खाते से सारा पैसा गायब कर देते हैं.

सिम स्वैप करने के तरीकेः

हैकरों द्वारा सिम स्वैप करने के तीन मुख्य तरीके हैं :

पहला तरीका : सिम कार्ड अपग्रेड करने की आड़ में

इसके अंतर्गत हैकर, टेलीकॉम कंपनी का कर्मचारी बनकर आपको कॉल करता है और आपके सिम कार्ड को 3जी से 4जी में अपग्रेड करने या वैधता बढ़ाने के कई ऑफर देता है. यदि आप उसके प्रस्ताव से सहमत हो जाते हैं, तो वह आपसे सिमकार्ड पर लिखा हुआ 20 अंकों का सिम नंबर, कस्टमर केयर के नंबर : जैसे 121 पर एसएमएस करने अथवा फोन पर डायल करने के पश्चात 1 नंबर दबाने के लिए कहता है. इस स्थिति में हैकर आपके मोबाइल नंबर वाली नई 3जी या 4जी सिम पहले ही निकलवाकर रखता है, जैसे ही आप 20 अंकों का सिम नंबर 121 पर मैसेज करते हैं अथवा फोन पर डायल कर 1 नंबर दबाते हैं तो टेलीकॉम कंपनी आपके इस अनुरोध को स्वीकार कर लेगी. कुछ समय पश्चात आपके मोबाइल में लगा हुआ सिम कार्ड काम करना बंद कर देता है और हैकर के पास मौजूद सिम कार्ड काम करना शुरू कर देता है.

दूसरा तरीका : मोबाइल नेटवर्क बढ़ाने की आड़ में

इस कार्यविधि के अंतर्गत हैकर आपको कॉल करता है और कहता है किः

"अभी आप जिस स्थान पर हैं, उस क्षेत्र के मोबाइल टावर में मेंटीनेंस का काम चल रहा है, जिसकी वजह से आपके मोबाइल सिम कार्ड का नेटवर्क बंद हो सकता है. यदि आपके साथ ऐसा होता है तो आपको 7 दिनों के अंदर आपके मोबाइल सेवा प्रदाता स्टोर पर जाकर सिम कार्ड लेना है अन्यथा आपका सिम कार्ड बंद कर दिया जाएगा. यदि आप स्टोर पर नहीं जा सकते हैं तो मैं अभी इसी फोन के जरिए आपके सिम कार्ड को नए सिमकार्ड में अपग्रेड कर देता हूँ."

जब हैकर ऐसा कहता है तो अधिकतर उपयोगकर्ता उसकी बात मान लेते हैं और अनजाने में उसे अपने सिमकार्ड को स्वैप करने की अनुमति दे देते हैं. इससे आपका सिम कार्ड बंद हो जाता है और हैकर के पास पहले से मौजूद सिमकार्ड एक्टिव हो जाता है. ऐसा करने के बाद हैकर आपसे यह भी कहता है कि सिम अपग्रेड होने में 6 से 7 घंटों का समय लगेगा और इस दौरान आपके मोबाइल पर नेटवर्क नहीं आएगा इसलिए आप परेशान न हों. इसी समयावधि में, हैकर आपके बैंक खाते को हैक कर सारी धनराशि ट्रान्सफर कर देता है.

तीसरा तरीका : मोबाइल नंबर पोर्टेबिलिटी (MNP) द्वारा

"एमएनपी" यानि मोबाइल नंबर पोर्टेबिलिटी के जरिए, ग्राहक किसी अन्य मोबाइल ऑपरेटर में अपना नंबर पोर्ट करते हैं. इसके अंतर्गत हैकर अलग-अलग तरीकों जैसे स्पैम मैसेज या मेल भेजकर या आपके मोबाइल में कोई एप्लिकेशन इन्स्टाल कर, आपके सिम कार्ड को, किसी अन्य ऑपरेटर में पोर्ट करवाने का अनुरोध कंपनी को भेज देता है और जब आपका अनुरोध पूर्ण हो जाता है तो जिस ऑपरेटर में आपकी सिम पोर्ट कारवाई गई है, उसी ऑपरेटर से नया सिम कार्ड प्राप्त कर लेता है. 7 दिनों बाद आपकी सिम स्वतः बंद हो जाती है और आपको इसकी भनक भी नहीं लगती.

हमारी जानकारी हैकर को कौन देता है ?

हैकर, हमारे विषय में ज़्यादातर जानकारियां सोशल मीडिया, जैसेः फेसबुक, ट्विटर, व्हाट्सएप आदि से प्राप्त करते हैं. इसके अलावा, हैकर्स कुछ ऐसे वेबसाइट तैयार करते हैं जिनमें, मनभावक ऑफर जैसे "**इस वेबसाइट पर दिए गए फॉर्म को भरें और पाएँ 150 रुपये का टॉकटाइम, जल्दी करें, ऑफर सीमित समय के लिए**" होते हैं और इनके लिंक फेसबुक, ट्विटर, व्हाट्सएप, एसएमएस आदि के माध्यम से आपको भेजते हैं. इन ऑफर के बदले वह आपसे एक फॉर्म भरवाते हैं जिसमें आपका नाम, मोबाइल नंबर, पता, आधार नंबर, पैन नंबर और बैंक खाते की जानकारियां शामिल होती हैं. ऑफर को देखकर आप उन वेबसाइट पर दिए गए फॉर्म को भरकर सबमिट कर देते हैं और आपकी सारी जानकारियां हैकर्स के पास पहुँच जाती हैं.

हैकर को आपके बैंक खाते की जानकारी कैसे मिलती है?

उपरोक्त वर्णित कार्यविधि के अलावा पिछले कुछ वर्षों से, देश में ई-पेमेंट, ऑनलाइन शॉपिंग और कैशलेस भुगतान बढ़ने के साथ ही प्रतिदिन नए एप्लिकेशन और पेमेंट गेटवे बाज़ार में उतारे जा रहे हैं. जब भी आप इनके माध्यम से फ़ंड-ट्रांसफर या भुगतान करते हैं तो आपको अपने डेबिटकार्ड/क्रेडिट-कार्ड की जानकारियां "एप्लिकेशन" से लिंक करनी पड़ती हैं. ऐसे में कई जगहों से आपकी गोपनीय जानकारियां चोरी से हैकर्स तक पहुँच जाती हैं.

हैकर कैसे करता है, बैंक खाता हैक?

जब हैकर के पास आपके बैंक खाते का ब्यौरा और डुप्लीकेट सिमकार्ड आ जाता है तो वह आपके इंटरनेट बैंकिंग पर लॉगिन करता है, परंतु उसके पास पासवर्ड नहीं होता. पासवर्ड को वह रीसेट करता है. पासवर्ड रीसेट करने के लिए, एक ओटीपी आता है. सिम, हैकर के पास होने के कारण, ओटीपी उसे आसानी से मिल जाता है और हैकर इंटरनेट बैंकिंग के जरिए आपके खाते में सेंध लगा सकता है. यदि आपके पास इंटरनेट बैंकिंग की सुविधा नहीं है तो हैकर आपके डेबिट-कार्ड की सहायता से भी आसानी से धनराशि ट्रांसफर कर सकता है क्योंकि इसके लिए भी मोबाइल पर आने वाले ओटीपी की ही आवश्यकता पड़ती है. खाते में धोखाघड़ी से पीड़ित व्यक्ति को इस बात का पता भी नहीं चलता, क्योंकि बैंक का एसएमएस अलर्ट भी हैकर के पास मौजूद सिमकार्ड पर ही पहुँचेगा.

सिम स्वैप धोखाधड़ी से बचने के उपाय :

"सिम स्वैप धोखाधड़ी" से बचने हेतु निम्नलिखित बातों का ध्यान रखना आवश्यक है :

1. यदि आपके मोबाइल में नेटवर्क वाले क्षेत्र में भी देर तक जैसे कि 1 घंटे से अधिक समय तक नेटवर्क न आए, तो तत्काल किसी अन्य मोबाइल फोन से अपने मोबाइल सेवा प्रदाता से, इस विषय में बात करें.
2. भरोसेमंद ई-वॉलेट और ऑनलाइन शॉपिंग वेबसाइट का ही इस्तेमाल करें और ई-वॉलेट में सीमित रकम ही रखें.
3. फोन या ई-मेल पर, किसी को अपने बैंक खाते, डेबिट-कार्ड, क्रेडिट-कार्ड से संबंधित कोई जानकारी न दें. कोई भी बैंक, कॉल कर, आपसे कभी भी पिन/पासवर्ड नहीं पूछता.
4. आधार कार्ड का नंबर अनजान मोबाइल नंबर पर एसएमएस न करें. बैंक में जाकर स्वयं आधार नंबर पंजीकृत कराएं.

5. "व्हाट्सएप" और "फेसबुक" पर आने वाले, वेबसाइट के ऑफर संबंधी लिंक को न खोलें.

6. सोशल मीडिया साइट पर, कभी भी, अपनी पूरी जानकारी न दें. अगर देना भी चाहें तो सभी सुरक्षा विकल्प सक्रिय कर दें ताकि वही लोग आपके बारे में जान सकें, जिन्हें आप पहले से जानते हैं.

7. किसी भी प्रकार के स्पैम मेल को न खोलें. उनमें वायरस होने की सबसे ज्यादा संभावनाएं होती हैं, जो आपकी सारी जानकारियां हैकर तक पहुंचा सकते हैं. इस प्रकार के ई-मेल, देखते ही बिना खोले डिलीट कर दें.

8. किसी भी अंजान व्यक्ति को अपना मोबाइल फोन न दें. मोबाइल फोन में लॉक लगाकर उसे सुरक्षित रखें.

9. विश्वसनीय एप्लिकेशन पर ही मोबाइल बैंकिंग का उपयोग करें जैसे यू मोबाइल, यू कंट्रोल आदि. 'मोबाइल एप्लिकेशन' विश्वस्त स्त्रोत जैसे गूगल प्ले स्टोर, एपल स्टोर से ही डाउनलोड करें.

10. समय-समय पर अपने खाते का स्टेटमेंट जाँचते रहें. अगर खाते से संबन्धित कोई भी जानकारी, अपडेट करनी है तो स्वयं ही बैंक में संपर्क करें.

11. मोबाइल नंबर के साथ-साथ ई-मेल एड्रैस को भी अपने खाते से जोड़ें ताकि बैंक खाता हैक होने की स्थिति में आपको पूरी जानकारी ई-मेल द्वारा मिलती रहे.

12. अपने घर और आस-पास के दोस्तों, रिशतेदारों, बुज़ुर्गों, महिलाओं, को इस विषय में अवश्य जागरूक करें.

अगर खाता हैक हो जाए, तो क्या करें?

जैसे ही आपको अपने मोबाइल नंबर के "सिम स्वैप" होने का अथवा "खाते के हैक" होने का पता चले तो निम्नलिखित कार्य करें:

1. तत्काल संबन्धित बैंक शाखा में संपर्क कर, अधिकारियों को इस बारे में बताएं. धोखाधड़ी के विषय में लिखित सूचना दें और उसकी एक प्रति, अपने पास संभालकर रखें. टोल फ्री नंबर 1800222244 (यूनियन बैंक ऑफ इंडिया के ग्राहकों हेतु) पर भी शिकायत करें और की गयी शिकायत का संदर्भ क्रमांक और एसएमएस सुरक्षित रखें.

2. अविलंब खाते से संबन्धित सभी कार्ड और इंटरनेट बैंकिंग सेवा बंद करवा दें. कुछ दिनों के लिए बैंक खाते को ब्लॉक करा दें.

3. बैंक में लिखित सूचना देने के पश्चात नजदीकी पुलिस थाने में जाकर पुलिस की साइबर अपराध शाखा में भी घटना की प्राथमिक सूचना रिपोर्ट (FIR) दर्ज़ करवाएँ. इस प्रकार के केस में अपराधी के लिए सूचना प्रौद्योगिकी (संशोधित) अधिनियम 2008 और भारतीय दंड संहिता की विभिन्न धाराओं के तहत सजा और जुर्माने का भी प्रावधान है.

4. 30 दिनों में बैंक से जरूरी सहायता न मिलने पर, बैंकिंग लोकपाल से संपर्क करें. ग्राहक, रिज़र्व बैंक ऑफ इंडिया के डिप्टी गवर्नर को भी शिकायत भेज सकते हैं.

जिस गति से तकनीकी विकास हमारे देश में बढ़ता जा रहा है, उसी गति से तकनीक से होने वाले अपरोधों की संख्या भी बढ़ती जा रही हैं. अपराधी ऐसे लोगों को अपना निशाना बनाते हैं, जो आसानी से उनके बहकावे में आ सकें और उनको सारी जानकारियां दे दें. यदि हम थोड़ी सी सावधानी बरतें और अपने आस-पास के लोगों को जागरूक करें तो सिम स्वैप जैसे साइबर अपराधों पर लगाम लगाई जा सकती है. ग्राहकों को साइबर अपराधों से बचने हेतु एसएमएस द्वारा समय-समय पर भेजा जा रहा संदेश उनके बीच जागरुकता बढ़ाने हेतु एक प्रशंसनीय कदम है.

एसएमएस, ईमेल और फिशिंग के माध्यम से धोखाधड़ी

प्रणिता कोठावड़े
सहायक प्रबंधक
सतर्कता विभाग, कें. का. मुंबई

आधुनिक युग में प्रौद्योगिकी के नए आविष्कारों ने न सिर्फ मानव विकास को और अधिक गति प्रदान की बल्कि हमारे आस-पास के परिवेश के भी हर पहलू में अपनी उपस्थिति दर्ज की है. प्राचीन काल से लेकर आज के आधुनिक युग तक मनुष्य सभ्यता और शिष्टता के साथ प्रकृति एवं विज्ञान के संयोजन और सामंजस्य के साथ नए चीजों के आविष्कार और इनके तर्कपूर्ण प्रयोग के साथ अपने जीवन-शैली और जीवन स्तर में सुधार कर मानव समाज के विकास में नित नए आयाम स्थापित कर रहा है. यह कहना अतिश्योक्तिपूर्ण नहीं होगा कि प्रौद्योगिकी आज हमारे जीवन के सभी आयामों में मौजूद है. फ्रिज के ठंडे पानी से लेकर रसोई गैस पर बनाया गया खाना एवं अपने प्रियजनों से मोबाइल में की गई बातों से लेकर अपने दफ्तर एवं स्कूल में ले जाने वाले मोटर गाड़ी का प्रयोग भी विज्ञान की देन है. आज के युग में हम सभी प्रत्यक्ष एवं परोक्ष रूप से विज्ञान पर आश्रित है.

यदि हम बैंकिंग परिप्रेक्ष्य में विज्ञान के आविष्कारों के प्रयोग संबंध में बात करें, तो यह पाएंगे कि पिछले कुछ दशकों से बैंकिंग जगत ब्रिक बैंकिंग से डिजिटल बैंकिंग के रूप में स्थापित हो गया है. जीवन के हर पहलुओं की भांति बैंकिंग जगत ने भी विज्ञान के माध्यमों के बखूबी प्रयोग से अत्यंत आधुनिक एवं नवीन रूप में हम सभी के समक्ष प्रस्तुत है. आज के समय में शायद ही कोई व्यक्ति ऐसा होगा जिसके द्वारा बैंकिंग सेवाओं का प्रयोग न किया जा रहा हो. यदि हम पिछले एक दशक के बैंकिंग लेनदेन का विश्लेषण करें तो यह पाएंगे कि वर्तमान समय में पूर्व की तुलना में अधिकतर बैंकिंग लेनदेन को इंटरनेट एवं एसएमएस बैंकिंग के माध्यम से निष्पादित किया जा रहा है. आने वाले समय में इनकी संख्या में और भी अधिक वृद्धि होने का अनुमान है.

प्रतिस्पर्धा के इस युग में आज बैंकिंग के सभी लेनदेन को इंटरनेट के माध्यम से डिजिटाइज रूप में निष्पादित किया जा रहा है. बदलते परिवेश में आज के समय बैंक के ग्राहकों की अपेक्षाएँ भी बैंक से काफी बढ़ गई है. आज ग्राहक बैंकों द्वारा प्रदत्त सेवाओं का 24X7 प्रयोग कर अपने बैंकिंग लेनदेन को निष्पादित कर सकता है. आज बैंक का आधे से अधिक लेनदेन प्रौद्योगिकी के माध्यम से ही किया जा रहा हैं.

जिस प्रकार संसार के सभी पहलुओं में पक्ष एवं विपक्ष का गुण विद्यमान होता है, ठीक उसी तरह इंटरनेट और फोन बैंकिंग के भी सकारात्मक के साथ-साथ कुछ नकारात्मक प्रभाव हैं. उत्कृष्ट ग्राहक सेवा प्रदान करने एवं अपने बैंकिंग चैनलों के माध्यम से निर्बाध कार्यान्वयन हेतु साइबर धोखाधड़ी एवं उनका निवारण सभी बैंकों के लिए एक बड़ी चुनौती बनकर उभरी है. वर्तमान युग में बैंकिंग के ई-माध्यम हमारे दैनिक जीवन के महत्वपूर्ण एवं अभिन्न अंग बन चुके है परंतु इनमें निहित जोखिमों को नकारा भी नहीं जा सकता है. यद्यपि, बैंकिंग लेन-देनों एवं तकनीकी अंतरणों के संबंध में भारतीय रिजर्व बैंक एवं अन्य नियामक संस्थाओं द्वारा समय-समय पर दिशानिर्देश जारी किए जाते है, तथापि इन जोखिमों के संबंध में जागरूकता एवं सतर्कता मानदंडों का प्रयोग सभी ग्राहकों से अपेक्षित है.

प्रस्तुत आलेख में हम इंटरनेट और फोन बैंकिंग के माध्यम से होने वाले धोखाधड़ियों एवं उनसे बचने के उपाय के संबंध में विस्तार से चर्चा करेंगे.

एसएमएस बैंकिंगः

यदि हम पिछले कुछ वर्षों के आंकड़े देखें, तो यह पाएंगे कि बैंकिंग सेवाओं में एसएमएस एवं फोन बैंकिंग के माध्यम से निष्पादित किए जा रहे लेनदेनों में दिन-प्रतिदिन वृध्दि होती जा रही है. सर्वेक्षणों के अनुसार भविष्य में इन आंकड़ों की संख्या में और भी अधिक वृद्धि होने का अनुमान है. इन बढ़ते आंकड़ों के साथ इन लेनदेन में धोखाधड़ी की संभावना में भी वृद्धि होना स्वाभाविक है.

एसएमएस बैंकिंग सेवाओं से संबंधित धोखाधड़ी से बचने के लिए हमें इन माध्यमों के प्रयोग संबंधी सभी निर्धारित मानदंडों का अनुपालन करना चाहिए, जिससे किसी भी प्रकार की अप्रिय स्थिति से बचा जा सकें. हम इसके साथ मोबाइल बैंकिंग एवं एसएमएस बैंकिंग से संबंधित कुछ बिन्दु प्रदान कर रहें हैं, जिनके उचित अनुपालन से आप इनसे संबंधित धोखाधड़ी से अपने आप को सुरक्षित रख सकते हैंः

- अपने मोबाइल में सदैव एंटीवायरस का प्रयोग करें.
- आपके फोन के गुम हो जाने की स्थिति में तत्काल इसकी सूचना पुलिस विभाग को दें.

- आपके फोन में ऐसा पासवर्ड सेट करें, जिसका अनुमान कोई और आसानी से न लगा पाएं.
- किसी भी अपरिचित लिंक के माध्यम से बैंकिंग लेनदेन निष्पादित न करें.
- सार्वजनिक स्थानों में उपलब्ध वाई-फाई के प्रयोग से बचें.
- किसी अनजान दूरभाष नंबर से प्राप्त फाइलों को न खोले एवं इसकी सूचना सभी संबंधितों को दें.
- अपने मोबाइल फोन को नियमित अंतराल में अद्यतन करते रहें.
- अपने फोन बैंकिंग पासवर्ड को नियमित अंतराल पर बदलते रहें.
- अपना फोन नंबर बार-बार न बदलें.
- बैंकिंग से जुड़ी जानकारी एवं आंकड़ें फोन में सेव करके न रखें.
- किसी भी अंजान व्यक्ति को अपने बैंकिंग आंकड़ों यथा एटीएम कार्ड का नंबर, पिन क्रमांक आदि की जानकारी फोन/सोशल मीडिया पर प्रदान न करें.

ईमेल के माध्यम से धोखाधड़ीः

सर्वेक्षण ब्यूरो द्वारा किए गए सर्वे के माध्यम से यह निष्कर्ष पाया गया है कि वर्तमान समय में डिजिटल माध्यमों से किए जाने वाले धोखाधड़ियों में ईमेल का प्रयोग सबसे अधिक किया जाता है. अवांछनीय तत्वों के द्वारा नकली एवं जाली (फेक) ईमेल आईडी बनाकर पीड़ित व्यक्तियों को लिंक भेजा जाता है, जिसे महज क्लिक करने से पीड़ित व्यक्ति की सभी निजी जानकारी अवांछनीय तत्वों के पास पहुँच जाती है एवं वे इनके माध्यम से अपने निजी स्वार्थ के लिए इन सूचनाओं का दुरुपयोग करते हैं.

किसी भी व्यक्ति की यह नैतिक ज़िम्मेदारी है कि वह अपने बैंकिंग लेनदेन के लिए इंटरनेट बैंकिंग का प्रयोग करने से पहले इनसे संबंधित धोखाधड़ियों से अपने आप को जागरूक करे. जागरूकता एक ऐसा माध्यम है, जिसके सही ज्ञान से बैंकिंग संबंधी धोखाधड़ियों के संभावित खतरे से काफी हद तक बचा जा सकता है.

आम जनता तक बैंकिंग के व्यापक विस्तार को ध्यान में रखते हुए यह सरकार/नियामक संस्थाओं/बैंकों/ग्राहक प्रतिनिधियों की सामूहिक ज़िम्मेदारी है कि वे बैंकिंग उपभोक्ताओं को साइबर सुरक्षा से संबंधित मुद्दों पर जागरूक करें. इन समस्याओं से निपटने हेतु जन-स्तर पर कार्यशालाओं एवं संगोष्ठियों का आयोजन कराया जाना

चाहिए, जिससे भारी संख्या में लोगों को इस प्रकार की अप्रिय घटनाओं से बचने हेतु प्रशिक्षित किया जा सके.

ईमेल के माध्यम से होने वाले धोखाधड़ियों के संबंध में ग्राहकों द्वारा निम्नलिखित बिन्दुओं का अनुपालन सुनिश्चित किया जाना अपेक्षित हैः

- किसी भी अपरिचित आईडी से प्राप्त ईमेल के संलग्नक को न खोलें.
- ईमेल के माध्यम से अपने बैंक खातों एवं पिन/पासवर्ड की जानकारी कभी भी साझा न करें. बैंक कभी भी अपने ग्राहकों से ये जानकारियां नहीं मांगता.
- साइबर कैफे या अन्य सार्वजनिक स्थानों पर ईमेल आईडी के प्रयोग से परहेज करें.
- किसी भी ईमेल आईडी को खोलने से पहले उसकी प्रामाणिकता सुनिश्चित करें.
- पॉप अप के माध्यम से किसी भी ईमेल को न खोलें.
- प्रामाणिक इंटरनेट माध्यमों से ही अपना ईमेल आईडी लॉगिन करें.
- नियमित अंतराल में अपने ईमेल आईडी के पासवर्ड को बदलते रहें.
- कोशिश करें कि एक ईमेल आईडी को अधिक कम्प्यूटरों अथवा मोबाइल फोनों के माध्यम से लॉगिन न करें.
- अपने कम्प्यूटर एवं मोबाइल में हमेशा एंटिवाइरस अपडेट रखें.

फिशिंगः

फिशिंग ईमेल के माध्यम से ही किए जाने वाला एक ऐसा साइबर क्राइम है, जिसमें अपराधी द्वारा पीड़ित व्यक्ति को फर्जी ईमेल, टेलीफोन, टेक्स्ट आदि के जरिये संपर्क किया जाता है एवं उनकी व्यक्तिगत जानकारी को एकत्रित कर उनका प्रयोग अपने व्यक्तिगत स्वार्थ के लिए किया जाता है. अपराधी दुर्भावनापूर्ण लिंक या अटैचमेंट डिस्ट्रीब्यूट करने के लिए फिशिंग ईमेल का उपयोग करता है, ऐसे ई मेल में विभिन्न प्रकार के फंक्शन निहित होते हैं, जिसमें पीड़ितों से लॉगिन क्रेडेंशियल्स या बैंक अकाउंट इनफॉर्मेशन की चोरी भी शामिल है. फ़िशिंग अब साइबर क्रिमिनल्स में लोकप्रिय है, क्योंकि किसी कंप्यूटर के डिफेंस को तोड़ने की कोशिश करने के बजाय फ़िशिंग ईमेल पर दुर्भावनापूर्ण लिंक भेजकर किसी को फसाना अधिक आसान है. फ़िशिंग अटैक आमतौर पर सोशल नेटवर्किंग तकनीकों को अपना माध्यम बनाते हैं, जो ईमेल या अन्य

इलेक्ट्रॉनिक कम्युनिकेशन मेथड पर लागू होते हैं, जिनमें सोशल नेटवर्क, एसएमएस टेक्स्ट मैसेजेस और अन्य इंस्टेंट मैसेजिंग मोड आदि शामिल हैं. सफल फ़िशिंग मैसेजेस, जो आमतौर पर किसी प्रसिद्ध कंपनी से होने के रूप में दर्शाए जाते हैं और मूल मैसेजेस से उनकी तुलना करना मुश्किल होता है. फ़िशिंग ईमेल में कॉर्पोरेट लोगो और डाटा होता है, जिससे वह ईमेल असली लग सके. फ़िशिंग मैसेजेस में दुर्भावनापूर्ण लिंक को भी इस तरह से डिज़ाइन किया जाता है जैसे कि वह मूल दिखाई दे.

सभी बैंकिंग ग्राहकों को इंटरनेट बैंकिंग के प्रयोग से पहले उनके माध्यम से होने वाली सभी प्रकार की घटनाओं के संबंध में पूर्ण रूप से जागरूक होना चाहिए, जिससे वो अग्रसक्रिय होकर किसी भी प्रकार की अप्रिय स्थिति को टाल सकें.

आज के आधुनिक युग में बैंकिंग जगत एक नए परिवर्तन के दौर से गुजर रहा है और आने वाले समय में इन लेनदेन में और भी अधिक परिवर्तन आएंगे. तकनीक और बैंकिंग का यह समावेश निश्चित रूप से हम सभी के जीवन का एक अभिन्न अंग बन चुका है, परंतु इस सत्य को नहीं नकारा जा सकता हैं कि इनसे संबंधित घटनाओं की संख्या निरंतर बढ़ती जा रही है. ऐसे में यह हम सभी का दायित्व है कि इस प्रकार की घटनाओं से सचेत होकर सभी प्रकार के बैंकिंग चैनलों में इनका सावधानीपूर्वक प्रयोग करें और किसी भी प्रकार की अप्रिय स्थिति से निपटने के लिए सतर्क रहें.

एटीएम हमलों एवं धोखाधड़ियों के प्रकार

सावन सौरभ
प्रबंधक
क्षे. का. रांची

राधा रमण शर्मा
सहायक प्रबंधक
क्षे. का. कोल्हापुर

प्रदीप सिंह फोनिया
वरिष्ठ प्रबंधक
डिजिटल बैंकिंग, के.का. मुंबई

प्रस्तावनाः

देश को एक डिजिटल रूप में सशक्त समाज और ज्ञान आधारित व्यवस्था के रूप में परिवर्तित करने के दृष्टिकोण से डिजिटल इंडिया भारत सरकार का एक अग्रणी कार्यक्रम है. नकदी रहित लेनदेन को बढ़ावा देने और भारत को कम नगदी प्रयोग करने वाले कैशलेस समाज के रूप में परिवर्तित करने के एक भाग के रूप में डिजिटल भुगतान के ई-वॉलेट, कार्ड प्रीपेड/डेबिट/क्रेडिट, पॉइंट ऑफ सेल (पीओएस), यूनिफाइड पेमेंट इंटरफेस (यूपीआई), अनस्ट्रक्चर्ड सप्लीमेंट्री सर्विस डाटा (यूएसएसडी) चैनल आदि जैसे विभिन्न तरीके उपलब्ध है, तथापि भारत जैसी अर्थव्यवस्था में एटीएम के प्रयोग से निजात पाना अभी दूर की बात है.

भारत में डिजिटल भुगतान में अधिक वृद्धि तथा कम नकदी वाली अर्थव्यवस्था की दिशा में अग्रसर होने से देश की वित्तीय साइबर सुरक्षा अवसंरचना और तैयारी को सुदृढ़ बनाने की आवश्यकता पर नए सिरे से ध्यान दिया जा रहा है. बैंक और वित्तीय संस्थान विभिन्न प्रकार के साइबर हमलों और ऑनलाइन धोखाधड़ी हेतु अत्यधिक सचेत हैं. कोर बैंकिंग के अतिरिक्त ई बैंकिंग, एटीएम और खुदरा बैंकिंग जैसी सेवाएँ साइबर अपराध का नियमित निशाना बनती जा रही हैं. जून 2015 में 40000 से अधिक साइबर घटनाओं की जानकारी दी, जिनमें अन्य के अतिरिक्त मालवेयर प्रसार, वेब अतिक्रमण, फिशिंग, "डिस्ट्रीब्युटेड डिनायल ऑफ सर्विसेस अटैक्स और वेब निरूपण" आदि शामिल है. यद्यपि यह संख्या वास्तविक खतरे के स्तर को नहीं दर्शाती है क्योंकि कंपनियां और व्यक्ति प्रायः सुरक्षा को लेकर लापरवाह होते हैं और साइबर हमलों की रिपोर्ट दर्ज कराने के प्रति अनिच्छुक होते हैं. अलग-अलग रूप में ऐसे हमले बैंकिंग प्रणाली को बड़े पैमाने पर क्षति पहुंचा सकते हैं, परंतु हमला रणनीतियों सहित एक समन्वित दृष्टिकोण, जिसमें सूचना की चोरी और इसी प्रकार के अन्य उद्देश्यों हेतु मालवेयर की सहायता से प्रणालियों से सेंध लगाना और संक्रमित करना शामिल है, एक वास्तविक खतरा पैदा करता है. इन हमलों में एटीएम के माध्यम से धोखाधड़ी की घटनाओं का निरंतर बढ़ते रहना एक

संवेदनशील मामला है.

इससे पहले कि कोई हमारे एटीएम नेटवर्क के साथ छेड़छाड़ करे और उसको क्षति पहुंचाये, अच्छा होगा कि हम इस पर होने वाले हमलों/धोखाधड़ियों या जोखिम की प्रवृति को समझें और समय रहते उसका निदान खोजें. तकनीक के माध्यम से एटीएम नेटवर्क को पूर्णतया सुरक्षित रखने के लिए अपार संभावनाएँ तलाशनी अभी भी बाकी हैं. हम सभी लोग जानते हैं कि विगत कुछ वर्षों में एटीएम पर होने वाले हमलों या यूं कहें कि धोखाधड़ियों में विभिन्न प्रकार के मामले सामने आए हैं. अतः हम कह सकते हैं कि आज बैंकिंग क्षेत्र में एटीएम पर हमला/धोखाधड़ी एक अहम जोखिम एवं चुनौती बन गया है और ग्राहक एवं बैंक दोनों ही इसके शिकार हो रहे हैं.

एटीएम लगने से बैंकों के कार्य में आसानी तो हुई है लेकिन इससे जुड़े अपराधों में भी तेज़ी से वृद्धि हुई है. जाहिर है यदि हम ज्यादा से ज्यादा एटीएम लगाते हैं, तो हमें यह जानना भी बहुत जरूरी है कि अपने कार्ड धारकों को इन अपराधों से और बैंक को एटीएम पर होने वाले हमले/धोखाधड़ी से कैसे सुरक्षित रखा जाए.

आज के बढ़ते तकनीकी युग में अभी भी दुनिया में लेनदेन करने के लिए एटीएम एवं उस पर प्रयोग होने वाला कार्ड सबसे अधिक लोकप्रिय साधनों में से एक है. लेकिन आज के दौर में हम इसे केवल बैंक द्वारा दी गई एक सेवा न समझकर, यदि स्वयं भी इसे इस्तेमाल की आवश्यक वस्तु समझकर कुछ सावधानियों का ध्यान रखें तो हम इसके शिकार होने से बच सकते हैं, खासतौर पर तब जब कि दुनिया भर में इससे संबंधित अपराध के सर्वाधिक मामले सामने आ रहें हों. हमारा बैंक भी आरबीआई के एटीएम सुरक्षा से संबन्धित दिशा निर्देशों का पालन कर उसे हर संभव अमल कर रहा है और पूरी कोशिश जारी है कि हम ज़ीरो डे अटैक पर कायम रहें और अपने ग्राहकों को इस प्रकार के अपराधों से पूरी तरह से सुरक्षित रखे. हमने अपने स्विच, एटीएम और कार्ड को ईएमवी आधारित किया है, जिसके जरिए ग्राहकों का डाटा इंक्रीप्टेड रूप में सुरक्षित रहेगा.

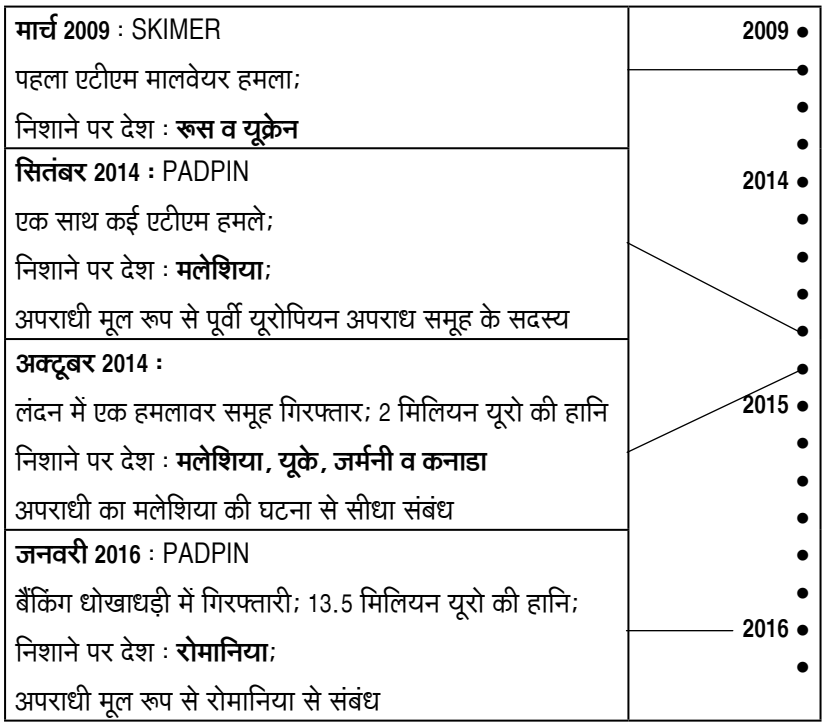
एटीएम हमलों एवं धोखाधड़ियों पर एक अवलोकनः

भारत में पिछले 10 वर्षों में एटीएम की संख्या 35 हज़ार से तेजी से बढ़कर 2.5 लाख के ऊपर पहुँच चुकी है, जाहिर है कि उतनी ही तीव्रगति से बैंकों का ग्राहक आधार भी बढ़ा है. अतः हम इस तथ्य को भी नकार नहीं सकते कि जिस तीव्रता से एटीएम लगे हैं उसी तीव्र गति से एटीएम पर होने वाले हमले या अपराध के तरीके भी बढ़े हैं और बैंकों के सामने ऐसे हमलों या अपराधों की रोकथाम एक ज्वलंत समस्या बनी हुई है या यूं कहे कि हमारे सामने अपने विशाल एटीएम नेटवर्क को पूर्णतया सुरक्षित रखना एक बड़ी चुनौती है. आज अपराधी एटीएम पर केवल अपराध की पुरानी तकनीक न अपनाकर नित

नई-नई तकनीकों का प्रयोग कर एटीएम पर अपराध कर रहे हैं.

यदि हमारे एटीएम पर ऐसी घटनाएँ नहीं हुई हैं, इसका मतलब यह नहीं कि हम ऐसे जोखिमों से पूर्णतया सुरक्षित हैं तो हमें यह नहीं समझना चाहिए कि हमारे एटीएम पूर्णतया सुरक्षित हैं बल्कि हमें अन्यत्र घट रही घटनाओं को ध्यान में रखते हुए इस प्रकार के जोखिमों से सुरक्षित रहने के लिए अपनी रणनीतियों को और चुस्त-दुरुस्त करते रहना चाहिए. विगत कुछ वर्षों में आरबीआई भी एटीएम सुरक्षा को लेकर बेहद संवेदनशील है और बैंकों को एटीएम की सुरक्षा के प्रति समय-समय पर दिशा निर्देश देता रहा है.

अगर हम आंकड़ों की बात करें तो वैश्विक स्तर पर आज तक कई ऐसे मामले सामने आए हैं, जिसके अंतर्गत कई देशों के एटीएम सिस्टम पर हमले हुए हैं. विश्व में एटीएम पर इन हमलों की शुरुआत सबसे पहले मार्च 2009 में एक एटीएम मालवेयर द्वारा रूस एवं यूक्रेन के एटीएम को स्कीमर द्वारा क्षति पहुंचा कर की गयी थी. एक प्रचलित अँग्रेजी समाचार पत्र टाइम्स ऑफ इंडिया (TOI) के रिपोर्ट के अनुसार इन आंकड़ों का सार इस फ्लो चार्ट के माध्यम से देख सकते हैं.



अप्रेल 2016 : ATMICH

एक साथ कई एटीएम हमले; $800,000 का नुकसान;

निशाने पर देशः **रूस व कज़ाकिस्तान;**

अपराधी का मूल रूप से पूर्वी यूरोपियन अपराधी संगठन से संबंध

जुलाई 2016 :

एक साथ कई एटीएम हैकिंग; 2 मिलियन डॉलर का नुकसान;

निशाने पर देशः **ताइवान**;

अपराधी का मूल रूप से पूर्वी यूरोपियन अपराधी संगठन से संबंध

जुलाई 2016 :

ताइवान में तीन विदेशी नागरिक गलत तरीके से नकदी निकालने हेतु गिरफ्तार;

16 अपराधियों का मूल रूप से एक अंतर्राष्ट्रीय अपराध समूह

अगस्त 2016 : RIPPER

एक साथ कई एटीएम हमले; 13 मिलियन डॉलर का नुकसान;

निशाने पर देशः **थाइलैंड**;

अपराधी का मूल रूप से पूर्वी यूरोपियन अपराधी संगठन से संबंध

नवंबर 2016 : ALICE

अंतर्राष्ट्रीय स्तर पर एक नया मालवेयर परिवार ALICE पाया गया.

जनवरी 2017

एटीएम हैकिंग के तहत गिरफ्तारी; 3 मिलियन यूरो की हानि;

निशाने पर देश : **ताइवान व बेलारूस**;

अपराधी मूल रूप से रोमानिया से संबंध

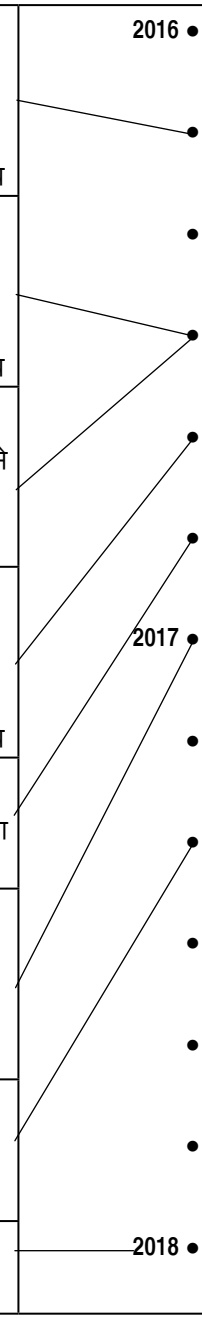
मई 2017 : BLACK BOX

यूरोप में हमला;

फ्रांस, नीदरलैंड, रोमानिया, स्पेन व नॉर्वे में कई गिरफ्तारियाँ

जनवरी 2018 : JACKPOTTING

अमेरिका में इस प्रकार के हमले; कई गिरफ्तारियाँ



एटीएम की सुरक्षा निश्चित रूप से एक चिंतनीय मुद्दा है. अतः यह जानना आवश्यक है कि एटीएम हमले कैसे होते हैं, इसका कारण क्या है और इस पर अंकुश लगाने के लिए क्या-क्या सावधानी बरती जानी चाहिए.

- **एटीएम मशीन पर हमलाः** इसके अंतर्गत एटीएम मशीन को क्षति पहुंचा कर हमले किए जाते हैं. जैसे लूट, **कार्ड स्किमिंग** (कार्ड क्लोनिंग, कार्ड ट्रेपिंग, कैशट्रेपिंग), मालवेयर द्वारा एटीएम मशीन पर हमला **(जैकपॉटिंग)**, एटीएम धोखाधड़ी के पुराने तरीके इत्यादि.

- **लूट :** यह सबसे आम हमला है जिससे एटीएम मशीन को भौतिक रूप से हटाने का या फिर उनसे छेड़-छाड़ करने का प्रयास किया जाता है और उसमें संरक्षित धन की चोरी की जाती है.

- **कार्ड क्लोनिंग :** क्लोन शब्द से ही स्पष्ट है कि कार्ड की समरूप प्रति तैयार की जाती है. इसके लिए हमलावरों द्वारा स्कीमर मशीन का प्रयोग किया जाता है, जिसे वे एटीएम मशीन में लगा देते हैं. कार्ड धारक के कार्ड स्वाइप करते ही कार्ड की सारी जानकारी इस मशीन में कॉपी हो जाती है. इसके बाद हमलावर इसकी सारी जानकारी एक खाली कार्ड में कॉपी कर लेते हैं. इस क्लोन कार्ड को दूर किसी स्थान से उपयोग कर लाखों का चूना लगाया जाता है. इसी प्रकार ठग कई एटीएम मशीनों में एक किट लगा देते हैं, जिसमें कीपेड पर एक मैट जैसा उपकरण, स्वाइप की जगह कॉपी मशीन और पासवर्ड देखने के लिए एक बटन जैसा कैमरा लगा होता है. मशीन में जितने कार्ड स्वाइप होते हैं, उनका डाटा इस उपकरण में स्टोर हो जाता है और फिर शुरू होता है, उसका खाली कार्ड में कॉपी कर दुरुपयोग.

- **कार्ड ट्रेपिंग :** यह भी एक प्रकार का स्किमिंग है, किन्तु इसमें कार्ड की क्लोनिंग ना करके सीधे कार्ड को पुनः प्राप्त करने से रोक कर इसे अंदर फाँसा जाता है और कीपेड पर एक मैट सा उपकरण लगा कर इसका पासवर्ड हैक किया जाता है और बाद में इससे कार्डधारक का सारा पैसा निकाल लिया जाता है.

- **कैश ट्रेपिंग :** स्किमिंग का यह भी एक नायाब तरीका है. इस प्रकार की चोरी में नकदी डिस्पेन्सर के सामने एक डिवाइस लगा दी जाती है, जिसमें कार्ड डिटेल भरने पर नकदी बाहर निकालने के बजाए उसमें फंस जाती है. ग्राहक यह समझता है कि मशीन में कोई त्रुटि है या फिर कोई तकनीकी समस्या है, किन्तु वास्तविकता इससे परे होती है. वास्तव में एटीएम से छेड़छाड़ की गयी होती है और ग्राहक के जाते ही हमलावर, जो आस-पास ही बैठकर इंतजार कर रहा होता है, उस मशीन से धन निकाल लेता है.

- **जैकपॉटिंग :** जैकपॉटिंग में हमलावर एटीएम में मालवेयर द्वारा मशीन की प्रणाली को संक्रमित कर देता है. यह उन्हें धोखाधड़ी करने में मदद करता है. मालवेयर का उपयोग हमलावर विशेष रूप से वर्चुअल स्किमिंग डिवाइस के रूप में करता है. जब कोई ग्राहक इस प्रकार मालवेयर से संक्रमित एटीएम का उपयोग नकदी निकालने के लिए करता है, तो उनकी नकदी तो निकल जाती है किन्तु इस वर्चुअल स्कीमर के पास उनके खाता संबंधी सारी जानकारी लॉग हो जाती है. मालवेयर या तो इसे वायरलेस के रूप से हमलावर के सिस्टम में भेज देता है या फिर हमलावर बाद में इस डाटा को कॉपी कर लेते हैं.

- **एटीएम धोखाधड़ी के पुराने तरीके :** आज के इस डिजिटल युग में हो सकता है कि हम एटीएम धोखाधड़ी के पुराने तरीकों को नज़र अंदाज कर दें, जिसके तहत एटीएम पर शारीरिक रूप से हमला करने या फिर जासूसी करने की संभावना होती है. किन्तु सुरक्षा के दृष्टिकोण से आवश्यक है कि हम सावधान रहें. आज भी दुर्भाग्यवश एटीएम हमलावरों को तकनीकी रूप से दक्ष होना आवश्यक नहीं है और ना ही कोई ऐसे तकनीकी उपकरण की आवश्यकता है, अपितु कोई भी आपको बंदूक की नोक पर रख कर एटीएम पर ले जाकर आपके कार्ड से नकद निकालने या फिर पिन की जानकारी देने हेतु मजबूर कर सकता है. आम तौर पर ये घटनाएँ अब कम हो गई हैं किन्तु आज भी इस प्रकार की घटनाएँ हमें सुनने को मिल ही जाती हैं. इसके लिए आवश्यक है कि ग्राहक सजग रहें, अगर आपके आस-पास कोई व्यक्ति स्वतः मदद के लिए आगे आए अथवा आपके द्वारा दर्ज किए जाने वाले पिन को देखने के लिए आपसे काफी सट कर खड़ा हो अथवा आपको लगे कि कोई आपकी जासूसी कर रहा है.

- **एटीएम जैकपॉट हमला (ATM Jackpot) :** इस प्रकार की धोखाधड़ी में यूएसबी (USB) के जरिये एटीएम में मालवेयर (Malware) प्रवेश कराके या यूं कहें कि एटीएम नेटवर्क को हैक करके मालवेयर के जरिये एटीएम सॉफ्टवेयर को नियंत्रण में लिया जाता है ताकि एटीएम से कैश खाली किया जा सके. इस प्रकार की धोखाधड़ी से बचने के लिए हमें सुनिश्चित करना होगा कि हर मशीन में एक विशिष्ट यूज़र नाम तथा पासवर्ड (User Name & password) हो. एटीएम में सिस्टम लॉक डाउन की विधि भी प्रयोग की जानी चाहिए. हमें यह भी सुनिश्चित करना चाहिए कि एटीएम में BIOS पासवर्ड रखा जाये ताकि एटीएम केवल प्राइमरी हार्ड डिस्क (Primary Hard Disk) से ही बूट (Boot) हो और किसी भी अनधिकृत माध्यम जैसे CD-ROM & USB का प्रयोग न हो सके. एटीएम निर्माताओं को यह सुनिश्चित करना चाहिए कि ओएस को पूरी तरह से Hardened किया जाये व हार्डडिस्क को पूरी तरह से सुरक्षित रखा जाये.

- **डेनोमिनेशन (Denomination) धोखाधड़ी :** यह धोखाधड़ी प्रायः किसी आंतरिक व्यक्ति जैसे एटीएम इंजीनियर या सीआरए के द्वारा की जा सकती है, जिसमें कैसेट्स के डेनोमिनेशन को बदल दिया जाता है, जैसे 500 वाली कैसेट्स को 100 वाली कैसेट्स के साथ कॉन्फ़िगर कर दिया जाता है. एटीएम सॉफ्टवेयर एवं ऑपरेटिंग सिस्टम को पूर्णतया हार्डनिंग करके कुछ हद तक इसे रोका जा सकता है.

- **एटीएम कार्ड (डेबिट/क्रेडिट कार्ड) पर हमला :** इस के अंतर्गत साइबर हमले के साथ-साथ ग्राहकों को झांसे में लेकर उनके व्यक्तिगत एवं गोपनीय जानकारी की चोरी या फिर सीधे उनकी कार्ड की अदला-बदली शामिल है, जिसके द्वारा ऑनलाइन लेन-देन के जरिए कार्ड धारक के धन की चोरी की जाती है. भारत में आज सबसे प्रचलित तरीका यही है. इसे हम आम बोलचाल में तकनीकी शब्द फिशिंग (Phishing) कहते हैं.

- **गुम एवं चोरी हुए कार्ड द्वारा धोखाधड़ी :** कार्ड के भौतिक रूप से गुम या चोरी हो जाने पर अपराधी द्वारा स्वयं को ग्राहक के रूप में प्रस्तुत कर अनधिकृत लेनदेन किए जाते हैं. इस प्रकार की धोखाधड़ी को अंजाम देने के लिए अपराधी द्वारा ग्राहक का कार्ड चोरी कर लिया जाता है और कार्ड गुम होने की सूचना बैंक को दिए जाने के बीच में उसका गलत इस्तेमाल कर धनराशि निकाल ली जाती है इस प्रकार की धोखाधड़ी से बचने के लिए जैसे ही आपका कार्ड कहीं गुम हो जाता है अथवा चोरी हो जाता है तो उसकी सूचना संबंधित बैंक की ब्रांच को तुरंत प्रदान करें अथवा बैंक के टोल फ्री नंबर पर तुरंत सूचित करें.

- **कार्ड की आईडी की चोरी :** अपराधी द्वारा कार्ड के ब्योरों को प्राप्त कर उसकी जानकारियों का उपयोग वास्तविक नाम से नया कार्ड खाता खोलने अथवा वास्तविक खाते के अधिग्रहण के लिए किया जाता है. इस प्रकार के अपराधों से बचने के लिए कोई भी व्यक्तिगत जानकारी किसी के साथ शेयर नहीं करनी चाहिए. कार्ड का सीवीवी नंबर, उसका पिन या कार्ड का नंबर किसी भी व्यक्ति को नहीं बताना चाहिए.

- **मेल प्राप्त न होने पर धोखाधड़ी :** ग्राहक को जारी नए अथवा पुराने कार्ड के बदले जारी कार्ड को गलत ढंग से प्राप्त कर उसका पंजीकरण करा लिया जाता है और धोखाधड़ी द्वारा उसका प्रयोग किया जाता है. इस प्रकार की धोखाधड़ी से बचने के लिए आप किसी भी अनजान कॉल से आए फोन को कार्ड से संबंधित कोई भी जानकारी न दें.

- **फर्जी पहचान :** किसी भी अपराधी व्यक्ति द्वारा गलत नाम अथवा अल्पकालीन पते का प्रयोग करके फर्जी पहचान देकर धोखाधड़ी की जाती है.

- **कार्ड से छेड़छाड़ करना :** कार्ड में उपस्थित धातु पट्टी को शक्तिशाली चुंबक द्वारा मिटा कर उसमें निहित ब्योरों को मिटा कर किसी अन्य वैध कार्ड में परिवर्तित कर दिया जाता है. कार्ड के कार्य न करने की स्थिति में अपराधी द्वारा कार्डधारक को चकमा देकर कार्ड के विवरणों को मैन्युअली प्रविष्ट कर दिया जाता है.

- उपर्युक्त प्रचलित धोखाधड़ियों के अलावा कैश ट्रेपिंग (Cash Trapping), डाईवर्जन (Diversion), अटेंडेंट (Attendant), घोस्ट एटीएम (Ghost ATM) एवं कार्ड स्वेपिंग (Card Swapping) जैसी धोखाधड़ियों को केवल ग्राहक जागरूकता के जरिए ही नियंत्रित किया जा सकता है. अभी तक तकनीक के जरिए ऐसी धोखाधड़ियों को रोकने में सफलता नहीं मिली है. केवल ऑनसाइट कैमरे के जरिये ही इसे सुलझाया जा सकता है या यूं कहे कि एटीएम साइट पर क्या करें और क्या न करें (सुरक्षा से संबंधित उपाय) की जानकारी भी ग्राहकों को दी जा सकती है. आज के दौर में ग्राहक जागरूकता बैंक के लिए एक महत्वपूर्ण विषय बन गया है. इसके जरिये ही हम ग्राहकों को समय-समय पर धोखाधड़ी संबन्धित जानकारी देकर पूर्णरूप से सतर्क एवं जागरुक बना सकते हैं.

आज इन सभी कारणों से अवगत होकर अन्य कारणों की खोज से ज्यादा आवश्यक है कि हम कैसे स्वयं को विभिन्न प्रकार के एटीएम धोखाधड़ी से और बेहतर तरीके से बचा सकते हैं. तकनीकी रूप से सक्षमता ऐसी किसी भी समस्या से निपटने में सहायक होती है.

अतः आवश्यक है कि हम रोज कुछ ऐसी नई जानकारियाँ ग्रहण करते रहें एवं उससे स्वयं को अद्यतन रख कर अपने सभी जानने वालों को ऐसे हमलों से एवं उन्हें उससे बचाने के तरीकों से अवगत कराते रहें. संदिग्ध गतिविधियों के संकेतों को तलाशी करें और सतर्क रहें. स्थान एवं समय कोई भी हो, अगर ऐसी कोई भी स्थिति नज़र आती है, तो उस एटीएम को तत्काल छोड़ कर दूसरे एटीएम मशीन का उपयोग करने का विकल्प चुनें. ध्यान रखें कि अगर कोई एटीएम ऐसे स्थान पर हो, जो या तो असुरक्षित हो या दूर एकांत में हो या फिर जहां पर्याप्त रोशनी न हो, ऐसे एटीएम को छोड़ किसी अन्य एटीएम का पता करें. आज गूगल जैसी कंपनियाँ आपको सदैव आस-पास के एटीएम और स्थानों की जानकारी आपके स्मार्टफोन पर तत्काल उपलब्ध करा देती है. भारत सरकार ने भी स्थान का सटीक पता लगाने के लिए एक जीआईएस (Geographic Information System) - डाटा तैयार किया है और इससे बैंक की सभी शाखाओं एवं एटीएम को जोड़ने को कहा गया है. यह सभी डाटा आप जीआईएस की साइट/एप पर भी देख सकते हैं.

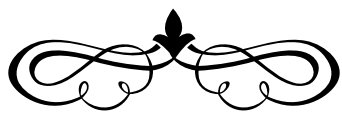
एटीएम पर नकदी की निकासी से पूर्व एटीएम की अच्छी तरह जांच कर लें कि एटीएम से कोई छेड़छाड़ तो नहीं की गई है. निकासी के समय अपने आस-पास नज़र

रखें. मशीन के सामने इस प्रकार खड़े रहें कि मशीन का स्क्रीन एवं की बोर्ड कोई अन्य न देख पाए. एटीएम में यह भी अनुशंसा की जाती है कि एटीएम लेनदेन के रिकॉर्ड को एटीएम के पास ना फेकें अपितु या तो इसे अपने साथ ले जाएं या फिर पूर्णतया नष्ट कर एटीएम के अंदर स्थित कूड़ेदान में डालें.

चिप कार्ड का प्रयोग करें : ऐसे भुगतान कार्ड का प्रयोग सदैव बेहतर होता है, जिसमें ईएमवी चिप होता है. इसका कारण यह है कि यह तकनीकी तौर पर स्कीमर्स से बचने के लिए आपके भुगतान कार्ड (डेबिट कार्ड/क्रेडिट कार्ड) को बेहतर तरीके से सुरक्षित करती है. अतः अगर अभी भी आपकी जेब में ईएमवी चिप कार्ड नहीं है तो तुरंत अपने सेवा प्रदाता बैंक से पुराने कार्ड बदलवा कर ईएमवी चिप कार्ड ले लें.

अपने एटीएम कार्ड को सुरक्षित रखें. उससे जुड़ी कोई भी गोपनीय जानकारी किसी से भी साझा न करें. एटीएम के पिन/पासवर्ड कहीं लिखे नहीं अपितु इसे याद रखें और समय-समय पर बदलते रहें. व्यापक तौर पर कहें तो सतर्क रहें एवं स्वयं के एटीएम सुरक्षा एवं सतर्कता संबंधी जानकारी से अन्यों को अवगत कराकर सभी को सुरक्षित रखने का हर संभव प्रयास करें.

जैसा कि विगत कुछ वर्षों में देखा गया है कि लगभग सभी वित्तीय संस्थानों द्वारा भारत सरकार के डिजिटल इंडिया के प्रोत्साहन हेतु हर क्षेत्र में डिजिटलाइजेशन पर काफी काम हुआ है, लेकिन जिस गति के साथ हम लोग इस क्षेत्र में आगे बढ़े हैं, उस गति से इससे जुड़ी हुई धोखाधड़ियों या यूं कहें कि साइबर अपराध या जोखिम को पूरी तरह से रोकने में नाकाम रहें हैं. हालांकि हाल के कुछ वर्षों से आरबीआई (RBI) ने इस दिशा में बहुत आक्रामक रुख अख्तियार किया है, सभी वित्तीय संस्थानों को इस ओर निरंतर सचेत किया जा रहा है. हर संस्था में सीसो (CISO) की उपस्थिति इस ओर उठाया गया एक महत्वपूर्ण कदम है. अतः यह कहना भी अतिशयोक्ति नहीं होगा कि आने वाले समय में डिजिटल बैंक एवं साइबर सुरक्षा अपने आप में पूर्णतया एक पूरे बैंक का ही आकार न ले ले. बैंक द्वारा इस विषय पर पुस्तक का प्रकाशन करना भी भारत सरकार के साइबर सुरक्षा अभियान को तीव्रता प्रदान करने से कम नहीं है. सरकारी रेगुलेशन, एनपीसीआई दिशानिर्देश, वेंडर तकनीक एवं ग्राहक जागरूकता के जरिए हम इसे सुरक्षित एवं अभेद्य बना सकते हैं. अतः हमें जरूरत है कि हम अपनी सम्पूर्ण प्रक्रिया एवं प्रणाली पर नज़र दौड़ाएँ तथा संवेदनशील क्षेत्रों व उससे जुड़े क्षेत्रों की पहचान कर आवश्यक कदम उठाएँ, ताकि सिस्टम आधारित जोखिमों का समय रहते निदान हो सके और विभिन्न हितधारकों का बैंक की मजबूती व अखंडता (Strength & Integrity) पर जो विश्वास है, वह भी बना रहें.



मोबाइल एक, खतरे अनेक

राहुल गुप्ता
वरिष्ठ प्रबंधक
भोपाल मुख्य शाखा

श्वेता सिंह
प्रबंधक (राजभाषा)
क्षे. म. प्र. का. कोलकाता

आज हम मोबाइल को जीवन के लिए अपरिहार्य वस्तु कहें तो कोई अतिश्योक्ति नहीं होगी. मोबाइल इस सदी का अविश्वसनीय एवं अत्यंत उपयोगी अविष्कार है. यह सदा हमारे साथ रहता है और आज विश्व में सर्वाधिक इस्तेमाल किया जाता है. यही नहीं, विश्व की जितनी आबादी है, मोबाइल फोनों की संख्या उससे अधिक हो गई है.

भारत में मोबाइल के नाम से प्रचलित स्मार्ट फोन की महत्ता से आज प्रत्येक व्यक्ति परिचित है. देश में आज 45 करोड़ से अधिक स्मार्ट मोबाइल फोन का प्रयोग हो रहा है तथा एक सर्वे के अनुसार इनकी संख्या 16 प्रतिशत वार्षिक की दर से बढ़ रही है. निःसंदेह मोबाइल फोन से इमरजेंसी में निकट सम्बन्धियों, दोस्तों, डाक्टर और पुलिस से संपर्क करने, घर से बाहर होने पर परिवार, दोस्तों या दफ्तर वालों से संपर्क करने, किसी को तत्काल महत्वपूर्ण संदेश पहुंचाने, किसी दुर्घटना का चित्र खींचने, समाचारों के तुरंत प्रेषण आदि जैसे बहुत लाभ हैं, परंतु प्रत्येक लाभकारी वस्तु का एक धुंधला पक्ष भी होता है. ऐसे में मोबाइल फोन का समुचित उपयोग करने की आवश्यकता है क्योंकि हम लाभ प्राप्ति के इतने आदी हो चुके हैं कि कई बार नकारात्मक पक्ष की उपेक्षा कर देते हैं.

प्रायः दैनिक समाचार पत्रों के पृष्ठ ऐसी घटनाओं से भरे पड़े रहते हैं, जिनमें यह बताया जाता है कि मोबाइल फोन का उपयोग करते हुए किस प्रकार अपराधियों ने किसी बड़ी दुर्घटनाओं को अंजाम दिया. एक बड़ी घटना जिसने समाचार पत्र वाचकों का ध्यान अपनी ओर आकृष्ट किया, वह थी जर्मनी के हेमबर्ग शहर में बच्चों द्वारा अपने माता-पिता के विरुद्ध किया गया एक विरोध प्रदर्शन. इस विरोध प्रदर्शन के पीछे मुख्य कारण था माता-पिता एवं अभिभावकों द्वारा मोबाइल का अधिक इस्तेमाल करना तथा बच्चों की ओर कम ध्यान देना. इस प्रदर्शन में सात वर्षीय एक नन्हीं बालिका ने भी भाग लिया. एटीएम कार्ड का नंबर चुरा कर तथा अन्य गोपनीय जानकारी प्राप्त कर खातों से धन स्थानांतरण करने तथा ऑनलाइन खरीददारी कर लेने के मामलों में वृद्धि हुई है. इसी तरह मोबाइल के अत्यधिक उपयोग के चलते स्वास्थ्य संबंधी समस्याओं ने भी जन्म

लिया है. ये समस्याएं कोई आम समस्याएं नहीं हैं, बल्कि कई प्रकार की बीमारियों का समन्वित रूप लेकर हमारे सामने चुनौती पूर्ण ढंग से खड़ी हैं. ऐसे में आज आवश्यकता है, मोबाइल फोन के उपयोग से होने वाली हानियों पर व्यापक जागरूकता उत्पन्न करने की. इस लेख के माध्यम से हम ऐसी ही कुछ समस्याओं तथा उनके समाधान पर प्रकाश डालेंगे.

मोबाइल के खतरे :

स्मार्ट फोन का उपयोग करने वाले व्यक्ति को स्वयं भी स्मार्ट होने की आवश्यकता है. यदि ऐसा नहीं है तो साइबर अपराधी उक्त व्यक्ति के मोबाइल का उपयोग कर महत्वपूर्ण सूचनाएं प्राप्त कर सकते हैं तथा प्राप्त जानकारियों से बहुत बड़ी हानि पहुंचाने में सक्षम हो जाते हैं. 21वीं सदी में उन्नति एवं विकास का आधार सूचनाएं ही हैं. ऐसे में सूचनाओं का अपने हित में लाभ उठाना अपराधियों के लिए कोई दूर की कौड़ी नहीं है. मोबाइल फोन विशेष रूप से स्मार्ट मोबाइल फोन सूचना एवं संवेदनशील जानकारियों के भंडार होते हैं. ऐसे में दुस्साहसी लोग किसी भी प्रकार की चूक से लाभ उठा सकते हैं. साइबर अपराधी निम्नलिखित प्रकार से मोबाइल फोन से सूचना चुराकर अपने पक्ष में उसका लाभ उठा सकते हैं :

1. **ऐप्लिकेशन्स के जरिए जानकारियां गलत हाथों में पहुंचना :** प्रायः यह देखा जाता है कि बहुत सारे एन्ड्राईड अथवा आईओएस एप्स हमसे मोबाइल फोन का मैसेजिंग, फोटो, विडियो इत्यादि का डाटा उपयोग करने की अनुमति इंस्टौलेशन के दौरान ही ले लेते हैं. कई एप्लिकेशनों का इस डाटा से कोई प्रत्यक्ष संबंध नहीं होता है, फिर भी वे ऐसे डाटा की जानकारी अपने निर्माताओं तक पहुंचाते हैं. इतना ही नहीं उक्त एप्स में दिखने वाले विज्ञापनों तक भी मोबाइल उपयोगकर्ता की जानकारी पहुंचती है. हो सकता है कि कई कम्पनियों का उद्देश्य केवल लोगों के व्यवहार की जानकारी हासिल करना हो, किंतु ऐसी जानकारियाँ अपराधियों के हाथ भी लग सकती हैं. किसी के मोबाइल की संपर्क सूची द्वारा दूर किसी अन्य देश में बैठा हुआ व्यक्ति भी हजारों लोगों के विषय में जानकारी हासिल कर लेता है. ऐसे में आवश्यकता इस बात की है कि यदि आवश्यक न हो तो प्रत्येक जानकारी को मोबाइल ऐप्लिकेशन्स के साथ साझा न किया जाए.

2. **असुरक्षित वाई-फाई :** संभवतः कोई भी जानबूझकर अपना शत्रु बनना नहीं चाहेगा, किंतु जब कहीं पर निःशुल्क वाई-फाई सेवा मिल रही हो तो लोग अपना मोह नियंत्रित नहीं कर पाते. ऐसे में वे निःशुल्क वाई-फाई का आनंद लेने के लिए जल्दी से पासवर्ड पता करते हैं तथा अपने मोबाइल से असीमित डाउनलोड सुविधा

का लाभ उठाने लगते हैं. कई लोग तो अपने व्यक्तिगत फोटो तथा विडियो भी ऐसे सार्वजनिक नेटवर्क से साझा करने लगते हैं. वे ऑनलाइन भुगतान प्रणाली एवं अन्य बैंकिंग सुविधाओं का उपयोग करने से भी नहीं चूकते और यहीं पर उनसे भूल हो जाती है, जिसका खामियाज़ा इन्हें अपनी मूल्यवान जानकारियां तथा गोपनीय तस्वीरें अपराधियों को साझा करके भुगतना पड़ता है. ब्रिटेन की तीन राजनैतिक हस्तियों ने स्वयं को एक निःशुल्क वाई-फाई मुहिम का हिस्सा बनाया. उक्त हस्तियों के भुगतान विवरण तथा गोपनीय वार्तालापों को साइबर सुरक्षा विशेषज्ञों द्वारा हैक करके सार्वजनिक वाई-फाई के उपयोग के प्रति आगाह किया था. अतः आवश्यकता इस बात की है कि सार्वजनिक वाई-फाई का उपयोग जहाँ तक संभव है न किया जाए, यदि करना भी पड़ता है तो समुचित सावधानी रखते हुए किसी भी प्रकार के संवेदनशील कार्य को मोबाइल फोन के माध्यम से ऐसे नेटवर्क पर न किया जाए.

3. **फर्जी नेटवर्क :** किसी सार्वजनिक स्थान पर जैसे रेस्तरां, काफी शॉप, रेलवे स्टेशन इत्यादि पर हैकरों द्वारा फर्जी नेटवर्क एक्सेस पाइंट बना दिये जाते हैं. इन पाइंट को भोलेभाले उपयोगकर्ता द्वारा निःशुल्क वाई-फाई सेवा समझ लिया जाता है. ऐसे में वह वाई-फाई से जुड़कर स्वयं अपना नुकसान कर लेता है. इन नेटवर्क के नाम भी प्रचलित सार्वजनिक स्थानों के नाम पर रखे जाते हैं. जैसे कॉफी शाप या लाइब्रेरी आदि-आदि. इन नामों के जाल में उपयोगकर्ता आसानी से फँस जाता है तथा अपने मोबाइल अथवा टेबलेट को नेटवर्क से जोड़ लेता है. ई-मेल तथा ई-कॉमर्स का उपयोग करना यहाँ पर बहुत भारी पड़ सकता है. ऐसे में ध्यान रखें कि सार्वजनिक वाई-फाई के माध्यम से संवेदनशील गतिविधियों का उपयोग न करें.

4. **फिशिंग हमले :** सोशल मीडिया तथा ई-मेल के माध्यम से कई फर्जी लिंक भेजी जाती है. इन लिंक पर क्लिक करते ही उपयोगकर्ता हैकरों के वेबसाइट पर पहुंच जाता है. उपयोगकर्ता को लगता है कि वह किसी उपयोगी जानकारी वाली वेबसाइट अथवा किसी नयी आनलाइन शापिंग वेबसाइट पर पहुंच गया है और वह अपनी समस्त वांछित जानकारी अवांछित लोगों को दे देता है. ऐसे में वह फिशिंग का शिकार हो जाता है. यहाँ ध्यान देने की बात यह है कि इस तरह के यूआरएल को हाथ से टाइप करके खोलें तथा वह सुरक्षित है अथवा नहीं यह अपने ब्राउजर की सैटिंग्स से भी जाँच लें.

5. **स्पाईवेयर :** स्पाईवेयर ऐसे जासूसी साफ्टवेयर होते हैं, जो उपयोगकर्ता का कोई अपना ही उसके कम्प्यूटर पर स्थापित कर उपयोगकर्ता की गतिविधियों पर दृष्टि रखता है. ऐसे में उपयोगकर्ता के लिए आवश्यक है कि मोबाइल पर किसी उच्च

स्तरीय एंटीवायरस का उपयोग किया जाए.

6. **कमजोर वेबसाइटों के माध्यम से जानकारी चुराना :** कुछ वेबसाइटों की कोडिंग इस तरह की होती है, जिन्हें हैकर आसानी से हैक कर लेते हैं. ऐसी वेबसाइटों पर यदि उपयोगकर्ता पहुंच जाते हैं, तो उनकी महत्वपूर्ण जानकारी मसलन उनके द्वारा फीड किया गया डाटा वेबसाइट से हैकर चुराकर उसका आपराधिक गतिविधियों में उपयोग करते हैं.

7. **ऐप्लिकेशन पर अनुपयुक्त सत्र प्रबंधन :** अपने ऐप्लिकेशन को अधिक आसान एवं तेज बनाने की होड़ में कई सेवा प्रदाता ऐप्लिकेशन के सत्रावसान (सेशन एडिंग अथवा लॉग आउट) किये जाने की प्रक्रिया को उपयुक्त तरीके से सुरक्षित नहीं बनाते. बिना सत्यापन के ही इन ऐप्लिकेशन्स पर कई बार संव्यवहार हो जाते हैं. यह टोकन जनरेट करते हैं, यह टोकन उस डिवाइस पर कई गतिविधियों को संचालित करने के लिए एक ही बार जनरेट होते हैं. इस तरह की ऐप्लिकेशन का उपयोग बहुत खतरनाक हो सकता है. इसके खतरे को समझते हुए ध्यान रखना चाहिए कि ऐसे एप्स का उपयोग करें, जिनमें चाहे सत्यापन हेतु अधिक समय लगे, किंतु सुरक्षा मानकों का पूरा ध्यान रखा गया हो.

8. **असक्रिय एप्स :** कुछ एप्स बिना कारण बताए प्ले स्टोर पर अनुपलब्ध कर दिये जाते हैं अथवा उनके अपडैट बंद हो जाते हैं. ऐसे एप उपयोगकर्ताओं की जानकारी हासिल करते रहते हैं. ऐसे में आवश्यकता इस बात की है कि इन एप्स को अपने मोबाइल से हटा दिया जाए.

9. **मोबाइल का खो जाना :** मोबाइल फोन का खो जाना केवल आर्थिक तौर पर नुकसानदायक नहीं है. इससे मोबाइल धारक की बहुत सी गोपनीय जानकारियाँ अपराधी के पास पहुंच सकती हैं, जिससे कई प्रकार के नुकसान हो सकते हैं. यदि फिंगर प्रिंट पासवर्ड वाला फोन अथवा चेहरे के सामने लाने पर स्क्रीन खुलने वाला फोन उपयोग में लाया जाए तो और भी अच्छा रहेगा.

10. **विकिरण का जंजाल :** अपने जीवन में हम बहुत प्रकार के विकिरणों का सामना करते हैं. विकिरणों से बचना संभव भी नहीं है क्योंकि प्रत्येक इलेक्ट्रिक अथवा इलेक्ट्रानिक उपकरणों से कुछ न कुछ मात्रा में विकिरण उत्पन्न होता है. मोबाइल फोन द्वारा जिस प्रकार का विकिरण उत्पन्न होता है, वह बहुत घातक है क्योंकि वह इलेक्ट्रोमेग्नेटिक विकिरण होता है. वैसे तो इस विकिरण को शरीर सहन कर सकता है, किंतु लगातार इस विकिरण को प्राप्त करते रहने से ब्रेन ट्यूमर तथा कैंसर का खतरा होने की संभावना बढ़ जाती है. अखिल भारतीय आयुर्विज्ञान

संस्थान, दिल्ली का एक शोध बताता है कि लगातार 10 वर्षों तक मोबाइल फोन का उपयोग करने वालों को ब्रेन ट्यूमर का खतरा 33 प्रतिशत अधिक हो जाता है. एक इजराइली शोध बताता है कि मोबाइल फोन के अधिक इस्तेमाल से पुरुषों में शुक्राणुओं की संख्या में कमी आ जाती है तथा नवजात शिशु का मस्तिष्क कम विकसित हो सकता है, उसका आकार छोटा रह सकता है. इसके साथ ही मानसिक क्षमता के विकास में भी कमी आ जाती है. प्रत्येक मोबाइल के विकिरण की जानकारी उसकी सैटिंग्स में अबाउट वाले विकल्प में दी जाती है. प्रत्येक मोबाइल उपयोगकर्ता उसे वहाँ से जान सकता है. इसके साथ ही धातुओं के संपर्क में लाने पर मोबाइल का विकिरण बढ़ जाता है, अतः आवश्यकता इस बात की है कि हम अपने मोबाइल को शरीर से दूर रखें. जेब में न रखकर इसे अपने बैग अथवा किसी अन्य स्थान पर रखें. हैंड्सफ्री विकल्प का चयन करें. लिफ्ट आदि में जाते समय मोबाइल का उपयोग न करें क्योंकि वहाँ पर विकिरण का खतरा अधिक रहता है. जब मोबाइल फोन का इस्तेमाल नहीं कर रहे हैं तो उसे ऐरोप्लेन मोड में रखें. कम्पनियों को भी अपने उत्पाद के विकिरण स्तर की जानकारी स्पष्ट रूप से मोबाइल फोन के कवर पर ही छाप देनी चाहिए.

11. **मोबाइल फोन की लत :** मोबाइल फोन का अत्यधिक उपयोग करने से लोगों पर नकारात्मक प्रभाव पड़ने लगा है. लगातार फ़ोन बजने से, अलर्ट आने से, अनुस्मारक आने से फ़ोन के उपयोगकर्ता पर तनाव पड़ता है. स्मार्ट मोबाइल फ़ोन के इस्तेमाल का संबंध सोने में गड़बड़ी, तनाव, अवसाद आदि के लक्षण पुरुष और महिला दोनों में पायें जाते हैं. कुल मिलाकर, अत्याधिक मोबाइल फ़ोन के उपयोग से युवा पीढ़ी के मानसिक स्वास्थ्य पर खतरा मंडरा रहा है.

बार-बार मोबाइल फोन का उपयोग करते रहना, किसी से बात करते हुए भी मोबाइल पर ध्यान होना, सोने से पहले मोबाइल तथा उठने के बाद मोबाइल को सबसे पहले देखना, मोबाइल का डाटा बंद हो जाने पर बेचैनी अनुभव करना, प्रत्येक 15 मिनट में मोबाइल पर ध्यान जाना, प्रत्येक मैसेज के आने पर उसे देखना, ये सभी ऐसी गतिविधियाँ हैं, जो किसी व्यक्ति को मोबाइल फोन की लत होने की ओर संकेत करती हैं. यह ठीक वैसा ही है जैसे किसी को किसी नशीले पदार्थ की लत हो जाती है. इसके परिणाम स्वरूप आँखों से धुंधला दिखाई देने लगता है. गर्दन एवं पीठ में दर्द रहता है. सुनने की क्षमता में कमी आती है. स्मरणशक्ति का अभाव हो जाता है. भारत में मोबाइल उपयोगकर्ताओं की संख्या 2021 में 81 करोड़ हो जाएगी. ऐसे में मोबाइल से जुड़े हुए शारीरिक एवं मानसिक खतरों में भी वृद्धि होगी. आवश्यकता इस बात की है कि हम अपने जीवन में

कोई समय ऐसा निर्धारित करें, जब हम इलेक्ट्रानिक अथवा डिजिटल उपकरणों से दूर रहें. इसके साथ ही लत अथवा आदत के स्तर तक पहुंचने वाले मोबाइल फोन अथवा टेबलेट के उपयोग को कम करें, उस पर नियंत्रण करें. टाइम पत्रिका के अध्ययन बताते हैं कि 68 प्रतिशत लोग सोते समय अपने मोबाइल फोन को पास में रखकर सोते हैं तथा 44 प्रतिशत लोग तो अपने तकिये के पास ही फोन को रखकर सोते हैं. स्मार्ट फोन की यह लत नोमो (मोबाइल के पास न रहने का डर) तथा मोमो (बाहरी दुनिया से मोबाइल के बिना कट जाने का भय) फोबिया होने लगता है. फोन के कंपन तथा बार-बार मोबाइल फोन के बजने का भ्रम फेंटम फोन फोबिया नामक बीमारी के रूप में जन्म लेता है. विश्वभर में मोबाइल फोन एवं कम्प्यूटर नशा मुक्ति केन्द्र खोले जा रहे हैं. जहाँ पर ऐसे लोगों को अपने इलेक्ट्रानिक उपकरणों से दूर रखा जाता है.

इस समस्या के निराकरण के रूप में कहा जा सकता है कि इन खतरों से बचने के लिए मोबाइल का न्यूनतम उपयोग करना चाहिए, उसे लत नहीं बनने देना चाहिए. विश्राम के समय मोबाइल को साइलेंट या एरोप्लेन मोड पर रखा जाना चाहिए ताकि हम आराम के वक्त सुकून महसूस कर सकें और उठने पर नई चेतना और जोश के साथ काम में जुट जाएं.

12. **प्रतिरक्षा प्रणाली में बीमारियों का खतरा बढ़ जाता है :** अपने मोबाइल फ़ोन को लगातार छूने से आप मोबाइल फोन पर चिपके रोगाणु के संपर्क में आते है. आप एक दिन के उपयोग के बाद अपने मोबाइल फ़ोन पर देख सकते हैं कि जो चिकने, तेल अवशेष दिखाई पड़ते हैं, उसकी तुलना उन बीमारियों के कीटाणुओं जैसी हैं जो शौचालय की सीट पर पाये जाते हैं : एक अनुसंधान से यह पता चला है कि 92 प्रतिशत मोबाइल फ़ोन पर कीटाणु जमा होते हैं, 82 प्रतिशत कीटाणु हमारे हाथों में रहते हैं - इससे मलीय पदार्थ एक फ़ोन से दूसरे फ़ोन में, एक व्यक्ति से दूसरे व्यक्ति में स्थानांतरित हो सकते हैं. इस समस्या के निराकरण के रूप में कहा जा सकता है कि मोबाइल प्रयोग के बाद साबुन से अथवा सेनेटाइजर से हाथ साफ ज़रूर करना चाहिए.

13. **अपरिपक्व दिमाग़ वाले व्यक्तियों को आशंकित ख़तरे :** किशोर अवस्था के बच्चे एवं वयस्क परन्तु मानसिक तौर पर अविकसित लोग अक्सर गलत लोगों की संगत में फंसकर अपनी आदतें खराब कर लेते हैं और मोबाइल पर इन्टरनेट की सहायता से अश्लील साहित्य पढ़कर या अश्लील चित्र/वीडियो देख कर अपनी मानसिकता दूषित कर लेते हैं और फिर ये लोग ही कुत्सित दुर्भावनाओं का शिकार हो कर समाज में घृणित दुष्कर्मों में संलिप्त हो जाते हैं. इस समस्या के निराकरण

के लिए पालकों को अपने बच्चों के साथ क्वालिटी टाइम बिताना चाहिए, इससे उनके मस्तिष्क भटकने से बच सकते हैं.

अपरिपक्व मस्तिष्क वाले लोगों को विश्वास में लेकर इनके मस्तिष्कों का रुझान गलत दिशा से हटा कर सही दिशा की ओर करने के यत्न किये जा सकते हैं और कहते हैं न "कोशिशें ही कामयाब होतीं हैं....." सकारात्मक विचारों वाले व्यक्ति समाज की पूंजी होते हैं. इनसे ही समाज का जीर्णोद्धार एवं विकास संभव है. अतः हमें मोबाइल से संभावित इन दूरगामी दुष्प्रभावों से यथासंभव बचने एवं अन्य लोगों को बचाने के प्रयत्न करने चाहिये.

14. **आँखों एवं अन्य अंगों पर दुष्प्रभाव :** मोबाइल को अधिक समय तक घूरने पर भी हमारी दृष्टि पर गलत प्रभाव होता है. उनके अधिकतर प्रयोग से आँखों पर तनाव बढ़ जाता है. मोबाइल के स्क्रीन कंप्यूटर से कई गुना छोटे होते हैं और उन्हें देखने के लिए तटस्थ निगाह डालना पड़ता है, इस से आँखों में तनाव और भी अधिक हो जाता है. आगे चलकर इसी कारण से लोगों में नेत्र संबंधित समस्याएं उत्पन्न होने लगती हैं. मोबाइल के अत्यंन्त उपयोग से हमारी शारीरिक मुद्रा में भी परिवर्तन आ सकता है, जिसके पीठ एवं गर्दन पर नकारात्मक प्रभाव पड़ सकते हैं. समस्या के निराकरण के रूप में कहा जा सकता है कि मोबाइल के इस दुष्प्रभाव से बचने के लिए हमें मोबाइल के उपयोग के दौरान अपने शरीर को बीच -बीच में आराम देना चाहिए.

15. **वाहन चलाते समय मोबाइल का उपयोग :** हम यह भी कह सकते हैं कि मोटर दुर्घटनाओं के प्रमुख कारणों में एक गाड़ी चलाते समय मोबाइल का उपयोग करना है. कई देशों में गाड़ी चलाते वक्त फोन का उपयोग करना नियम विरुद्ध माना जाता हैं. इससे बचने के लिए हमें अपने देश में न सिर्फ़ तगड़ा कानून बनाना होगा, बल्कि इस बुरी आदत से खुद को दूर रखना होगा और समाज को इस खतरे से बचना होगा.

16. **गर्भवती महिलाएं एवं बच्चों के लिए मोबाइल :** इसके अलावा हम यह भी देख सकते हैं कि मोबाइल फोन के उपयोग से गर्भवती महिलाओं के व्यवहार में एवं समस्याओं के साथ पैदा होने वाले बच्चों की आशंका बनी रहती है. उनके एक दिन में दो या तीन बार मोबाइल के उपयोग से उनके बच्चों में भावानात्मक समस्याओं के उत्पन्न होने का भी खतरा है. इस समस्या के निराकरण के रूप में कहा जा सकता है कि मोबाइल के इस दुष्प्रभाव से बचने के लिए गर्भवती महिलाओं को इसका उपयोग कम करना चाहिए. स्पीकर फोन का उपयोग करना भी कारगर हो सकता है.

17. **लापरवाही से हो सकने वाले ख़तरे :** आये दिन हम अख़बारों में खबरें पढ़ते हैं कि एक व्यक्ति रेलवे ट्रैक/रोड पर कानों में ईयर फोन लगा कर मोबाइल से गाने सुन रहा था, ट्रेन/वाहन के आने की आवाज़ और उसके हॉर्न को वह न सुन सका और दुर्घटना घट गई या फिर मोबाइल पर बात करते हुए सड़क पार करते वक्त दोनों ओर ध्यान न देने से दुर्घटना हो गई. इसी प्रकार रात को सोते समय मोबाइल सिरहाने रख कर चार्ज करने एवं ओवर चार्ज होने से उसमें ब्लास्ट हो गया और दुर्घटना घटी. इस समस्या के निराकरण के रूप में कहा जा सकता है कि हमें मोबाइल के उपयोग के समय सावधानीपूर्वक कार्य करना चाहिए. आज कल जो मल्टीटास्किंग यानि एक समय में कई कार्य करने का फैशन चल पड़ा है, उसे अत्यन्त समझ बूझ कर इत्मिनान से करना चाहिये. चार्जिंग के समय मोबाइल को शरीर से दूर रखना चाहिए और उस पर ध्यान रखना चाहिए कि वह ओवर चार्ज न हो जाये. वैसे आजकल ऐसे मोबाइल चलन में आ गए हैं जो पूरी तरह चार्ज होने पर स्वतः चार्जिंग बन्द कर देते हैं.

18. **मोबाइल द्वारा अपराध :** मोबाइल फोन के प्रचलन ने साइबर अपराधों को बढ़ावा दिया है. आज विश्वभर में पोर्नोग्राफी तथा अन्य आपराधिक कृत्यों को मोबाइल फोन, विशेष रूप से स्मार्ट फोन के माध्यम से तेजी से अंजाम दिया जा रहा है. बच्चों पर इसका बुरा प्रभाव पड़ रहा है. अधिकांश मामलों में यह पाया गया है कि अपराधियों ने अपने दुष्कर्म मोबाइल फोन पर देखकर ही किए थे.

19. **डिजिटल बैंकिंग में मोबाइल फोन का उपयोग :** ऑनलाइन कारोबार के बढ़ने से आनलाइन धोखाधड़ी भी बढ़ी है. आज क्रेडिट कार्ड का नंबर चुराना, पासवर्ड हैक करना, फिशिंग के जरिये वित्तीय व्यवहार की जानकारी हासिल करना, फोन पर कपट द्वारा जानकारी प्राप्त कर लेना इत्यादि कई ऐसे अपराध हैं जिन्हें अंजाम दिया जाता है. ऐसे अपराधों से स्वयं को बचाने के लिए निम्नांकित उपचारात्मक उपाय अपनाए जाने चाहिए :

- किसी सार्वजनिक स्थान, जैसे साइबर कैफे अथवा रेलवे स्टेशन के वाई-फाई का उपयोग करते हुए अपना बैंक ट्रांजेक्शन न करें.
- अपने डेबिट तथा क्रेडिट कार्ड की जानकारी को फोन में सेव करके न रखें.
- क्रेडिट एवं डेबिट कार्ड की संव्यवहार सीमा को उपयोग न किए जाने पर लॉक करें अथवा उसे कम करें.
- हमेशा ऑनलाइन शापिंग से जुड़ी हुई वेबसाइट के यूआरएल को अपने हाथ से टाइप करें.

- अस्थायी क्रेडिट कार्ड नंबर भी कुछ कम्पनियों द्वारा जारी किए जाते हैं. किसी असुरक्षित स्थान पर लेन-देन करना पड़े, तो ऐसे अस्थायी नंबरों का प्रयोग करें.
- जहाँ तक संभव हो कम्प्यूटर द्वारा इंटरनेट बैंकिंग का उपयोग करें.
- कुछ अन्य बातें जो ध्यान रखना आवश्यक हैं :

अपने बच्चों की इंटरनेट गतिविधियों पर ध्यान रखें. यदि उनका व्यवहार संदिग्ध पाया जाता है तो उनसे बात करें. मोबाइल फोन अथवा अन्य किसी डिजिटल उपकरणों के उपयोग से बच्चों को पूरी तरह रोक पाना संभव नहीं है, किंतु वे उसका किस तरह से उपयोग कर रहे हैं, यह जानना अति आवश्यक है. यदि आपके कम्प्यूटर अथवा मोबाइल फोन की हिस्ट्री को लगातार मिटाया जाता है, तो यह संदेह करने का उपयुक्त कारण होता है. ऐसे में बात करके हिस्ट्री मिटाने वाले व्यक्ति से जानना आवश्यक होगा कि वह ऐसा क्यों कर रहा है.

अपने साफ्टवेयर तथा आपरेटिंग सिस्टम को हमेशा अपडैट करके रखें. यदि ऐसा नहीं करते हैं तो बहुत से जोखिम भरे मालवेयर अथवा वायरस मोबाइल में प्रवेश कर सकते हैं. ऐसे में यह आवश्यक है कि अपने मोबाइल फोन से जुड़ी हुई समस्त सुरक्षा व्यवस्था को पुख्ता करें तथा सारे पैचेस को समय पर इन्स्टॉल करें.

सोशल मीडिया का उपयोग बहुत सावधानीपूर्वक किया जाना चाहिए. अपनी निजी जानकारियों तथा व्यक्तिगत फोटोग्राफ्स को बिना सोचे-समझे किसी के साथ भी साझा किया जाना बहुत महंगा सौदा हो सकता है. ऐसे में यह आवश्यक है कि हम अपने लिए सही और गलत को समझें. चैटिंग करते समय यह ध्यान रखा जाना चाहिए कि किसी अजनबी व्यक्ति को विडियो काल न किया जाए क्योंकि कई बार विडियो काल की रिकार्डिंग कर उसका गलत लाभ उठाने की कोशिश अपराधियों द्वारा की जाती है.

साइबर अपराधों की रोकथाम

साइबर अपराधों की रोकथाम हेतु भारत सरकार द्वारा एक पोर्टल शुरू किया गया है. यह पोर्टल वर्तमान में बाल पोर्नोग्राफी पर केन्द्रित है. इस पोर्टल पर मोबाइल फोन से जुड़े हुए तथा साइबर अपराधों की शिकायत बिना पहचान बताए दर्ज की जा सकती है. इसमें महत्वपूर्ण जानकारी जो पूछी जाती है, वह है नाम, फोन, ईमेल, घटना अथवा अपराध जो हुआ है. ओटीपी के माध्यम से शिकायतकर्ता का सत्यापन किया जाता है.

पोर्टल का पता है https://cybercrime.gov.in/cybercitizen/home.htm

उपर्युक्त अध्ययन से यह कहा जा सकता है कि प्रकृति ने मनुष्य में दिमाग़ का प्रादुर्भाव सुविचारों एवं उच्च उद्देश्यों की पूर्ति के लिए किया था. अगर मनुष्य बुरी संगत में पड़कर या भटक कर अपने समाज के अहित के लिए मस्तिष्क का दुरूपयोग करने लगता है तो यह कदम आत्मघाती कहलायेगा.

उसी प्रकार मनुष्य के लिए मोबाइल भी एक वरदान भी है और एक अभिशाप भी. अगर इसका सन्तुलित एवं उपयोगी साधन के रूप में उपयोग किया जाये तो यह एक अच्छा दोस्त है, वरना यह इस्तेमाल करने वाले का मालिक बन कर उसका विनाश भी कर सकता है.

एक कहावत से इसे और अच्छी तरह समझा जा सकता है-

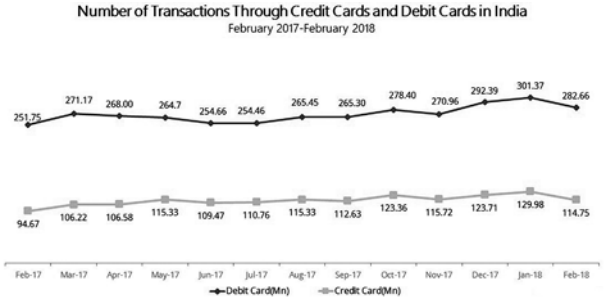
अति का भला न बोलना,
अति की भली न चुप
अति का भला न बरसना,
अति की भली न धूप.

इस तरह से हम पाते हैं कि मोबाइल फोन अथवा स्मार्ट फोन एक उपयोगी उपकरण होकर भी कई कारणों से खतरनाक साधन बन गया है. आज आवश्यकता इस बात की है कि हम 21वीं सदी के इस उत्तम आविष्कार के गुण एवं इसके दोष को समझते हुए इसका समुचित उपयोग करें. इस विषयक जागरूकता का प्रचार-प्रसार करें ताकि इसके उपयोग से होने वाली किसी भी दुर्घटना से बच सकें.

कार्ड धोखाधड़ी

सुनील दत्त,
प्रबंधक (राजभाषा)
क्षे. का. दिल्ली (दक्षिण)

भारतीय रिज़र्व बैंक के आंकड़ों के अनुसार फरवरी 2017 से जून 2018 तक क्रेडिट कार्ड एवं डेबिट कार्ड से किए जाने वाले लेनदेनों (Transactions) का कुल मूल्य रु. 362256 करोड़ था.



इन आंकड़ों से कार्डों की लोकप्रियता का सहजता से अनुमान लगाया जा सकता है.

इन कार्डों के बढ़ते प्रयोग से, जहां एक ओर कार्डधारकों को अनेक प्रकार की नई बैंकिंग सुविधाएँ प्राप्त हुई हैं वहीं, दूसरी ओर कई बार उन्हें, नए प्रकार के खतरों का भी सामना करना पड़ता है. मुख्य रूप से कार्ड से संबंधित धोखाधड़ी दो प्रकार से होती है, पहला - खो गए अथवा चोरी किए कार्डों के द्वारा और दूसरा नकली या क्लोन किए गए कार्डों द्वारा.

यहां पर यह समझना आवश्यक है कि आखिर कार्ड क्लोनिंग अथवा स्किमिंग होती क्या है? भारतीय रिज़र्व बैंक की परिभाषा के अनुसार, कार्ड क्लोनिंग से डेबिट अथवा क्रेडिट कार्ड की चुम्बकीय पट्टी पर दर्ज सूचनाओं की अनधिकृत एवं अवैध रूप से नकल कर, प्राप्त की गई सूचनाओं से क्लोन या नकली कार्ड बनाकर, विभिन्न प्रकार की धोखाधड़ी की जाती है.

यदि आप सोच रहे हैं कि कार्ड की 'क्लोनिंग' अथवा नकल करना कोई अत्यन्त कठिन या तकनीकी कार्य है, तो आप गलत हैं. कार्ड पर लिखी सूचनाओं की चोरी करने में, मात्र कुछ सेकेंड ही लगते हैं और यह कार्य एक अत्यंत छोटे से उपकरण के माध्यम से किया जा सकता है, जिसमें से केवल असली कार्ड को ठीक उसी प्रकार एक बार गुजारना होता है, जैसे कि हम किसी एटीएम या पॉस में करते हैं. इस उपकरण में कार्ड 'स्वाइप' करने से, कार्ड की सारी सूचनाएँ उसमें 'स्टोर' हो जाती हैं, जिससे नकली 'क्लोन' कार्ड बनाकर उसका दुरुपयोग कर लिया जाता है.

इस प्रकार की कार्ड क्लोनिंग में, सामान्यतः यह पाया गया है कि कार्ड क्लोन करने वाले लोग, अधिकतर सेल्समैन, होटल के वेटर, पेट्रोल पंप पर कार्य करने वाले कर्मचारी इत्यादि का सहयोग लेते हैं. यदि आप अपने कार्ड को, किसी अन्य के हाथों में सौंप रहे हैं तो इस बात की सावधानी बरतें कि कहीं वह व्यक्ति आपके कार्ड की क्लोनिंग तो नहीं कर रहा है.

यहां पर यह ध्यान देने की बात है कि कार्ड की क्लोनिंग होने के लिए यह आवश्यक नहीं है कि यह तभी हो, जब आप अपने कार्ड को किसी और व्यक्ति के हाथों में दे रहे हों वरन कार्ड की क्लोनिंग आपके द्वारा कार्ड के प्रयोग के दौरान भी हो सकती है और वह भी बिना आपकी जानकारी के. जब आप एटीएम से पैसे निकालने जाते हैं तो सामान्यतः आप अपना कार्ड खुद 'स्वाइप' करते हैं, परन्तु यह भी संभव है कि उस एटीएम मशीन में असली कार्ड रीडर के ऊपर नकली 'कार्ड रीडर' लगा हो, जो आपके कार्ड की क्लोनिंग कर उसमें निहित सूचनाओं को कापी कर रहा हो.

कार्ड क्लोनिंग के संदर्भ में, इस संभावना से भी इन्कार नहीं किया जा सकता है कि आपके कार्ड की क्लोनिंग आपको कार्ड मिलने के पहले ही कर ली गई हो. यदि आपने कार्ड के लिए आवेदन किया है तो यह अवश्य सुनिश्चित करें कि कार्ड आपको सुरक्षित रूप से बंद लिफाफे में ही प्राप्त हुआ हो. यदि कार्ड आपको खुले लिफाफे में प्राप्त हो या आपको किसी प्रकार का भी संदेह हो तो उसे स्वीकार न करें और संबंधित बैंक को तुरंत उसकी सूचना दें.

एटीएम कार्ड की क्लोनिंग के साथ-साथ, कई बार क्लोनिंग करने वाले लोग एटीएम में एक कैमरे का प्रयोग भी करते हैं, जिससे कार्ड प्रयोगकर्ता के पिन की चोरी संभव हो जाती है. 'पिन' की चोरी के लिए एक और तरीके का प्रयोग भी किया जाता है, जिसमें एटीएम के 'की-बोर्ड' पर एक नकली 'की-बोर्ड' लगा दिया जाता है, जो पिन की सूचना दर्ज कर उन्हें क्लोनिंग करने वाले व्यक्ति को प्रेषित कर देता है.

चेतावनी, संकेत एवं सावधानियां

जैसा कि हमने देखा, कार्ड की क्लोनिंग विभिन्न प्रकार से की जा सकती है. एक कार्ड-उपभोक्ता अपनी सतर्कता से क्लोनिंग के खतरे को कम कर सकता है. कार्ड-उपभोक्ता को क्लोनिंग से संबंधित कुछ चेतावनी संकेतों से सावधान रहना चाहिए. इन संकेतों में से कुछ निम्न प्रकार के हो सकते हैं :-

(i) एटीएम पर व्यवहार करने से पहले, क्या आप ध्यान देते हैं कि एटीएम देखने में सामान्य लग रहा है और उसमें कुछ असामान्य परिवर्तन नहीं है ?

(ii) क्या एटीएम में कहीं खुले तार, टेप या गोंद इत्यादि तो नहीं दिखाई दे रहा है?

(iii) क्या कार्ड रीडर सामान्य दिख रहा है? कहीं उसमें उपर से कुछ और तो नहीं लगा हुआ प्रतीत हो रहा है?

(iv) एटीएम पर पिन डालते समय क्या स्क्रीन पर **** (स्टार) दिखायी दे रहा है?

(v) कार्ड से खरीदारी करते समय कैशियर अथवा अन्य कर्मचारी आपका कार्ड लेकर, अल्प समय के लिए आपके सामने से हट तो नहीं गया है?

(vi) क्या दुकान का कैशियर या कर्मचारी आपका कार्ड, एक से अधिक बार 'स्वाइप' तो नहीं कर रहा है?

(vii) कहीं आप होटल में या किसी दुकान पर अपना कार्ड, बिल के भुगतान के लिए या किसी को ले जाने के लिए तो नहीं दे रहे हैं?

(viii) कहीं आप पेट्रोल भरने के बाद कार में बैठे-बैठे कार्ड देकर पेट्रोल का भुगतान तो नहीं कर रहे हैं?

(ix) क्या आप अपने कार्ड के स्टेटमेंट को ध्यान से देखकर उसकी जॉच करते हैं?

यदि आपको लगता है कि उक्त में से कुछ सावधानियाँ आप नहीं रखते हैं, तो तुरन्त अपने कार्ड के स्टेटमेंट और खाते की जांच करें और संदेह होने पर आवश्यकता अनुसार 'पिन' परिवर्तित कर लें या कार्ड के द्वारा आगे व्यवहार रोक देने के लिए संबंधित बैंक को सूचित करें.

क्लोन कार्ड के दुरुपयोग

कार्ड की चोरी अथवा क्लोनिंग के उपरांत, उसके द्वारा अधिकतर मामलों में वस्तुओं या सेवाओं की खरीदारी कर ली जाती है, जिसका बिल कार्ड उपभोक्ता के पास पहुंचता है. यदि कार्ड की क्लोनिंग के साथ- साथ, पिन की चोरी भी हो जाती है, तो कई बार क्लोन कार्ड से, एटीएम द्वारा धनराशि भी निकाल ली जाती है.

एक आँकड़े के अनुसार, क्लोन कार्ड धोखाधड़ी के 60% मामले इंटरनेट, टेलीफोन या डाक द्वारा खरीदारी के होते हैं, जिसे सी.एन.पी. (Cardholder-Not-Present) धोखाधड़ी भी कहा जाता है.

क्लोनिंग रोकथाम के उपाय

कार्ड क्लोनिंग रोकने के लिए तकनीकी रूप में भी कई प्रकार के उपाय किए गए हैं. इस संदर्भ में, हाल ही में 'भारतीय राष्ट्रीय भुगतान निगम' ने कुछ दिशानिर्देश जारी किए हैं, जो मुख्य रुप से निम्नवत हैं :-

(i) एटीएम कार्ड रीडर में 'जिटर' (Jitter) तकनीक का प्रयोग

(ii) कार्ड क्लोनिंग की रोकथाम प्रणाली - कार्ड प्रोटेक्शन किट (CPK) का प्रयोग करना

(iii) पिन पैड की सुरक्षा प्रणाली लगाना

(iv) एटीएम कक्ष में अतिरिक्त कैमरे लगाना

(v) हर एटीएम पर सुरक्षा गार्ड की पदस्थापना करना

(vi) ग्राहकों को जागरूक करना

जिटर (Jitter) तकनीक

जिटर तकनीक का प्रयोग, उन एटीएम में किया जा सकता है, जिसमें 'मोटर' से चलने वाले कार्ड रीडर लगे होते हैं अथवा जिन एटीएम में कार्ड मशीन द्वारा अंदर खींच लिया जाता है. जिटर तकनीक में एटीएम, कार्ड को रूक-रूक कर अंदर खींचता है और सूचनाएं पढ़ता है, जिसके कारण यदि कोई बाहरी कार्ड क्लोनिंग उपकरण लगा भी हो तो वह ठीक प्रकार से सूचनाएं ग्रहण नहीं कर पाता.

यह तकनीक उन एटीएम में प्रभावी नहीं हो सकती जहां पर कार्ड उपभोक्ता द्वारा कार्ड रीडर में डालकर निकाल लिया जाता है अर्थात स्वाइप किया जाता है.

सीपीके (CPK) तकनीक

सीपीके (Card Protection Kit) तकनीक से लगातार प्रसारित संकतों के द्वारा किसी बाहरी क्लोनिंग उपकरण को कार्ड की सूचनाओं को पढ़ने से रोका जा सकता है.

एसडीके (SDK) तकनीक

एसडीके (Surface Detection Kit) तकनीक के द्वारा एटीएम के कार्ड रीडर के ऊपर लगाए गए किसी उपकरण की पहचान की जा सकती है और आवश्यकतानुसार

एटीएम कार्ड रीडर अथवा एटीएम मशीन को बंद कर क्लोनिंग की संभावना कम की जा सकती है.

ईएमवी चिप कार्ड (EMV Chip Card)

ईएमवी कार्ड को चिप कार्ड या स्मार्ट कार्ड के नाम से भी जाना जाता है. इसका नाम यूरोपे, मास्टर कार्ड एवं वीज़ा के पहले अक्षर को मिलाकर EMV कार्ड रखा गया था. इस प्रकार के कार्ड में सूचनाएं चिप में सुरक्षित रखी जाती हैं, जिसकी नकल या क्लोनिंग करना अत्यंत कठिन होता है. इन कार्डों की लागत अधिक होती है और इनके लिए विशेष कार्ड रीडर की आवश्यकता होती है. भारत में भी कई बैंकों द्वारा इस प्रकार के कार्ड जारी किए जा रहे हैं.

अतिरिक्त सूचनाओं द्वारा कार्डधारक की पहचान (Multi Factor Authentication)

इस तकनीक में क्लोन किए गए कार्ड के दुरुपयोग को रोकने के लिए एवं सही कार्ड उपभोक्ता पहचान के लिए 'पिन' के अतिरिक्त अन्य सूचनाएं भी उपभोक्ता से मांगी जाती हैं, जो क्लोन करने वाले के पास उपलब्ध नहीं होती. उदाहरण के लिए उपभोक्ता के मोबाइल पर आने वाला ओटीपी पासवर्ड (One Time Password) या एटीएम कार्ड पर बने ग्रिड पर बिना क्रम में लिखी संख्याओं में से किसी एक का पूछना. यदि कार्ड क्लोन किया गया हो, तो भी इन सूचनाओं के अभाव में, उसका दुरूपयोग एटीएम पर संभव नहीं हो सकेगा.

भुगतान प्रणाली की सुरक्षा

भारत में वर्तमान समय में एटीएम और पॉस (POS) पर किए जाने वाले लेनदेनों (Transactions) का डाटा (पिन को छोड़कर), बिना इनक्रिप्ट हुए प्रवाहित होता है, जिसके कारण इस डाटा की चोरी और उसका दुरुपयोग सम्भव है. भारतीय रिज़र्व बैंक ने हाल में ही इस बारे में दिशा निर्देश जारी किये हैं, जिनमें सभी बैंकों को यूकेपीटी (Unique Key Per Terminal), डीयूकेपीटी (Derived Unique Key Per Transaction) अथवा टीएलई (Terminal Line Encryption) की तकनीक से एटीएम और पॉस पर किए जाने वाले लेनदेनों का डाटा इनक्रिप्ट करने की सुविधा एक निश्चित समय सीमा में उपलब्ध करानी है.

इस प्रकार हम देखते हैं कि तकनीकी रूप से कार्ड की क्लोनिंग को रोकने के कई उपाय उपलब्ध हैं, परन्तु किसी भी एक तकनीक से कार्ड की क्लोनिंग को पूर्णतः रोक पाना आसान नहीं है.

निष्कर्षतः हम कह सकते हैं कि टेक्नोलॉजी का बैंकिंग क्षेत्र में सार्थक उपयोग हुआ है लेकिन उसके कुछ खतरे भी हैं. कुछ जोखिम मानवीय भूलों से जुड़ें हैं तो कुछ अपराधियों के दिमाग की उपज हैं. मानवीय भूलों से तो सजगता और सावधानी से निपटा जा सकता है लेकिन साइबर अपराधियों से बचने के लिए हमें तकनीक में और सुधार लाने होंगे और ऐसे कारगर उपाय करने होंगे कि किसी बैंक की साइट को हैक न किया जा सके, क्रेडिट/डेबिट कार्ड का क्लोन तैयार न किया जा सके. इसके अलावा, हमें सख्त साइबर कानून बनाने होंगे; जिससे कि हैकर तकनीक का इस्तेमाल करते हुए किसी के साथ धोखाधड़ी न कर सकें. बैंकिंग क्षेत्र में तकनीक के प्रयोग से पहले की अपेक्षा जोखिम बढ़ें हैं, लेकिन तकनीक ने बैंकिंग को नई ऊँचाइयां भी दी हैं, जिसे हम नजर अंदाज नहीं कर सकते. यदि हम जागरुक और सजग रहें तो जोखिम को कम अवश्य किया जा सकता है.

कार्ड की क्लोनिंग और उसका दुरुपयोग बचाने के लिए हमारी जागरूकता ही सबसे कारगर उपाय है.

साइबर हमले और इंटरनेट बैंकिंग/कार्ड में धोखाधड़ी से सावधानियां

शारदा साव
सहायक प्रबंधक (राभा)
क्षे. का. दुर्गापुर

चंडीगढ़ के पास जिराकपुर में एक सरकारी स्कूल शिक्षक श्री नरेंद्र पाल को मध्यरात्रि से पहले एक एसएमएस मिला, जो कि सूरत में एक एटीएम के माध्यम से ₹10,000 रुपये आहरण के संदर्भ में था. जब तक वह समझ पाते कि क्या हो रहा है, उन्हें पुनः ₹10,000 रुपये और ₹20,000 रुपये आहरण के बारे में आधी रात में दो और एसएमएस मिले. वे ऑनलाइन धोखाधड़ी के शिकार हो गए थे. जैसा कि पहला डेबिट 12 बजे से कुछ मिनट पहले हुआ था, धोखाधड़ी करने वाला अगले दिन की निकासी सीमा का तत्काल उपयोग करने में सक्षम था.

जैसे-जैसे अधिक से अधिक लोग ऑनलाइन बैंकिंग सेवाओं का उपयोग कर रहे हैं, वैसे-वैसे बैंकिंग धोखाधड़ी की घटनाएँ भी बढ़ रहीं हैं. इसके अलावा, विमुद्रीकरण के बाद ऑनलाइन लेनदेन में तेजी से वृद्धि हुई है. श्री नरेंद्र पाल ने तत्काल हेल्पलाइन नंबर पर फोन करके, लेनदेन के बारे में अपने बैंक को सूचित किया. उन्होंने बैंक शाखा और आरबीआई को भी लिखा कि उन्होंने किसी के साथ अपने बैंक खाते और एटीएम कार्ड का विवरण साझा नहीं किया है. उन्होंने क्राइम ब्रांच के साइबर सेल में शिकायत भी दर्ज की. अधिकारी उन्हें पेट्रोल पंप पर ले गए, जहां उन्होंने आखिरी बार कार्ड का इस्तेमाल किया था, लेकिन इससे भी कोई हल नहीं निकला. श्री पाल का कहना है कि बैंक के कर्मचारी सहयोग कर रहे थे लेकिन फिर भी उनकी क्षतिपूर्ति में दो महीने से ज्यादा समय लगा और शाखा में दो-तीन बार आने-जाने की परेशानी से उन्हें गुजरना पड़ा.

श्री पाल जैसे लोगों को अब चिंता करने की ज़रूरत नहीं है. "भारतीय रिजर्व बैंक" ने इस संदर्भ में दिशानिर्देश जारी किए हैं, जिसके अनुसार यदि ग्राहक निर्धारित अवधि के भीतर अनधिकृत/धोखाधड़ी लेनदेन के बारे में सूचित करता है, तो बैंक को पूरे नुकसान की भरपाई करनी होगी. आरबीआई ने ऑनलाइन धोखाधड़ी लेनदेन से संबंधित ग्राहक देयता के मसौदे पर अगस्त 2016 में जारी किए गए दिशानिर्देशों को विस्तृत किया है. "गैरकानूनी इलेक्ट्रॉनिक लेनदेन" से जुड़ी ग्राहक शिकायतों में हो रही वृद्धि को ध्यान में रखते हुए आरबीआई द्वारा साझा की गई, हालिया अधिसूचना में एक और विशिष्ट दिशानिर्देश शामिल है, जो ग्राहकों की रक्षा के लिए धोखाधड़ी या दुरुपयोग के संभावित

मामलों से संबंधित हैं.

इसलिए, ई वाई इंडिया के धोखाधड़ी जांच और विवाद सेवाओं के सहयोगी विक्रम बब्बर कहते हैं कि "बैंकों को ऑनलाइन और डिजिटल स्पेस को कवर करने वाली धोखाधड़ी पहचान और प्रारंभिक चेतावनी सिस्टम का मजबूत ढांचा स्थापित करना होगा."

बैंक पर दायित्व

पहले, यह ग्राहक को साबित करना होता था कि उसने किसी के साथ अपने बैंक के विवरण साझा नहीं किए हैं, किन्तु अब यह बैंक को साबित करना है कि गलती ग्राहक की थी और ऑनलाइन बैंकिंग सुविधाओं का उपयोग करते समय उसने पर्याप्त सावधानी नहीं बरती. पहले वाली प्रणाली के परिणामस्वरूप ग्राहक को नुकसान पहुंच रहा था अथवा बैंक को पैसों के भुगतान करने में काफी समय लग रहा था क्योंकि धनवापसी के लिए, कोई स्पष्ट दिशानिर्देश या निर्धारित अवधि नहीं थी. डेलोइट हास्किन्स और सेल के साझेदार कलपेश जे.मेहता कहते हैं, "कई लोग ऑनलाइन लेन-देन करने से डरते हैं. ये दिशानिर्देश बैंक और ग्राहकों के बीच विश्वास बढ़ाएंगें."

एजीएस ट्रांजैक्ट टेक्नोलॉजीज़ के अध्यक्ष और सीईओ महेश पटेल का मानना है कि यह एक बड़ा कदम है क्योंकि इससे बैंकों को धोखाधड़ी निगरानी हेतु बेहतर प्रणाली का उपयोग करने के लिए प्रोत्साहित किया जाएगा. पटेल कहते हैं "चूंकि पहले दायित्व ग्राहक पर था और बैंकों के लिए धोखाधड़ी निगरानी हेतु बेहतर प्रणाली की लागत वास्तविक धोखाधड़ी की लागत से अधिक थी, इसके परिणामस्वरूप शीर्ष कुछ बैंकों को छोड़कर शेष धोखाधड़ी निगरानी प्रणाली में निवेश करने से बचना चाहते थे." भारतीय रिजर्व बैंक के दिशानिर्देश, बैंकों को सुदृढ़ और गतिशील तथा धोखाधड़ी का पता लगाने और निवारण तंत्र को लागू करने व अन्य त्रुटियों की जांच कर सुधार करने के निर्देश देते हैं.

ग्राहक को धन की पूर्ण वापसी

निम्नलिखित मामलों में बैंक पूरे नुकसान का भुगतान करेगा.

1. जब बैंक की तरफ से किसी कमी या लापरवाही के कारण धोखाधड़ी का लेनदेन हुआ हो इस तथ्य के बावजूद कि ग्राहक ने इसकी सूचना दी है या नहीं दी है, डेलोइट हास्किन्स और सेल के श्री मेहता कहते हैं, "एक डिजिटल लेनदेन विभिन्न मध्यवर्ती प्लेटफार्मों जैसे कि भुगतानकर्ता बैंक, प्राप्तकर्ता बैंक, भुगतान गेटवे इत्यादि के माध्यम से किया जाता है और इस सब में लेनदेन को इनक्रिप्ट किया जाना चाहिए. किसी भी मध्यस्थों के साथ, कोई डाटा संग्रहीत नहीं

किया जाना चाहिए बल्कि केवल स्थानांतरित किया जाना चाहिए. इसलिए यदि इस प्रक्रिया के दौरान धोखाधड़ी होती है ग्राहक को उत्तरदायी नहीं ठहराया जा सकता. आरबीआई की सिफारिशों के अनुसार ऐसे मामलों में बैंक को ग्राहक को धनवापसी करनी होगी.

2. कभी-कभी तृतीय-पक्ष द्वारा उल्लंघन होता है जहां गलती न तो बैंक की होती है और न ही ग्राहक की बल्कि कहीं न कहीं सिस्टम की गलती होती है और ग्राहक तीन कार्य दिवसों के भीतर लेनदेन के संबंध में बैंक को सूचित करता है.

उदाहरण के लिए पिछले साल हिताची भुगतान सेवा प्रणाली जिनके साथ कुछ बैंकों ने अपने एटीएम लेनदेन प्रसंस्करण की आउटसोर्सिंग का समझौता किया था जैसेः आईसीआईसीआई, एसबीआई, येस और एचडीएफसी आदि के लगभग 3.2 मिलियन कार्ड प्रभावित हुए थे.

इस परिदृश्य में, यदि ग्राहक सूचना मिलने के तीन कार्य दिवसों के भीतर बैंक को धोखाधड़ी लेनदेन के बारे में सूचित करता है, तो बैंक को ग्राहक के पूरे नुकसान की भरपाई करनी होगी.

यदि ग्राहक की लापरवाही के कारण धोखाधड़ी हुई है तो लेनदेन के बारे में बैंक को सूचित होने तक सीमित देयता होगी और ग्राहक को पूरा नुकसान उठाना होगा.

- यदि ग्राहक जानबूझकर या अनजाने में किसी के साथ एटीएम पिन, कार्ड नंबर इत्यादि जैसी गोपनीय जानकारी साझा करता है, तो बैंक को लेनदेन के बारे में सूचित होने तक उसे पूरा नुकसान उठाना होगा.
- यदि न तो बैंक और न ही ग्राहक जिम्मेदार है लेकिन सिस्टम में गलती के कारण धोखाधड़ी हुई है और ग्राहक बैंक को चार या सात दिनों के भीतर सूचित कर देता है, तो ग्राहक देयता, लेनदेन की राशि या ₹ 10,000, जो भी कम हो, तक सीमित होगी. यह सीमा केवल बचत बैंक खातों के लिए है. क्रेडिट कार्ड के लिए ₹5 लाख तक और चालू खातों के मामले में वार्षिक औसत शेष राशि ₹25 लाख तक की सीमा लागू होती है. यदि कोई व्यक्ति तीन दिनों के भीतर सूचित करता है तो उसे पूरी राशि का वापस भुगतान किया जाता है. ₹5 लाख से अधिक की सीमा वाले चालू खातों, ओवर ड्राफ्ट खातों और क्रेडिट कार्ड के लिए अधिकतम सीमा ₹25,000 है. मूल बचत बैंक जमा खातों यथा नो-फ्रिल्स खातों के लिए यह सीमा ₹5,000 है.
- यदि सात दिनों से अधिक की देरी हो गई है, तो ग्राहक की देयता बैंक के बोर्ड द्वारा अनुमोदित नीति के अनुसार तय की जाएगी.

बैंक द्वारा मोबाइल नंबर और ईमेल पंजीकृत ग्राहकों को, ईमेल और एसएमएस के माध्यम से प्रत्येक लेनदेन के बारे में पूरी जानकारी भेजी जाती है. अब आरबीआई ने बैंकों को ग्राहकों से मोबाइल नंबर लेने की सलाह दी है, जिससे यदि ग्राहक ऑनलाइन लेनदेन सूचना सुविधा लेना चाहता है, तो उसे हर लेनदेन के बारे में सूचित किया जा सकें. बैंक उन ग्राहकों को एटीएम नकद निकासी के अलावा इलेक्ट्रॉनिक लेनदेन की सूचना नहीं भेज सकते हैं, जो बैंक को मोबाइल नंबर प्रदान नहीं करते हैं. वर्तमान में, बैंक एसएमएस सेवा के लिए शुल्क प्रभारित करते हैं. हालांकि, एसएमएस शुल्क का प्रभार किसके द्वारा उठाया जाएगा इस बारे में भारतीय रिज़र्व बैंक के दिशानिर्देशों में कुछ भी उल्लेख नहीं है. वर्तमान में, एसएमएस शुल्क का प्रभार खाताधारकों द्वारा उठाया जाता है.

उत्तर विकल्प

धोखाधड़ी लेनदेन की रिपोर्ट करने के लिए वेबसाइट, फोन बैंकिंग, एसएमएस, ई-मेल, आईवीआर, निर्दिष्ट टोल-फ्री हेल्पलाइन नं., होम शाखा को रिपोर्ट करने आदि जैसे कई चैनलों के अलावा, बैंक को ग्राहक को एसएमएस और ईमेल अलर्ट का जवाब देने का विकल्प भी प्रदान करना होगा. इसके अलावा, आरबीआई ने बैंकों को बैंक की वेबसाइट के होम पेज पर, अनधिकृत इलेक्ट्रॉनिक लेनदेन की रिपोर्ट करने हेतु विशिष्ट विकल्प के साथ शिकायत दर्ज कराने के लिए सीधा लिंक प्रदान करने के निर्देश भी दिए हैं.

बैंकों की धोखाधड़ी रिपोर्टिंग प्रणाली यह सुनिश्चित करेगी कि पंजीकृत शिकायत संख्या के साथ शिकायत को स्वीकार करने वाले ग्राहकों को तत्काल प्रतिक्रिया (ऑटो प्रतिक्रिया सहित) भेजी जाए. बैंकों द्वारा अलर्ट भेजने और उनके जवाब प्राप्त करने के लिए उपयोग की जाने वाली संचार प्रणालियों को संदेश की डिलीवरी का समय और तारीख का रिकॉर्ड रखना होगा और यदि ग्राहक की कोई प्रतिक्रिया हो तो, वह प्राप्त करनी होगी. यह ग्राहक की देयता की सीमा निर्धारित करने में महत्वपूर्ण होगा.

धनवापसी के लिए समय सीमा

ग्राहक द्वारा लेनदेन के बारे में बैंक को सूचित करने के बाद बैंक नए दिशानिर्देशों के अनुसार 10 कार्य दिवसों के भीतर ग्राहक के खाते में राशि जमा करेगा. इसके अलावा, जिन मामलों में ग्राहक देयता बैंक के बोर्ड द्वारा तय की जानी है, उसमें शिकायत को 90 दिनों के भीतर बंद किया जाना चाहिए और यदि बोर्ड ग्राहक देयता तय करने में असमर्थ है, तो उसे शून्य देयता और सीमित देयता प्रावधान के अनुसार मुआवजा दिया जाना चाहिए.

यदि हम "लेनदेन करते समय" कुछ सावधानी बरतें तो हम ऑनलाइन धोखाधड़ी के शिकार नहीं होंगे-

यदि आपका तकनीकी कौशल खराब है और आप ऑनलाइन बिल का भुगतान करते समय, ई-कॉमर्स वेबसाइट से गैजिट खरीदते समय या एटीएम से पैसे निकालते समय आप सावधानी नहीं बरतते और किसी पर तुरंत विश्वास कर लेते हैं तो आप ऑनलाइन धोखाधड़ी के शिकार हो सकते हैं और अपने मेहनत के पैसों से हाथ धो सकते हैं.

आरबीआई के आकड़ों के अनुसार वर्ष 2015-16 में बैंकों द्वारा एटीएम, क्रेडिट कार्ड और डेबिट कार्ड के साथ-साथ नेट बैंकिंग धोखाधड़ी से जुड़े 11,997 मामले सामने आए थे. वर्ष 2015 में, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (सीईआरटी-इन) द्वारा फिशिंग, स्कैनिंग, वेबसाइट घुसपैठ इत्यादि सहित 49,455 "साइबरसुरक्षा" घटनाएं रिपोर्ट की गइ. हालांकि, जो मामले दर्ज नहीं होते यदि उनको भी शामिल किया जाए तो उक्त संख्या पूरे देश में हो रही ऑनलाइन धोखाधड़ी का एक महत्वपूर्ण हिस्सा होगी.

धोखाधड़ी की संख्या इतनी अधिक है कि आरबीआई के पूर्व उप गवर्नर श्री एसएस मुंदड़ा ने पिछले वर्ष मई में बैंकिंग कोड्स और स्टैंडर्ड बोर्ड ऑफ इंडिया द्वारा आयोजित एक कार्यक्रम में ग्राहकों को साइबर धोखाधड़ी से राहत प्रदान करने की आवश्यकता को दोहराते हुए कहा है कि "आरबीआई धोखाधड़ी और इलेक्ट्रॉनिक बैंकिंग लेनदेन से उत्पन्न धोखाधड़ी लेनदेन पर ग्राहकों की देयता को सीमित करने के संबंध में नियामक दिशानिर्देश जारी करने या न करने पर विचार कर रहा है."

लेकिन इसकी रोकथाम सबसे बेहतर विकल्प है, इस सर्वव्यापी धोखाधड़ी से खुद को बचाने की जरूरत है. हम धोखाधड़ी करने वालों की कार्यप्रणाली और उससे भी अधिक महत्वपूर्ण है कि अपने पैसों को इस प्रकार की धोखाधड़ी से कैसे बचाएं और ऑनलाइन लेनदेन करते समय क्या-क्या सावधानियाँ बरतें इस पर चर्चा करेंगेः

ऑनलाइन खरीदारी

ई-कॉमर्स साइट पर जाने से पहले यह सुनिश्चित करें कि वेबसाइट, विक्रेता और भुगतान मोड सुरक्षित हैं. ऑनलाइन शॉपिंग की सुविधा पर कोई संदेह नहीं है, चाहे वह इलेक्ट्रॉनिक गैजिट्स या घरेलू उपकरणों, कपड़े या फर्नीचर के लिए हों, हमें घर बैठे सभी चीजों की खरीद की सुविधा प्राप्त है. अफसोस की बात है, इससे नई धोखाधड़ी तकनीकें और बिक्री/वितरण की कमी भी पैदा हुई है.

कार्य पद्धति

जब आप ऑनलाइन ऑर्डर करते हैं, तो यह संभव है कि उत्पाद डिलीवर न हो या आपको नकली या क्षतिग्रस्त उत्पाद मिले. आपको पत्थरों से भरा खाली पैकेट भी मिल सकता है या इससे भी बदतर कुछ हो सकता है. 32 वर्षीय, गाजियाबाद स्थित संतोष कुशवाहा से पूछें जिन्होंने 2015 में ₹46,000 के आईफोन 6 का ऑर्डर दिया था वे कहते हैं, "पैकेजिंग बेकार थी, पैकेट टुकड़े-टुकड़े में था, वजन सही था और किसी प्रकार की छेड़छाड़ नहीं की गई थी. लेकिन जब मैंने इसे खोल कर देखा तो मुझे पत्थरों से भरा बॉक्स मिला."

समस्या किसी भी स्तर पर हो सकती है, जिसके लिए आपको बिक्री और वितरण प्रक्रिया को समझने की आवश्यकता है. फैब इंडिया जैसी साइट हैं, जो अपने उत्पादों को बेचती हैं और वितरित करती हैं. ऐसी कई साइट्स हैं, जो विभिन्न विक्रेताओं के लिए मंच के रूप में कार्य करती हैं. ये मार्केटप्लेस हैं, जैसे फ्लिपकार्ट, अमेजॉन या स्नैपडील, जो विभिन्न ब्रांडों और विक्रेताओं द्वारा उत्पाद होस्ट करते हैं. इन उत्पादों को या तो साइट द्वारा या विक्रेता द्वारा स्वयं वितरित किया जाता है. ज्यादातर मामलों में, वितरित करने वाला विक्रेता ही होता है. कुछ साइट विशेष सेवाएं भी प्रदान करती हैं, जिनमें प्रीमियम द्वारा उत्पाद की गुणवत्ता और वितरण की गारंटी है. ये साइट विक्रेताओं से उत्पाद लेती है, लेकिन गुणवत्ता जांच कर उन्हें स्वयं वितरित करती हैं. उदाहरण के लिए, फ्लिपकार्ट ने FAssured लॉन्च किया है, जो बेहतर वितरण सेवा और ठोस गुणवत्ता जांच का वादा करता है, जबकि अमेजॉन प्राईम एक सःशुल्क सेवा है, जो अपने सदस्यों के FAssured के समान फायदे प्रदान करती है. यहां विभिन्न बिन्दु ऐसे हैं, जिन पर धोखाधड़ी हो सकती हैः

नकली वेबसाइटः तकनीकी-समझदारी वाले स्कैमस्टर्स ऐसी साइट सेट करते हैं, जो समान लोगों और डोमेन नाम वाले वास्तविक लोगों की तरह दिखतीं हैं. कुछ स्कैमस्टर्स उत्पाद लाइन-अप के साथ, एक डमी साइट बना देते हैं जो केवल ऑनलाइन मौजूद है. इनका उद्देश्य कमजोर खरीदारों से पैसे निकलवाना और धोखाधड़ी करके गायब हो जाना है.

वास्तविक साइट, नकली विक्रेताः यदि आपको कोई उत्पाद नहीं मिला है या उत्पाद क्षतिग्रस्त व नकली है, तो इस प्रकार का घोटाला, विक्रेता या कुरियर कंपनी द्वारा किया गया है न कि साइट द्वारा. यद्यपि ऐसी साइट, उनके द्वारा होस्ट किए गए विक्रेताओं को स्कैन करती हैं किन्तु फिर भी सभी स्कैमस्टर्स की पहचान करना संभव नहीं है.

कुरियर कंपनीः यहां, साइट और विक्रेता दोनों को दोषी नहीं ठहराया जा सकता है. यदि वे एक कुरियर चुनने जाते हैं, तो आप एक डमी पैकेज ले सकते हैं. इस सब के अलावा, कुरियर फर्म के कर्मचारी भी फर्जी डिलीवरी के लिए जिम्मेदार हो सकते हैं.

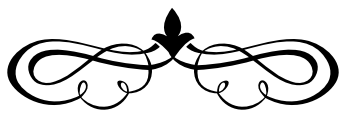
निवारक कदम

साइट की जांच करें: यदि आप नई साइट्स को आजमाना चाहते हैं, तो डोमेन नाम की जांच करना सुनिश्चित करें. सुनिश्चित करें कि यूआरएल में 'https' है (न कि केवल 'http') और लॉक आइकॉन और साइट की वर्तनी जांचें. यह जानने के लिए कि किसी विशेष डोमेन नाम का स्वामी कौन है और यदि वास्तविक है, तो https: // रजिस्ट्री में लॉग इन करें. In/WHOIS, जो वर्तमान में दुनिया में पंजीकृत प्रत्येक डोमेन की खोज योग्य सूची है. यदि यह साइट कोई संपर्क विवरण प्रदान नहीं करती है या अस्पष्ट विनिमय या रिटर्न पॉलिसी दिखाती है तो साइट को छोड़ दें. आप http://www पर कंपनी की ट्रस्ट रेटिंग भी देख सकते हैं. Scamadviser.com आपको फर्म के बारे में पूर्ण विवरण देगा और साइट से खरीदारी करना कितना सुरक्षित है यह भी बताएगा. एक्सपीरियन के जयरामन कहते हैं, "सुनिश्चित करें कि कंपनी की आधारभूत संरचना सही है, जिसमें आप डिलीवरी और भुगतान जानकारी ट्रैक कर सकते हैं."

विक्रेता की रेटिंग जांचें: यदि आपने एक स्थापित साइट चुनी है, तो उत्पाद आश्वासन सेवाओं यदि कोई हो का चयन करें. यदि आप, अतिरिक्त भुगतान नहीं करना चाहते हैं, तो विक्रेता की खरीदार समीक्षा और रेटिंग के माध्यम से पता लगाएं कि क्या उसके पास प्रतिष्ठित डिलीवरी सुविधा है या नहीं. फ्लिपकार्ट के प्रवक्ता का कहना है, "हम उन विक्रेताओं के खिलाफ सख्त कार्रवाई करते हैं, जिनकी सेवाओं के बारे में, नकारात्मक प्रतिक्रिया मिलती हैं या नकली उत्पादों को बेचने में लगे हुए हैं या कॉपीराइट या किसी अन्य कानूनों का उल्लंघन करते हैं."

सुरक्षित भुगतान: भुगतान के लिए, विक्रेताओं को प्रत्यक्ष भुगतान करने से बचें. EBay में PaisaPay जैसी भुगतान सेवाओं का चयन करें, जो यह सुनिश्चित करता है कि विक्रेता को साइट द्वारा तब तक भुगतान नहीं किया जाता है, जब तक कि उत्पाद वितरित नहीं हो जाता है और तब तक आपके पैसे सुरक्षित रहते हैं. साथ ही यह ध्यान रखें कि इलेक्ट्रॉनिक बैंक हस्तांतरण के माध्यम से भुगतान न करें क्योंकि बैंक से निकालने के बाद उस राशि को पुनः प्राप्त करना मुश्किल है. क्रेडिट कार्ड के माध्यम से भुगतान का चयन करें, जिसमें क्रेडिट सीमा कम है, जिसका उपयोग ऑनलाइन खरीददारी के लिए हमेशा किया जाता है एवं जोखिम को और कम करने के लिए कैश ऑन डिलिवरी का चयन करें.

स्त्रोत- इंटरनेट एवं विकिपीडिया



सोशल मीडिया : सुविधा एवं सावधानियां

आशीष गुप्ता
प्रबंधक (राजभाषा)
क्षे. का. मुंबई (पश्चिम)

अभिषेक राज
प्रबंधक (सुरक्षा)
क्षे. का. मेरठ

ग्लोबलाइज़ेशन के इस दौर में जब पूरा विश्व एकीकरण की राह पर है, इस धरती पर एक नए राष्ट्र का उदय हुआ है, जिसकी कोई निश्चित भौगोलिक सीमाएं नहीं हैं. ये राष्ट्र पूरे विश्व में फैला हुआ है और इसकी आयु बमुश्किल 15 साल है. इस देश की जनसंख्या भारत और चीन की जनसंख्या को भी पार कर चुकी है. जिस संख्या तक पहुंचने में आधुनिक मानव को 2 लाख साल लगे हैं, उस जनसंख्या को केवल साइबर स्पेस पर मौजूद इस राष्ट्र ने महज 15 सालों में प्राप्त कर लिया है. इस राष्ट्र का नाम है, **'सोशल मीडिया'**. ये ऐसा ताक़तवर राष्ट्र है, जिसने तमाम बने बनाए मानकों को तोड़ते हुये बहुत तेज़ी से पूरे विश्व में अपनी पैठ बनाई है.

परंपरागत मीडिया माध्यमों जैसे- प्रिंट, इलेक्ट्रॉनिक तथा अन्य मीडिया से अलग सोशल मीडिया एक ऐसा मंच है, जो इंटरनेट के माध्यम से एक आभासी दुनिया की रचना करता है. इस आभासी दुनिया में आपको ले जाने के लिये फेसबुक, ट्विटर, व्हॉट्सएप, इंस्टाग्राम आदि जैसे कई प्लेटफॉर्म मौजूद हैं. अपरंपरागत मीडिया होने के बावजूद सोशल मीडिया एक विशाल नेटवर्क है, जो कि पूरे विश्व को आपस में जोड़ रहा है. इसके माध्यम से जिस तेजी से सूचनाओं का आदान-प्रदान हो रहा है, उसने

सूचना क्रांति की दिशा में एक नया अध्याय जोड़ा है. अगर आप आंकड़ों पर जाएं तो निम्नलिखित तस्वीर आपके सामने आती है.

उपरोक्त आंकड़ों से आपको ये स्पष्ट हुआ होगा कि सोशल मीडिया की उपस्थिति कितनी व्यापक है और सूचनाओं का संसार कितनी तेज़ी से सोशल मीडिया द्वारा प्रभावित हो रहा है. निस्संदेह सूचना क्रांति के इस युग में सोशल मीडिया ने अभिव्यक्ति की आज़ादी की दिशा में अभूतपूर्व योगदान दिया है. सोशल मीडिया अभिव्यक्ति के साथ-साथ बहुत सी आर्थिक और राजनीतिक गतिविधियों में भी महत्त्वपूर्ण भूमिका निभा रहा है. इन सब सकारात्मक भूमिकाओं के साथ-साथ समाज में बहुत सी नकारात्मक गतिविधियों का वाहक भी सोशल मीडिया ही बना है, जिस पर हम नीचे के अनुच्छेदों में बिंदुवार चर्चा करेंगे.

सोशल मीडिया के सकारात्मक प्रभाव/सुविधाएं

- **संचार का तीव्र माध्यम** - इक्कीसवीं सदी को सूचना क्रांति का युग इसलिये कहा जाता है क्योंकि बीते कुछ सालों में सूचनाओं के आदान- प्रदान के बहुत से माध्यम विकसित हुये हैं और इन माध्यमों ने सूचनाओं के प्रेषण और प्राप्ति में लगने वाले समय को बहुत कम कर दिया है. इन सभी माध्यमों में सोशल मीडिया सबसे अभिनव है क्योंकि यह सबसे कम लागत और समय में बहुत अधिक लोगों तक सूचनाएं पहुंचाने का सर्वश्रेष्ठ माध्यम साबित हुआ है. यही कारण है कि दुनिया भर के राजनीतिक दल और राजनेता अपने प्रचार-प्रसार और चुनावी अभियानों के लिये सोशल मीडिया का इस्तेमाल कर रहे हैं, वहीं ज़्यादातर औद्योगिक घराने/कारोबारी संस्थाएं भी आम लोगों तक अपनी पहुंच बनाकर कारोबार का विस्तार करने के लिये सोशल मीडिया का सहारा ले रही हैं.

- **अभिव्यक्ति का खुला मंच** - सोशल मीडिया के आने से पहले परंपरागत संचार माध्यमों के द्वारा संचार तो होता था, लेकिन ये माध्यम अभिव्यक्ति का खुला मंच नहीं थे. यहां अगर आपको कोई बात कहनी है तो वो सीधे लक्षित समूह तक नहीं पहुंचती थी, बल्कि इन माध्यमों के नियंत्रणकर्ताओं के माध्यम से पहुंचती थीं, जहां इसमें कुछ संशोधन किये जाते थे. ये संशोधन उन संचार माध्यमों की नीतियों के अनुसार किये जाते थे. लेकिन सोशल मीडिया के माध्यम से आप अपनी बात को लक्षित समूह तक सीधे और बिना किसी संशोधन के पहुंचा सकते हैं.

- **प्रतिबंधित नहीं** - परंपरागत संचार माध्यमों में एक बड़ी बाधा यह थी कि इन माध्यमों के द्वारा प्रत्येक व्यक्ति अपनी अभिव्यक्ति नहीं दे सकता था. इन माध्यमों के ज़रिये चुने हुये लोगों को ही अपनी अभिव्यक्ति देने का अवसर मिलता था, वहीं

सोशल मीडिया इस प्रतिबंध से मुक्त है. सोशल मीडिया प्लैटफॉर्म पर कोई भी व्यक्ति अपना खाता बनाकर अपनी अभिव्यक्ति देने के लिये स्वतंत्र है, बशर्ते वह अभिव्यक्ति असामाजिक क़िस्म की न हो.

- **संवाद का दोतरफ़ा माध्यम** - परंपरागत मीडिया के साथ यह समस्या भी थी कि वे सभी माध्यम संवाद का एकतरफ़ा माध्यम थे, यानि आप सिर्फ़ सूचनाएं या अभिव्यक्तियां देख/सुन सकते थे लेकिन उस पर अपनी प्रतिक्रिया नहीं दे सकते थे. हालांकि, परंपरागत माध्यमों के विकास के क्रम में आंशिक रूप से प्रतिक्रिया देने की सुविधा भी आई लेकिन यह ऐसी नहीं थी कि इनके माध्यम से दोतरफ़ा संवाद किया जा सकें. वहीं सोशल मीडिया ऐसा संचार माध्यम है जहां प्रत्येक अभिव्यक्ति पर प्रतिक्रिया दी जा सकती है और प्रतिक्रियाएं भी उतनी ही तीव्रता से दी जा सकती हैं जितनी तीव्रता से अभिव्यक्तियां दी जाती हैं.

- **समय की बाध्यता नहीं** - सोशल मीडिया माध्यमों की एक बड़ी विशेषता यह भी है कि इन माध्यमों ने अभिव्यक्ति या संचार के लिये समय की सीमाओं को समाप्त कर दिया है. कोई व्यक्ति अपने हाथ में एक छोटी सी डिवाइस स्मार्टफोन और इंटरनेट के माध्यम से कभी भी संचार कर सकता है. वहीं परंपरागत माध्यमों में समय को लेकर ये स्वतंत्रता नहीं थी.

- **विज्ञापन का सशक्त एवं अपेक्षाकृत सस्ता माध्यम** - कारोबारी संस्थाओं के लिये तो सोशल मीडिया बहुत काम का है क्योंकि इस माध्यम से विज्ञापन करना बहुत सरल और सस्ता है साथ ही, इसका प्रभाव और पहुंच भी परंपरागत माध्यमों से अधिक है. यहां रुचि के अनुसार चयनित विज्ञापन दिये जाने की सुविधा ने इसे विज्ञापन का और भी प्रभावी माध्यम बना दिया है.

यदि हम **सोशल मीडिया के सकारात्मक पक्ष** को देखें तो पाएंगे कि सोशल मीडिया ने लोगों को एक ही समय पर अलग-अलग रहते हुये एक साथ किया है और लोगों के हित, लगाव और व्यवहार के नए पहलुओं को जन्म दिया है. सोशल मीडिया अपनी सकारात्मक भूमिका से किसी भी व्यक्ति, संस्था, समूह और देश आदि को आर्थिक, सामाजिक, राजनैतिक और सांस्कृतिक रूप से समृद्ध बना सकता है. सोशल मीडिया के माध्यम से कई ऐसे कार्य हुये और हो रहे हैं, जिनसे लोकतंत्र समृद्ध हुआ है. इसका सशक्त उदाहरण **अन्ना हज़ारे** के नेतृत्व में किया गया **इंडिया अगेन्स्ट करप्शन** का आंदोलन था, जिसने भ्रष्टाचार के विरुद्ध एक युद्ध छेड़ा, जो सड़क और सोशल मीडिया दोनों जगह साथ-साथ लड़ा गया. परिणामस्वरूप, देश में लाखों लोग अन्ना हज़ारे के साथ जुड़े. 2014 के आम चुनाव के दौरान भी सोशल मीडिया के माध्यम से प्रचार और मतदाता जागरूकता का अभियान छेड़ा गया, जिससे मतदान के प्रति सकारात्मक प्रभाव देखने

को मिला. यह सोशल मीडिया ही था, जिसने 'निर्भया' को न्याय दिलाने के लिये लाखों लोगों को सड़कों पर ला दिया था. यही कारण है कि विशेषज्ञों ने इसे **इन्फॉर्मेशन हाइवे** का नाम दिया है, जिस पर कोई भी चल सकता है और यह सबके काम का है. माननीय प्रधानमंत्री जी के **'बेटी बचाओ-बेटी पढ़ाओ'**, **'स्वच्छ भारत मिशन'** आदि अभियानों में सम्पूर्ण भारत देश हाथ से हाथ मिला कर खड़ा हुआ. 2014 के आम चुनाव के दौरान राजनीतिक पार्टियों ने सोशल मीडिया का जमकर उपयोग करते हुए देश की आम जनता को चुनाव के प्रति जागरूक बनाने में महत्वपूर्ण भूमिका अदा की. सोशल मीडिया के उपयोग से ही युवाओं में चुनाव के प्रति जागरूकता बढ़ी, जिससे वोटिंग प्रतिशत अप्रत्याशित रूप से बढ़ा. 2014 के लोकसभा चुनावों में सोशल मीडिया के इस्तेमाल को देखकर फायनेंशियल टाईम्स ने मोदी को भारत का पहला सोशल मीडिया प्रधानमंत्री कहा.

लोकप्रियता के प्रसार में सोशल मीडिया एक बेहतरीन प्लेटफॉर्म है, जहां व्यक्ति स्वयं को अथवा अपने किसी उत्पाद को ज्यादा लोकप्रिय बना सकता है. आज फिल्मों के ट्रेलर, टीवी प्रोग्राम का प्रसारण भी सोशल मीडिया के माध्यम से किया जा रहा है. वीडियो तथा ऑडियो चैट भी सोशल मीडिया के माध्यम से सुगम हो पाई है. व्यापार के लिए सोशल मीडिया का प्रयोग समग्र विपणन लागत को कम करने में मदद करता है. सोशल मीडिया से आप संभावित ग्राहकों को संगठित कर सकते हैं और अपने व्यापार में वृद्धि कर सकते हैं. इसके द्वारा तीव्र गति से सूचनाओं का आदान प्रदान किया जा सकता है, जहां कोई भी व्यक्ति किसी भी कंटेंट का मालिक नहीं होता है. इसके जरिये फोटो, वीडियो, सूचना, डॉक्यूमेंटस आदि को बहुत आसानी से और तीव्र गति से एक-दूसरे तक पहुंचाया जा सकता है.

लेकिन जिस प्रकार हाईवे सड़क दुर्घटनाओं से अछूता नहीं रह पाता, वैसे ही यहां भी दुर्घटनाएं होती रहती हैं.

सोशल मीडिया के नकारात्मक पक्ष के रुप में उत्तर प्रदेश के मुजफ्फरनगर के एक छोटे से गांव कवाल में 27 अगस्त 2013 को घटित घटना को देख सकते है, जहॉ दो पक्षों के मध्य मामूली छेड़छाड़ का मामला था जिसने विकराल रूप धारण कर पूरे मुजफ्फरनगर को जला दिया. जगह-जगह लोग मार दिये गए, माँ बहनों की इज्ज़त के साथ खिलवाड़ किया गया, लोग घर से बेघर हो गए तथा महीनों लोगों ने सरकारी कैंपों में गुज़ार दिये. क्यों दो पक्षों के मध्य की चिंगारी ने पूरे मुजफ्फरनगर तथा समस्त देश का माहौल बिगाड़ दिया ? क्या था, जिसने इस खबर को जंगल की आग की तरह पूरे देश में फैला दिया? वो क्या था, जो लोग इतने उग्र हो गए कि भाईचारा भुला कर खून के

प्यासे हो गए? ऐसा क्या था, जिसने जवानी के जोश से भरे युवाओं को इतना उत्तेजित कर दिया कि उन्होंने अंजाम की परवाह नहीं की? ऐसे ही कई मामले उजागर हुए हैं, जिसमें छोटे से मामले को तूल देकर अंजाम की परवाह किए बिना, बड़ा मुद्दा बना दिया गया. इनके मध्य समान कारक क्या हैं?

जवाब है सोशल मीडिया !! सोशल मीडिया !! सोशल मीडिया !!

जिस प्रकार सोशल मीडिया ने सूचनाओं को लोकतांत्रीकरण कर सबको अभिव्यक्ति के लिये खुला मंच प्रदान किया है वहीं ये खुलापन समाज और व्यक्तिगत रूप से बहुत से लोगों के लिये परेशानी का सबब भी बना है. हिंदुस्तान टाइम्स में दिनांक 25 अगस्त 2016 को छपी एक रिपोर्ट के अनुसार राष्ट्रीय अपराध रिकॉर्ड्स ब्यूरो के अनुसार 2013-15 के बीच साइबर क्राइम में सालाना 70 प्रतिशत की वृद्धि हुई थी. इसी रिपोर्ट के अनुसार राष्ट्रीय जांच एजेंसी (एनआईए) के प्रमुख आलोक मित्तल के अनुसार भारत में प्रत्येक छठा साइबर अपराध सोशल मीडिया के ज़रिये ही किया जा रहा है. साइबर विशेषज्ञों का कहना है कि ऐसे समाज में साइबर अपराध बढ़ना स्वाभाविक है, जहां लोग तकनीक तो तेज़ी से अपना रहे हैं लेकिन उनमें जागरूकता की कमी है. ऐसे में साइबर क्राइम देश की सुरक्षा एजेंसियों, पुलिस और सेना के लिए भी एक गंभीर चुनौती बना हुआ है, क्योंकि इससे निपटना अब भी एक टेढ़ी खीर है. आइये जानते हैं कि कैसे सोशल मीडिया अपनी विविध विशेषताओं के साथ-साथ बहुत सी समस्याओं का कारण भी बना हुआ है, जिनसे निपटने के लिये देश और दुनिया की बहुत सी एजेंसियां दिन-रात एक कर रही हैं.

सोशल मीडिया के नकारात्मक प्रभाव/सावधानियां

- **ग़लत/भ्रामक सूचनाओं का प्रसार** - सोशल मीडिया प्लैटफॉर्म्स पर ऐसी सूचनाओं की भरमार है जो या तो पूरी तरह ग़लत हैं या ग़लत तरीक़े से पेश की गई हैं. उससे भी बड़ी बात यह है कि सोशल मीडिया पर दी जा रही जानकारी को बहुत बड़ी संख्या में लोग सही मानकर उसके अनुसार कार्य भी कर रहे हैं. ऐसी सूचनाओं का प्रसार किसी व्यक्ति को बदनाम करने, किसी संस्था की साख बिगाड़ने या किसी व्यक्ति अथवा संस्था को अनुचित तरीक़ों से फ़ायदा पहुंचाने के लिये किया जा रहा है. कई बार ऐसी सूचनाएं तथ्यों की जानकारी के अभाव और अतिवादी होने के कारण भी की जा रही हैं, लेकिन इसके निहितार्थ बहुत दूरगामी एवं गंभीर हैं. हाल ही, में मॉब लिचिंग की घटनाएं, कई इलाक़ों में दंगे और आपसी तनाव की घटनाएं इसी प्रकार की सूचनाओं के प्रसार का परिणाम हैं. इस प्रकार की सूचनाओं की भरमार इतनी है कि बहुत से संचार माध्यमों द्वारा इस प्रकार की भ्रामक सूचनाओं के खंडन के लिये विशेष कार्यक्रम प्रसारित किये जा रहे हैं.

- **साइबर बुलिंग (बदमाशी)** - सोशल मीडिया पर अभिव्यक्ति की स्वतंत्रता की जगह उच्चश्रृंखलता ने ले ली है. लोग अभिव्यक्ति की स्वतंत्रता की आड़ में आपराधिक संवाद कर रहे हैं. चरित्र हनन/ट्रोलिंग जैसे बेहद गंभीर अभियान चलाए जा रहे हैं. बहुत से नामी-गिरामी लोगों को केवल इसलिये अपने ट्विटर हैंडल और फेसबुक प्रोफाइल बंद करने पड़ रहे हैं क्योंकि उनके द्वारा की गई किसी टिप्पणी पर बहुत से लोगों ने सुनियोजित तरीक़े से साइबर हमला किया, उन्हें गालियां दी और अपमानित किया. यहां तक कि उन्हें जान से मारने या उनके परिवारजनों पर हमले की धमकियां भी दी जाती हैं. ऐसा नहीं है कि यह सिर्फ़ व्यक्तिगत तौर पर किया जाता है, बल्कि बहुत से लोग अनौपचारिक रूप से संगठित तौर पर किसी व्यक्ति के विरुद्ध साइबर बुलिंग करते हैं.

- **आपराधिक/आतंकी गतिविधियाँ** - ब्लू ह्वेल जैसा ख़तरनाक खेल भी सोशल मीडिया के माध्यम से ही प्रचारित हुआ, जिसने सैकड़ों बच्चों की जाने लीं. सोशल मीडिया के माध्यम से इस प्रकार की और भी आपराधिक और आतंकी गतिविधियां चलाई जा रही हैं. यह ख़बर बहुत चर्चा में रही कि आईएसआईएस (ISIS) जैसे आतंकवादी संगठनों ने सोशल मीडिया के सहारे अपना बड़ा नेटवर्क तैयार किया था और इन्हीं प्लैटफॉर्म्स के सहारे नवयुवकों को आतंकी गतिविधियों में शामिल किया जा रहा था. जम्मू-कश्मीर में भी आतंकी संगठनों की ऐसी सक्रियता की कई बार ख़बरें प्रकाशित होती रहती हैं.

- **निजता का हनन** - सोशल मीडिया प्लैटफॉर्म्स ने आपकी निजता को लगभग ख़त्म कर दिया है. निजी जानकारियां सोशल मीडिया पर दिये जाने के कारण साइबर और सामाजिक ख़तरे तेजी से बढ़े हैं. सोशल मीडिया पर दी गई आपकी निजी जानकारी को चुराकर या ग़लत तरीक़े से बेचकर मार्केटिंग और व्यापारिक गतिविधियों के लिये इस्तेमाल किया जा रहा है. बहुत से सोशल मीडिया प्लैटफॉर्म्स पर इस संबंध में आरोप भी लगे हैं कि उन्होंने ग़ैर-क़ानूनी तरीक़े से सोशल मीडिया का इस्तेमाल कर रहे लोगों की निजी जानकारियां मार्केटिंग कंपनियों से साझा की हैं. इसी निजता के हनन की मुख़ालिफ़ में बहुत से पश्चिमी देशों ने 'राइट टु फॉरगेट' अभियान भी चलाया था. निजता पर हमले का आलम यह है कि महिलाओं की तस्वीरों की मॉर्पिंग कर उन्हें पॉर्न साइटों पर इस्तेमाल किया जा रहा था. बहुत से नेताओं और प्रसिद्ध व्यक्तियों की तस्वीरों का इस्तेमाल भ्रामक और ग़लत प्रचार करने के लिये किया जा रहा है.

- **साइबर स्टॉकिंग (पीछा करना)** - सोशल मीडिया के माध्यम से आपकी अवस्थिति (लोकेशन) का पीछा किया जाए और फिर आपराधिक वारदातों को अंजाम दिया

जाए तो इसे साइबर स्टॉकिंग का नाम दिया जाता है. इस प्रकार के अपराध महिलाओं के साथ तो बड़ी मात्रा में हो रहे हैं. अन्य बहुत से अपराधों में भी साइबर स्टॉकिंग का सहारा लिया जाता है. उदाहरण के लिये आप रोज़ाना सुबह 8 बजे सोशल मीडिया पर जानकारी देते हैं कि आप अपने कार्यालय के लिये निकल गए और रोज़ाना शाम 5 बजे यह साझा करते हैं कि आप कार्यालय से निकल गए. ऐसा आप लिखकर या अपनी तस्वीर के ज़रिये साझा कर सकते हैं. अब यहां गौर करने वाली बात यह है कि किसी आपराधिक मानसिकता के व्यक्ति को आपके द्वारा साझा की गई इस जानकारी से यह आभास हो जाएगा कि अगर आप रोज़ाना 8 बजे सुबह कार्यालय से निकल रहे हैं और शाम 5 बजे कार्यालय से घर के लिये, तो स्पष्ट है कि आपका घर फिलहाल खाली है/या घर पर पत्नी अकेली है/या घर पर वृद्ध माता-पिता अकेले हैं/या ऐसी ही कोई पैटर्न को दर्शाने वाली जानकारी. ऐसे में कोई भी आपराधिक मानसिकता का आदमी आपके घर में आपराधिक वारदात को अंजाम दे सकता है.

- **फिशिंग** - सोशल मीडिया के माध्यम से लोगों तक लॉटरी जीतने या फिर अप्रत्याशित दामों पर कोई वस्तु ख़रीदने का ऑफर दिया जाता है, बहुत से लोग ऐसे झांसों में आकर फिशिंग गतिविधियों में फंस जाते हैं. आर्थिक अपराधी ऐसे लोगों के बैंक खातों की जानकारी चुराकर आर्थिक धोखाधड़ी करते हैं. कई बार ऐसे ऑफर देने के बाद लोगों से निश्चित रकम की मांग की जाती है और वह रकम प्राप्त होने पर लाखों-करोड़ों रुपये की लॉटरी का भरोसा दिया जाता है.

- कुछ असामाजिक तत्व सोशल मीडिया का फायदा झूठ और अफवाह फैलाने के लिए भी करते हैं. दुख का विषय यह है कि कुछ नकली यूज़र्स सोशल मीडिया का प्रयोग गलत कार्यों के लिए भी कर रहे हैं, जहां गुनहगार को पकड़ने या रोकने के विकल्प बहुत ही सीमित हैं.

- **साम्प्रदायिक तनाव फैलाने का माध्यम** - सोशल मीडिया जातिवाद को बढ़ावा देता है क्योंकि इस मंच पर कई बार किसी धर्म विशेष के लिये आपत्तिजनक सामग्री प्रसारित कर दी जाती है, जो कई बार साम्प्रदायिक रूप लेकर तनाव का कारण बन जाती है. देश में जहाँ भी हिंसा होती है वहाँ स्थिति सामान्य होने तक प्रायः इंटरनेट सेवाएँ बंद कर दी जाती हैं, ताकि अफवाहों को बल न मिले. ऐसी स्थिति में देश के सामाजिक ताने-बाने को बनाए रखना एक बड़ी चुनौती बन गया है.

- सोशल मीडिया, विशेषकर युवा पीढ़ी के बीच सामाजिक व्यवहार और नैतिकता की परिभाषा को बदल रहा है.

- सोशल मीडिया का अत्यधिक और अनियंत्रित उपयोग गंभीर लत का कारण बन गया है. सोशल मीडिया पर काम करते समय आप काम को एक दूसरे में बदलते रहें. एक ही काम पर ध्यान केंद्रित करने से आपकी एकाग्रता की क्षमता कम हो जाती है. ऐसी गतिविधियाँ आपके मस्तिष्क को शिथिल कर देती हैं. इसका प्रचुर मात्रा में उपयोग मस्तिष्क को थकान और तनाव की ओर ले जाता है.

- इंटरनेट की दुनिया में ट्रोल का मतलब उन लोगों से होता है, जो किसी भी मुद्दे पर चल रही चर्चा में कूद पड़ते हैं और फिर आक्रामक या अनर्गल कमेंट्स कर विषय को भटका देते हैं तथा लोगों को उकसाकर अकारण ऐसे मामलों में घसीटते हैं, जिनसे उन्हें मानसिक परेशानी हो सकती है. कई बार भड़काऊ या आपत्तिजनक भाषा का प्रयोग कर मुद्दे से भटका दिया जाता है. कई बार धार्मिक, सामाजिक या व्यक्तिगत भावनाएँ आहत हो जाती हैं. इसके परिणामस्वरूप दंगे-फसाद भी होते देखे गए हैं. लोकप्रियता बढ़ाने या किसी मुद्दे पर सामने वाले को बदनाम करने के लिये ट्रोलिंग की जाती है. ट्रोलिंग के परिणाम घातक सिद्ध हो सकते हैं और इसको रोकने के लिए कठोर उपाय करने की आवश्यकता है.

- कई बार पत्रकारिता की जानकारी नहीं होने पर भी लोग यह सोचते हुए कि उनके पास जो सूचना है वह सबसे पहले लोगों तक उनके माध्यम से पहुँचनी चाहिये, बिना सूचना की जांच किए पोस्ट कर देते हैं, इसे **सिटिज़न जर्नलिज़्म का** दौर कहा जा सकता है.

इस प्रकार सोशल मीडिया ने अपराधी प्रवृत्ति के लोगों के लिये घर बैठे अपराधों को अंजाम देने हेतु भी एक प्लैटफॉर्म मुहैया करा दिया है. यदि सोशल मीडिया यूज़र निम्नलिखित कुछ सावधानी बरतें तो इस तरह के अपराधों का शिकार होने से बचा जा सकता है.

सोशल मीडिया में क्या करें

- सोशल मीडिया के किसी भी प्लैटफॉर्म का प्रयोग ख़त्म हो जाने के बाद लॉगआउट ज़रूर करें.

- सोशल मीडिया प्लैटफॉर्म पर आपकी बहुत सी निजी एवं संवेदनशील जानकारियां होती हैं. इसलिये भूलकर भी इसका पासवर्ड किसी से साझा न करें.

- सोशल मीडिया में कोई भी खाता बनाते समय पासवर्ड ऐसा बनाएं, जिसका जल्दी अनुमान न लगाया जा सके अन्यथा आपके खाते के हैक होने का ख़तरा होता है.

- मोबाइल या इंटरनेट पर मौजूद बहुत सी साइट और एप पर फेसबुक के माध्यम से लॉगिन करने से बचें क्योंकि ऐसा करने से आपकी निजी जानकारियां धीरे-धीरे बहुत से एप और साइट के साथ साझा हो जाती हैं.

सोशल मीडिया में क्या न करें

- सोशल मीडिया पर कोई भी निजी जानकारी साझा न करें.
- सोशल मीडिया पर बैंक, खातों या संपत्ति से जुड़ी जानकारी साझा न करें.
- सोशल मीडिया पर अपनी अवस्थिति (लोकेशन) की जानकारी, जब तक आवश्यक न हो साझा न करें.
- सोशल मीडिया पर अपने घर व परिवार से जुड़ी जानकारियों का विस्तृत विवरण न दें. उदाहरण के लिये आप सोशल मीडिया में लगातार ऐसी तस्वीरें या जानकारी साझा करते हैं, जिससे लोगों को पता चलता है कि आपके घर में कौन-कौन है और आप कब घर में और कब बाहर रहते हैं, ऐसे में ये जानकारियां अपराध को बुलावा दे सकती हैं.
- सोशल मीडिया पर बहुत अधिक सक्रिय रहने पर जो जानकारियां साझा की जाती हैं, उन पर ध्यान दें, कहीं वो आपकी दिनचर्या के संबध में कोई पैटर्न तो प्रस्तुत नहीं कर रहीं. ऐसा करना आपराधिक वारदातों को न्योता दे सकता है
- सोशल मीडिया की कार्यपद्धति तथा इसके नकारात्मक प्रभावों को समझने के लिए यह समझना ज़रूरी है कि इन पर लगाम लगाना क्यों मुश्किल है. सोशल मीडिया के तीन पक्ष है. 1. वह व्यक्ति जो लिख रहा है, 2. सेवा प्रदाता, (ISP) जो उसे प्रसारित कर रहा है तथा 3. समाचार-पत्र या पत्रिकाओं जैसा कोई प्लेटफॉर्म, जहाँ से चीज़ें आ रही हैं. इन तीनों में ही गड़बड़ी लिख रहा है उसकी जवाबदेही नहीं है, इसमें 25 से 30% लोग नकली/जाली (Fake) हैं. ये नकली लोग ही सोशल मीडिया पर ट्रोल या गड़बड़ करने के लिये इस्तेमाल किये जाते हैं. इसके बाद जब ISP का नंबर आता है तो वे यह कहते हुए अपने हाथ खड़े कर देते हैं कि वे तो मध्यस्थ (Intermediary) हैं. इसके बाद जो समस्या है वह फिल्टरेशन की है, जिसके तहत तथा अपशब्द वाले कमेंट्स को हटाने का काम होना चाहिए. वस्तुस्थिति तो यह है कि भारत में इसके लिए **फिल्टर नाम** की कोई चीज़ है ही नहीं; और यही अधिकांश फसादों की जड़ है.

देशव्यापी स्तर पर सावधानियाँ : सोशल मीडिया के बढ़ते दुरुपयोग को देखते हुए देश में कंटेंट पर निगरानी के लिये एक प्रभावी तंत्र बनाए जाने की आवश्यकता है.

इसके लिये सोशल मीडिया चलाने वालों को शिकायत अधिकारी की नियुक्ति तथा अपने कार्यालय तथा सर्वर भारत में लगाने हेतु विवश होना पड़ेगा. जहाँ तक इसके विनियमन के लिये कानून बनाने की बात है, तो देश में कानून बहुत हैं लेकिन देश में इन क़ानूनों को अमल में लाये जाने की ज़रूरत है.

जर्मनी की संसद ने इंटरनेट कंपनियों को उनके सोशल मीडिया प्लेटफॉर्म पर निंदनीय, अवैध, नस्लीय सामग्री के लिये जवाबदेह ठहराने वाला कानून पारित किया है. इसके तहत एक निश्चित समयावधि में आपत्तिजनक सामग्री को न हटा पाने पर 50 मिलियन यूरो तक का जुर्माना लगाया जा सकता है. वहाँ जब इंटरनेट कंपनियों ने इस कानून को अभिव्यक्ति की वैध स्वतंत्रता के लिये संभावित खतरा बताते हुए चिंता जताई, तो जर्मनी के न्याय मंत्री ने यह कहकर इसका प्रतिवाद किया कि "**अभिव्यक्ति की स्वतंत्रता वहाँ समाप्त होती है, जहाँ आपराधिक कानून शुरू होता है. (Freedom of opinion ends where criminal law begins.)**" वर्तमान समय में अपने देश में सोशल मीडिया पर पोस्ट की गयी सामग्री के सख्त क़ानूनों को लागू करने की ज़रूरत है.

आज के प्रगतिशील दौर में सोशल मीडिया लोगों को जोड़ने में महत्त्वपूर्ण भूमिका निभा रहा हैं, परन्तु इसका इस्तेमाल हिंसा भड़काने, अफवाहें फैलाने तथा देश और समाज विरोधी कार्यों के लिये भी हो रहा है. लोगों की अभिव्यक्ति के अधिकार का पूरा समर्थन किया जाना चाहिये, लेकिन देश तथा समाज की सुरक्षा अहम है. सोशल मीडिया के गलत इस्तेमाल पर अंकुश लगाना बहुत ज़रूरी है. परिस्थितियाँ बिगड़ने पर इंटरनेट पर प्रतिबंध लगा देना समाधान नहीं है, कठोर क़ानूनों की अनुपालना कर दोषियों को सजा देकर समाज को आईना दिखाने की ज़रूरत आन पड़ी है. वर्तमान में सोशल मीडिया **रोटी, कपड़ा और मकान** के बाद अहम ज़रूरत बन चुका है. इस कदर हमें इसकी आदत पड़ चुकी हैं कि इसके बिना जीवन की परिकल्पना शायद संभव नज़र नहीं आती है. वर्तमान परिप्रेक्ष्य में सोशल मीडिया उस दुधारी तलवार के समान है, जिस पर चलने के लिये सूझबूझ के **साथ-साथ चौकन्ना रहने की ज़रूरत है.**

यदि सोशल मीडिया की सुविधा और उसके नकारात्मक प्रभावों को साथ में देखते हुये समग्र विश्लेषण किया जाए तो हम पाते हैं कि आज के गतिशील दौर में लोगों को क़रीब लाने में, उन्हें विचाराभिव्यक्ति के लिये खुला मंच देने और विचारों के लोकतंत्रीकरण में सोशल मीडिया की बहुत बड़ी भूमिका है, लेकिन इसी सोशल मीडिया का इस्तेमाल जब साइबर अपराध करने, हिंसा भड़काने, अफवाहें फैलाने और इसी प्रकार के अन्य देश एवं समाज विरोधी कार्यों के लिये होने लगता है, तब गंभीरता से इस पर सोचने की ज़रूरत होती है. स्वतंत्रता ज़रूरी है, लेकिन कोई भी स्वतंत्रता बिना ज़िम्मेदारी के नहीं हो सकती. हमें अपनी स्वतंत्रता के साथ-साथ समाज और देश के प्रति

अपने कर्तव्यों की जानकारी भी होनी आवश्यक है. नियामक एजेंसियों को चाहिये कि वो इस दिशा में पहल कर सोशल मीडिया के सही इस्तेमाल का रास्ता प्रशस्त करें. साइबर सुरक्षा और सोशल मीडिया के दुरुपयोग का मुद्दा ऐसा है, जिसे अब अनदेखा नहीं किया जा सकता है. नफ़रत भड़काने वाली सामग्री को साझा करने से सामाजिक सौहार्द बिगड़ता है, क़ानून-व्यवस्था के भी बिगड़ने का ख़तरा रहता है, आंतरिक सुरक्षा पर भी आंच आ सकती है. ऐसे में इसके ख़िलाफ़ सख़्त क़ानून की नितांत आवश्यकता है.

संदर्भ : हिंदुस्तान टाइम्स 25 अगस्त 2016

"लालच बुरी बला है" - साइबर धोखाधड़ी के संदर्भ में

विक्रांत कुमार
प्रबंधक (राजभाषा)
क्षे. का. वाराणसी

लालच बुरी बला है, यह वाक्य जब भी सुनो तो दिमाग में बचपन में सुनी एक कहानी दौड़ने लगती है, जिसका शीर्षक था "लालची कुत्ता." यह एक छोटी सी कहानी थी, जिसमें एक कुत्ता, भूखा होने पर, इधर-उधर अपने लिए खाने की तलाश कर रहा होता है. बहुत देर तक इधर-उधर भटकने के बाद कहीं से उसे एक हड्डी का टुकड़ा मिल जाता है.वह उस टुकड़े को मुँह में दबाकर अपने ठिकाने की ओर चल पड़ता है. रास्ते में एक लकड़ी का पुल पड़ता है. लकड़ी के पुल को पार करते समय उसे अपनी परछाई पानी में दिखती है. उसे लगता है यह कोई दूसरा कुत्ता है, जिसके पास एक और हड्डी का टुकड़ा है. उसके मन में लालच आ जाता है और वह सोचने लगता है कि अगर मुझे यह हड्डी भी मिल जाये तो फिर आज मैं पेट भर के खाना खा सकता हूँ. ऐसा सोचते ही वो तुरंत अपनी परछाई पर गुर्राने लगता है, बदले में परछाई भी गुर्राने लगती है. कुत्ते को गुस्सा आ जाता है और वो परछाई वाली हड्डी पाने के लिए गुस्से से भौंकने के लिए जैसे ही अपना मुँह खोलता है, उसके मुँह की हड्डी नीचे पानी में गिर जाती है और कुत्ते को भूखा ही रहना पड़ता है. लालच में वह अपने पास की हड्डी भी गँवा बैठता है इसलिए कहते हैं "लालच बुरी बला है".

इस कहानी से लालच, असंतुष्टि, स्वविवेक आदि को समझने का मौका मिलता है. कहानी के मुख्य पात्र कुते को अधिक पाने की चाह होती है साथ ही जो उसके पास उपलब्ध होता है उससे वह असंतुष्ट रहता है. लालच और असंतुष्टि में वह स्वविवेक का उपयोग नहीं करता है और जो हड्डी का टुकड़ा उसके पास होता है उसे भी वह गवां बैठता है. इस कहानी से लालची बनने एवं असंतुष्टि की अवस्था में भी स्वविवेक का प्रयोग करने की शिक्षा मिलती है.

बैंकिंग के संदर्भ में लालच के कई मायने हैं. बैंक में ग्राहकों के खाते से, जमा रकम को निकालने या दूसरे खाते में अंतरित करने के लिए, वर्तमान में वैकल्पिक माध्यमों का

ज्यादा से ज्यादा प्रयोग किया जाता है. वैकल्पिक माध्यमों में एटीएम, इंटरनेट बैंकिंग, मोबाइल बैंकिंग आदि का प्रयोग किया जाता है. इन वैकल्पिक माध्यमों के प्रयोग के समय बैंक से जुड़े प्रशिक्षित स्टाफ मौजूद नहीं होते हैं बल्कि ग्राहक स्वयं इसका प्रयोग करता है. ग्राहक अपनी सूझबूझ से इन सभी माध्यमों का प्रयोग कर, रकम निकासी या अंतरण करता है और उन्हें इसकी सूचना भी एसएमएस तथा मेल के माध्यम से प्रदान की जाती है.

वैकल्पिक माध्यमों के बारे में, कई बार मेल के माध्यम से धोखाधड़ी करने वाली संस्थाओं या व्यक्तियों द्वारा लॉटरी लगने या इनाम मिलने की सूचना प्रदान की जाती है. लॉटरी या इनाम प्राप्त करने के लिए ग्राहक को कुछ रकम मेल के माध्यम से प्रदान किए गए खाते में 'कर' के रूप में जमा करना होता है. ग्राहक को सूचित किया जाता है कि आपको इनाम या लॉटरी की राशि तभी प्रदान की जायेगी जब आप कर की राशि, खाते में जमा करवा देंगे. खाते में राशि के जमा होने के पश्चात आपके द्वारा पुष्टि प्रेषित करने के उपरांत ही इनाम या लॉटरी की राशि आपके खाते में क्रेडिट की जायेगी. रकम क्रेडिट करने के लिए, कई बार खाते के पूर्ण विवरण, जिसमें बैंक द्वारा प्रदान की गयी गुप्त जानकारियां भी, ग्राहक से ले ली जाती है. इनाम या लॉटरी की राशि प्राप्त करने हेतु, ग्राहक द्वारा खाते में रकम क्रेडिट करने और अपने खाते का पूर्ण विवरण प्रदान करने के पश्चात धोखाधड़ी करने वाली संस्था या व्यक्ति अचानक गायब हो जाता है. ग्राहक को इनाम या लॉटरी की राशि तो प्राप्त होती नहीं बल्कि उसके द्वारा जमा की गयी राशि को भी निकाल लिया जाता है. ठगी का शिकार होने के पश्चात ग्राहक द्वारा खाते का विवरण जानने की कोशिश भी बेकार हो जाती है क्योंकि जिस खाते में ग्राहक को रकम जमा करने हेतु निर्देशित किया जाता है, उससे जुड़ी सभी जानकारी गलत होती है या फिर नहीं होती है. इस तरह ग्राहक इनाम या लॉटरी की राशि पाने के लालच में धोखाधड़ी का शिकार हो जाता है.

इसी प्रकार मेल के माध्यम से बैंक से जुड़ी सभी गुप्त जानकारियां, जो बैंक द्वारा केवल ग्राहकों को प्रदान की जाती हैं, उसे धोखाधड़ी करने वाली संस्थाओं या व्यक्तियों द्वारा मांगा जाता है एवं आश्वस्त किया जाता है कि आपको प्राप्त लॉटरी/इनाम की रकम आपके खाते में प्रदान की जायेगी. खाते की समस्त जानकारियां प्राप्त कर, किसी भी वैकल्पिक चैनल द्वारा ग्राहक के खाते से रकम निकासी या अंतरण कर लिया जाता है. हम सभी को सदैव यह ध्यान देना चाहिए कि लॉटरी या इनाम वाले बेवजह इसके भुगतान के लिए सभी सूचनाएँ क्यों मांग रहे हैं. ठगी का शिकार होने वाला ग्राहक अधिक पाने की लालच में अपना पैसा गंवा बैठता है.

धोखाधड़ी के अन्य रूपों में कई बार नकली बैंककर्मी बनकर, ग्राहकों को कार्ड बंद होने का झांसा देकर टेलीकॉलिंग के माध्यम से बैंक से जुड़ी जानकारियां जैसे - कार्ड नंबर, सीवीवी, एक्सपायरी डेट मांगी जाती हैं एवं वेरिफिकेशन कोड के नाम पर ओटीपी (वन टाइम पासवर्ड) भी मांग लिया जाता है तथा ग्राहक के खाते से ऑनलाइन शॉपिंग करके या अन्य किसी प्रकार से रकम अंतरित कर ली जाती है या खर्च कर दी जाती है.

ऊपर वर्णित सभी प्रकार की घटनायें वैकल्पिक माध्यमों के द्वारा ग्राहकों से की गई धोखाधड़ी से संबन्धित हैं. गलत योजनाओं की जानकारी देकर ग्राहकों से रकम का निवेश करवाया जाता है जिसमें, कई बार निवेश करवाने वाले को पहले से ही पता होता है कि रकम की वापसी बहुत कम होगी, फिर भी ग्राहकों को गलत जानकारी देकर गलत योजना में, रकम का निवेश करवा दिया जाता है, जो बाद में डूब जाता है. निवेश के समय कम समय में अधिक रकम प्राप्त होने का झांसा दिया जाता है और ग्राहक भी पूरी जानकारी प्राप्त किए बिना ठगी का शिकार हो जाता है. ग्राहक कम जानकारी और अधिक पाने की चाहत में ऐसी झूठी योजनाओं में रकम निवेश के लिए तैयार हो जाते हैं और योजनाओं की सत्यता की पुष्टि भी नहीं करते हैं.

लेंडिंग दिशानिर्देशों का पालन करते हुए डिजिटल लेंडिंग

संजीव कुमार
सहायक महाप्रबंधक
सरल, रांची

"लेंडिंग" बैंकिंग जगत का प्राचीनतम व्यवसाय रहा है और यह तब से चलता आ रहा है, जब से बैंकिंग व्यवस्था अस्तित्व में आई, बैंकिंग परंपरा की शुरुआत ही इस व्यवस्था से हुई कि जिन लोगों के पास, आवश्यकता से ज्यादा राशि उपलब्ध हो, उन लोगों से पैसे जमा के रूप में स्वीकार करना और जिन लोगों को पैसों की जरूरत हो, उन लोगों को पैसे लोन के रूप में देना और उस पर ब्याज अर्जित करना. मुख्यतः बैंक का आधारभूत कारोबार ही यही रहा है. आज के परिप्रेक्ष्य में, बैंकों के आय के अनेकों श्रोत हैं लेकिन परंपरागत बैंकिंग के आय का, एकमात्र श्रोत लोन देकर ब्याज अर्जित करना ही रहा है. यह एक महत्वपूर्ण तथ्य है कि बैंक जिसे लोन के रूप में पैसे देता है, वो ब्याज के साथ ऋण को अदा भी करे, जिसके लिए समय-समय पर दिशानिर्देश जारी किए जाते रहे हैं. यहाँ पर यह बताना आवश्यक है कि हमारे देश में बैंकिंग नियामक बहुत ही सशक्त है और ग्राहकों के हितों को पूरी तरह से सुरक्षित रखकर ही, बैंकिंग व्यवहार किया जाता है. खासकर लेंडिंग के मामले में, यह पूरी तरह से रेगुलेटेड इंडस्ट्री है.

बदलते परिवेश में, बैंकिंग जगत में आमूलचूल परिवर्तन देखने को मिला है. परंपरागत बैंकिंग, जो सबसे पहले, बही खाते की बैंकिंग थी, से कंप्यूटर युग की शुरुआत हुई और बैंकिंग भी उससे अछूती नहीं रही, फिर पहले कोर बैंकिंग सोल्यूशंस और अब डिजिटल इंडिया. ये बैंकिंग जगत में विभिन्न बदलाव के युग रहे हैं. सबसे महत्वपूर्ण इस बात को समझना है कि बैंक पैसे के लेन-देन से जुड़ा क्षेत्र होने के कारण इसमें हमेशा जोखिम भरा रहता है. अतः हर एक परिवर्तन के युग में, "जोखिम प्रबंधन" मुख्य मुद्दा रहा है. उसी क्रम में, आज हम डिजिटल माध्यम से लेंडिंग की बात करते हैं तो उससे जुड़े जोखिम को पहचानना, उसका सही आंकलन करना एवं उसके प्रबंधन के उचित उपाय करना विशेष महत्व रखता है. इसी क्रम में बैंकिंग दिशानिर्देशों का पालन करना भी अनिवार्य है.

लेंडिंग के दिशानिर्देश

जैसा कि हम जानते हैं, लेंडिंग करना और उसके द्वारा ब्याज अर्जित कर लाभ कमाना ही बैंकिंग का प्राचीनतम व्यवसाय रहा है. लेकिन समय के साथ बदलते परिदृश्य में, इस व्यवसाय से जुड़े जोखिम भी हमारे सामने चुनौती खड़े करते रहे हैं. इसमें बैंकिंग लोन में धोखाधड़ी सबसे अहम रहा है. मुख्यतः, बैंक उन लोगों को लोन देता है, जिन्हें पैसे की तत्काल जरूरत हो और फिर समयांतराल में, पूर्व निर्धारित समय सीमा के अंदर ग्राहक ब्याज के साथ उस लोन की रकम को वापस लौटा दे. पुराने समय में या फिर हमारे देश के ग्रामीण क्षेत्रों में इस तरह के व्यवसाय में महाजन पहले से जुड़े हुए थे, लेकिन उनके व्यवसाय गैर संगठित होने कारण वे मनमाना तरीके से मोटी रकम ब्याज के रूप में वसूलते थे. बैंकिंग का विस्तार होने से धीरे-धीरे उन जरूरतमन्द लोगों के लिए बैंक लोन एक सहारा बन गया और लोगों को संगठित क्षेत्र से एक सम्मानजनक दर पर लोन मिलने लगा. लेकिन लोगों ने इसे भी धोखाधड़ी का एक माध्यम बना लिया. बैंक से लिए गए लोन को वापस नहीं लौटाने के युग की शुरुआत हुई. अतः जैसे-जैसे इस तरह के मामले सामने आते गए आरबीआई द्वारा दिशानिर्देश जारी होते गए और आज यह पूरी तरह से एक रेगुलेटेड इंडस्ट्री बन गयी है. कुछ दिशानिर्देश आरबीआई खुद जारी करता है जबकि कुछ बैंकों के निदेशक मण्डल के ऊपर छोड़ देता हैं.

मुख्यतः लोन दो प्रकार के होते हैं. पहला कंज़्यूमर लोन और दूसरा बिज़नेस लोन. अगर सरल भाषा में लिखा जाए तो कंज़्यूमर लोन वो होता है, जिसका भुगतान उधारकर्ता की आय से होता है और बिज़नेस लोन वो होता है, जिसका भुगतान इस लोन से किए गए व्यवसाय से अर्जित आय से होता है. अर्थात लोन देने से पहले हमें यह सुनिश्चित करना अति आवश्यक है कि जिस किसी को भी लोन दे रहे हैं, उसे पर्याप्त आय अर्जन हैं, जिससे कि वो इस लोन का भुगतान सही समय पर करता रहेगा या फिर इस लोन के माध्यम से वह एसेट बना पाएगा, जिससे वह पर्याप्त मात्रा में आय अर्जित कर सके और लोन का भुगतान आसानी से हो सके. इस संबंध में, बैंक द्वारा समय-समय पर काफी व्यापक दिशानिर्देश जारी किए जाते रहे हैं.

डिजिटल बैंकिंग - अनिवार्यता

डिजिटल माध्यम से लेंडिंग हमारा विकल्प नहीं बल्कि मजबूरी बन चुकी है. तेजी से बदलते डिजिटल परिवेश में ग्राहकों की मांग और सुविधा को नजर में रखते हुए हमें अपने आप को अपडेट रखना है नहीं तो आज के इस अति प्रतिस्पर्धात्मक बाज़ार में अपना अस्तित्व बचाना मुश्किल हो जाएगा. आज पूरे विश्व में "डिजिटल क्रांति" ने एक वृहद रूप ले लिया है और निजी क्षेत्र के बैंक एवं विदेशी बैंक, जो भारत में अपना व्यापार कर रहे हैं, वो तेजी से अपना डिजिटल प्रॉडक्ट लोगों को ऑफर कर रहे हैं. चूंकि हम भी

उसी मार्केट में हैं, अतः इस प्रतिस्पर्धा में बने रहने के लिए हमें निश्चित रूप से डिजिटल होना ही पड़ेगा और लोगों की सुविधा को ध्यान में रखते हुए "डिजिटल लेंडिंग" करनी ही पड़ेगी.

अगर "डिजिटल इंडिया" की गहराई की बात करें तो एक आंकड़े के अनुसार भारत में लगभग 46 करोड़ इंटरनेट यूज़र्स हैं. तेजी से बढ़ते सोशल मीडिया आजकल संचार के सबसे तेज माध्यम बन चुके हैं. लोगों की पसंद है कि इंटरनेट के माध्यम से उसे सारी सुविधाएँ मिलें, जिसे वे अपनी सुविधा के अनुसार उचित समय पर इस्तेमाल कर सकें. इंटरनेट बैंकिंग की शुरुआत सिर्फ बचत बैंक खातों से हुई थी, लेकिन धीरे-धीरे लोन खाते भी इंटरनेट बैंकिंग से जुड़ते गए और ग्राहकों को बैंक की किसी भी शाखा से बैंकिंग करने की अनुमति प्रदान कर दी गयी. आज ऋण खाता धारकों को भी इंटरनेट बैंकिंग की सुविधा प्रदान की जाती है ताकि वे अपनी सुविधानुसार फ़ंड का ट्रान्सफर (चुकौती) खुद कर सकें.

ऐसे भी जब से कोर बैंकिंग सोल्यूशंस ने बैंकिंग जगत में मूर्त रूप लिया है, ऋण खातों पर हमारी पकड़ धीरे-धीरे कमजोर होती गई है. पहले जो खाता एक शाखा तक सीमित था, आज वो केंद्रीकृत हो गया हैं और ग्राहक उसे कहीं से भी किसी भी समय ऑपरेट कर सकता हैं. चेक का प्रचलन अब लगभग विलुप्त हो गया है और इंटरनेट बैंकिंग के माध्यम से ग्राहक खुद अपना फ़ंड रेमिट करते हैं और उसे मॉनिटर करना बैंक के लिए मुश्किल सा हो गया है.

सरकार द्वारा उठाए गए कदम

भारत सरकार और आरबीआई ने भी इस दिशा में कई कदम उठाए हैं और खुदरा लोन से शुरू होकर धीरे-धीरे अब यह लगभग सभी प्रकार के ऋणों के अनुमोदन प्रणाली को ऑनलाइन करने तक आ गया है. समस्त बैंकों को अनिवार्य रूप से अपने वेबसाइट पर ऑनलाइन अप्लाई करने के लिए लिंक की अनिवार्यता, सारे शिक्षा ऋण को विद्या लक्ष्मी पोर्टल के माध्यम से ही अनुमोदित करना, एमएसएमई ग्राहकों के लिए ऑनलाइन एप्लिकेशन की सुविधा उपलब्ध कराने से लेकर हाल ही में भारत सरकार द्वारा एमएसएमई ग्राहकों को ₹ 10 लाख से लेकर ₹ 1 करोड़ तक के लोन को ऑनलाइन "इन-प्रिन्सिपल" अनुमोदन 59 मिनट में देना शामिल है. इसके लिए एक समर्पित वेबसाइट www.psbloanin59minutes.com बनायी गयी है, जिसके माध्यम से कोई भी ग्राहक ऑनलाइन एप्लिकेशन कर सकता है और जिस बैंक को चुना जाता है, उसे 59 मिनट के अंदर इन-प्रिन्सिपल अनुमोदन प्रदान करना होता है. अपना बैंक भी इसका सदस्य है और हम भी ऐसे ऋण आवेदनों को ऑनलाइन इन-प्रिन्सिपल अनुमोदन दे रहे हैं. इसमें आवेदन करने वाले ग्राहक को अपने सारे दस्तावेज़ ऑनलाइन 'अपलोड' करना होता है, जो कि

बैंक के पास ऑनलाइन उपलब्ध होता है और उसी के आधार पर बैंक अपना अनुमोदन प्रदान करता है.

हमारे बैंक द्वारा उठाए गए कदम

डिजिटल माध्यम से लोन स्वीकृत करने की दिशा में हमारा बैंक काफी अग्रणी रहा है. हमारे बैंक में काफी पहले से ही LAS (लेंडिंग ऑटोमेशन सिस्टम) के माध्यम से लोन का अनुमोदन किया जाता है. आज अपने बैंक के समस्त रिटेल लोन को अनिवार्य रूप से LAS के जरिये ही स्वीकृत करना है और उसी आंकड़े के आधार पर फ़िनेकल में खाता भी खोलना है. दूसरे शब्दों में कहा जाए तो किसी भी रिटेल लोन का खाता फिनेकल में सीधे नहीं खोल सकते हैं.

इस प्रयास को और आगे बढ़ाते हुये आज हमें नॉन-रिटेल लोन भी LAS के जरिये ही प्रोसेस करना होता है. सरल के गठन के साथ ही डिजिटल लेंडिंग पर ज़ोर दिया जा रहा है. शाखाओं को ऋण प्रस्ताव एवं सारे दस्तावेज़ LAS के माध्यम से ही भेजना है एवं उसे LAS में ही अनुमोदित करना है. सरल का परफॉर्मेंस भी ऑनलाइन ट्रैक किया जा रहा है. अर्थात सिर्फ उन्हीं आँकड़ों के आधार पर परफॉर्मेंस की समीक्षा होगी, जो ऑनलाइन उपलब्ध हैं. नॉन-रिटेल लोन के खाते भी सीधे तौर पर फिनेकल में खोला जाना संभव है.

डिजिटल बैंकिंग की जड़ों को और मजबूत करने के लिए अपने बैंक ने इसे अपने स्ट्रैटजी पेपर में अहम स्थान दिया है. "विजन 20-20" में भी डिजिटल माध्यम से लेंडिंग प्रणाली को आगे बढ़ाने पर ज़ोर दिया गया है. वित्तीय वर्ष 2018-19 के स्ट्रेटजी पेपर में डिजिटल बैंकिंग के आंकडें एवं लक्ष्यों पर एक नजर डालते हैं.

वित्तीय वर्ष 2018-19 के लिए डिजिटल बैंकिंग का लक्ष्य

क्र सं	विवरण	मार्च 2017	मार्च 2018	मार्च 2019
1	ई-ट्रांज़ैक्शन (सारे लेन-देन के अनुपात में)	67.90	75.70	77.50
2	कुल एटीएम	7518	7642	7700
3	कुल डेबिट काड्र्स (लाख में)	309	356	375
4	कुल क्रेडिट कार्ड (लाख में)	1.80	2.20	6.00
5	मोबाइल बैंकिंग (लाख में)	11.30	20.50	40.00
6	इंटरनेट बैंकिंग - खुदरा (लाख में)	14.30	17.10	19.75
7	इंटरनेट बैंकिंग - कॉर्पोरेट (लाख में)	1.00	1.40	1.75

(श्रोतः अपने बैंक का स्ट्रेटजी पेपर 2018-19)

मुख्य अड़चनें

जैसा कि हम ऊपर चर्चा कर चुके हैं, हम लेंडिंग करने के लिए पैसे भी, जनता से जमा के रूप में स्वीकार करते हैं और इस तरह से हम जनता के पैसे के रखवाले हैं. अतः यह सुनिश्चित करना होगा कि जो लेंडिंग की जाए, वह सुरक्षित हाथ में जाए और उसका इस्तेमाल विकास कार्यों के लिए ही हो, जिससे कि लोन की अदायगी भी नियत समय पर होती रहे. किसी भी तरह की लापरवाही जिससे कि जनता का पैसा गलत हाथों में चला जाए और उसका गलत इस्तेमाल हो, हमारी विश्वसनीयता पर सवाल खड़े करेगा. वह विश्वास जो जनता हम पर करती है, उसे कायम रखना हमारी सबसे बड़ी ज़िम्मेदारी है.

दूसरी दिक्कत डाटा चोरी होने की है क्योंकि डिजिटल बैंकिंग में सबसे बड़ा जोखिम डाटा का चोरी होना है और लेंडिंग के मामले में यह अत्यंत चिंता का विषय है.

निष्कर्ष

जैसा कि ऊपर वर्णित है कि एक तरफ लेंडिंग हमारी आय का मुख्य श्रोत है तो दूसरी तरफ डिजिटल लेंडिंग हमारी मजबूरी या कहा जाए तो इस प्रतिस्पर्धात्मक बैंकिंग में बने रहने के लिए अत्यावश्यक. ना ही हम लेंडिंग को रोक सकते हैं और ना ही डिजिटल से अपने आप को दूर रख सकते हैं. अतः डिजिटल लेंडिंग हमारी आज की मांग है और हम इसके लिए कटिबद्ध हैं. हालांकि हमारे पास जनता का पैसा है और लेंडिंग करते समय इसके सदुपयोग की ज़िम्मेदारी हमारी है, जिसके लिए हमारे बैंक द्वारा जारी दिशानिर्देशों का पालन करना जरूरी है और हमारा बैंक यूनियन बैंक ऑफ इंडिया इसमें सदैव ही अग्रणी रहा है.

ई-टेंडरिंग (प्रतिवर्ती नीलामी)

राजेश कुमार
सहायक महा प्रबंधक (राजभाषा)
राजभाषा कार्यान्वयन प्रभाग, के. का. मुंबई.

ई-टेंडरिंग निविदा प्रक्रिया में पारदर्शिता, निष्पक्षता एवं सभी निविदाकर्ताओं को समान अवसर प्रदान करने की आवश्यकता के लगभग पक्के समाधान के रूप में उभर कर सामने आया है. इसके द्वारा किसी वस्तु या सेवा में उस न्यूनतम मूल्य को पता लगाने में मदद मिलती है, जिसके वास्तविक मूल्य का अनुमान कभी-कभी क्रेता को भी नहीं होता और इसके द्वारा पारदर्शी रुप से क्रेता संस्था को उपयुक्त न्यूनतम कीमत पर वस्तु अथवा सेवा उपलब्ध हो जाती है और निविदाकर्ता को भी कोई शिकायत नहीं होती. निविदा प्रक्रिया में लोगों की विश्वसनीयता एवं इस प्रक्रिया में सरकार द्वारा जारी सभी मानदंडों के अनुपालन का समावेश होने से यह प्रक्रिया दिन-प्रतिदिन अपने पांव पसारती जा रही है और अब यह भारतीय बाजार विशेषतया सूचना प्रौद्योगिकी के क्षेत्र में विधिवत स्थापित हो चुकी है. इसे प्रतिवर्ती नीलामी (रिवर्स ऑक्शन) के नाम से भी जाना जाता है.

केन्द्रीय सतर्कता आयोग ने वर्ष 2003 एवं उसके बाद समय-समय पर जारी आदेशों के अधीन सभी बैंकों एवं सरकारी प्रतिष्ठानों को एक ऐसी ई-प्रोक्योरमेंट नीति तैयार करने के निर्देश दिए हैं, जो पारदर्शी एवं निष्पक्ष हो एवं जिसमें सभी पक्षकारों के हितों को समुचित सुरक्षा प्रदान की गयी हो. इस प्रक्रिया में निविदा प्रस्ताव दो अलग-अलग मुहरबंद लिफाफों में प्राप्त किए जाते हैं - तकनीकी एवं कारोबारी. कारोबारी प्रस्ताव केवल उन्हीं निविदाकर्ताओं के खोले जाते हैं, जो निविदा में वर्णित सभी तकनीकी आवश्यकता को पूरी करते हों और तकनीकी मूल्यांकन हेतु गठित समिति द्वारा तकनीकी मूल्यांकन में उपयुक्त पाए गए हों.

यह पूरी प्रक्रिया इलेक्ट्रानिक माध्यम से संचालित होने के कारण इसमें भौतिक दस्तावेजों का न्यूनतम प्रयोग होता है. बैंक द्वारा अनुमोदित हार्डवेयर एवं सॉफ्टवेयर खरीदी के अतिरिक्त अन्य बड़ी खरीदों के लिए ई-टेंडरिंग प्रक्रिया ही प्रयुक्त की जाती है, जिससे खरीद में पारदर्शिता और निष्पक्षता के साथ-साथ बाजार में उपलब्ध प्रतियोगिता का समुचित लाभ बैंक को प्राप्त हो सके.

ई-टेंडरिंग क्या है?

ई-टेंडरिंग ई-प्रोक्योरमेंट के लिए प्रयोग में लाए जा रहे विभिन्न तरीकों में से एक है. इसके द्वारा कॉमर्शियल प्रस्ताव हेतु प्रस्तावित राशि का मोल-तोल इलेक्ट्रानिक नीलामी के माध्यम से किया जाता है, जिससे न्यूनतम बोली लगाने वाले वेंडर का चयन किया जा सके. इससे न केवल मूल्य का पता लगाने में सहायता मिलती है बल्कि तकनीकी मूल्यांकन में सही पाए गए सभी वेंडर्स को बिना हटाए हुए शामिल होने का अवसर भी प्राप्त होता है.

ई-टेंडरिंग को विशेष नीलामी के रूप में भी परिभाषित किया जा सकता है, जो बैंकों को किसी टेंडर को घटती हुई मूल्य नीलामी के माध्यम से व्यावसायिक मूल्य निर्धारण का अवसर प्रदान करती है. दूसरे शब्दों में, यह सामान्य नीलामी के एकदम पलट है, जिसमें माल की बिक्री नीलामी द्वारा बढ़ती हुई मूल्य दरों पर की जाती है. यह सामान्य नीलामी अर्थात् बढ़ते मूल्य से उल्टी प्रक्रिया है, इसीलिए इसे प्रतिवर्ती नीलामी (रिवर्स ऑक्शन) के नाम से जाना जाता है.

परंपरागत टेंडरिंग प्रक्रिया, जिसमें बैंक केवल एल-1 वेंडर से ही मूल्य के बारे में बातचीत कर सकता था, के उलट प्रतिवर्ती नीलामी में सभी बोली लगाने वालों, जो तकनीकी मूल्यांकन में योग्य पाए गए हैं, के पास एक अवसर होता है कि वे पूरी 'बोली अवधि' के दौरान लगातार अपने मूल्य में सुधार कर सकते हैं.

प्रतिवर्ती नीलामी के फायदे

बैंक को फायदे

बैंक पारदर्शिता एवं कुशलतापूर्वक व्यावसायिक मूल्य निर्धारण के लिए पूरी प्रक्रिया को डिटिडाइज्ड कर पाता है. इसलिए, मैन्युअल प्रोसेस में आने वाली कमियों का निदान हो जाता है. इसके अलावा, बैंक को तकनीकी रूप से सफल सभी वेंडरों से एक साथ मूल्य निर्धारण का अवसर प्राप्त हो जाता है और इस प्रक्रिया में मूल्यों को कई बार नीचे लाने का अवसर प्राप्त होता है, जिससे बातचीत के द्वारा मूल्यों को कम करने की प्रक्रिया में लगने वाले समय की बचत होती है.

विक्रेता को फायदा

प्रतिवर्ती नीलामी में न केवल एक अर्थात् एल-1 बल्कि तकनीकी रूप से सफल सभी वेंडरों को व्यावसायिक मूल्य निर्धारण में भाग लेने का अवसर प्राप्त होता है. वेंडरों को प्रतिवर्ती नीलामी के नियमों की जानकारी स्पष्टतया वहीं मिल जाती है और उनको नीलामी अवधि के दौरान लगातार कई बार मूल्यों में सुधार करने का अवसर प्राप्त होता है.

सतर्कता अनुपालन

प्रतिवर्ती नीलामी प्रक्रिया में टेंडरिंग के सभी तीन आवश्यक घटक अर्थात् पारदर्शिता, निष्पक्षता एवं समान अवसर का समावेश होता है. चूंकि यह पूरी प्रक्रिया डाटा इन्क्रिप्शन एवं डिजिटल हस्ताक्षर जैसी डिजिटाइज्ड विशेषताओं से निहित होती है, इसलिए बैंक को किसी भी विवाद की स्थिति में इलेक्ट्रानिक रिकार्ड उपलब्ध होने का लाभ मिलता है.

निम्नलिखित कारणों से शिकायतों की संभावनाएं कम हो जाती हैं :

1. वेंडर के केवल प्राधिकृत प्रतिनिधि ही भाग लेते हैं.
2. पूरी प्रक्रिया में गोपनीयता और पारदर्शिता को बनाए रखा जाता है.
3. नीलामी अवधि के दौरान सभी प्रतिभागी वेंडरों को वेंडर का नाम जाने बगैर न्यूनतम मूल्य की जानकारी प्राप्त होती रहती है.
4. नीलामी अवधि के दौरान सभी वेंडरों को न्यूनतम मूल्य भरने का समान अवसर प्राप्त होता है.

प्रतिवर्ती नीलामी प्रक्रिया की शुरुआत

प्रतिवर्ती नीलामी प्रक्रिया का आरंभ किसी आरएफपी प्रक्रिया का सफलतापूर्वक तकनीकी मूल्यांकन और तदुपरांत उत्पाद/प्रस्ताव में एकरुपता सुनिश्चित करने के उद्देश्य से सामान्यीकरण, यदि कोई हो, के द्वारा की जाती है. आरएफपी का तकनीकी मूल्यांकन करते समय आरएफपी में वेंडर हेतु वर्णित नियम एवं शर्तों की कड़ाईपूर्वक जांच की जानी चाहिए.

किसी भी तकनीकी मूल्यांकन में सामान्यतः निम्नलिखित नियम एवं मानदंड होते हैं :

- ईओआई/आरएफपी में वर्णित पात्रता मानदंडों के साथ अनुपालन.
- आरएफपी में वर्णित तकनीकी/कार्यात्मक और एएमसी मानदंडों का अनुपालन.
- आरएफपी में वर्णित नॉक आउट मानदंड, यदि कोई हो, का अनुपालन.
- इसके अलावा, प्रेज़ेंटेशन, संदर्भित साइट निरीक्षण, ग्राहकों के फीडबैक आदि जैसे विभिन्न परिभाषित पैरामीटरों पर मूल्यांकन.
- विभिन्न पैरामीटरों के लिए परिभाषित स्कोरिंग पैटर्न के अनुसार अंक प्रदान करना और मूल्यांकन में अर्जित अंकों के आधार पर वेंडरों को शार्ट लिस्ट करना.

- सभी अन्य तकनीकी पहलुओं पर आधारित सामान्यीकरण, यदि कोई हो, और अनप्राइज़्ड कामर्शियल बोली, रिकार्ड में उपलब्ध अन्य सूचनाओं, पिछली प्रक्रिया से प्राप्त अनुभवों, उद्योग में अन्य सहभागियों से सूचना प्राप्त करना आदि.

सामान्यीकरण Normalization:

किसी प्रतिवर्ती नीलामी प्रक्रिया को आरंभ करने से पहले, सामान्यतः यह आवश्यक हो जाता है कि तकनीकी प्रस्तावों का सामान्यीकरण किया जाए. ऐसा इसलिए किया जाता है जिससे कि विभिन्न प्रस्तावों को उनकी विशेषताओं के आधार पर एक समान रुप दिया जा सके. हांलाकि आरएफपी में उत्पाद की आवश्यकताओं के बारे में विस्तृत सूची वर्णित होती है, फिरभी, यह आवश्यक नहीं कि विभिन्न वेंडरों के उत्पाद में निहित विशेषताओं एवं निरंतर बाजार में हो रहे बदलावों को पूरी तौर पर आरएफपी में शामिल कर लिया गया हो. बैंक की अपेक्षाएं स्वीकार्य और पर्याप्त होने एवं आसानी से पूरी होने पर, बैंक न केवल प्रस्ताव को स्वीकार करने के लिए बाध्य होगा बल्कि स्वयं को इस बात का दोषी भी नहीं मानेगा कि उसने किसी प्रस्ताव को आरएफपी में वर्णित शर्तों का बहुत कड़ाई से पालन करते हुए सामान्य रीडिंग द्वारा निरस्त कर दिया. प्रस्तावों की पर्याप्त परख और समझ की प्रक्रिया को ही 'प्रस्तावों का सामान्यीकरण' कहा जाता है.

वेंडर्स अपनी कंपनी की कार्यप्रणाली के कारण अपने प्रस्ताव में विभिन्न नाम एवं विशेषताएं और बिलिंग की शर्तें देते हैं. इन्हें समझने की आवश्यकता होती है और केवल सामान्यीकरण की प्रक्रिया ही यह सुनिश्चित करती है कि बैंक द्वारा वांछित टीसीओ में सभी पहलुओं को शामिल किया गया है. इसलिए, सामान्यीकरण की प्रक्रिया किसी बोली को आरंभ करने से पहले किया जाना आवश्यक है, जिससे कि उत्पाद/प्रस्ताव में एकरुपता लायी जा सके.

आरएफपी में वर्णित उत्पाद/सेवाओं के सामान्यीकरण में प्रायः निम्नलिखित चीजें शामिल होती हैं:

- आरएफपी दस्तावेज के प्रत्युत्तर में विभिन्न वेंडरों द्वारा आपूरित किए जा रहे प्रत्येक उत्पादों या सेवाओं के बारे में आरएफपी दस्तावेजों में वर्णित सभी अपेक्षाओं का सत्यापन.
- पायी गयी विसंगतियों, कमियों का सूचीयन.
- बैंक द्वारा पायी गयी कमियों, नोटिंग पर वेंडरों का स्पष्टीकरण. वेंडर द्वारा प्रस्तुतीकरण के दौरान उत्पाद/प्रस्ताव के संबंध में उठाई गई समस्याएं एवं उनका स्पष्टीकरण, संदर्भित साइट निरीक्षण, ग्राहकों के फीडबैक आदि जैसे विभिन्न परिभाषित पैरामीटरों पर मूल्यांकन.

- लाइसेंस फीस के संबंध में बैंक द्वारा वर्णित लागत की बिल, ऑपरेटिंग सिस्टम की लागत (व्यक्तिगत प्रस्तावों/उत्पाद विशेष पर लागू लाइसेंस फीस), लागू वारंटी अवधि और यदि किसी वेंडर द्वारा अतिरिक्त वारंटी दी जा रही हो, तो उसकी लागत का आकलन.
- प्रस्ताव में वर्णित कोई अन्य विशिष्ट संभावित लागत, जैसे कि प्रशिक्षण लागत, इंजीनियर्स के रहने एवं उनके ट्रैवल का व्यय, बैंक द्वारा वहन किये जाने वाले अन्य व्यय आदि का आकलन.
- प्रस्तावों में एकरुपता लाने के लिए अन्य पहलू, यदि कोई हों, पर विचार करना.

प्रतिवर्ती नीलामी की कार्यविधि

इलेक्ट्रानिक माध्यमों से प्रतिवर्ती नीलामी प्रक्रिया संपादित करने हेतु सॉफ्टवेयर उपलब्ध हैं, जो पूर्णतया स्थापित हो चुके हैं. बैंक स्वतः सॉफ्टवेयर का लाइसेंस खरीद कर स्वतः भी प्रतिवर्ती नीलामी संचालित कर सकता है. वैकल्पिक रूप में, बैंक सेवाप्रदाताओं से प्रतिवर्ती नीलामी प्रक्रिया आउटसोर्स करा सकते हैं. इस प्रकार चयनित सेवा प्रदाता बैंक की ओर से प्रतिवर्ती नीलामी प्रक्रिया पूरी कराते हैं. ऐसी आउटसोर्सिंग व्यवस्था हेतु उपयुक्त एसएलए (सेवा स्तर करार) निष्पादित किया जाना चाहिए.

सेवा प्रदाता

प्रतिवर्ती नीलामी सुरक्षित वेब पोर्टलों के माध्यम से इलेक्ट्रानिक रूप में संपन्न कराई जाती है. नीलामी ई-प्रोक्योरमेंट नीलामी कंपनियों द्वारा संपादित कराई जाती हैं. ई-प्रोक्योरमेंट/प्रतिवर्ती नीलामी की आउटसोर्सिंग के लिए बैंक एक या दो कंपनियों का चयन कर सकते हैं. बैंक उनकी योग्यता और प्रचलित चयन प्रक्रिया के माध्यम से सेवा प्रदाताओं का चुनाव कर सकते हैं. सेवा प्रदाताओं के चयन के लिए निम्नलिखित पात्रता मानदंड होगाः

- सेवा प्रदाता के पास प्रतिवर्ती नीलामी हेतु एक अलग वेब पोर्टल होना चाहिए.
- सेवा प्रदाता एक आईएसओ 9001-2000 कंपनी होना चाहिए.
- वेब पोर्टल सुरक्षित साइट होनी चाहिए, जिसमें न्यूनतम 128 बिट एसएसएल इन्क्रिप्शन उपलब्ध हो.
- सेवा प्रदाता के पास ऐसी प्रतिवर्ती नीलामी का कम से कम दो वर्षों का अनुभव अवश्य होना चाहिए.

- सेवा प्रदाता को कम से कम एक राज्य सरकार, एक बड़े सार्वजनिक क्षेत्र के उपक्रम/सरकारी संगठन और एक सार्वजनिक क्षेत्र के बैंक में प्रतिवर्ती नीलामी प्रक्रिया कराने का अनुभव होना चाहिए एवं यह सुनिश्चित किया जाए कि उनके द्वारा सभी संबंधित संगठनों को संतोषजनक सेवा प्रदान की गयी है.
- प्रतिवर्ती नीलामी का सेवा प्रदाता या उसकी कोई सहयोगी संस्था स्वयं बैंक द्वारा की जा रही उस प्रतिवर्ती नीलामी प्रक्रिया में भाग लेने वाला वेंडर नहीं होना चाहिए.
- सेवा प्रदाता बैंक के साथ एक करार करेगा, जिसमें उसे प्राप्त अधिकार एवं दायित्वों का स्पष्ट उल्लेख होगा और यह करार उस समय तक अवश्य वैध होना चाहिए, जब उसे किसी प्रतिवर्ती नीलामी प्रक्रिया का कार्य सौंपा जा रहा हो.
- बैंक सामान्यतः सेवा प्रदाताओं की एक सूची बना लेते हैं और अपनी सुविधा/पसंद के आधार पर उनसे प्रतिवर्ती नीलामी प्रक्रिया संपादित कराते हैं.

प्रतिवर्ती नीलामी पर व्यय

प्रतिवर्ती नीलामी पर किया जाने वाला व्यय बैंक द्वारा वहन किया जाएगा. यह स्पष्ट है कि प्रतिवर्ती नीलामी में निहित लागत अधिक नहीं होती है और इससे होने वाले लाभ को देखते हुए यह तर्कसंगत भी है.

प्रतिवर्ती नीलामी की प्रक्रिया

जिन मामलों में बैंक प्रतिवर्ती नीलामी की प्रक्रिया अपनाना चाहता है, उनमें प्रतिवर्ती नीलामी प्रक्रिया अपनाने के बैंक के इरादे का उल्लेख आरएफपी दस्तावेज में किया होता है. प्रतिवर्ती नीलामी के कारोबारी नियम, जिनमें बैंक एवं भाग लेने वाले वेंडरों के अधिकारों एवं दायित्वों का उल्लेख होता है, को बैंक की वेबसाइट पर स्थायी रूप से उपलब्ध कराया जाता है. इसे किसी भी संभावित वेंडर को मांग किए जाने पर उपलब्ध कराया जाएगा. नियमों की हार्ड प्रति उपलब्ध तभी कराई जाए, जब वेंडर से लिखित आवेदन प्राप्त हो. हार्ड प्रति बैंक के प्राधिकृत प्राधिकारी द्वारा हस्ताक्षरित अग्रेषण पत्र के माध्यम से ही सौंपी जाए.

प्रत्येक आरएफपी दस्तावेज में 'वेबसाइट पर डिस्प्ले' का संदर्भ होगा और कारोबारी नियम मांग करने पर उपलब्ध कराए जाएगें, जैसा कि ऊपर वर्णित किया गया है. आरएफपी दस्तावेजों में बैंक द्वारा अपनाए जा रहे विकल्पों का निम्नानुसार स्पष्ट उल्लेख भी किया जाएगाः

- विभिन्न मदों एवं सेवाओं के लिए एक संयुक्त प्रोक्योरमेंट की नीलामी प्रक्रिया के मामलों में बैंक द्वारा वहन की जाने वाली संपूर्ण लागत (टीसीओ) का उल्लेख और
- आरएफपी में शामिल प्रोक्योरमेंट की प्रत्येक मदों के लिए एक से अधिक प्रतिवर्ती नीलामी का प्रावधान.

कारोबारी नियम में परिवर्तन

यदि अनुभवों के आधार पर कारोबारी नियमों में कोई परिवर्तन करना आवश्यक समझा जाए तो इसे महा प्रबंधकों की एक समिति की सहमति से ही किया जा सकता है, जिसमें निम्नलिखित शामिल होंगे (1) महा प्रबंधक (आईटी) (2) महा प्रबंधक (सहायक सेवाएं) और (3) महा प्रबंधक (लेखापरीक्षा एवं निरीक्षण). किसी महा प्रबंधक की अनुपस्थिति में उनके विभाग के उप विभाग प्रमुख बैठक में उपस्थित रहेंगे. समिति कार्यसूची में वर्णित मदों पर चर्चा के उपरांत निर्णय लेगी. समिति बैठक के 3 कार्यदिवसों के अंदर प्रबंध निदेशक एवं मुख्य कार्यपालक अधिकारी और कार्यपालक निदेशक को बैठक के कार्यवृत्त प्रस्तुत करेगी.

आरंभिक मूल्य

प्रत्येक प्रतिवर्ती नीलामी प्रक्रिया बैंक द्वारा 'आरंभिक मूल्य' को इलेक्ट्रानिक मोड में भर देने के बाद आरंभ होगी. आरंभिक मूल्य का निर्धारण पूर्व अनुभवों, उद्योग से प्राप्त सूचनाओं एवं जानकारियों आदि के आधार पर किया जाता है.

आरएफपी दस्तावेज में उचित समय पर नीलामी में भाग लेने वाले वेंडरों से विशेष तौर पर सांकेतिक प्राइज़ बैंड का पता लगाया जा सकता है.

'आरंभिक मूल्य' हमेशा बैंक को होने वाली स्वामित्व की कुल लागत के आधार पर तय होगा और इसमें चुंगी, प्रवेश शुल्क नहीं शामिल होंगे, जबकि स्थापना, कमिशनिंग प्रभार/व्यय, संबंधित साइट तक का विज़िट व्यय, ट्रांसपोर्टेशन व्यय सहित वारंटी अवधि के दौरान समग्र रखरखाव प्रभार, ट्रांज़िट से स्थापना अवधि तक का बीमा प्रभार आदि सहित सभी प्रकार के कर जैसे, बिक्री कर, वैट, सेवा कर इत्यादि शामिल होंगे. तथापि, चुंगी, प्रवेश शुल्क आदि से संबंधित दंड कभी भी बैंक द्वारा भुगतान नहीं किया जाए.

प्रतिवर्ती नीलामी में आरएफपी के नियम एवं शर्तें

बैंक को प्रतिवर्ती नीलामी के माध्यम से एल-1 वेंडर चुनने का अपना इरादा उन सभी मामलों में आरएफपी दस्तावेज में वर्णित करना चाहिए, जिसमें मूल्य का निर्धारण प्रतिवर्ती नीलामी के द्वारा किया जाना प्रस्तावित है. आरएफपी के प्रत्युत्तर के रुप में

प्रत्येक वेंडर को एक विशेष वचनपत्र प्रस्तुत करना होगा कि उसने सभी नियमों एवं शर्तों को पढ़ एवं समझ लिया है और वह प्रतिवर्ती नीलामी के दौरान लागू होने वाले सभी नियमों एवं शर्तों का पालन करने के लिए तैयार है. वचनपत्र का प्रारूप बैंक द्वारा उपलब्ध कराया जाएगा और यह बैंक की वेबसाइट पर भी उपलब्ध रहेगा. आरएफपी के प्रत्युत्तर में प्रत्येक प्राप्त प्रस्ताव में दो प्राधिकृत प्रतिनिधियों के नाम का प्राधिकार पत्र होना चाहिए, जिनको नीलामी प्रक्रिया में भाग लेने की अनुमति प्रदान की जाएगी और जिन्हें बैंक/सेवा प्रदाता द्वारा यूज़र आईडी एवं पिन प्रदान किया जाएगा. यदि कोई वेंडर ऐसा वचन पत्र देने का इच्छुक नहीं है, तो उसको प्रोक्योरमेंट प्रक्रिया में शामिल होने से वंचित कर दिया जाएगा.

प्रतिवर्ती नीलामी में भाग लेने वाले वेंडरों को उसी सक्षम प्राधिकारी द्वारा विधिवत हस्ताक्षरित निम्नलिखित दस्तावेज प्रस्तुत करने होंगे, जिसने आरएफपी के प्रत्युत्तर में प्रस्तुत प्रस्ताव पर हस्ताक्षर किए थे.

प्रतिवर्ती नीलामी प्रक्रिया अन्य अनुपालनों का प्रतिस्थापन नहीं है

प्रतिवर्ती नीलामी प्रक्रिया तकनीकी मूल्यांकन में सक्षम पाए गए वेंडरों में से एल-1 वेंडर को चुनने की प्रक्रिया मात्र है और इसलिए, इसके द्वारा प्रोक्योरमेंट नीति के किसी अन्य संबद्ध प्रावधानों को अभिभावी नहीं बनाया जा सकता. प्रस्तावित पूंजीगत या आयगत व्यय, जैसा भी मामला हो, के बारे में प्रत्यायोजित प्राधिकारों के अनुसार सक्षम प्राधिकारी का अनुमोदन लिया जाना आवश्यक होगा.

पुनर्निविदा

ऐसी परिस्थितियों में, जब बैंक प्रतिवर्ती नीलामी के माध्यम से टेंडर प्रक्रिया करता है और केवल एक ही वेंडर तकनीकी रूप से सफल पाया जाता है, तब यह स्पष्ट है कि प्रतिवर्ती नीलामी नहीं की जा सकती. ऐसी स्थिति में, बैंक टेंडर प्रक्रिया को रद्द करेगा और इसका टू-पार्ट बिड तरीके से दोनों तकनीकी एवं कामर्शियल बिड बिना प्रतिवर्ती नीलामी के एक साथ पुनः आमंत्रित किया जाएगा.

पुनर्नीलामी

बैंक निम्नलिखित परिस्थितियों में पुनर्नीलामी प्रक्रिया के विकल्प पर विचार कर सकता हैः

- प्रतिवर्ती नीलामी के दौरान, यदि लॉगिन किए गए वेंडरों द्वारा कोई बिड न की गयी हो या केवल एक वेंडर द्वारा ही बिड की गयी हो, तो बैंक सभी पात्र वेंडरों से केवल

मुहरबंद लिफाफों में नवीन इंडिकेटिव मूल्य प्राप्त कर पुनर्नीलामी के लिए नया आरंभिक मूल्य निर्धारित कर पुनर्नीलामी करा सकता है.

- यदि प्रतिवर्ती नीलामी का आरंभिक मूल्य बैंक द्वारा तय किया जाता है और प्रतिवर्ती नीलामी में कोई बिड नहीं है या केवल एक बिड है, तो बैंक आरंभिक मूल्य में संशोधन कर पुनर्नीलामी का निर्णय ले सकता है.
- प्रतिवर्ती नीलामी तभी वैध मानी जाएगी, जब दो या दो से अधिक वेंडर प्रतिवर्ती नीलामी प्रक्रिया में शामिल हों.
- किसी निविदा की पुनर्नीलामी के असफल हो जाने पर, बैंक खुली बिड आमंत्रित करना सुनिश्चित करेगा, जिससे नीलामी प्रक्रिया में शामिल वेंडरों द्वारा आपसी तालमेल से या तो बिड में भाग न लेकर या केवल एक बिडर द्वारा बोली लगाकर बैंक के आरंभिक मूल्य को असफल बनाने की साजिश रचने से रोका जा सके.
- उपरोक्त सभी परिस्थितियों में, विभाग का प्रमुख कार्यकारी अधिकारी पुनर्नीलामी कराने का निर्णय ले सकता है.

प्रतिवर्ती नीलामी में शिकायतों का निदान

प्रतिवर्ती नीलामी के दौरान या उससे संबंधित कोई भी वेंडर की शिकायत लिखित रूप में बैंक के मुख्य अनुपालन अधिकारी को भेजी जाएगी. मुख्य अनुपालन अधिकारी तुरंत उस शिकायत को एक समिति के समक्ष प्रस्तुत करेगा, जिसमें निम्नलिखित शामिल होंगे : (1) मुख्य अनुपालन अधिकारी (2) महा प्रबंधक (केन्द्रीय लेखापरीक्षा एवं निरीक्षण विभाग एवं (3) महा प्रबंधक (प्रभारी, केन्द्रीय विधि विभाग). समिति का निर्णय वेंडर को सूचित कर दिया जाएगा और यदि कोई सुधारात्मक कार्रवाई अपेक्षित होगी, तो उसे संबंधित विभाग द्वारा पूरा किया जाएगा.

नीतियों को लागू करने में संदिग्धता के कारण विवाद

यदि प्रतिवर्ती नीलामी को लागू करने में संदेह होने से संबंधित कोई विवाद उत्पन्न होता है, तो उस मामले का निपटान भी एक समिति के द्वारा किया जाएगा, जिसमें निम्नलिखित शामिल होंगे : (1) मुख्य अनुपालन अधिकारी (2) महा प्रबंधक (केन्द्रीय लेखापरीक्षा एवं निरीक्षण विभाग एवं (3) महा प्रबंधक (प्रभारी, केन्द्रीय विधि विभाग).

प्रयोज्यता एवं समीक्षा

यह नीति उन प्रोक्योरमेंट पर लागू होगी, जिनमें आरएफपी में विशेषतः प्रतिवर्ती नीलामी प्रक्रिया अपनाने का प्रस्ताव हो और सामान्यतः उन प्रोक्योरमेंट में भी लागू होगी,

जिनमें स्वामित्व की कुल लागत ₹ 25.00 लाख से अधिक हो. इसके अलावा, नीति में वर्णित दिशानिर्देश विभिन्न प्रोक्योरमेंट नीतियों के अनुपूरक होंगे न कि उनके प्रतिस्थापक. यह नीति परामशर्दाताओं/सेवा प्रदाताओं की नियुक्ति में लागू नहीं होगी.

प्रतिवर्ती नीलामी का निर्णय लेने हेतु प्रत्यायोजित प्राधिकार

विभागों में पदस्थ महा प्रबंधक/क्षेत्रीय प्रमुख/स्टाफ कालेज सहित अन्य प्रशासनिक कार्यालयों के प्रमुख यह निर्णय लेने के लिए सक्षम प्राधिकारी होंगे कि किन मामलों में प्रतिवर्ती नीलामी प्रक्रिया अपनायी जाए.

बैंक अधिकारी - क्या करें

- नीलामी की तारीख से वेंडरों को पर्याप्त समय पहले अवगत कराया जाना चाहिए.
- सूचीबद्ध वेंडरों को प्रतिवर्ती नीलामी के आरंभ से पहले प्रशिक्षण दिया जाना चाहिए.
- आरंभिक नीलामी मूल्य एवं घटते हुए नीलामी मूल्य की जानकारी उस एजेंसी को प्रदान की जाएगी, जो प्रतिवर्ती नीलामी प्रक्रिया संपादित करा रही हो.
- बैंक अधिकारियों के पास वैध डिजिटल प्रमाणपत्र होना चाहिए, जिससे वे प्रतिवर्ती नीलामी की पूरी प्रक्रिया पर नज़र रख सकें.
- बैंक अधिकारियों द्वारा लगातार प्रतिवर्ती नीलामी प्रक्रिया का अनुश्रवण किया जाना चाहिए.
- प्रतिवर्ती नीलामी प्रक्रिया आरंभ होने से पूर्व सूचीबद्ध किए गए वेंडरों से प्राधिकार पत्र लिया जाना चाहिए.
- प्रतिवर्ती नीलामी प्रक्रिया की समाप्ति पर एल-1 वेंडर से न्यूनतम मूल्य राशि का पता कर लेना चाहिए.

बैंक अधिकारी - क्या न करें

- प्रतिवर्ती नीलामी की प्रक्रिया के आरंभ से पहले नीलामी में भाग लेने वाले वेंडर्स को नीलामी की आरंभिक बोली राशि से न अवगत कराया जाए.
- प्रतिवर्ती नीलामी प्रक्रिया के दौरान, बोली राशि एवं प्रत्येक वेंडरों की रैंकिंग उनके वास्तविक नाम से न दिखाकर काल्पनिक नाम से दिखायी जानी चाहिए.

स्वामित्व की कुल लागत (टीसीओ)

स्वामित्व की कुल लागत (टीसीओ) से आशय बैंक द्वारा वस्तु के स्वामित्व के अंतरण अथवा सेवा हेतु अदा की जाने वाली कुल राशि से है, जिसमें प्रायः निम्नलिखित शामिल होंते हैं :

उपस्कर/उत्पाद या सेवाओं की लागत.

- ओएस/डाटा बेस/एप्लीकेशन लाइसेंस सहित कुल लाइसेंस फीस (कार्पोरेट या यूज़र विशेष, जैसा भी आरएफपी में वर्णित हो).
- सभी वर्तमान कर, शुल्क एवं प्रभार
- प्रतिस्थापन एवं कमिशनिंग प्रभार, यदि कोई हो.
- मूल्य में सभी घटकों को शामिल करते हुए उपस्करों की समग्र ऑनसाइट वारंटी/ रखरखाव, सेवाएं और संबंधित कार्यालयों का दौरा, जैसा भी आरएपी में वर्णित हो, शामिल होंगे.
- आरएफपी में वर्णित अवधि के लिए वार्षिक रखरखाव प्रभार.
- प्रत्येक साइट तक का वाहन एवं अग्रेषण प्रभार.
- उत्पाद/सेवा/उपस्कर के लिए प्रशिक्षण की लागत, जैसी भी आरएफपी में वर्णित हो.
- लागू अवधि के लिए सेवा स्तरीय समझौता (एसएलए) लागत, जैसी कि आरएफपी में वर्णित हो.
- आरएफपी में बताए अनुसार सुविधा प्रबंधन/मूलभूत सुविधाओं की लागत.
- मार्गस्थ अवधि से लेकर स्थापना तक का उपस्करों का बीमा कवर.

टीसीओ की गणना 'बॉय बैक' में वर्णित राशि, यदि कोई हो, को घटाकर की जाएगी.

तथापि, टीसीओ में चुंगी एवं प्रवेश शुल्क शामिल नहीं होगा. इनकी वास्तविक राशि का भुगतान प्राप्त रसीद के अनुसार किया जाएगा. इसके अलावा, चुगी एवं प्रवेश शुल्क के संबंध में कोई भी दंड राशि का भुगतान बैंक द्वारा नहीं किया जाएगा और वेंडर को ही ऐसे सभी व्यय वहन करने होंगे.

प्रतिवर्ती नीलामी की तारीख/समय

प्रतिवर्ती नीलामी के आरंभ की तारीख और समय एवं 'प्रतिवर्ती नीलामी की अवधि' की सूचना नीलामी की तारीख से कम से कम 7 दिन पहले सूचित कर दी जाएगी. यदि किन्हीं अपरिहार्य कारणों से नीलामी को स्थगित करना पड़े, तो बैंक नीलामी की सूचना देने के बाद भी उसे स्थगित कर सकता है, लेकिन, बैंक को 'प्रतिवर्ती नीलामी' के स्थगन की सूचना नीलामी में भाग लेने वाले सभी वेंडरों को नीलामी आरंभ होने से पहले देनी होगी.

सेवा प्रदाता की भूमिका एवं जिम्मेदारियां

- बैंक द्वारा सेवा प्रदाता के माध्यम से कराई गई प्रत्येक प्रतिवर्ती नीलामी के लिए बैंक एक अलग करार करेगा, जिसमें प्रतिवर्ती नीलामी के लिए वेब पोर्टल उपलब्ध कराने वाले सेवा प्रदाता की भूमिका एवं जिम्मेदारियों का स्पष्ट उल्लेख होगा.
- समुचित बाध्यताएं एवं अधिकारों के लिए सेवा प्रदाता भी प्रत्येक वेंडर के साथ एक करार करेगा, जिसके लिए प्रारुप का निर्धारण स्वयं सेवा प्रदाता करेगा. वेंडर एवं सेवा प्रदाता के बीच होने वाले ऐसे करार के बारे में किसी समस्या का निदान बैंक द्वारा किया जाएगा.
- जबकि बैंक और सेवा प्रदाता के बीच किया गया सेवा स्तरीय समझौता प्रतिवर्ती नीलामी को सुगमतापूर्वक और सही तरीके से निष्पादित कराने के लिए की गयी एक व्यवस्था है, फिर भी, बैंक प्रतिवर्ती नीलामी के पारदर्शितापूर्ण तरीके से निष्पादन के लिए वेंडर्स के प्रति सीधे जिम्मेदार है.
- प्रत्येक प्रतिवर्ती नीलामी के उपरांत सेवा प्रदाता प्रतिवर्ती नीलामी का पूरा विवरण एवं रिपोर्ट बैंक को प्रस्तुत करेगा.
- सेवा प्रदाता प्रतिवर्ती नीलामी से संबंधित सभी जानकारी को अपने पास कम से कम अगले 3 वर्षों तक सुरक्षित रखेगा.

नीलामी प्रक्रिया

- सेवा प्रदाता/नीलामकर्ता सभी तकनीकी रुप से पात्र बोली लगाने वालों को समुचित प्रशिक्षण प्रदान करने के लिए जिम्मेदार हैं. प्रत्येक वेंडर/बोली लगाने वाला प्रशिक्षण में अपनी लागत पर भाग लेगा.
- जब भी आवश्यक समझा जाए और बोली लगाने वालों द्वारा कहा जाए या नीलामकर्ता या बैंक द्वारा निर्णय लिया जाए, सभी संबंधित के हित को ध्यान में रखते हुए मॉक नीलामी कराई जा सकती है.

- बोली लगाने वालों के प्राधिकृत प्रतिनिधि, जिनके नाम वेंडर द्वारा प्राधिकार पत्र में दिए गए हैं, को सेवा प्रदाता/नीलामकर्ता द्वारा विशिष्ट यूज़र नाम एवं पासवर्ड प्रदान किया जाएगा. आरंभिक पासवर्ड प्राप्त होने पर प्रत्येक बोली लगाने वाला रजिस्ट्रेशन पेज पर जाकर अपना पासवर्ड और सूचनाएं बदल देगा. बोली लगाने वालों को दी गई लॉगिन आईडी से की गई सभी बोली स्वतः ही उसी वेंडर/बोली लगाने वाले की मानी जाएगी, जिसे सेवा प्रदाता/नीलामकर्ता द्वारा लॉगिन आईडी एवं पासवर्ड दिया गया था. वेंडर/बोली लगाने वाले के द्वारा पंजीकृत लॉगिन/पासवर्ड से एक बार लगाई गई बोली को निरस्त नहीं किया जा सकेगा. दूसरे शब्दों में, बोली लगाने वाला टीसीओ के बोली मूल्य पर आरएफपी के अनुसार 'प्रस्ताव' को बेचने के लिए बाध्य होगा.
- चूंकि बोली घटते हुए मूल्य पर लगाई जाएगी, इसलिए प्रत्येक अगली बोली पिछली बोली को स्वतः ही निरस्त कर देगी और समय एवं लॉगिन आईडी के अनुसार अंतिम बोली पिछली बोलियों पर अभिभावी होगी.
- बैंक प्रतिवर्ती नीलामी स्टैंडर्ड इंग्लिश रिवर्स आक्शन के अनुसार करेगा, जिसमें दो अलग-अलग वेंडरों द्वारा दो बोलियां एक ही राशि की नहीं हो सकतीं. दूसरे शब्दों में, बोलियों में कभी भी 'टाई' की स्थिति नहीं होगी.

प्राक्सी बोली

प्राक्सी बोली वह बोली होती है, जिसमें कोई वेंडर पूरी तरह से गोपनीय रहते हुए सिस्टम में सीधे न्यूनतम बोली राशि अंकित कर देता है. इससे वह बोली लगाने की प्रक्रिया से तब तक दूर रहता है, जब तक कि अन्य बोली लगाने वाले प्राक्सी बोली राशि से कम तक न पहुंच जाएं. जब प्राक्सी बोली राशि तक अन्य बोलियां पहुंच जाती हैं, तब वेंडर के पास विकल्प रहता है कि वह या तो प्राक्सी बोली राशि को संशोधित कर दे या फिर वह बोली लगाने की प्रक्रिया में भाग लेना आरंभ कर दे.

बोलियों में पारदर्शिता

सभी बोली लगाने वाले नीलामी समय के दौरान पोर्टल में लगाई गई न्यूनतम बोली को देख सकेंगे. बोली लगाने वाले न केवल न्यूनतम बोली राशि को देख सकेंगे बल्कि नीलामी अवधि के दौरान किसी भी समय उनके द्वारा लगाई गई पिछली बोली को भी देख सकेंगे.

नामों को छुपाना

प्रतिवर्ती नीलामी प्रक्रिया में वेंडरों/बोली लगाने वालों के नाम काल्पनिक होते हैं और उन्हें उपयुक्त डमी नाम प्रदान किए जाएगें. प्रतिवर्ती नीलामी की समाप्ति पर, सेवा प्रदाता/नीलामकर्ता नीलामी के सभी विवरण, बोली लगाने वालों के असली नाम के साथ ही साथ एल-1 बोली लगाने वाले के नाम सहित विस्तृत रिपोर्ट बैंक को प्रस्तुत करेगा.

बोली घटाने की राशि

- वेंडरों को नीलामी के दौरान केवल निर्धारित घटता हुआ मूल्य वर्णित करना होगा किसी अन्य गुणक में नहीं. नीलामी की घटती हुई दर रु.7500/- या प्रतिवर्ती नीलामी के आरंभिक मूल्य का 0.25%, जो भी अधिक हो, होगी.
- बोली की घटती हुई राशि रु. हजार के गुणक में होगी.
- वेंडरों की सुविधा के लिए, वेब पार्टल पर नीलामी का अगला घटता हुआ मूल्य दिखाई देगा. तथापि, वेंडरों के लिए यह अनिवार्य नहीं होगा कि वे अगले न्यूनतम मूल्य की ही बोली लगाएं. (अर्थात् वे अगली न्यूनतम बोली राशि से 2-3 कम स्तर पर भी बोली लगा सकते हैं.)

आदेशों को अलग-अलग करना

यदि किसी आरएफपी में आपूर्ति के स्रोत या सेवा की आपूर्ति पर किसी एक वेंडर की निर्भरता को कम करने के उद्देश्य से आदेश को एक से अधिक भागों में बांटने का विकल्प उपलब्ध है, तो बैंक आरएफपी में वर्णित किए अनुसार क्रमवार आदेश को कई भागों में बांट सकता है. आदेशों को अलग-अलग करते समय, बैंक को आरएफपी में अधिकतम संख्या एल-1, एल-2 आदि का उल्लेख करना होगा. यदि एल-2 वेंडर एल-1 द्वारा दी गयी राशि पर आपूर्ति के लिए तैयार नहीं है, तो बैंक एल-3, एल-4 आदि को निर्धारित संख्या तक आदेश को विभक्त करने के लिए बुला सकता है.

प्रतिवर्ती नीलामी की प्रक्रिया :

- प्रोक्योरमेंट प्रक्रिया में निहित समय को कम करने के क्रम में, बैंक एक ही प्रतिवर्ती नीलामी के माध्यम से पूरी प्रोक्योरमेंट प्रक्रिया को पूरा करने का हकदार होगा. इस उद्देश्य से, बैंक एल-1 बोली लगाने वाले को ठेका प्रदान कर सकता है या फिर इन परिस्थितियों में, आरएफपी में किए गए प्रावधानों के अनुसार एल-2, एल-3 बोली लगाने वालों को ठेका प्रदान किया जा सकता है.

- बैंक प्रतिवर्ती नीलामी प्रक्रिया के माध्यम से प्रोक्योरमेंट को रद्द भी कर सकता है, यदि उसके ध्यान में यह बात आती है कि प्रतिवर्ती नीलामी प्रक्रिया सही तरीके से नहीं सम्पन्न हो सकी है और/या यह बैंक के हित में नहीं है.
- सफल वेंडर नीलामी के उपरांत अंतिम बोली मूल्य पर माल की आपूर्ति करने के लिए बाध्य होगा.

प्रतिवर्ती नीलामी का व्यय

प्रतिवर्ती नीलामी पर किया जाने वाला सभी व्यय बैंक द्वारा वहन किया जाएगा. तथापि, वेंडर प्रशिक्षण अथवा मॉक नीलामी में अपनी लागत पर शामिल होगें.

व्यावसायिक नियमों में बदलाव

- यदि पूर्व अनुभवों के आधार पर कारोबारी नियमों में कोई परिवर्तन करना आवश्यक हो जाता है, तो ऐसा केवल बैंक के वरिष्ठ/उच्च कार्यपालकों की एक समिति के द्वारा ही किया जा सकता है और इसे तुरंत वेबसाइट पर अपलोड किया जाएगा.
- यदि कोई प्रतिवर्ती नीलामी प्रक्रिया आरंभ हो चुकी है और कारोबारी नियमों में कोई परिवर्तन किया जाता है, तो इसकी सूचना तुरंत सभी वेंडरों/बोली लगाने वालों को दी जाएगी और बैंक द्वारा उस पर उनके विचार/उनकी सहमति लिखित रुप में उनसे प्राप्त की जाएगी.

बोली लगाने वाले/वेंडर क्या न करें

- कोई भी वेंडर स्वयं या उसका कोई प्रतिनिधि प्रत्यक्ष या अप्रत्यक्ष रुप से अन्य बोली लगाने वालों के साथ मूल्यों में घट-बढ़ करने जैसी गतिविधियों में शामिल नहीं होगा. यदि ऐसी कोई घटना बैंक के ध्यान में आती है, तो बैंक वेंडर/बोली लगाने वाले को प्रतिवर्ती नीलामी प्रक्रिया से निष्कासित कर देगा.
- बोली लगाने वाला बैंक की प्रतिवर्ती नीलामी प्रक्रिया में लगाई गई बोली या अन्य उससे जुड़ी कोई जानकारी बैंक की लिखित एवं विशिष्ट अनुमति प्राप्त किए बगैर किसी अन्य तीसरे पक्षकार से साझा नहीं करेगा.
- न तो बैंक और न ही सेवा प्रदाता/नीलामकर्ता पावर सप्लाई के फेल होने, सिस्टम समस्या, सिस्टम का प्रयोग न कर पाने, इलेक्ट्रानिक डाटा के नष्ट हो जाने, बिजली आपूर्ति में विघ्न, यूपीएस सप्लाई फेल होने आदि जैसी आकस्मिक

घटनाओं के लिए जिम्मेदार नहीं ठहराया जा सकेगा. (तथापि, बैंक पूरी प्रक्रिया में पारदर्शिता बनाए रखने के लिए इस तरह के किसी व्यवधान, समस्या आदि पर खुले दिमाग से विचार करते हुए नीलामी को रोकने या बढ़ाने पर विचार कर सकता है.)

शिकायतों का निदान

प्रतिवर्ती नीलामी प्रक्रिया में भाग लेने वाला कोई वेंडर/बोली लगाने वाले को यदि कोई शिकायत है, तो वह बैंक के मुख्य अनुपालन अधिकारी को अपनी लिखित शिकायत नीलामी समाप्ति के 48 घंटों के भीतर प्रस्तुत कर सकता है. मुख्य अनुपालन अधिकारी बैंक के मुख्य विधि अधिकारी एवं लेखापरीक्षा विभाग के प्रमुख के साथ शिकायतकर्ता बोली लगाने वाले/वेंडर से व्यक्तिगत मुलाकात कर उसकी शिकायत को सुनेगा और शिकायत के संबंध में समुचित निर्णय लेगा. शिकायत निवारण समिति द्वारा लिया गया निर्णय बैंक के साथ ही साथ प्रतिवर्ती नीलामी में शामिल सभी वेंडरों पर बाध्यकारी होगा.

कमियां एवं भूल सुधार

प्रतिवर्ती नीलामी से संबंधित ऐसी कोई प्रमुख बात या क्षेत्र, जिसका उल्लेख कारोबारी नियमों में नहीं किया गया है, से संबंधित समस्याओं के निदान में बैंक का निर्णय अंतिम एवं सभी संबंधित पर बाध्यकारी होगा.

ब्लॉकचेन

शालिनी कुमारी
सहायक प्रबंधक (आईटी)
क्षे. का. समस्तीपुर

दयानंद चौधरी
सहायक महाप्रबंधक
क्षे. का. विशाखापट्टनम

ब्लॉकचेन तकनीक की जानकारी और अध्ययन बहुत ही रोचक एवं अत्यंत उपयोगी है. भविष्य में यह तकनीक विभिन्न क्षेत्रों में अपनी विश्वसनीयता, स्वीकार्यता और बहुआयामी उपयोग के कारण एक नयी क्रांति लाने वाली है. आज आम लोगों के लिए भले ही यह उपेक्षित विषय हो सकता है लेकिन आनेवाले समय में इसका सबसे ज्यादा असर आम लोगों पर ही पड़ेगा. यही वजह है कि ब्लॉकचैन के विषय में चर्चा करना आवश्यक हो जाता है. ब्लॉकचेन लगातार बढ़ने वाले रिकार्डों की सूची को कहते हैं. इन रिकार्डों को ब्लॉक कहा जाता है, जो क्रिप्टोग्राफी का उपयोग कर लिंक द्वारा सुरक्षित की गई होती हैं.

ब्लॉकचैन एक ऐसी तकनीक है, जिसे वित्तीय संव्यवहार रिकॉर्ड करने के लिए प्रोग्राम किया गया है. यह एक डिजिटल प्रणाली है, जिसमें एक इंटरनेट तकनीक की अंतर्निहित मजबूती होती है और जो अपने नेटवर्क पर समान जानकारी के ब्लॉक को संग्रहित कर सकता है.

ब्लॉकचैन डिजिटल जानकारी (डाटाबेस) को वितरित करने की क्षमता रखता है अर्थात यह एक डिस्ट्रीब्यूटेड नेटवर्क की तरह कार्य करता है. डाटाबेस के सभी रिकॉर्ड एक कंप्यूटर में स्टोर नहीं होते बल्कि हजारों या लाखों कम्प्युटरों में वितरित होते हैं.

ब्लॉकचैन का हर एक कंप्यूटर सभी रिकॉर्ड के पूरे इतिहास का वर्णन कर सकता है. यह डाटाबेस एंक्रिप्टेड है और गोपनीय तरीके से दर्ज़ किया गया होता है.

ब्लॉकचैन फ़ाल्ट टोलेरेंट भी है, यानि इस प्रणाली में यदि एक कंप्यूटर खराब भी हो जाता है तो यह सिस्टम काम करता रहता है. इसमें कोई भी नए समझौते या रिकॉर्ड को दर्ज़ करना होता है तो इसके लिए कई साझेदारों की स्वीकृति की जरूरत पड़ती है.

ऐसा कहा जाता है कि ब्लॉकचेन का आविष्कार सातोशी नमाकोटो ने वर्ष 2008 में क्रिप्टोकरेंसी बिटक्वॉइन हेतु परिचालन लेजर के रखरखाव के लिए किया था. यह तकनीकी बिटक्वॉइन के प्रचलन के साथ वर्ष 2009 से चर्चा में आयी और आज हर जगह आपको बिटक्वॉइन और ब्लॉक चेन पर लोग बातें करते मिलेंगे. इस लेख को पढ़ने के बाद बिटक्वॉइन की परिधि के परे भी आप इस तकनीक की गहराई तथा भविष्य में इसके उपयोग को बारीकी से समझ पायेंगे.

1. **ब्लॉकचेन तकनीक (बैंकिंग शब्दों में) क्या है?**

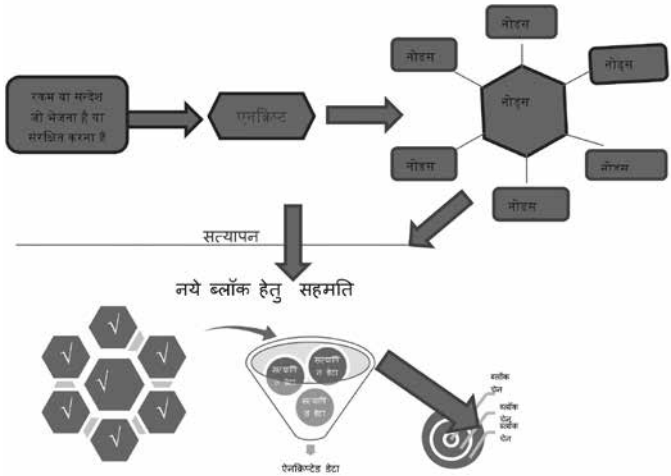
   ब्लॉकचेन एक डिजिटल लेजर है, जहां खाते में डेबिट(नामे) और क्रेडिट(जमा) संव्यवहार की प्रविष्टि होती है. हम कह सकते हैं कि एक ब्लॉकचेन डिजिटलाइज्ड डिसेंट्रलाइज्ड पब्लिक लेजर होता है.

   ब्लॉकचेन तकनीक और बिटक्वॉइन का आविर्भाव आम लोगों के बीच लगभग साथ-साथ ही हुआ. जैसे-जैसे बिटक्वॉइन से लेन-देन और व्यापार बढ़ा, इसकी चमक और लोगों की इनमें अभिरूचि भी बढ़ती गयी, परंतु दोनों पूरी तरह से अलग हैं. बिटक्वॉइन जहां एक क्रिप्टोमुद्रा है, जिसे देख तो नहीं सकते, पर किसी भी देश की मुद्रा से यह मूल्यवान है. यह जिसकी डिजिटल तिजोरी में विद्यमान रहती है, वही इसका उपयोग कर सकता है अर्थात खुले बाज़ार में इसका मूल्य कुछ भी नहीं. ब्लॉकचेन वह तिजोरी/लेजर है, जहां बिटक्वॉइन अपनी चमक के साथ अमूर्त रूप में विद्यमान रहता है. ना तो इसे रखने का झंझट और ना ही इसके वहन करने की चिंता अर्थात ब्लॉकचेन एक तकनीक कोष है, जहां ना सिर्फ डिजिटल करेंसी बल्कि किसी भी रिकार्ड को डिजिटल बनाकर उसे सुरक्षित रखा जा सकता है.

2. **ब्लॉक चेन की क्रियाविधि :** यह पूरी तरह विकेन्द्रित प्रणाली है तथा इसके संचालन के लिये कोई केंद्रित प्राधिकरण नहीं है. यह कार्य विशेष रूप से निर्मित उच्च शक्ति वाले कम्प्यूटरों के माध्यम से किया जाता है, जिनमें जटिल गणितीय प्रश्नों को हल करने की विधा होती है; जिससे कोडिंग/डिकोडिंग के जरिये कार्य

आगे बढ़ता जाता है. इस प्रकार के कम्प्यूटर नोड्स को माइंस कहा जाता है. इस पर काम करने वाला माइनर कहलाता है. कोई भी संदेश सत्यापन के पश्चात टेक्स्ट क़े रूप में न रहकर गणितीय भाषा में परिवर्तित हो जाता है तथा हजारों नोड्स में संरक्षित होता है. जब तक प्रत्येक नोड लेनदेन को सत्यापित नहीं करता है, लेनदेन पूरा नहीं हो सकता है. इस कारण इसे हैक करना जटिल कार्य है. प्रत्येक लेनदेन गोपनीय चाभी द्वारा गणितीय पहेली के रूप में संरक्षित होता है. लेनदेन के स्रोत और सत्यता की वेटिंग के पश्चात ही उनका ब्लॉक बनता है. इस प्रकार अनगिनत लेनदेन के ब्लॉक बनते जाते हैं और ये ब्लॉक चेन में जुड़ते जाते हैं. इस जटिलता के कारण इसकी गोपनीयता बनी रहती है और पारदर्शी होते हुए भी इस पर केंद्रीकृत नियंत्रण नहीं होता है. डाटा अभीष्ट व्यक्ति के डिजिटल बटुए में डिजिटल गणितीय चाभी से बंद रहता है. इस प्रकार जटिल ब्लॉक चेन में आपके ब्लॉक को कोई ढूंढ ही नहीं सकता है और बिना कठिन जांच-परख के इसमें कोई भी लेनदेन संभव नहीं है. यह प्रक्रिया या इस संचार माध्यम को क्रिप्टोग्राफी कहते हैं, जिसमें भेजा गया सन्देश पहले एनक्रिप्ट होता है अर्थात इस प्रकार कोडिंग होती है कि मध्य में कोई भी इसे न तो जान सकता है न ही हाइजैक कर सकता है. बस जहां इसे भेजा गया है, वहीं यह पुनः डीक्रिप्ट होगा और सत्यापन के पश्चात ही ब्लॉक चेन में संरक्षित होता है.

इस पूरी प्रक्रिया को नीचे दिए गए प्रवाह चार्ट के जरिए भी बेहतर तरीके से समझा जा सकता है.



3. **ब्लॉक चेन की मुख्य विशेषताएं :-**

- यह एक प्रकार की डिजिटल डायरी है, जो समाहित लेन-देन को अभेद्य सुरक्षा में और पारदर्शी तरीके से संरक्षित रखती है.
- प्रत्येक लेन-देन के साथ उत्पन्न हैश इसकी महत्वपूर्ण कुंजी है.
- हैश अत्यंत संवेदनशील होता है और छोटे से छोटे परिवर्तन होने पर भी हमेशा नया हैश बन जाता है.
- ब्लॉक चेन उच्च शक्ति वाले अनेकों उन्नत तकनीक के कम्प्यूटर में सुरक्षित होते हैं.
- ब्लॉक चेन नोड्स में सतत अद्यतन होते रहते हैं.
- निर्मित डिज़ाइन के कारण यह किसी भी प्रकार के अवांछित हस्तक्षेप और डाटा के बदलाव को स्वीकार नहीं करता है, इसलिए इसे हाइजैक करना अत्यंत दुर्लभ है.

उपर्युक्त कार्यप्रणाली और विशेषताओं के कारण ब्लॉक चेन के उपयोग की परिसीमा और स्वीकार्यता विभिन्न क्षेत्रों में बढ़ती जा रही है.

4. **ब्लॉक चेन का बहुआयामी उपयोग :** ब्लॉक चेन तकनीक, डाटा की बारीकी से जाँच करने के पश्चात ही उसे संरक्षित और गोपनीय रखता है. साथ ही प्रत्येक बदलाव को सतत अद्यतन करता रहता है. इन विविधताओं, विशेषताओं और विश्वसनीयता के कारण इसके बहुआयामी उपयोग की संभावनाएं दिन प्रति दिन बढ़ती जा रही है.

- **पब्लिक रिकार्ड :** सरकारी एवं गैरसरकारी कंपनियों को विभिन्न दस्तावेज़ सुरक्षित एवं गोपनीय रखने होते हैं, जिन्हें आज डीमैट के रूप में रखा जाता है तथा ब्लॉकचेन में इसकी सत्यता की जाँच के पश्चात ही सुरक्षित घेरे में, विश्वसनीय और प्रामाणिक रूप में रखा जाता है. इनका उपयोग केवल प्राधिकृत संचालक ही कर सकता है. यदि कोई इसमें छेड़-छाड़ करने का प्रयास करता है तो वह भी रिकार्ड होता जाता है तथा श्रोत और प्रामाणिकता की तत्क्षण जाँच होती है, जो डीमैट में संभव नहीं है.
- **मानव- संसाधन :** मानव संसाधन विभाग अपने कार्मिकों का रिकार्ड इसमें रख सकते हैं. उनके बदलते प्रोफाइल और प्रोन्नति हेतु उनकी उपलब्धियों एवं कार्यप्रणाली पर नज़र रख सकते है. यदि ब्लॉक चेन के जरिए उनकी

गतिविधियों के कार्यकलाप को निरंतर संरक्षित किया जाता है तो उनका कार्य और सहज तथा पारदर्शी हो जाएगा. इसके साथ ही, कार्मिकों में कार्य करने का उत्साह जागृत होता है, क्योंकि उन्हें पता है कि उनके कार्यों की परख और अनुश्रवण सतत पारदर्शी तरीके से हो रही है. कार्मिकों का अपने कंपनी पर विश्वास बढ़ता है, जो किसी भी कंपनी के विकास का मूल आधार होता है.

- **बैंकिंग क्षेत्र में संभावनाएं :** बैंकिंग क्षेत्र का व्यापार मूलतः भुगतान एवं समाधान प्रणाली पर आधारित है. ब्लॉक चेन की लेज़र वितरण प्रणाली पारंपरिक व्यावसाय के भुगतान एवं समाधान को सुरक्षित और पारदर्शी तरीके से राष्ट्रीय- अंतर्राष्ट्रीय स्तर पर सुगमता पूर्वक कर सकती है. विगत वर्षों में बार्क्लेज, क्रेडिट स्विस्स, एच एस बी सी, कैनेडियन इम्पीरियल बैंक औफ कामर्स ने मिलकर एक "यूटिलिटी सेट्लमेंट मुद्रा" विकसित करने का विचार किया है. यह किसी भी देश की मुद्रा में, मूल्य अनुसार परिवर्तित की जा सकती है. अन्य बड़े विदेशी बैंकों ने भी इसमें शामिल होने के संकेत दिये हैं. (श्रोतः बिजिनेस लाइन/ इ टी समाचार पत्र में प्रकाशित लेख)

  निजी जिंदगी में निम्नलिखित क्षेत्रों में ब्लॉकचेन तकनीकी का उपयोग किया जा सकता हैः-

  1. सूचना प्रौद्योगिकी और डाटा प्रबंधन
  2. सरकार और संगठनात्मक प्रशासन
  3. शिक्षा
  4. गेमिंग प्रणाली
  5. शेयर बाज़ार और कमोडिटीस
  6. सामाजिक नेटवर्क
  7. डिजिटल पहचान और प्रमाणीकरण
  8. रियल एस्टेट
  9. सामुदायिक सेवा
  10. नेटवर्क इन्फ्रास्ट्रक्चर
  11. मीडिया और बाज़ार
  12. ई-वोटिंग, आदि

5. **ब्लॉकचेन कितना सुरक्षित है? :** जैसा कि हम सभी जानते हैं कि इंटरनेट में तो कोई भी चीज़ सुरक्षित नहीं है. वहीं अगर हम ब्लॉकचेन तकनीक की बात करें, तो दूसरी तकनीकों की तुलना में यह बहुत हद तक सुरक्षित है. ब्लॉकचैन में कोई भी लेनदेन करने के लिए पूरे नेटवर्क के सभी कंप्यूटर नोड्स को सहमत (एग्री) होना पड़ेगा, तभी जाकर लेनदेन होगा. इसे हैक (hack) करना बहुत ही मुश्किल है क्योंकि हैकर को डाटाबेस हैक करने के लिए एक साथ कई हजार कम्प्यूटरों को हैक करना पड़ेगा. यही कारण है कि ब्लॉकचेन तकनीक एक सुरक्षित और सरल तकनीक है.

6. **ब्लॉक चेन के गुण-अवगुण :** प्रत्येक नव विकसित तकनीक अपनी विशेषताओं के साथ कुछ जोखिम भी साथ लाता है. आइए ऊपर किए गये वर्णन के अनुसार ब्लॉक चेन के गुण-अवगुणों का विश्लेषण किया जाए.

गुणः

सबसे बड़ा गुण यह है कि यह केंद्रीकृत नहीं है और डाटा किसी एक नोड्स पर निर्भर नहीं रहता है. अतः कहीं एक-दो जगह बाधा होने पर कार्य अवरुद्ध नहीं होता और 24 घंटे निरंतर इसका निर्वाध उपयोग किया जा सकता है.

- डाटा को संरक्षित करने से पूर्व इसकी सत्यता और श्रोत को गहन छान-बीन की प्रक्रिया से गुज़रना होता है. अतः यह पूर्ण विश्वसनीय है.
- बहुस्तरीय डिजिटल संरक्षण के कारण डाटा में अनावश्यक हेरफेर दुःसाध्य है.
- बैंकिंग, व्यापार, मानव संसाधन आदि अनेक क्षेत्रों में विश्वसनीयता और पारदर्शिता के कारण इसका निर्बाध उपयोग किया जा सकता है.
- वित्तीय/राजनीतिक संकट की स्थिति में भी इस पर रोक लगाना मुश्किल है, अर्थात इन संकटों से यह अप्रभावित रहता है.
- यह बैंक, वकील, पेचीदे कानून तथा सरकार के नियंत्रण से मुक्त है.

अवगुण :

वैसे तो ब्लॉकचेन तकनीक के बहुत सारे लाभ हैं, फिर भी इसमें भी कुछ कमियां हैं, जिसके बारें में चर्चा करना आवश्यक है :-

1. **बहुत पावर की जरूरत :** ब्लॉकचेन के ऑपरेशन में बहुत ज्यादा कम्प्यूटिंग पावर की आवश्यकता होती है, जिसके परिणामस्वरूप इलेक्ट्रिसिटी की

खपत बहुत अधिक होती है. वहीं जहां विकसित देश के लिए ब्लॉकचेन का संचालन आसान होता है, वहीं विकासशील देश के लिए यह उनकी अर्थव्यवस्था को पंगु बनाने वाला साबित हो सकता है.

2. **प्राइवेट की (key) सिक्योरिटी :** इसकी 'प्राइवेट की' को हमेशा सिक्रेट रखना चाहिए क्योंकि तीसरी पार्टी को इसके विषय में जानकारी होने पर इसे हैक भी किया जा सकता है. इसके अलावा भी 'प्राइवेट की' को बैकअप करके और प्रोटेक्ट करना चाहिए, जिससे कि दुर्घटनागत हानि से बचा जा सके क्योंकि अगर यह एक बार खो जाए, तो इनमें निहित निधि या सूचना की रिकवरी नहीं की जा सकती और ये हमेशा के लिए खो जाएगीं.

3. **लेनदेन स्पीड :** लेनदेन स्पीड भी एक समस्या बन सकती है, क्योंकि सुरक्षा के लिए चेन में ब्लॉक को डिस्ट्रीब्यूटेड नेटवर्क से वेरिफ़ाई कराना बहुत ही जरूरी है और ऐसा करने में काफी समय लगता है.

   - केंद्रीकृत नहीं होने के कारण, किसी की जवाबदेही तय नहीं की जा सकती है.
   - यह कोई संस्था नहीं है, जिसके विरूद्ध शिकायत या कानूनी कार्रवाई की जा सके. केवल विश्वसनीयता पर आधारित है.
   - अत्यधिक महंगी होने के कारण छोटी-मोटी कंपनियों या व्यापारियों की पहुंच के परे है.
   - सामान्य लोगों को इसे समझने, विश्वास करने और उपयोग करने में अभी वक्त लगेगा.

1. ब्लॉकचेन के अनुप्रयोगों (Applications) का भविष्य निम्नलिखित क्षेत्र में है :

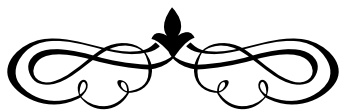
- स्मार्ट कांट्रैक्ट्स- कोई भी इंडस्ट्री हो, अगर वो बड़े कांट्रैक्ट्स पर निर्भर करती है जैसेः बीमा, वित्तीय संस्थान, रीयल इस्टेट, कन्स्ट्रक्शन, एंटरटेनमेंट और लॉ, ये सभी उद्योग इस तकनीक से लाभान्वित होंगे क्योंकि इस तकनीक की मदद से बिना किसी विवाद के आपके सारे कांट्रैक्ट्स को अद्यतन, प्रबंधन, ट्रैक और सुरक्षित किया जा सकता है. स्मार्ट कांट्रैक्ट्स में ये सारे एम्बेडेड (समाहित) होते हैं.
- सप्लाइ चैन प्रबंध - जब भी कोई वैल्यू बदलता है या कोई एसेट का स्टेटस बदलता है तब इन सभी प्रक्रिया को प्रबंध करने में ब्लॉकचेन एक बहुत ही बढ़िया विकल्प साबित हो सकता है.

- आस्ति(Asset)सुरक्षा - अगर आप प्रॉपर्टी के मालिक हो और आप अपने संपत्ति(Asset) की सुरक्षा चाहते हैं तब ब्लॉकचेन तकनीक आपकी रीयल-टाइम ऑनरशिप की एक विवादरहित सूची बनाकर आपकी मदद कर सकता है.
- भुगतान प्रक्रिया- ब्लॉकचेन की ये खासियत है कि यह किसी भी बड़ी कंपनी की भुगतान प्रक्रिया को आसानी से संभाल सकता है. यह बिचौलियों की जरूरत को पूरी तरह से खत्म कर सकता है जैसे कि हम प्रायः भुगतान प्रक्रिया में देखते हैं.

बहुत सारी कंपनियां यथा : कोकाकोला, फोर्ड, उबर ट्रैवल कम्पनी, कुछ बड़ी निजी अंतर्राष्ट्रीय बैंकिंग कंपनियों आदि ने आवश्यकताओं के अनुसार संभावनाओं को तलाश करना आरम्भ कर दिया है. यदि इन्हें सफलता मिलती है, तो भविष्य के कारोबार पर ब्लॉकचेन का ही राज होगा. "It's the first native digital medium for value, just as the internet was the first native digital medium for information." - Harvard Business Review.

यह सुरक्षित लेजर रखरखाव तकनीक की आधारशिला के लिये एक क्रांतिकारी बदलाव को स्थापित कर मील का पत्थर साबित हो सकती है. विभिन्न देश की सरकारों की इस पर पैनी नज़र है कि इसे कानूनी मान्यता दी जाए या नहीं. वक्त सबसे शक्तिशाली है. किस करवट लेगा, इसे वक्त के अलावा कोई नहीं जान सकता है; बस, अनुमान लगाया जा सकता है. आप, बस पढ़ते रहिए और ब्लॉकचेन तकनीक की जानकारी तथा इसके उपयोग से अपने को अद्यतन करते रहिए. भविष्य आपका भी उन्नतिशील हो सकता है बशर्ते कि आप वक़्त के दस्तक़ को समय पर पहचान लें और दरवाज़ा खोल कर समय के साथ चल दें.

आगे-आगे देखिए होता है क्या ----------



क्यू आर कोड

निधि सोनी
प्रबंधक (राभा)
क्षे. का. इंदौर

सीमा यादव
सहायक प्रबंधक
क्षे. का.वाराणसी

क्विक रेसपान्स कोड/त्वरित प्रतिक्रिया संकेत एक ऐसी तकनीक है, जिसका आविष्कार जापान में 1994 में, डेन्स वेव नामक, टोयोटा आटोमोबाइल कंपनी की सहायक कंपनी द्वारा, वाहनों के पुर्जों को ट्रैक करने हेतु किया गया था. इसकी जल्द पठनीयता एवं बड़ी भंडारण क्षमता के चलते हाल ही में यह मोटर वाहन उद्योगों से परे भी लोकप्रिय हो गया है. क्यू आर कोड एक मैट्रिक्स बार कोड है, जो कि मशीन द्वारा पढ़े जाने वाला ऑप्टिकल लेबल है. यह कोड जिस आइटम से जुड़ा होता है, उस आइटम से संबन्धित समस्त जानकारी, इसमें निहित रखी जाती है. इस प्रकार क्यू आर कोड को एक प्रकार का ट्रेड मार्क भी कहा जा सकता है.

क्यू आर कोड के माध्यम से हम किसी भी उत्पाद संबन्धित समस्त जानकारी को डिकोड कर सकते हैं. क्यू आर कोड में एक यू आर एल एम्बीडेड होता है. दूसरे शब्दों में, क्यू आर कोड इमेज बेस्ड हाइपर टेक्स्ट लिंक है, जिसका प्रयोग इंटरनेट के ऑफ लाइन मोड में भी किया जा सकता है. क्यू आर कोड में किसी वेब साइट के यू आर एल को एनकोड कर सकते हैं. जब क्यू आर कोड को स्कैन किया जाता है तब उत्पाद/आइटम से संबन्धित समस्त जानकारी हमें प्राप्त हो जाती है. जहां तक बार कोड का संबंध है, यह क्यू आर कोड से भिन्न है. यह एक मशीन पठनीय लेबल होता है, जिसमें वस्तु से जुड़ी हुई सीमित जानकारी स्टोर होती है.

क्यू आर कोड की विशेषताएं :

- बार कोड के मुकाबले क्यू आर कोड अधिक प्रभावी है. बार कोड केवल 1 डाइमेन्शनल होता है. अतः इसे एक खास एंगल पर ही स्कैन किया जा सकता है. जबकि क्यू आर कोड को 360 डिग्री पर स्कैन किया जा सकता है.
- बार कोड में केवल 20-25 केरेक्टर्स ही स्टोर हो सकते हैं, जबकि, क्यू आर कोड में 7,089 न्यूमेरिक केरेक्टर्स स्टोर हो सकते हैं.

- बार कोड लंबे होते हैं जबकि क्यू आर कोड, बार कोड की तुलना में कम जगह लेता है.
- बार कोड कुछ समय बाद एक्सपायर हो जाता है अथवा बार कोड पर किसी प्रकार का स्क्रेच आने पर वो स्कैन नहीं हो पाता, जबकि, क्यू आर कोड 30% तक खराब होने के बावजूद भी स्कैन हो जाता है.
- बार कोड केवल अल्फा न्यूमेरिक केरेक्टर को स्कैन कर सकता है, जबकि क्यू आर कोड, न्यूमेरिक, अल्फा न्यूमेरिक, बाइनेरी और कांजी केरेक्टर को एनकोड करने में सक्षम होता है.
- कोई भी व्यक्ति, जिसके पास एक स्मार्ट फोन है, मुफ्त में एक क्यू आर कोड रीडर अप्लीकेशन डाउनलोड कर सकता है. इससे आप अपने व्यवसाय से संबद्ध किसी भी व्यक्ति के बारे में अपने द्वारा जेनरेट किए गए क्यू आर कोड को स्कैन कर सकते हैं और विशेष सौदों, सर्वेक्षण या अन्य जानकारी तक पहुँच सकते हैं.
- क्यू आर कोड पाठक न केवल स्वतंत्र होते हैं बल्कि क्यू आर कोड़ जेनरेटर भी होते हैं. अपने कोड डाउनलोड करें और उन्हें अपने स्टोर में या बाहर उपयोग किए जाने वाले प्रिंट विज्ञापन, मेनू, पोस्टर, बिलबोर्ड या प्रिंट विज्ञापन के किसी अन्य रूप में प्रिंट करें.
- ऑनलाइन दुनिया में क्यू आर कोड की उपस्थिति काफी अनूठी है, इसलिए जब कोई ग्राहक किसी क्यू आर कोड को देखता है तो वह जानता है कि यह वास्तव में क्या है और इसके साथ क्या करना है. कोड के दूसरे छोर पर क्या है यह देखने के लिए यह एक त्वरित स्कैन है.
- क्यू आर कोड ग्राहक को मैन्युअल रूप से यूआरएल दर्ज़ करने के बजाय, अपने फोन के कैमरे के साथ 2D छवि स्कैन करके एक वेब पेज एड्रैस पर जाने की अनुमति देता है. परिणामी यू आर एल में आमतौर पर ट्रैकिंग फीचर्स शामिल होते हैं, जो ग्राहक द्वारा टाइप किए जाने पर अनावश्यक जानकारी भी प्रदर्शित कर देते हैं.

क्यू आर कोड की व्यापक उपयोगिता :

क्यू आर कोड एक महत्वपूर्ण विपणन उपकरण है. चूंकि क्यू आर कोडों को मार्केटिंग में पर्याप्त अवसर मिला, इसलिए वे लगभग किसी अभियान का एक अनिवार्य हिस्सा बन गए हैं. आधुनिक क्यू आर कोड जनरेटर द्वारा प्रदान की जाने वाली अतिरिक्त सुविधाएं कोड को विशेष रूप से संभावित ग्राहकों तक पहुँचने के लिए उपयुक्त बनाती

हैं. चूंकि क्यू आर कोड ऑनलाइन दुनिया में एक सीधा लिंक प्रदान करते हैं, इसलिए यह उपयोगकर्ताओं को सकारात्मक तरीके से संलग्न करने के लिए अनगिनत संभावनाएँ पैदा करते हैं. क्यू आर कोड आपके ग्राहकों के साथ सीधा संपर्क स्थापित कर सकते हैं और उनके साथ एक संवाद को बढ़ावा देते हैं. उदाहरण के लिए, एक क्यू आर कोड उपयोगकर्ता को उत्पादों या सेवाओं पर प्रतिक्रिया देने की संभावना प्रदान कर सकता है. इस अवसर पर, आप अपने उपयोगकर्ताओं से ईमेल पते एवं संपर्क जानकारी भी प्राप्त कर सकते हैं और इस डाटा को भविष्य में प्रयोग कर सकते हैं.

क्यू आर कोड के फायदे :

- इसके माध्यम से एसएमएस संदेश शेयर किए जा सकते हैं एवं इसे डिस्काउंट कार्ड, बिज़नेस कार्ड के तौर पर भी प्रयोग किया जा सकता है.
- इसे गूगल मैप, यू ट्यूब, फ़ेस बुक से भी लिंक किया जा सकता है.
- इसे एप से जोड़ा जा सकता है, ताकि लोग उस एप का इस्तमाल कर सकें.
- इसे अपनी वेबसाइट के कांटैक्ट पेज से लिंक किया जा सकता है. इससे उस वेबसाइट की पूरी संपर्क जानकारी अपने फोन में सेव की जा सकती है.
- क्यू आर कोड का फायदा विज्ञापन के क्षेत्र में सर्वाधिक है. क्यू आर कोड को किसी विशेष वेबसाइट के यू आर एल पर रिडाइरैक्ट कर सकते हैं. जिससे, उत्पाद संबंधी समस्त जानकारी भावी ग्राहक तक पहुँचायी जा सके.
- क्यू आर कोड का उपयोग उत्पादों और सेवाओं के भुगतान हेतु किया जाता है. केवल क्यू आर कोड को स्कैन करने मात्र से, यह यूज़र को पेमेंट एजेंट अथवा कंपनी के वेब पेज पर रिडाइरैक्ट कर "वन क्लिक पेमेंट" अनुमत करता है. विभिन्न देशों में क्यू आर कोड का उपयोग भुगतान प्रणालियों के रूप में बड़ी व्यापकता से किया जा रहा है. साथ ही वैश्विक तकनीकी कंपनियों एवं सेवा प्रदाताओं से भी इसे लगातार समर्थन प्राप्त हो रहा है, किन्तु इसका व्यापक अंगीकरण इस बात पर निर्भर करता है कि वे अन्य भुगतान प्रणालियों की तुलना में अपने ग्राहकों एवं व्यापारियों को कितनी अधिक, आसान एवं सुरक्षित सुविधाएं प्रदान करते हैं.
- क्यू आर कोड, साइबर सुरक्षा में भी महत्वपूर्ण योगदान निभाता है. वन टाईम पासवर्ड के साथ क्यू आर कोड का मेल बेहतरीन साइबर सुरक्षा प्रदान करता है.
- बचत के उद्देश्य से, किसी भी उत्पाद संबंधी बार कोड/क्यू आर कोड को स्कैन

किया जाता है एवं ऑनलाइन कीमतों से इसकी तुलना की जाती है. कई पेमेंट एप जैसे - मोबाइल वॉलेट, मोबीक्विक, पेटीएम इत्यादि से पेमेंट करते समय क्यू आर कोड की आवश्यकता पड़ती है. यह कोड सेक्योर और सेफ ट्रान्जेक्शन हेतु आवश्यक होता है.

- व्यापक रूप से क्यू आर कोड वित्तीय समावेशन और बैंक देयता उत्पादों को अत्यधिक प्रभावित करता है. दूर-दराज के क्षेत्रों में उपभोक्ताओं को होने वाली कठिनाइयों में यह एक डिजिटल मनी के रूप में कार्य करता है.
- उपभोक्ताओं के पास प्लास्टिक कार्ड हो या फोन, पॉस टर्मिनलों को कार्ड या मोबाइल भुगतान व्यवहार्य बनाने के लिए पर्याप्त संख्या में स्थापित करना अत्यधिक महंगा होता था. क्यू आर कोड व्यापारियों को डिजिटल भुगतान स्वीकार करने का एक सस्ता और आसान तरीका प्रदान करता है.

क्यू आर कोड बनाने संबंधी सावधानियाँः

क्यू आर कोड बनाते समय निम्नलिखित सावधानियां बरतनी चाहिए :

- ऐसा संभव है कि क्यू आर कोड निर्माता को कुछ काले परिदृश्यों में काले रंग की पृष्ठभूमि और एक सफेद या हल्के रंग की परिदृश्यों में सफ़ेद या हल्के रंग की पृष्ठभूमि अच्छी लग सकती है, लेकिन ऐसे क्यू आर कोड को सभी क्यूआर कोड स्कैनर एप्स के साथ स्कैन नहीं किया जा सकता है. क्यू आर कोड का रंग चुनाव करते समय यह अपेक्षा की जाती है कि पृष्ठभूमि तथा उसके अग्रभूमि में रंग चुनाव विपरीत हो, अर्थात हल्के रंग के साथ गहरे रंग और गहरे रंग के साथ हल्के रंग का प्रयोग किया जाए बशर्ते कि यह चयन एक जैसे रंगों के साथ किया जाए.
- अपने क्यूआर कोड छवियों को सभी स्क्रीन और प्रिंट प्रारूपों पर तेज दिखने के लिए पर्याप्त रिज़ॉल्यूशन दें. पर्याप्त रिज़ॉल्यूशन किए बिना बड़े आकार में कोड छवि को स्केल करने से आपके क्यूआर कोड धुंधले लग सकते हैं. एक धुंधला क्यूआर कोड क्यूआर कोड रीडर के लिए कोड की सीमाओं का पता लगाने और स्कैन करने में रुकावट डाल सकता है.
- स्मार्टफोन कैमरों की गुणवत्ता बहुत अलग है. कुछ बहुत अच्छे हैं और बहुत छोटे क्यूआर कोड स्कैन करते हैं लेकिन कुछ कैमरे बहुत छोटे क्यूआर कोड को रीड नहीं कर पाते हैं. आपको क्यूआर कोड को प्रदर्शित या प्रिंट करते समय कोड को कम से कम 2X2 सेमी (0.8X0.8 इंच) का आकार देने की सलाह दी जाती हैं. इस कोड के आधार पर आप कोड में जो भी सूचनाएं डालते हैं, वह बड़ी एवं स्पष्ट होनी

चाहिए.

- क्यूआरकोड में कम और सटीक सामग्री ही डालें, इसका मतलब यह है कि कोड में जितनी अधिक जानकारी होगी, आपका क्यूआर कोड उतना ही अधिक पिक्सल में होगा. यदि आप कोड में बहुत सारी सामग्री डालते हैं तो आपके द्वारा दी गई जानकारी पिक्सल के महासागर में समाप्त हो जाएगी. यह आपके कोड को स्कैन करने और इसे पठनीय बनाने के लिए क्यूआर कोड पाठकों के लिए समस्याएं पैदा कर सकती है. अगर आपको अपने कोड में बहुत सारी सामग्री की ज़रूरत है, तो गतिशील क्यूआर कोडों का प्रयोग करें. क्यूआर कोड आपके 10 पेज के दस्तावेज़ को पकड़ने के लिए नहीं हैं, बल्कि सही और सटीक जानकारी प्रदान करने के लिए हैं.
- हमेशा अपने क्यूआर कोड और उसके आस-पास की सामग्री या डिज़ाइन के बीच एक जगह छोड़ दें. यह ध्यान रखें कि क्यूआर कोड हमेशा पृष्ठभूमि पर अकेले हो और अग्रभूमि को अन्य तत्वों से घेरे हुए ना हो.

आपका व्यवसाय चाहे छोटा हो या बड़ा, कई तरीकों से क्यू आर कोड का उपयोग कर सकते हैं. आप अपनी वेबसाइट पर प्रत्येक उत्पाद के लिए एक क्यू आर कोड बना सकते हैं, जिसमें उत्पाद विवरण, कॉल करने के लिए नंबर एवं वेब पृष्ठ के यू आर एल लिंक शामिल हैं. अपने उत्पादों/वेबसाइट के क्यू आर कोड को किसी भी प्रिंट विज्ञापन, फ्लायर, पोस्टर, आमंत्रण, टीवी विज्ञापन इत्यादि में दे सकते हैं. क्यू आर कोड का मार्केटिंग के क्षेत्र में बड़ा फायदा है. इसमें निम्नलिखित जानकारी डाल सकते हैं :-

- उत्पाद विवरण
- संपर्क विवरण
- प्रस्ताव विवरण
- अवसर की जानकारी
- प्रतियोगिता विवरण
- कोई कूपन
- ट्विटर, फेसबुक, माइस्पेस आईडी
- आपके यूट्यूब वीडियो का एक लिंक, आदि

आजकल क्यू आर कोड का इस्तेमाल व्यापक स्तर पर देखा जा सकता है. किसी पत्रिका में, किसी रेस्तरां में, फेसबुक पर, आपके आधार कार्ड पर इत्यादि.

क्यू आर कोड और बार कोड का प्रयोग किसी उत्पाद को ट्रैक करने या अंकित करने के लिए किया जाता है. स्मार्ट फोन के आने से बड़ी आसानी से क्यू आर कोड को स्कैन किया जा सकता है. क्यू आर कोड को स्कैनर की मदद से कैप्चर किया जाता है फिर क्यू आर कोड में एम्बिडेड यू आर एल हमें उत्पाद संबंधित वेब साइट से लिंक कर देता है, जहां से हमें संबंधित उत्पाद की सम्पूर्ण जानकारी प्राप्त हो जाती है. इसे हम किसी भी दिशा में स्कैन कर सकते हैं. सिंगल डाईमेन्शन वाले बार कोड में जहां पहले सिर्फ 20-25 केरेक्टर की ही स्टोरेज क्षमता होती थी, वहीं क्यू आर कोड में, 7089 केरेक्टर स्टोर किए जा सकते हैं. इसी बड़ी स्टोरेज क्षमता के कारण बड़ी बड़ी फ़ाइलें, फोटो, वीडियो इत्यादि इसमें स्टोर हो जाते हैं, जिसे सोशल नेटवर्किंग साइट्स पर शेयर किया जा सकता है. इसीलिए सोशल नेटवर्किंग साइट्स के बढ़ते चलन के साथ क्यू आर कोड का चलन भी बढ़ता जा रहा है.

क्यू आर कोड के फायदे :

- इसके माध्यम से मेसेजेस शेयर किए जा सकते हैं एवं इसे डिस्काउंट कार्ड, बिज़नेस कार्ड के तौर पर भी प्रयोग किया जा सकता है.
- इसे गूगल मैप, यू ट्यूब, फ़ेस बुक, एप से भी लिंक किया जा सकता है.
- इसे अपनी वेबसाइट के कांटैक्ट पेज से लिंक किया जा सकता है, जिससे उस वेबसाइट की पूरी संपर्क जानकारी अपने फोन में सेव की जा सकती है.
- क्यू आर कोड का फायदा विज्ञापन के क्षेत्र में सर्वाधिक है. क्यू आर कोड को किसी विशेष वेबसाइट के यू आर एल पर रिडाइरैक्ट कर सकते हैं. जिससे, उत्पाद संबंधी समस्त जानकारी भावी ग्राहक तक पहुँचायी जा सके.
- क्यू आर कोड का उपयोग उत्पादों और सेवाओं के भुगतान हेतु किया जाता है. केवल क्यू आर कोड को स्कैन करने मात्र से, यह यूज़र को पेमेंट एजेंट अथवा कंपनी के वेब पेज पर रिडाइरैक्ट कर "वन क्लिक पेमेंट" अनुमत करता है. विभिन्न देशों में क्यू आर कोड का उपयोग भुगतान प्रणालियों के रूप में बड़ी व्यापकता से किया जा रहा है. साथ ही वैश्विक तकनीकी कंपनियों एवं सेवा प्रदाताओं से भी इसे लगातार समर्थन प्राप्त हो रहा है, किन्तु इसका व्यापक अंगीकरण इस बात पर निर्भर करता है कि वे अन्य भुगतान प्रणालियों की तुलना में अपने ग्राहकों एवं व्यापारियों को कितनी अधिक, आसान एवं सुरक्षित सुविधाएं प्रदान करते हैं.
- बचत के उद्देश्य से, किसी भी उत्पाद संबंधी बार कोड/क्यू आर कोड को स्कैन किया जाता है एवं ऑनलाइन कीमतों से इसकी तुलना की जाती है. कई पेमेंट

एप जैसे - मोबाइल वॉलेट, मोबीक्विक, पेटीएम इत्यादि से पेमेंट करते समय क्यू आर कोड की आवश्यकता पड़ती है. यह कोड सेक्योर और सेफ ट्रान्जेक्शन हेतु आवश्यक होता है.

- व्यापक रूप से क्यू आर कोड वित्तीय समावेशन और बैंक देयता उत्पादों को अत्यधिक प्रभावित करता है. दूर-दराज के क्षेत्रों में उपभोक्ताओं को होने वाली कठिनाइयों में यह एक डिजिटल मनी के रूप में कार्य करता है.
- उपभोक्ताओं के पास प्लास्टिक कार्ड हो या फोन, पॉस टर्मिनलों को कार्ड या मोबाइल भुगतान व्यवहार्य बनाने के लिए पर्याप्त संख्या में स्थापित करना अत्यधिक महंगा होता था. क्यू आर कोड व्यापारियों को डिजिटल भुगतान स्वीकार करने का एक सस्ता और आसान तरीका प्रदान करता है.

भारत क्यूआर कोड :

- विमुद्रीकरण के बाद भुगतान करने के तरीके को आसान बनाने वाली सुविधा प्रदान करने के संदर्भ में डिजिटल आर्थिक तंत्र का समर्थन करना अत्यंत अनिवार्य था. वास्तव में कई फिनटेक्स कंपनियों ने इस अवसर का इस्तेमाल उन मोबाइल एप्लिकेशन को सुधारने के लिया किया, जो व्यापारियों और ग्राहकों की आवश्यकताओं के अनुरूप हों. इसी चरण में एनपीसीआई मोबाइल एप भीम के साथ आगे आया, जिसका उपयोग क्यूआर कोड व्यक्ति से अन्य व्यक्ति को भुगतान करने के लिया किया जा सकता है. एप का उपयोग आधार, आईएफ़एससी कोड को स्कैन करके व्यक्ति से व्यक्ति को भुगतान करने के लिए भी किया जा सकता है.
- इसके बाद भारत क्यूआर व्यक्ति से व्यापारी को मोबाइल भुगतान समाधान प्रारंभ करने की आवश्यकता महसूस की गई. यह समाधान पारस्परिक रूप से एनपीसीआई, वीजा और मास्टरकार्ड नेटवर्क के बीच भुगतान की शुरुआत है. एक बार व्यापारी के कारोबार स्थल पर भारत क्यूआर कोड उपलब्ध करा दिए जाते हैं, इसके बाद उपयोगकर्ता भारत क्यूआर कोड समर्थित बैंकिंग एप का प्रयोग करते हुए व्यापारियों की महत्वपूर्ण जानकरियों को साझा किए बगैर उपभोक्ता बिलों का भुगतान कर सकता है. यह भुगतान का एक त्वरित माध्यम है, जिसमें कोई पॉस टर्मिनल आवश्यक नहीं है. ग्राहक व्यापारी के आउटलेट में रखे गए क्यूआर का उपयोग कर यूपीआई के अतिरिक्त भारत क्यूआर से जुड़े कार्ड का उपयोग करके भुगतान कर सकता है. भारत क्यूआर कोड में व्यापारी का नाम, पता, मर्चेंट बैंक की जानकारी इत्यादि जैसी कई अतिरिक्त सूचनाएं निहित होती हैं. भारत क्यूआर कोड अन्य क्यूआर कोडों की तुलना में अधिक व्यापक स्वीकार्य और सुरक्षित है.

उपयोगकर्ता किसी भी कार्ड योजना जैसे रुपे, वीज़ा, मास्टरकार्ड और एक्सेस इत्यादि का उपयोग कर भुगतान की शुरुआत कर सकते हैं.

नोट बंदी के उपरांत भारत में, भुगतान प्रणाली में क्यू आर कोड का बढ़ता चलन :

- भारत में नोटबंदी के उपरांत, क्यू आर कोड आधारित भुगतान का तेजी से उपयोग किया जा रहा है. मोबाइल एप के माध्यम से ग्राहक क्यू आर कोड को स्कैन कर उपभोग की गयी सेवाओं अथवा खरीदी गयी वस्तुओं जैसे- उपभोक्ता बिल, ईंधन, किराना, खाद्य सामग्री, यात्रा और अन्य भुगतान कर सकता है.
- वर्तमान में एक विशिष्ट पॉस मशीन की लागत करीब रू 12,000/- और एम-पॉस मशीन की लागत रू 5000/- है. व्यापारी इसे कम लागत पर प्राप्त कर सकते हैं. साथ ही आज का युग कम समय में अधिक प्रभावशील तरीके से कारोबार करने का युग है. अतः व्यापारियों को एक ऐसा भुगतान समाधान चाहिए, जो उन्हें आसानी से उपलब्ध हो. ऐसी सेवा क्यू आर कोड उन्हें प्रदान करता है. क्यू आर कोड को कागज़ पर मुद्रित किया जा सकता है और ग्राहक इसे स्कैन कर व्यापारी से प्राप्त माल या सेवाओं के एवज में दी जाने वाली राशि का भुगतान उसे कर सकता है.

किसी क्यू आर कोड को स्कैन करने के उपरांत क्या खुलेगा इसके आधार पर क्यूआर कोड निम्न प्रकार का है :

1- **यूआरएल (URL)** - इस क्यू आर कोड को स्कैन करने के बाद ये हमें इसमें भंडारित वेब साइट पर निर्दिष्ट करता है.

2- **व्यापार कार्ड (Business Card)** - बिज़नेस क्यू आर कोड को स्कैन करने के बाद, इसमें भंडारित जानकारी जैसे नाम, पता, दूरभाष संख्या, ई-मेल आदि स्मार्ट फोन में सेव हो जाते हैं.

3- **भू स्थिति (Geo Location)** - इस क्यू आर कोड में किसी स्थान का अक्षांश एवं देशांतर सेव होता है. इसे स्कैन करने पर हम अपने स्मार्ट फोन के मैप (मानचित्र)एप में सीधे इस स्थान को देख सकते हैं.

4- **एप डाउनलोड (App download)** - इस क्यू आर कोड को स्कैन करने पर हम एप डाउन लोड के पते पर निर्दिष्ट किये जाते हैं.

5- **कूपन प्राप्ति (Get a Coupon)** - इस क्यू आर कोड को स्कैन करने पर फोन में कूपन प्राप्ति पृष्ठ पर हमें निर्दिष्ट कर दिया जाता है.

6 **सोशल नेटवर्किंग** - सोशल नेटवर्किंग के लिए भी क्यू आर कोड का प्रयोग किया जाता है. जैसे फेसबुक पृष्ठ के क्यू आर कोड को स्कैन करने के बाद सीधे हम फेसबुक पृष्ठ पर निर्दिष्ट कर दिये जाते हैं.

क्यू आर कोड में व्याप्त जोखिम :

क्यू आर कोड ने हमारे जीवन को बहुत आसान बना दिया है, किन्तु इससे जुड़े हुये कुछ जोखिम भी हैं. बार-बार होने वाले साइबर अटैक में से सबसे ज्यादा पाया जाने वाला साइबर अटैक है - सोशल इंजीनियरिंग. यह एक ऐसी कपटपूर्ण प्रक्रिया है, जिसके माध्यम से लोगों की व्यक्तिगत एवं गोपनीय जानकारी में छलपूर्वक छेड़-छाड़ कर, उसे चुराकर, उसका अनैतिक रूप से प्रयोग किया जाता है. इस हेतु किए जा रहे प्रयासों में एक महत्वपूर्ण तरीका "फिशिंग" है. हमलावरों द्वारा, छलपूर्ण क्यू आर कोड के माध्यम से यूजर्स को धोखाधड़ी वाली वेबसाइट (जोकि दिखने में किसी अन्य वैध वेबसाइट की तरह ही होती है) की ओर डाइरैक्ट किया जाता है और उनकी गोपनीय जानकारी नेम, पासवर्ड अथवा क्रेडिट कार्ड/डेबिट कार्ड संबंधित जानकारी चुरा ली जाती है. हमलावर द्वारा, पूर्व से बने वैध क्यू आर कोड की ही तरह नया फर्जी क्यू आर कोड बनाकर, वैध क्यू आर कोड पर पेस्ट कर दिया जाता है. इस प्रकार यूजर्स/उपभोक्ताओं को भ्रम की स्थिति में डालकर उनकी गोपनीय जानकारियां चुरा ली जाती हैं. हालांकि वर्ष 2011 के अंत तक चीन जैसे तकनीकी रूप से विकासशील देश में, क्यू आर कोड के माध्यम से डिजिटल भुगतान प्रक्रिया को बहुत अधिक बढ़ावा मिला किन्तु वर्ष 2016 के अंत तक धोखाधड़ी वाले क्यू आर कोड की बहुतायत के कारण चीन की सरकार को भी अस्थायी रूप से क्यू आर कोड भुगतान पर प्रतिबंध लगाना पड़ा. यह अलग बात है कि क्यू आर कोड को अधिक सुरक्षित करने के तकनीकी प्रयास पूरे विश्व में जारी है, किन्तु किसी भी अन्य डिजिटल प्रक्रिया की भांति इसे भी पूर्ण रूप से सुरक्षित नहीं कहा जा सकता.

अपने व्यक्तिगत और गोपनीय डाटा की सुरक्षा के लिए क्यू आर कोड स्कैन करते समय इन सावधानियों को ध्यान में रखें :

क्यू आर कोड स्टिकर से सावधान रहें. कभी-कभी एक साइबर क्रिमिनल उन्हें वैध क्यू आर कोडों पर चिपकाएगा. जब आप किसी क्यू आर कोड को स्कैन करते हैं तो ध्यान दें, कोड स्कैन करने और ब्राउज़र के लॉंच के बीच एक अन्तरिम चरण है, जब आप देख सकते हैं कि यह आपकी अपेक्षा के विपरीत किसी और स्थान पर निर्दिष्ट तो नहीं हो रहा है. ऐसे में आप लिंक को कैन्सल कर आगे बढ़ने से रुक सकते हैं.

उन लोगों को शिक्षित करें, जो आपके मोबाइल को इस्तेमाल करते हैं. अगर आपके बच्चे आपका मोबाइल फोन इस्तेमाल करते हैं तो उनको इस संबंध में अनिवार्य

रूप से शिक्षित करें ताकि संभावित खतरों से बचा जा सके. ऐसे क्यू आर कोड से सावधान रहें, जो उसके लिंक से संबंधित उचित जानकारी उपलब्ध नहीं करवाते. एक क्यू आर कोड बनाने का सबसे अच्छा अभ्यास यह बताना है कि वे क्यू आर कोड को स्कैन करते समय क्या प्राप्त करेंगे. यदि आपके पास मोबाइल है जो कि एंड्राइड मोबाइल ऑपरेटिंग सिस्टम पर चलता है तो विशेष रूप से सावधान रहें. चूंकि एंड्राइड एक खुला मंच है, साइबर अपराधी आसानी से इसका फायदा उठा सकते हैं. सिस्टम की सुरक्षा की दृष्टि से ये अत्यंत महत्वपूर्ण है कि केवल विश्वसनीय स्रोतों के ही क्यू आर कोड को स्कैन करें. क्यू आर कोड प्रौद्योगिकी आसानी से सुलभ है. विपणन के लिए विशेष रूप से आकर्षक क्यू आर कोड बनाया जा सकता है, जिसकी लागत काफी कम एवं सार्वभौमिक प्रयोज्यता होती है. क्यू आर कोड मोबाइल उपयोगकर्ताओं को किसी भी लक्षित स्थान और समय पर अपने ग्राहकों तक पहुँचने में मदद करते हैं. इसके लिए एक स्मार्ट फोन के अलावा किसी विशेष उपकरण की आवश्यकता नहीं है.

आज दुनिया में 1.76 बिलियन से अधिक स्मार्ट फोन उपयोगकर्ताओं की संख्या है. यह मोबाइल मार्केटिंग को बढ़ावा देने की दिशा में सबसे उपयुक्त समय है. क्यू आर कोड एक अत्यंत सरल प्रणाली है और इसका उपयोग बहुत व्यापक स्तर पर किया जा सकता है, किन्तु इसको पूर्ण रूप से सफल तभी बनाया जा सकता है जब लोग इससे जुड़े हुए खतरों से अवगत होकर, सचेत होकर इसका इस्तेमाल करें.

डिजिटल मार्केटिंग के विभिन्न तरीके

बृजेश कुमार तिवारी
मुख्य प्रबन्धक
सीएजी क्षे. का. पुणे

हमारा देश भारत, क्षेत्रफल की दृष्टि से विश्व का सातवाँ सबसे बड़ा तथा जनसंख्या की दृष्टि से दूसरा सबसे बड़ा देश है. पारंपरिक तरीके से इतनी बड़ी जनसंख्या तक बैंकिंग सेवाएँ पहुंचाना बहुत ही मुश्किल और महँगा होगा. तीन दशकों पहले बैंकिंग सेवाएँ सिर्फ शाखा में प्रदान की जा सकती थी, परंतु पिछले तीन दशकों में हमारे देश में वित्तीय प्रभाग में अभूतपूर्व बदलाव हुए हैं, वित्तीय संसाधनों में वृद्धि के साथ-साथ इसकी पहुँच भी बढ़ी है. इस परिवर्तन का सबसे बड़ा श्रेय तकनीकी विकास को जाता है, तकनीकी विकास ने वित्तीय संसाधनों को उपयोग में सरल बनाने के साथ-साथ सस्ता भी कर दिया है. वित्तीय संसाधन ही किसी देश और उसके नागरिकों को समृद्ध और शक्तिशाली बना सकते हैं.

पिछले चार-पाँच वर्षों में हमारे देश में वित्तीय संसाधनों और बैंकिंग सेवाएँ पहुंचाने के लिए हमारी सरकार और बैंक बहुत ही सुनियोजित ढंग से प्रयासरत हैं और इस प्रयास में काफी हद तक सफल भी हुए हैं.

डिजिटल बैंकिंग : डिजिटल बैंकिंग में वो सारी बैंकिंग सेवाएँ जैसे कि नकदी जमा करना, निकालना, ट्रान्सफर करना, बचत और चालू खातों का परिचालन करना इत्यादि शामिल है अर्थात ग्राहक, ज़्यादातर रोज़मर्रा की जरूरत की बैंकिंग सेवाओं का परिचालन खुद से अपने घर बैठे या अपनी सुविधा के अनुसार जब भी जहाँ चाहे कर सकता है.

डिजिटल बैंकिंग की शुरुआत : डिजिटल बैंकिंग की शुरूआत सन 1960 से मानी जाती है तथा इसके प्रथम उत्पाद एटीएम मशीन एवं एटीएम कार्ड माने जाते हैं. ऑनलाइन बैंकिंग की शुरुआत 1981 में ब्राड बैंड के आविष्कार के बाद अमेरिका के न्यूयॉर्क शहर से मानी जाती है.

डिजिटल बैंकिंग के प्रमुख उत्पाद : डिजिटल बैंकिंग के प्रमुख उत्पाद इस तरह हैं. 1. डेबिट कार्ड 2. क्रेडिट कार्ड 3. ऑनलाइन/इंटरनेट बैंकिंग 4. डिजीपर्स 5. मोबाइल बैंकिंग 6. टेलीफ़ोन बैंकिंग 7. एसएमएस बैंकिंग 8. पॉस मशीन 9. एम पासबुक इत्यादि.

डिजिटल मार्केटिंग की आवश्यकता : हमारे देश में डिजिटल बैंकिंग की शुरुआत 1990 के दशक के अंत से मानी जाती है तथा इंटरनेट बैंकिंग की शुरुआत 2000 ई. के आस-पास मानी जाती है, इसके बावजूद भी हमारे देश की अर्थव्यवस्था ज़्यादातर नकदी पर ही निर्भर रही है. शाखाओं में भीड़ इकट्ठा होना सामान्य बात है, परंतु इसमें एक बड़ा परिवर्तन देश में दि. 08 नवम्बर 2016 को लागू किए गए नोटबंदी के बाद से महसूस किया जा रहा है. नोटबंदी में ₹ 500 और ₹ 1000 के नोटों को तत्काल प्रभाव से, कुछ अपवादों को छोड़कर, बंद कर दिया गया था, जिससे लोगों को नकदी प्राप्त करने में काफी कठिनाई हुई और लोगों ने विकल्प के रूप में डिजिटल बैंकिंग के कुछ चैनलों का उपयोग करना शुरू किया. पीओएस मशीन, मोबाइल बैंकिंग और डिजीपर्स का उपयोग बढ़ने लगा, लोगों ने विभिन्न आदान-प्रदान में क्रेडिट कार्ड, डेबिट कार्ड तथा आईएमपीएस जैसी सुविधाओं का उपयोग करना शुरू किया और भुगतान के क्षेत्र में बहुत सारी निजी कंपनियां आ गयीं, जैसे पे-टीएम, क्विक पे इत्यादि.

सरकार ने भी भुगतान प्रणाली को ऑनलाइन करने के उद्देश्य से भीम एप आरंभ किया और ऑनलाइन नकदी आदान-प्रदान के लिए पुरस्कार देना भी शुरू किया, लॉटरी भी की गयी, जिसमें कुछ ग्राहकों ने भारी इनाम भी जीते, जिससे 'लोगों में ऑनलाइन बैंकिंग के प्रति विश्वास बढ़ना शुरू हुआ. स्वयं प्रधानमंत्री ने अपने विभिन्न कार्यक्रमों में डिजिटल बैंकिंग पर ज़ोर दिया और 'डिजिटल इंडिया' मिशन के नाम से एक कार्यक्रम चलाया.

डिजिटल मार्केटिंग के विभिन्न तरीके : किसी उत्पाद का आविष्कार जितना महत्वपूर्ण है, मार्केटिंग उससे भी ज्यादा महत्वपूर्ण और आवश्यक है, क्योंकि जब तक हम उत्पाद को ग्राहकों तक नहीं पहुंचाएंगे, तब तक लाभ अर्जित करना और उसके उत्पादन को लाभप्रद बनाना मुश्किल होगा, जो कि किसी भी व्यापारिक प्रतिष्ठान के लिए अति आवश्यक है. इसी तरह से हमारे बैंक ने बहुत सारे 'डिजिटल उत्पाद' तो बना दिये परंतु जब तक हम उसे अधिक से अधिक लोगों तक नहीं पहुंचाएंगे तब तक उसकी उपयोगिता साबित नहीं होगी और न ही हमें उस मेहनत का फल मिलेगा, जो हमने किया है और न ही अपने निर्धारित उद्देश्य को प्राप्त कर पाएंगे, इसलिए हमें अपने डिजिटल उत्पादों का विपणन करना अति आवश्यक है, उसके कुछ तरीके इस प्रकार हैं:

1. **वेबसाइट को सरल और उपयोगी बनाना :** डिजिटल उत्पाद को ग्राहकों तक आसानी से पहुंचाने का सबसे अच्छा तरीका है कि हमारी वेबसाइट ग्राहक सहयोगी हो अर्थात् ग्राहक आसानी से हमारी वेबसाइट पर पहुंच सकें और जरूरी उत्पाद को आसानी से प्राप्त कर सकें, जहां उसके उपयोग के तरीके आसानी से और विस्तारपूर्वक दिये गए हों, जिससे ग्राहकों को किसी बाहरी व्यक्ति या भौतिक

सहायता की जरूरत न पड़े. वेबसाइट पर सभी जरूरी सूचनाएं और उसके फायदे, नुकसान, सावधानियां सब कुछ स्पष्ट रूप से वर्णित हो, डिजिटल बैंकिंग के सारे उत्पाद प्रयोग में आसान हों और सेल्फ गाइडेड हों, जिससे उनको मोबाइल में स्थापित करने तथा उनके उपयोग में कोई परेशानी न हो तथा किसी भी परेशानी की स्थिति में बैंक के लोग मदद के लिए आसानी से उपलब्ध हों या फिर वेबसाइट की मॉनिटरिंग होती रहे और किसी ग्राहक को किसी प्रकार की परेशानी होने पर बैंक उनको तुरंत संपर्क करें और उनकी परेशानियों का निवारण करें.

2. **विभिन्न प्रचार माध्यमों से प्रचार करना :** हम अपने डिजिटल उत्पादों को विभिन्न प्रचार माध्यमों जैसे कि समाचार पत्र, टेलीविजन, रेडियो, होर्डिंग इत्यादि के माध्यम से लोगों तक पहुंचा सकते हैं. हम अपने उत्पादों की रेटिंग कराकर भी ग्राहकों को इनकी विशेषताएं बता सकते हैं, जो उन्हें इसके उपयोग करने के लिए प्रेरित करेगा. इन माध्यमों का उपयोग करने से बैंक के प्रति ग्राहकों की विश्वसनीयता भी बढ़ती है.

3. **ग्राहकों को सीधे एसएमएस के माध्यम से :** हम अपने उत्पादों के बारे में ग्राहकों को सीधे एसएमएस भेजकर उनको इसकी उपयोगिता की जानकारी दे सकते हैं तथा साथ में लिंक भेजकर उनको डाउनलोड करके इस्तेमाल करने के लिए प्रेरित कर सकते हैं, साथ ही यदि हम अपने ग्राहक के खर्च करने के तरीके को समझ कर उन्हें उपयुक्त उत्पाद देने की कोशिश करें तो इससे ग्राहक भी संतुष्ट होगा और हमारे उत्पाद का उपयोग भी बढ़ेगा.

4. **ई-व्यापार और ज्यादा उपयोग होने वाली वेबसाइटों पर प्रचार करना और लिंक प्रदान करना :** आजकल छोटी-छोटी भुगतान कंपनियां इस माध्यम का सबसे ज्यादा इस्तेमाल कर रही हैं. इस माध्यम से ग्राहकों को इस्तेमाल के समय ही हम अपने उत्पाद जैसे डिजीपर्स या भीम इत्यादि अपने मोबाइल पर इंस्टॉल करने के लिए प्रेरित कर सकते हैं और इस समय ग्राहक अक्सर सरल माध्यम की तलाश में रहता है, साथ ही साथ इसमें हम ग्राहकों को भेंट के रूप में अपने उत्पाद को इस्तेमाल के एवज में कुछ दे सकते हैं, जैसे कि कुछ डिस्काउंट या फिर ईएमआई की सुविधा इत्यादि. अमेजॉन, फ्लिपकार्ट और अन्य व्यावसायिक साइट पर हम इस तरह के प्रचार का इस्तेमाल कर सकते हैं. वर्तमान वातावरण में डिजिटल उत्पादों के प्रचार-प्रसार में यह बहुत उत्तम तरीका साबित हो रहा है.

5. **शाखाओं तथा अन्य सार्वजनिक स्थानों पर कैंप करके :** ऐसी शाखाओं में जहाँ बहुत भीड़ होती है अर्थात् जहाँ पर ग्राहक हमारी शाखाओं में भौतिक रूप से ज्यादा संख्या में आते हैं वहां हम कैंप लगाकर ग्राहकों को डिजिटल उत्पाद के बारे

में शिक्षित करने के साथ-साथ उन्हें उपयोग करने के तरीके भी बता सकते हैं. शाखा में ग्राहक हमारे कर्मचारियों पर काफी विश्वास करते हैं, वो हमारे कर्मचारी की बात मानते हुए इन उत्पादों का ज्यादा इस्तेमाल करेंगें क्योंकि यहां पर उनकी कोई भी समस्या हमारे कर्मचारी या अधिकारी के द्वारा आसानी से सुलझाई जा सकती है और ग्राहक हमसे जुड़ने में गौरव का भी अनुभव करता है. हमारे अधिकारी ग्राहक को व्यक्तिगत रूप में सेवा प्रदान करते हैं, जो काफी विश्वासनीय होता है. हम सार्वजनिक जगहों जैसे पार्क, शापिंग मॉल, खेल के मैदानों में भी कैंप लगाकर ग्राहकों तक अपने उत्पाद की जानकारी प्रदान कर सकते हैं और उन्हें इसके इस्तेमाल के लिए प्रेरित कर सकते हैं.

6. **सरकार द्वारा विपणन और डिजिटल भुगतान की अनिवार्यता :** जैसा कि हम सभी जानते हैं कि हमारी वर्तमान सरकार 'डिजिटल इंडिया' मिशन चला रही है इस से भी डिजिटल मार्केटिंग को काफी बढ़ावा मिल रहा है तथा सरकार द्वारा ज़्यादातर सरकारी सेवाओं जैसे - कर भुगतान, बिजली बिल भुगतान, ट्रेन टिकट आरक्षण इत्यादि हेतु ऑनलाइन माध्यम से भुगतान की अनिवार्यता लोगों को डिजिटल भुगतान प्रणाली को उपयोग करने के लिए बाध्य कर रही है. इस सुनहरे अवसर का फायदा उठाकर हम ग्राहकों तक अपने उत्पादों को पहुंचाकर बाजार में अपना वर्चस्व स्थापित कर सकते हैं.

7. **रेफरल कोड के माध्यम से :** हम अपने ग्राहकों को लिंक भेजकर उन्हें दूसरे लोगों तक भेजने का आग्रह कर सकते हैं और इसके बदले में उन्हें कुछ पुरस्कार या कुछ पॉइंट दे सकते हैं, जिसका उपयोग कोई भौतिक वस्तु खरीदने में किया जा सकता हो, इससे ग्राहक हमारे लिंक को अपने जान-पहचान में आगे प्रेषित करेंगे और हमारे उत्पाद की जानकारी अधिक से अधिक लोगों तक पहुंचाई जा सकेगी.

8. **प्रोमोशनल कार्यक्रमों के माध्यम से :** प्रोमोशनल कार्यक्रमों के माध्यम से भी हम डिजिटल बैंकिंग उत्पादों का विपणन आसानी से कर सकते हैं, जैसे आजकल हम अपने बैंक का डेबिट कार्ड इस्तेमाल करने वालों ग्राहकों को कुछ वस्तुओं की खरीद में छूट इत्यादि दे रहे हैं, इस तरह के कार्यक्रम हम अपने बाकी उत्पादों को बढ़ावा देने के लिए भी कर सकते हैं. डिजीपर्स, मोबाइल बैंकिंग अथवा भीम, यूपीआई इत्यादि उत्पादों का इस्तेमाल बढ़ाने के लिए भी हम इस तरह के कार्यक्रम कर सकते हैं.

9. **ग्राम पंचायत अथवा संगठित समाज का उपयोग करके :** हमारे देश की बहुत बड़ी जनसंख्या गाँव में रहती है. वहां पर आज भी नगदी का प्रचलन सबसे ज्यादा है क्योंकि लोग डिजिटल उत्पाद का उपयोग करने में अभी भी डरते हैं. अगर हम

ऐसी जगहों पर सुनियोजित ढंग से ग्राम पंचायतों और संगठित समाज का उपयोग करके अपने उत्पादों का लाइव प्रस्तुतीकरण करें तो उनमें भी इस तरह के उत्पादों के प्रति विश्वास जगेगा और हम एक बड़ी जनसंख्या को डिजिटल चैनल से जोड़ सकेंगे. इस तरह का कार्यक्रम खासकर कम पढ़े-लिखे और दूर-दराज के क्षेत्रों में काफी प्रभावशाली हो सकता है.

उपसंहार : नोटबंदी हमारे देश के इतिहास में एक बहुत ही महत्वपूर्ण घटना मानी जा रही है और इसके बाद से हमारे देश में आर्थिक जगत और लेन देन में बड़ा परिवर्तन आया है, जहां एक तरफ सरकार लोगों को डिजिटल लेन देन को बढ़ावा दे रही है वहीं वित्तीय संस्थान भी इस दिशा में काफी प्रयत्न कर रहे हैं. हमें इससे जुड़ी मुश्किलों को दूर करते हुए लोगों के अंदर विश्वास पैदा करना है कि डिजिटल बैंकिंग उनके लिए बहुत ही उपयोगी और सुविधाजनक है. इसके प्रयोग की जानकारी और इससे होने वाले फायदों को लोगों तक पहुंचाना प्राथमिकता और उत्तरदायित्व है. हम निश्चित रूप से इस दिशा में आगे बढ़ रहे हैं और भविष्य में इसको जन-जन तक पहुंचाएंगे.

सरकारी ई-बाजार-GEM

अनुराग सरोलिया
वरिष्ठ प्रबंधक
सरकारी कारोबार कक्ष, नई दिल्ली

मिथिलेश कुमार झा
मुख्य प्रबंधक
डीआईटी, के. का. मुंबई

हमारे देश में सैकड़ों सरकारी विभागों के हजारों दफ्तरों की करोड़ों जरूरतें होती हैं. उदाहरण स्वरूप पेन, पेपर, फ़ाइल से लेकर कम्प्यूटर, फोटोस्टेट मशीन और वाहन आदि, जिन पर सालाना हजारों करोड़ रुपये खर्च होते हैं. यह सारी खरीद-बिक्री अक्सर सवालों के घेरे में रहती है. ऐसा प्रतीत होता है कि सबसे अधिक भ्रष्टाचार की वजह भी यही खरीद-बिक्री की प्रक्रिया होती है. परंतु यदि यह सारी खरीद-बिक्री प्रक्रिया ऑनलाइन हो जाए, तो हमें ज्ञात होता रहेगा कि बिजली के दफ्तर से लेकर पीडब्ल्यूडी कार्यालय में कौन-कौन सी चीज कितने मूल्य पर और किस गुणवत्ता की खरीदी गई है. इन कठिनाइयों को दूर करने के लिए एवं पारदर्शिता रखने हेतु भारत सरकार ने जीईएम पोर्टल पर खरीद-बिक्री को अनिवार्य किया है. यह पूरी तरह पेपरलेस, कैशलेस और सिस्टम संचालित ई-मार्केट प्लेस है, जो कम से कम मानव दखल के सामान्य उपयोग की वस्तुओं एवं सेवाओं की खरीद हेतु सक्षमता प्रदान करता है. इस पोर्टल की विशेषता यह है कि यह किसी भी सरकारी खरीद को बिचौलियों से भी मुक्ति दिलाता है.

जीईएम (सरकारी ई-मार्केटप्लेस), डीजीएस एवं डी (आपूर्ति और निपटान महानिदेशालय) द्वारा आयोजित राष्ट्रीय सार्वजनिक खरीद पोर्टल है. यहां आम सामान और सेवाएं खरीदी और बेची जा सकती हैं और यह केंद्र और राज्य सरकार के मंत्रालयों/विभागों, केंद्र और राज्य के सार्वजनिक उपक्रमों (सीपीएसयू और एसपीएसयू), स्वायत्त संस्थानों और स्थानीय निकायों को पारदर्शी और कुशल तरीके का वन स्टॉप ऑनलाइन बाजार उपलब्ध कराती है.

जनवरी, 2016 में माननीय प्रधान मंत्री ने अपने सचिवों के समूह की सिफारिशों के आधार पर, डिजिटलीकरण को प्रोत्साहित करने और पारदर्शिता बढ़ाने के लिए विभिन्न सरकारी विभागों/संगठनों/सार्वजनिक क्षेत्र के उपक्रमों द्वारा सामान और सेवाएं ऑनलाइन खरीद की सुविधा के लिए सरकारी ई-मार्केटप्लेस (जीईएम) बनाने का फैसला किया. इसके बाद, वित्त वर्ष 2016-17 के लिए अपने बजट भाषण में माननीय वित्त मंत्री

ने सरकार के विभिन्न मंत्रालयों और एजेंसियों द्वारा माल और सेवाओं की खरीद को सुविधाजनक बनाने के लिए एक प्रौद्योगिकी संचालित मंच की स्थापना की घोषणा की. यह पोर्टल दि. 9 अगस्त 2016 को माननीय वाणिज्य और उद्योग मंत्री द्वारा लॉन्च किया गया.

सार्वजनिक खरीद सरकारी गतिविधियों का एक बहुत ही महत्वपूर्ण हिस्सा रहा है और सार्वजनिक खरीद में सुधार वर्तमान सरकार की शीर्ष प्राथमिकताओं में से एक है. सरकारी ई-मार्केटप्लेस (जीईएम, URL-https://gem.gov.in) सरकारी मंत्रालयों और विभागों, सार्वजनिक क्षेत्र के उपक्रमों और केंद्र/राज्य सरकार के अन्य शीर्ष स्वायत्त निकायों द्वारा माल और सेवाओं की खरीद के तरीके को बदलने के उद्देश्य से सरकार द्वारा उठाया गया एक बहुत ही साहसिक कदम है. जीईएम पोर्टल सरकारी संगठनों द्वारा खरीद के लिए डाइनैमिक, आत्मनिर्भर और यूज़र फ्रेंडली है. जीईएम के माध्यम से खरीद को सामान्य वित्तीय नियमों (जीएफआर) 2017 द्वारा प्राधिकृत किया गया है. सरकार ने सभी सार्वजनिक क्षेत्र के बैंकों को भी जीईएम पोर्टल के माध्यम से उत्पादों की खरीद प्रक्रिया को अपनाने और बैंकों से एक नोडल अधिकारी नामित करने के निर्देश दिये हैं.

वर्तमान में लगभग 350 उत्पाद श्रेणियों में 5 लाख से अधिक उत्पाद जीईएम पोर्टल पर उपलब्ध हैं. जीईएम के माध्यम से ₹ 12,000 करोड़ से अधिक के लिए लेनदेन किए जा चुके हैं. जीईएम अधिकतम खुदरा मूल्य (एमआरपी) पर अनिवार्य रूप से 10% की न्यूनतम छूट (जीईएम पर जब तक अन्यथा उनके उत्पादों की पेशकश के लिए निर्दिष्ट नहीं किया जाता है) के साथ सामान्य वस्तुओं और सेवाओं की खरीद उपलब्ध कराता है. इसमें विक्रेता अधिक छूट प्रदान करने के लिए स्वतंत्र हैं. यह ई-बोली-प्रक्रिया, ई-नीलामी (रिवर्स/फॉरवर्ड) और सरकारी विभागों की सुविधा के लिए मांग एकत्रीकरण के साधन प्रदान करता है, जिससे उन्हें सर्वोत्तम मूल्य प्राप्त होता है.

सरकारी विभागों द्वारा जीईएम के माध्यम से खरीद को प्राधिकृत किया गया है और वित्त मंत्रालय द्वारा सामान्य वित्तीय नियम, 2017 में एक नया नियम संख्या 149 जोड़कर अनिवार्य किया गया है. डीजीएस एवं डी संभावित आपूर्तिकर्ताओं के वस्तुओं के खरीद के लिए जीईएम के माध्यम से आवधिक विज्ञापन सहित पर्याप्त प्रचार सुनिश्चित करेगा. डीजीएस एवं डी द्वारा जीईएम पर प्रमाणिक आपूर्तिकर्ताओं और पोर्टल पर पंजीकृत आपूर्तिकर्ताओं को प्रमाणित किया जाएगा. खरीद प्राधिकरण वस्तुओं एवं सेवाओं की दरों की तर्कसंगतता को प्रमाणित करेंगे. जीईएम पोर्टल का उपयोग सरकारी खरीददारों द्वारा सीधे ऑनलाइन खरीद के लिए किया जाएगा, जिससे संबंधित दिशानिर्देश निम्नानुसार हैं:

I. जीईएम पर उपलब्ध किसी भी आपूर्तिकर्ता के माध्यम से ₹50,000/- तक की खरीद, जो आवश्यक गुणवत्ता, विनिर्देश और आपूर्ति की अवधि को पूरा करता हो.

II. जीईएम विक्रेता के माध्यम से ₹50,000/- से ऊपर और ₹30,00,000/- तक की खरीद के लिए जीईएम में उपलब्ध विक्रेताओं के बीच सबसे कम कीमत एवं अन्य वांछित मानदंडों पर तुलना की जा सकती है. यदि सक्षम प्राधिकारी द्वारा निर्णय लिया जाता है, तो खरीददार जीईएम पर उपलब्ध ऑनलाइन बोली-प्रक्रिया और ऑनलाइन रिवर्स नीलामी टूल्स का उपयोग कर सकता है.

III. जीईएम पर उपलब्ध आपूर्तिकर्ताओं के माध्यम से ₹30,00,000/- से अधिक मूल्य के खरीद लिए बोलियां प्राप्त करना, ऑनलाइन बोली-प्रक्रिया या रिवर्स नीलामी टूल का उपयोग कर आवश्यक गुणवत्ता, विनिर्देश और वितरण अवधि पूरा करने वाली सबसे कम कीमत की बोली के माध्यम से खरीद को अनिवार्य बनाया गया है.

IV. जीईएम ऑनलाइन ई-बोली-प्रक्रिया/रिवर्स नीलामी के लिए आमंत्रण पोर्टल पर उन सभी मौजूदा विक्रेताओं या अन्य पंजीकृत विक्रेताओं को उपलब्ध होगा, जिन्होंने नियम और शर्तों के अनुसार विशेष उत्पाद/ सेवा श्रेणी के तहत अपनी माल/सेवाओं की पेशकश की है. सरकारी खरीददार जीईएम पर उपलब्ध बिज़नेस एनालिटिक्स (बीए) टूल का उपयोग करके आदेश देने से पहले कीमतों की तर्कसंगतता का पता लगा सकते हैं.

V. जीईएम पर एल-1 खरीददारी/बोली/रिवर्स नीलामी के माध्यम से खरीद से बचने के लिए एक अंश की खरीद करने के लिए सामानों की मांग को कम मात्रा में विभाजित नहीं किया जाना चाहिए.

खरीददारों को लाभः

- माल/सेवाओं की व्यक्तिगत श्रेणियों के लिए उत्पादों की संपूर्ण सूची की उपलब्धता.
- खोज, तुलना, चयन और खरीद की सुविधा.
- जब कभी आवश्यक हो, माल और सेवाओं की ऑनलाइन खरीद की सुविधा.
- पारदर्शी और खरीदने में आसान.
- विक्रेता रेटिंग प्रणाली का निरंतर अद्यतन किया जाता है.
- खरीद, निगरानी, आपूर्ति और भुगतान के लिए उपयोगकर्ता के अनुकूल डैश बोर्ड.
- आसान वापसी नीति का भी प्रावधान है.

विक्रेताओं को लाभः

- सभी सरकारी विभागों तक प्रत्यक्ष पहुँच.
- न्यूनतम प्रयासों से विपणन के लिए वन-स्टॉप शॉप.
- उत्पादों/सेवाओं पर बोली/रिवर्स नीलामी के लिए वन-स्टॉप शॉप.
- विक्रेता को उपलब्ध नए उत्पाद सुझाव की सुविधा.
- डाइनैमिक मूल्य निर्धारण - बाजार के आधार पर मूल्य बदला जा सकता है.
- आपूर्ति और भुगतान की बिक्री और निगरानी के लिए विक्रेता अनुकूल डैशबोर्ड.
- सुसंगत और एक समान खरीद/बिक्री प्रक्रिया.

सरकार, विक्रेताओं, भारतीय उद्योग और अर्थव्यवस्था के लिए जीईएम के माध्यम से खरीद के लाभः

- पारदर्शिता
- दक्षता
- सुरक्षित और निरापद
- 'मेक इन इंडिया' को समर्थन
- सरकार की बचत
- 'डिजिटल इंडिया' पहल को प्रोत्साहन

जीईएम पोर्टल पर उपलब्ध सामान्य वस्तुएं एवं सेवाएँः

- डेस्कटॉप, लैपटाप, टैबलेट एवं अन्य आवश्यक बाह्य उपकरण, पेनड्राइव, पावरबैंक
- फोटोकॉपी मशीन, प्रिंटर, बारकोड स्कैनर, कार्टेज
- ए-4 एवं लीगल कागज, नोटशीट
- एयर कंडीशनर, मल्टीमीडिया प्रोजेक्ट्स, डिब्बा बंद पेयजल
- यूपीएस
- लेखन सामाग्री इत्यादि.

जीईएम पोर्टल का उपयोग करने हेतु पूर्व अपेक्षाएँः

- आधार संख्या

- मोबाइल संख्या
- सरकारी या एनआईसी ईमेल
- डिजिटल हस्ताक्षर
- विभाग के सक्षम प्राधिकारी का अनुमोदन
- प्रयोक्ताओं को जीईएम पोर्टल पर स्वयं को पंजीकृत कराना

जीईएम पोर्टल के माध्यम से खरीद की प्रक्रियाएं:

- स्वयं को जीईएम पर पंजीकृत करें.
- मांगकर्ता के रूप में मांग प्रस्तुत करना.
- जीईएम पर सर्च करना और उत्पाद चुनना.
- खरीदार के रूप में आदेश प्रस्तुत करना.
- आदेश प्रस्तुत करने के बाद, पूर्तिकर्ता नियत डिलीवरी तारीख के अंदर परेषिती (Consignee) को माल की सुपुर्दगी करेगा.
- वस्तुएं एवं सेवाएँ प्राप्त होने के बाद परेषिती प्रोविजनल रिसीट सर्टिफिकेट अपडेट करेगा.

जीईएम पोर्टल के माध्यम से खरीद के लिए उत्तरदायित्व:

- **क्रेता पंजीकरण :** क्रेता को जीईएम पोर्टल पर दो प्रकार के उपयोगकर्ता बनाना है अर्थात् प्राथमिक और द्वितीयक उपयोगकर्ता. प्राथमिक उपयोगकर्ता जीईएम पोर्टल में पंजीकरण कर सकते हैं, संगठन की जानकारी जोड़ सकते हैं, अपने संगठन के भीतर डिवीज़न बना सकते हैं और द्वितीयक उपयोगकर्ता (यानि क्रेता, परेषिती, भुगतान प्राधिकारी) भी बना सकते हैं. प्राथमिक उपयोगकर्ता आवश्यकता के आधार पर कई द्वितीयक उपयोगकर्ता बना सकते हैं. पंजीकरण के दौरान, उपयोगकर्ताओं का आधार के माध्यम से ई-सत्यापन किया जाता है.

  प्राथमिक उपयोगकर्ता खरीददार की भूमिका नहीं निभा सकता. खरीद का अधिकार द्वितीयक उधारकर्ता के पास होता है. द्वितीयक उपयोगकर्ता को विभाग के प्रमुख से वित्तीय अनुमोदन प्राप्त करना होता है.

- **खरीद प्रणाली :** द्वितीयक उपयोगकर्ता जीईएम पोर्टल में लॉगिन कर सकते हैं, अपनी व्यक्तिगत जानकारी अपडेट कर सकते हैं. द्वितीयक उपयोगकर्ता को "मार्केट" मेनू विकल्प में जाना है, उत्पाद चुनना है और विभिन्न खरीद गतिविधियों

अर्थात सीधे खरीद, एल-1 खरीद, योग्यता मानदंडों का चयन, विनिर्देशों का चयन, बोली निर्मित करना और रिवर्स नीलामी करना और विक्रेता आदि का चयन करना है. पहले अनुबंध आदेश और उसके बाद खरीद आदेश जारी किया जाता है. प्रत्येक चरण में खरीददार प्राथमिक उपयोगकर्ता भुगतान प्राधिकारियों के साथ-साथ विक्रेताओं को एसएमएस और ई-मेल द्वारा सूचनाएं भेजी जाती हैं. केवल ई-साइन के बाद ही पोर्टल पर आवश्यक दस्तावेज अपलोड किए जाते हैं.

- **परेषिती की कार्यवाही :** चयनित विक्रेता उत्पाद की आपूर्ति करेगा और उत्पादों की डिलीवरी के बाद विक्रेता बीजक तैयार करेगा. परेषिती को पहले वितरित उत्पादों का निरीक्षण करना होगा और 'परेषिती रसीद सह स्वीकृति प्रमाणपत्र' (सीआरएसी) प्रदान करना होगा.

- **भुगतान प्रणाली :** परेषिती द्वारा माल स्वीकार करने के बाद भुगतान प्राधिकारी की भूमिका क्रेता द्वारा भुगतान की शर्तों और भुगतान के तरीके के आधार पर भुगतान जारी करना है, यानि पीएफएमएस द्वारा भुगतान एसबीआई इंटरनेट बैंकिंग या ऑफलाइन मोड के माध्यम से भुगतान.

सरकार ने जागरुकता बढ़ाने के लिए दि. 6 सितंबर से 17 अक्तूबर 2018 तक जीईएम पर छः सप्ताह का राष्ट्रीय मिशन चलाया या जीईएम के साथ 23 राज्यों एवं 4 केन्द्र शासित प्रदेशों ने समझौता किया है. इसके अलावा जीईएम पोर्टल से खरीद बिक्री करने हेतु हेल्प डेस्क/कॉलसेंटर की व्यवस्था भी की गई है, जो क्रेताओं/विक्रेताओं की समस्याओं का हल करते हैं. हेल्प डेस्क की सेवाएँ कार्य दिवसों में सुबह 9:30 बजे से शाम 5:30 बजे तक उपलब्ध हैं.

ऑनलाइन खरीददारी और ई-निविदा जैसे प्रौद्योगिकी का लाभ उठाकर सार्वजनिक खरीद को बेहतर किया जा रहा है. जीईएम मानव लेनदेन दखल को कम करके भ्रष्टाचार को रोकने में सहायक होगा. जीईएम आसानी, दक्षता और पारदर्शिता के द्वारा प्रतियोगी कीमतों में वस्तुओं एवं सेवाओं को उपलब्ध कराने वाला एक दक्ष माध्यम है.

डिजिटल भुगतान पहल

नंदा सोमकुंवर
मुख्य प्रबंधक
स्टाफ प्रशिक्षण केन्द्र, पवई

भारत में सूचना प्रौद्योगिकी में तीव्र गति से हो रहा तकनीकी उन्नयन डिजिटल बैंकिंग उत्पादों के रूप में कई इनोवेशनों को लाया है. ये उत्पाद ग्राहकों की आवश्यकताओं के अनुसार कहीं भी और कभी भी बैंकिंग सुविधा प्रदान करने में सक्षम है. प्रत्येक बैंक ग्राहकों की सेवा और अधिक से अधिक नए ग्राहकों को जोड़ने के लिए अपने डिजिटल उत्पादों का विकास कर रहा है. मोबाइल के बढ़ते प्रयोग ने दूरस्थ इलाकों से संपर्क साधना भी आसान कर दिया है. देश में सुदूर ग्रामीण क्षेत्र, जहाँ बैंकिंग की पहुंच नहीं है, वहाँ मोबाइल पहुंच चुके हैं, इस तरह सूचना प्रौद्योगिकी के विकास ने भारतीय बैंकिंग क्षेत्र को अपने उत्पाद और सेवाओं को लोगों तक पहुँचाने के पर्याप्त अवसर प्रदान किए हैं. डिजिटल उत्पाद, बैंकिंग सेवाएँ प्रदान करने में लगने वाली परिचालन लागत को कम करने में एक महत्वपूर्ण भूमिका निभाते हैं, इसलिए इन उत्पादों को समग्र बैंकिंग क्षेत्र का समर्थन मिला है और सभी बैंक डिजिटल उत्पादों का उपयोग बढ़ाने हेतु प्रयासरत हैं, क्योंकि यह बैंकिंग क्षेत्र की प्रशासनिक प्रक्रियाओं को बेहतर बनाता है और लेन-देन की लागत को कम कर बैंकों की प्रतिस्पर्धी क्षमता को भी बढ़ाता है.

डिजिटल बैंकिंग

डिजिटल बैंकिंग का अर्थ प्रौद्योगिकी की सहायता से बैंकिग सुविधाओं को ग्राहकों तक पहुंचाना है. यह पारंपरिक शाखा बैंकिंग से अलग एक चलती-फिरती ऑनलाइन व्यवस्था है, जहां ग्राहक को अपने खाते से लेनदेन के लिए किसी बैंक की शाखा तक जाने की जरूरत नहीं होती बल्कि वह कंप्यूटर, लैपटॉप, टैबलेट, मोबाइल आदि इलेक्ट्रोनिक उपकरणों के माध्यम से किसी भी स्थान से, किसी भी समय अपने खाते से स्वयं लेनदेन कर सकता है. कोर बैंकिंग सॉल्यूशंस (सीबीएस) ने डिजिटल उत्पादों के प्रचलन को एक नई दिशा प्रदान की है. सीबीएस प्लेटफार्म बैंकिंग सेवाओं को तकनीकी माध्यम से दूरस्थ क्षेत्रों में अन्तर-बैंक लेनदेन को प्रभावी रुप से ग्राहकों तक पहुंचा पाया है. कोर बैंकिंग सॉल्यूशंस, एटीएम, इंटरनेट एवं मोबाइल बैंकिंग आदि की प्रगति ने उपभोक्ता अनुभव

में महत्वपूर्ण सुधार किए हैं, जिससे ग्राहकों का विशेष रूप से युवा ग्राहकों का पर्याप्त समर्थन मिला है.

डिजिटल भुगतान

डिजिटल भुगतान का अभिप्राय बैंक/ग्राहक द्वारा प्रौद्योगिकी का उपयोग कर इलेक्ट्रॉनिक संसाधनों के माध्यम से किए गए भुगतान से है, जिसमें आरटीजीएस/एनईएफ़टी और ऑनलाइन खुदरा/थोक भुगतान एनएसीएच, चेक ट्रंकेशन सिस्टम (सीटीएस), ईसीएस, डेबिट/क्रेडिट कार्ड, एटीएम, इंटरनेट बैंकिंग, मोबाइल बैंकिंग, आईएमपीएस आदि प्रमुख हैं और इनके द्वारा एक खाते से दूसरे खाते में लेनदेन आसानी से संभव हो सका है. प्रौद्योगिकी और दूरसंचार सुविधाओं के सुधार ने वैकल्पिक डिजिटल भुगतान को प्रोत्साहन दिया है. भारत सरकार और भारतीय रिज़र्व बैंक डिजिटल भुगतान को लोकप्रिय बनाने के लिए निरंतर प्रयासरत हैं. विमुद्रीकरण ने डिजिटल भुगतान को एक नई दिशा प्रदान की है. सरकार ने डिजिटल भुगतान को बढ़ावा देने हेतु कई उपाय किए हैं, जिसके कार्यान्वयन में नेशनल पेमेंट कॉर्पोरेशन ऑफ इंडिया (NPCI) ने अहम भूमिका निभाई है. रुपेकार्ड, आधार नंबर आधारित भुगतान, यूपीआई, भीम एप, यूएसएसडी *99#, भारत क्यूआर, बीबीपीएस, भीम आधार पे आदि के माध्यम से डिजिटल लेनदेन पर ज़ोर दिया जा रहा है, जिसका मुख्य उद्देश्य लोगों को डिजिटल लेनदेन के लिए प्रेरित करना है. आज डिजिटल पेमेंट के बहुतेरे विकल्प उपलब्ध हैं, ग्राहक अपनी आवश्यकता एवं सुविधानुसार लेनदेन हेतु बेहतर विकल्प चुन सकता है.

डिजिटल भुगतान की आवश्यकता

- उपभोक्ता का बदलता व्यवहार
- टेक्नोसेवी युवा ग्राहक वर्ग
- कम लागत पर बैंकिंग सेवाओं की उपलब्धता
- जनसाधारण तक पहुँचने का एक सशक्त माध्यम
- सूचना प्रौद्योगिकी का विकास एवं मोबाइल तथा स्मार्ट फोन का बढ़ता प्रयोग

डिजिटल भुगतान की विशेषताएं

- उपयोग में आसानी
- दूरस्थ पहुँच
- कम लागत

- 24*7 उपलब्धता
- स्वीकार्यता
- सरकारी प्रोत्साहन

यूनियन बैंक ऑफ इंडिया डिजिटल भुगतान के विकास कार्यक्रमों में हमेशा अग्रणी रहा है. वर्तमान में बैंक द्वारा समस्त लेनदेन के लगभग 75% लेनदेन इलेक्ट्रॉनिक साधनों के माध्यम से किए जा रहे हैं. डिजिटल भुगतान को बढ़ावा देने हेतु किए गए उपाय निम्न हैं :

चेक ट्रंकेशन सिस्टम (सीटीएस)

भारतीय रिजर्व बैंक ने सीटीएस को नई दिल्ली, चेन्नई और मुंबई में क्रमशः दि. 1 फरवरी, 2008, 24 सितंबर, 2011 और 27 अप्रैल, 2013 से लागू किया है. सीटीएस, समाशोधन परिचालन में चेक की डिजिटल इमेज स्कैन करके एक बैंक से दूसरे बैंक भेजने की प्रक्रिया है, जिसमें चेक भौतिक रूप से भेजने की आवश्यकता न होने से समाशोधन प्रक्रिया में लगने वाला समय कम हो गया है. पुष्टीकरण के पश्चात राशि खाते में तुरंत जमा की जाती है.

रियल टाइम ग्रास सेटेलमेंट (आरटीजीएस)/नेशनल इलेक्ट्रॉनिक फंड ट्रांसफर (एनईएफटी)

आरटीजीएस एक बैंक से दूसरे बैंक में धन प्रेषण का सबके तेज एवं लोकप्रिय साधन है, जिसके माध्यम से ₹ 2 लाख से अधिक की राशि का वास्तविक समय में एक साथ प्रेषण किया जाता है. यह किसी अन्य लेनदेन के साथ नहीं जुड़ा होता, इसलिए राशि अंतरण के निर्देशों का निपटान एक साथ होता है.

एनईएफटी आरटीजीएस की तरह ही बैंक खातों में धनराशि के हस्तांतरण की सुविधा प्रदान करता है, प्रेषण के न्यूनतम मूल्य पर कोई प्रतिबंध नहीं है. यह एक डिफर्ड नेट निपटान (डीएनएस) आधार पर संचालित व्यवस्था है, जो बैंकों के बीच आपसी लेनदेन का निपटान करता है. विशेष समय सीमा तक प्राप्त सभी लेनदेन का एक बैच में निपटान किया जाता है.

लाभार्थी के नाम, खाता संख्या, आईएफएससी कोड, बैंक और शाखा का नाम आदि की जानकारी देकर, नेट बैंकिंग सुविधा या बैंक शाखा के माध्यम से नाममात्र शुल्क पर सभी कार्य दिवसों पर सुबह 8.00 बजे से रात 7.00 बजे के बीच आरटीजीएस/एनईएफटी प्रेषण किया जा सकता है.

डेबिट /क्रेडिट कार्ड/ प्रीपेड कार्ड

डेबिट कार्ड एक ऐसा भुगतान उपकरण है, जिसमें ग्राहक के खाते से संबंधित महत्वपूर्ण जानकारी कार्ड की एम्बेडेड चिप में संग्रहित की जाती है, जिसे बैंक अपने खाता धारकों को जारी करते हैं तथा इसका उपयोग एटीएम से नकदी आहरण के साथ बैलेंस पूछताछ, फंड ट्रांसफर, मोबाइल रिचार्ज, टैक्स पेमेंट इत्यादि में किया जा सकता है. डेबिट कार्ड से पॉस मशीन और ऑनलाइन मोड सभी प्रकार के भुगतान किए जा सकते हैं. दुनिया भर में वीज़ा/मास्टरकार्ड/रुपे कार्ड लोगो प्रदर्शित करने वाले सभी एटीएम और व्यापारिक प्रतिष्ठानों में डेबिट कार्ड स्वीकार किए जाते हैं. यह डिजिटल भुगतान का सबसे प्रचलित उपकरण है. क्रेडिट कार्ड अपने खाताधारकों के अलावा अन्य व्यक्तियों या संस्थाओ को भी जारी किये जा सकते हैं. बैंक द्वारा ग्राहकों की आय के आधार पर क्रेडिट कार्ड के माध्यम से खर्च की सीमा निर्धारित की जाती है, जिसका विभिन्न निर्धारित तारीख पर भुगतान करना होता है. प्रीपेड कार्ड में राशि पहले ही जमा कर दी जाती है, जिसे ग्राहक कार्ड की परिपक्वता से पूर्व अपनी आवश्यकतानुसार खर्च करता है.

स्वचालित टेलर मशीन (एटीएम)

एटीएम एक ऐसी मशीन है, जो किसी शाखा प्रतिनिधि की सहायता के बिना ग्राहकों के नकद लेनदेन पूरा करती है. बैंकिंग में एटीएम के माध्यम से काफी विकास हुआ है. एटीएम अपने बैंक और अन्य बैंक कार्डधारकों को 24*7, जिसमें नकद लेनदेन के अलावा बैलेंस पूछताछ, मिनी-स्टेटमेंट इत्यादि शामिल हैं, की सुविधा प्रदान करता है,

एटीएम के माध्यम से निम्नलिखित सुविधाएं प्रदान की जाती हैं

- नकदी जमा/निकासी
- ग्रीन पिन जनरेशन और व्यक्तिगत पहचान संख्या (पिन) में परिवर्तन
- चेकबुक के लिए अनुरोध
- मिनी स्टेटमेंट
- बैलेंस पूछताछ
- इंटर बैंक फंड ट्रांसफर - आईएमपीएस के माध्यम से फंड ट्रांसफर
- मोबाइल रिचार्ज, टेलीफोन बिल इत्यादि का भुगतान
- खुदरा उत्पादों की जानकारी
- खातों से आधार नंबर जोड़ना
- ई-कैश विकल्प का उपयोग कर मोबाइल नंबर पर फंड ट्रांसफर

- कार्ड से कार्ड में भुगतान
- पीएमजेडीवाई खातों में एटीएम के माध्यम से ओवरड्राफ्ट आवेदन
- खुदरा ऋण और बचत खाते की लीड जनरेशन

माइक्रो एटीएम (पॉस)

माइक्रो एटीएम एक ऐसा उपकरण है, जिसका उपयोग बैंक मित्रों द्वारा मूल बैंकिंग सेवाओं को प्रदान करने के लिए किया जाता है. यह कम बिजली का उपयोग कर जीपीआरएस के माध्यम से केन्द्रीय बैंकिंग सर्वर से जुड़ता है, जिससे परिचालन लागत काफी कम हो जाती है. माइक्रो एटीएम ग्रामीण जनता को बैंकिंग की मूल सेवाओं को काफी प्रभावी तरीके से उपलब्ध कराता है. बैंक मित्रों द्वारा इसका उपयोग वित्तीय समावेशन में मील का पत्थर साबित हुआ है. प्रारम्भ से अभी तक माइक्रो एटीएम बैंक मित्रों का अभिन्न अंग बनता जा रहा है. देश में वित्तीय समावेशन को और अधिक मजबूती प्रदान करने के लिए सरकार ने बैंकों को ग्रामीण क्षेत्रों में अधिकाधिक माइक्रो एटीएम स्थापित करने की सलाह दी है, जिसके परिणामस्वरूप देश में मार्च 2018 तक 1.15 लाख माइक्रो एटीएम प्रचलन में हैं.

कैश रीसाइक्लिंग मशीन (सीआरएम)

यह मशीन ग्राहक के खाते से नकदी भुगतान के साथ खाते में नकदी जमा करने की सुविधा भी प्रदान करती है. मशीन लेनदेन को संसाधित करने से पहले नकली नोटों की गणना और पहचान करने में भी यह सक्षम है. सीआरएम ₹50, ₹100, ₹500 और ₹2000 मूल्यवर्ग के साथ ₹200 के नोटों को स्वीकार करने और वितरण करने में सक्षम है. सीआरएम द्वारा एनएफएस सदस्य बैंक के कार्डधारकों को नकदी जमा और निकासी की अनुमति है.

भारतीय रिज़र्व बैंक ने एटीएम नीतियों का उदारीकरण कर एटीएम नेटवर्क के विस्तार करने के लिए गैर-बैंकिंग संस्थाओं को एटीएम शुरू करने की अनुमति दी है, जिसे 'व्हाइट लेवल एटीएम' कहा जाता है. व्हाइट लेवेल एटीएम का संचालन एवं स्वामित्व दोनों ही गैर-बैंकिंग संस्थाओं के पास है.

इंटरनेट बैंकिंग

इंटरनेट बैंकिंग सुविधा ग्राहकों को विभिन्न लेनदेन करने में सक्षम बनाती है, जैसे उत्पादों और सेवाओं का भुगतान, धन प्रेषण, कर भुगतान आदि के साथ-साथ ग्राहक अपने विभिन्न खातों को किसी भी समय देख सकते हैं. इंटरनेट बैंकिंग में उपलब्ध सुविधाएं निम्न हैं :

- विभिन्न जमा और ऋण उत्पादों के संबंध में जानकारी
- विभिन्न जमाओं के साथ-साथ ग्राहक के ऋण खातों की जानकारी
- भुगतान रोकने के ऑनलाइन निर्देश स्वीकार करना
- एक खाते से अपने दूसरे खाते या किसी तीसरे पक्ष के खाते में धन का प्रेषण
- टेलीफोन, बिजली बिलों का ऑनलाइन भुगतान
- ऑनलाइन रेलवे टिकट एवं एयर टिकट बुकिंग की सुविधा
- चेकबुक आवेदन स्वीकार करना, एफडी खोलना, एफडीआर/एसडीआर नवीनीकरण
- ऑनलाइन आरटीजीएस/एनईएफटी फंड अंतरण
- ऑनलाइन कर भुगतान

मोबाइल बैंकिंग

भारत में सूचना प्रौद्योगिकी में तेज विकास के साथ मोबाइल उपयोग में भी तेजी से वृद्धि देखी जा रही है. आज देश की 70% से अधिक आबादी के पास मोबाइल फोन है जिसमें ग्रामीण आबादी का एक बड़ा हिस्सा शामिल है. मोबाइल फोन के बढ़ते चलन ने जहां एक ओर बैंकों को दूरस्थ ग्रामीण क्षेत्रों तक बैंकिंग और भुगतान सेवाओं को पहुंचने के अवसर प्रदान किए हैं, वहीं दूसरी ओर उपयोगकर्ताओं ने भी इसके मूल्य, सुविधा और आसानी को समझकर औपचारिक अर्थव्यवस्था से जुड़ना शुरू कर दिया है. बैंक खाते से मोबाइल नंबर को जोड़ने और मोबाइल बैंकिंग सेवा शुरू करने हेतु पंजीकरण करने के बाद उपयोगकर्ता स्वयं ही खाते से लेनदेन कर सकता है. मोबाइल बैंकिंग बैंक द्वारा प्रदान की जाने वाली एक ऐसी सेवा है, जो ग्राहक को मोबाइल फोन या टैबलेट का उपयोग करके वित्तीय लेनदेन करने में सक्षम बनाती है. ग्राहक एसएमएस, यूएसएसडी, जीपीआरएस के माध्यम से मोबाइल बैंकिंग सेवा का लाभ उठा सकते हैं.

बैंक ग्राहकों को भुगतान हेतु एसएमएस, यूएसएसडी, मोबाइल बैंकिंग एप्लिकेशन (यूमोबाइल) इत्यादि मोबाइल बैंकिंग चैनल प्रदान करता है. यूमोबाइल ग्राहकों को कभी भी कहीं से भी बैंकिंग का एक सुरक्षित और सुविधाजनक माध्यम प्रदान करता है, जिसमें बैलेंस पूछताछ, मिनी स्टेटमेंट, पंजीकृत ग्राहकों के बीच यूनियन बैंक में किसी भी खाते में फंड ट्रांसफर अन्य बैंकों में फंड ट्रांसफर (एनईएफटी), तत्काल भुगतान सेवा (आईएमपीएस) मोबाइल से मोबाइल, मोबाइल से खाते, मोबाइल से आधार नंबर, ई-कैश, मोबाइल रिचार्ज, बिल पे आदि प्रमुख हैं. इसके अलावा, मोबाइल बैंकिंग सेवा में डेबिट कार्ड संबंधित लेनदेनों को नियंत्रित करने, चेक का भुगतान रोकने, चेक की

स्थिति जानने, चेक बुक के लिए बैंक से अनुरोध करने तथा आधार लिंकिंग की सुविधा भी उपलब्ध है.

आईएमपीएस (तत्काल भुगतान सेवा)

डिजिटल भुगतान में मोबाइल का प्रयोग बढ़ाने के लिए नेशनल पेमेंट्स कॉर्पोरेशन ऑफ इंडिया(एनपीसीआई) द्वारा वर्ष 2010 में आईएमपीएस आरंभ किया गया. बाद में, आईएमपीएस को तत्काल भुगतान सेवा के रूप में सक्षम किया गया. एनपीसीआई यह सुविधा अपने मौजूदा एनएफएस स्विच के माध्यम से प्रदान करता है. आईएमपीएस ग्राहकों के मोबाइल उपकरणों को धन प्रेषण के एक चैनल के रूप में उपयोग करने में सक्षम बनाता है, जिससे ग्राहक अपने खाते से किसी अन्य बैंक खातों में तुरंत राशि भेज सकता है. आईएमपीएस मोबाइल फोन के माध्यम से तत्काल, 24*7, इंटरबैंक इलेक्ट्रॉनिक फंड ट्रांसफर सेवा प्रदान करता है. यह बैंकों के भीतर तुरंत धन प्रेषण करने के लिए एक शक्तिशाली उपकरण है, जिसके माध्यम से ₹2 लाख तक की राशि का तुरंत भुगतान किया जा सकता है. लेनदेन की शुरुआत के लिए मोबाइल मनी आइडेंटिफायर (एमएमआईडी) और मोबाइल बैंकिंग पिन (एमपीएन) की जरूरत होती है. एमएमआईडी 7 अंकों का नंबर है, जिसे बैंक द्वारा पंजीकरण के समय जारी किया जाता है. मोबाइल, इंटरनेट बैंकिंग, बैंक शाखा और एटीएम के माध्यम से आईएमपीएस सेवा से निम्नलिखित तरीकों से भुगतान किया जा सकता है :

- मोबाइल द्वारा एमएमआईडी (मोबाइल मनी आइडेंटिफायर)) का उपयोग कर
- खाता संख्या और आईएफएस कोड का उपयोग कर
- आधार संख्या के माध्यम से

यूएसएसडी * 99 #

एनपीसीआई द्वारा पीएमजेडीवाई के एक हिस्से के रूप में *99# सेवा शुरू की गई है, जिसमें आम आदमी को बैंकिंग सेवाएं प्रदान करने के लिए तथा कम मूल्य वाले प्रेषण के लिए बेसिक मोबाईल पर भी बैंकिंग सुविधाओं की उपलब्धता की संभावना और आवश्यकता पर विचार किया गया. ग्राहक अपने मोबाइल फोन पर *99# डायल करके मोबाइल पर प्रदर्शित एक इंटरैक्टिव मेनू के माध्यम से लेनदेन कर इस सेवा का लाभ उठा सकते हैं. *99# यूएसएसडी मूल्य वर्धित सेवा है, जो एसएमएस आधारित मोबाइल बैंकिंग सेवा के माध्यम से ग्राहकों को बैंक खाते से निधि अंतरण, बैलेंस राशि की जानकारी, मिनी स्टेटमेंट, आधार संख्या लिंकिंग की स्थिति की जांच आदि सुविधा प्रदान करती है. यूएसएसडी सभी जीएसएम हैंडसेट पर काम करता है और इसे एक बहुत ही बुनियादी हैंडसेट से एक्सेस किया जा सकता है.

ई-वॉलेट क्या है?

ई-वॉलेट एक प्रकार का वर्चुअल कार्ड है, जिसका उपयोग ई-वॉलेट एप मोबाइल बैंकिंग के अन्य तरीकों की तरह ही भुगतान के लिए किया जाता है. ई-वॉलेट में पहले राशि जमा जाती की जाती है तथा बाद में इसे आवश्यकता अनुसार भुगतान किया जाता है. ई-वॉलेट का मुख्य उद्देश्य कागज़ रहित भुगतान को अधिक आसान बनाना है. हमारे बैंक द्वारा डिजीपर्स नामक ई-वॉलेट चालू किया गया, जिसमें प्रतिमाह 10000 रुपये तक की राशि जमा/भुगतान कर सकते हैं.

एकीकृत भुगतान इंटरफेस या यूपीआई (UPI)

यूपीआई नेशनल पेमेंट्स कॉर्पोरेशन ऑफ इंडिया(एनपीसीआई) द्वारा नकद रहित अर्थव्यवस्था में भुगतान को सरल बनाने के उद्देश्य के विकसित की गयी एक ऐसी प्रणाली है, जो विभिन्न बैंकों के खातों से एक ही मोबाइल एप्लिकेशन के द्वारा सहज रूप से फण्ड मंगाने एवं भुगतान की सुविधा उपलब्ध कराती है. यूपीआई एक भुगतान प्रणाली है, जो आईएमपीएस भुगतान ढांचे का उपयोग कर ग्राहक को बैंक खाते या आईएफएससी कोड के बिना उसी बैंक या अन्य बैंकों के ग्राहकों को तत्काल धन अंतरण करने की अनुमति देती है. लाभार्थी को प्रेषक की खाता संख्या और आईएफएससी कोड को उजागर करने की आवश्यकता नहीं है और केवल वर्चुअल पता जैसे xxxx @ unionbank या xxxx @ axis देने पर राशि निर्बाध रूप से भेजी जा सकती है. उपयोगकर्ता एक ही एप पर अन्य बैंक के खाते भी जोड़ सकता है और एक ही खाते के लिए एकाधिक वर्चुअल पते भी बना सकता है. इस एप की सहायता से ग्राहक आसानी से लेन-देन कर सकते हैं, भीम उपयोगकर्ताओं और व्यापारियों को सीधे अपने अलग-अलग बैंक के खाते से लिंक करने की सुविधा प्रदान करता है.

यूपीआई के लाभः

- यूपीआई के माध्यम से राशि प्रेषण के साथ-साथ राशि प्राप्त भी की जा सकती है
- वर्चुअल पता, खाता संख्या या आधार संख्या का उपयोग करके धन प्रेषण किया जा सकता है
- खाता संख्या याद रखने या शेयर करने की कोई आवश्यकता नहीं है
- फंड का वास्तविक समय पर निपटान
- एक ही एप में एकाधिक बैंकों के खाते जोड़े जा सकते हैं
- एप के माध्यम से ही लेनदेन की स्थिति की जांच करने और विवाद/शिकायत करने की सुविधा

भारत इंटरफेस फॉर मनी (भीम)

नकद रहित अर्थव्यवस्था में होने वाले बदलाव के साथ भुगतान के तरीकों को अत्यंत सरल बनाने की दिशा में नेशनल पेमेंट्स कॉर्पोरेशन ऑफ इंडिया (एनपीसीआई) के माध्यम से सरकार द्वारा की गई पहल के रूप में भीम एप आरंभ किया गया था. शुरुआत से ही भीम डिजिटल भुगतान में एक बड़े योगदानकर्ता के रूप में उभरा है, भीम ने इंटरऑपरेबिलिटी के साथ उपयोगकर्ता को एकीकृत भुगतान में एक आधारभूत संरचना प्रदान की है. यूपीआई की तरह भीम भी आईएमपीएस प्लैटफॉर्म का उपयोग कर खाता संख्या, आईएफएससी कोड और नाम शेयर किए बिना, मोबाइल नंबर या वर्चुअल पेमेंट एड्रेस पर पैसे भेजने और एकत्र करने का एक आसान और तत्काल तरीका प्रदान करता है. भीम उपयोगकर्ता को उनके यूपीआई सक्षम बैंक खाते से किसी को भी वीपीए (वर्चुअल पेमेंट एड्रेस) या यूपीआई सक्षम मोबाइल नंबर पर पैसा भेजने एवं पैसे का अनुरोध करने की सेवा प्रदान करता है. लाभार्थी का मोबाइल नंबर बैंक के साथ पंजीकृत नहीं होने की स्थिति में खाता संख्या और आईएफएससी या आधार का उपयोग करके लाभार्थी को पैसा भेजा जा सकता है. भीम एप में पहले से एक अंतर्निहित क्यूआर कोड स्कैनर है, जिससे लाभार्थी के यूपीआई क्यूआर कोड स्कैन करके भुगतान कर सकता है, इसी तरह उपयोगकर्ता क्यूआर कोड जनरेट कर अपना वीपीए या मोबाइल नंबर शेयर किए बिना क्यूआर कोड पर भुगतान प्राप्त कर सकता है. यह सुविधा व्यापारियों के लिए विशेष रूप से उपयोगी है.

भीम आधार पे

व्यापारियों के भुगतान तरीकों में सरलता प्रदान करने के उद्देश्य से भारत सरकार ने भीम-आधार पे मोबाइल एप आरंभ किया है. यह सुविधा देश के उन सभी व्यापारियों के लिए उपलब्ध है, जिनके बैंक खाते आधार नंबर से जुड़े हैं. इसके माध्यम से लेनदेन पूरा करने के लिए आधार संख्या और बायोमेट्रिक फिंगरप्रिंट लिंक करना आवश्यक है. यह व्यापारी को एंड्रॉइड आधारित मोबाइल डिवाइस का उपयोग करके आधार पे आवेदन में मान्य प्रमाण-पत्रों के साथ साइन-इन करने में सक्षम बनाता है. भीम आधार पे सॉफ्टवेयर और हार्डवेयर डिवाइस का एक संयोजन है, जो व्यापारी को अपने मोबाइल फोन की मदद से आधार आधारित बायोमेट्रिक प्रमाणीकरण के माध्यम से अपने ग्राहक से वस्तुओं और सेवाओं के लिए भुगतान को स्वीकार करने की सुविधा देता है. पंजीकृत व्यापारियों को सत्यापित और सक्रिय करने के लिए IPay पोर्टल का उपयोग किया जाता है. भीम आधार पे के माध्यम से लेनदेन को सक्षम करने के लिए व्यापारियों को फिंगरप्रिंट स्कैनर की आवश्यकता होती है. व्यापारी खाते में लेनदेन का निपटारा वास्तविक समय में किया जाता है और व्यापारी तुरंत क्रेडिट प्राप्त करते हैं. यूनियन बैंक

लंबे समय से प्वाइंट ऑफ टर्मिनल के माध्यम से व्यापारी अधिग्रहण के कारोबार में रहा है और इस व्यवसाय के तहत कई व्यापारियों को अधिग्रहित किया गया है तथा भीम आधार एप के उपयोग से व्यापारी अधिग्रहण के कारोबार में और वृद्धि की संभावना है.

आधार कार्ड

आधार भारत सरकार द्वारा चलाई गयी महत्वाकांक्षी परियोजना है, जिसके अंतर्गत प्रत्येक नागरिक को उसकी डेमोग्राफिक एवं बायोमेट्रिक जानकारी के आधार पर 12 अंको का पहचान कार्ड जारी किया जाता है. यूआईडीएआई डेटाबेस में संग्रहीत सूचनाओं के आधार पर व्यक्ति की पहचान को ऑनलाइन अधिप्रमाणीकरण सेवाएं प्रदान करता है, जो सम्पूर्ण देश में समान रूप से मान्य है. ग्रामीण तथा पिछड़े वर्ग की पहचान के लिए यह अत्यंत महत्वपूर्ण है, जो उन्हें सरकारी सुविधाओं का लाभ प्राप्त करने में मदद करता है. इस योजना को केंद्र और राज्य सरकार निकायों की सामाजिक सुरक्षा पेंशन योजना, विकलांगता पेंशन आदि के भुगतान के लिए शुरू किया गया है. इस योजना के तहत बैंक खाता एवं यूआईडीएआई द्वारा आधार संख्या प्रमाणीकरण के बाद लाभार्थी को मिलने वाले प्रत्यक्ष लाभ की राशि सीधे लाभार्थी के बैंक खातों में अंतरित की जाती है, जिससे सब्सिडी का लाभ सीधे वास्तविक हितग्राही तक पहुंचना सुनिश्चित हुआ है.

आधार एनेबल्ड पेमेंट सिस्टम (एईपीएस) :

एईपीएस एक भुगतान सेवा है, जो बैंक ग्राहक को अपने आधारकार्ड संबंधी पहचान के आधार पर बैंक मित्र (बीसी) की सहायता से पॉस (माइक्रो एटीएम) पर बैंक-से-बैंक लेनदेन की सुविधा प्रदान करती है. बैंक खाता से आधार को लिंक करने के बाद एईपीएस से फंड ट्रांसफर, बैलेंस इंक्वायरी, कैश डिपॉजिट या कैश निकालने जैसी सेवाएं प्रदान की जा सकती हैं. एईपीएस की मदद से मोबाइल फोन उपयोगकर्ता अपने आधार नंबर और फिंगरप्रिंट के जरिए कार्ड-रहित और पिन-रहित डिजिटल लेनदेन करते हैं. आधार सेवाओं से डिजिटल लेनदेन को बहुत बल मिला है. जो ग्राहक डेबिट कार्ड का उपयोग करते हैं, उन लोगों के लिए एनपीसीआई एवं यूआईडीएआई द्वारा प्रस्तुत आधार आधारित लेनदेन एक वरदान साबित हुआ है. देश भर के सभी ग्रामीण ग्राहक सूक्ष्म एटीएम, मोबाइल एवं कम्प्यूटर की मदद से करीब 40 से 70 प्रतिशत लेनदेन बैंक मित्रों के पास उपलब्ध एईपीएस के माध्यम से कर रहे हैं. देश में 80 प्रतिशत से अधिक खातों को आधार से जोड़ा जा चुका है तथा एईपीएस तकनीक द्वारा लेनदेन त्वरित गति से बढ़ता ही जा रहा है.

भारत क्यूआर

भारतीय रिज़र्व बैंक (आरबीआई) के निर्देशों के तहत मास्टरकार्ड, वीज़ा और अमेरिकन एक्सप्रेस के साथ रुपे कार्ड के माध्यम से संयुक्त रूप से डिजिटल भुगतान सक्षम करने के लिए एनपीसीआई ने भारत क्यूआर विकसित किया है. यह एक प्रौद्योगिकी मंच है, जो मोबाइल फोन के माध्यम से बड़े पैमाने पर ग्राहकों को बैंकिंग सेवाएं प्रदान करने के लिए बैंकों और टीएसपी (दूरसंचार सेवा प्रदाता) को एक दूसरे के साथ सहजता से एकीकृत करता है.

बीबीपीएस

बीबीपीएस भारतीय रिजर्व बैंक की भुगतान प्रणाली है, जो ग्राहकों को बिल भुगतान में सहायता प्रदान करेगा. यह बैंकों और गैर-बैंकिंग ईकाइयों को जोड़ने वाला एकीकृत मंच है, जो बिजली, पानी, गैस, टेलीफोन और डीटीएच जैसी उपयोगी सेवाओं के बिल भुगतान को कवर करता है. एनपीसीआई अधिकृत भारत बिल भुगतान केंद्रीय इकाई (बीबीपीसीयू) के रूप में कार्य करता है, जो समाशोधन करेगा. लेनदेन से संबंधित गतिविधियों के निपटान के लिए आरबीआई ने बीबीपीओयू को अधिकृत किया है, जो एजेंटों के नेटवर्क के माध्यम से ग्राहकों को तत्काल और सुलभ बिल भुगतान सेवाएं प्रदान करता है तथा भुगतान की पुष्टि प्रदान करता है. बीबीपीसीयू का भुगतान प्रणाली परिप्रेक्ष्य से आर्थिक रूप से किसी लेनदेन का स्वामित्व नहीं होगा, बल्कि विभिन्न ऑपरेटिंग इकाइयों के माध्यम से इसे कई बिलर्स और एजेंटों को जोड़ने के लिए केवल एक माध्यम के रूप में कार्य करना होगा. यह मानकों को स्थापित करने और पूरे आर्थिक तंत्र के लिए लेनदेन सुरक्षा सुनिश्चित करने के अलावा, ग्राहकों द्वारा उठाए गए प्रश्न, अनुरोध और शिकायतों पर निगरानी और समाधान करना भी सुनिश्चित करेगा.

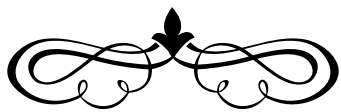
डिजिटल भुगतान प्रोत्साहन हेतु किए गए प्रयास

डिजिटल भुगतान को बढ़ावा देने के लिए बैंकों के साथ सरकार द्वारा भी कई उपाय किए गए हैं, जिसमें एनपीसीआई ने विभिन्न बैंकों के बीच अंतःक्रियात्मक लेनदेन की सुविधा के लिए विभिन्न डिजिटल उत्पादों का विकास कर नकदी लेनदेन को कम करने में महत्वपूर्ण भूमिका निभाई है. इलेक्ट्रॉनिक टोल संग्रह (ईटीसी) टैग आधारित टोल भुगतान है, जो वाहनों को टोल गेट्स के माध्यम से स्वतंत्र रूप से आवाजाही करने में सक्षम बनाता है. एनपीसीआई ने एनसीएमसी लॉन्च करने की योजना बनाई है, जिसका उपयोग सभी महानगरों, बसों और उपनगरीय रेलगाड़ियों में एक अंतःक्रियात्मक तरीके से किया जा सकता है. इसी तरह ग्रामीण इलाकों में डिजिटल भुगतान को आसान बनाने के लिए गावों में पॉस मशीनें लगाने हेतु नाबार्ड की मदद से बैंकों को आर्थिक सहायता दी

जाती है. ये पॉस मशीनें को-ऑपरेटिव सोसायटी/दुग्ध सोसायटी/कृषि से जुड़ा सामान बेचने वाले डीलरों के पास लगाई जाएंगी, ताकि गांवों में खेती से जुड़ी जरूरतों के लिए डिजिटल तरीके से लेन-देन हो सके. इसी तरह रेलवे में ऑनलाइन टिकट बुक कराने वालों को मुफ्त दुर्घटना बीमा, रेलवे नेटवर्क में मासिक और सीजन टिकट के लिए डिजिटल तरीके से भुगतान करने वालों को छूट, सार्वजनिक क्षेत्र की बीमा कंपनियों को कस्टमर पोर्टल के जरिए डिजिटल पेमेंट किए जाने पर प्रीमियम में डिस्काउंट, डिजिटल तरीके से ₹2000 तक भुगतान करने पर ट्रांजेक्शन फीस या एमडीआर चार्ज ग्राहकों से न वसूलना, निजी उपभोग पर किए जाने व्यय का भुगतान डिजिटल माध्यमों का प्रयोग करने वाले व्यापारियों तथा उपभोक्ताओं को नकद पुरस्कार देने की लक्की ग्राहक योजना आदि प्रमुख हैं, जिनका लक्ष्य गरीब, निम्न मध्यम वर्ग और छोटे व्यापारियों को डिजिटल भुगतान के दायरे में लाना तथा डिजिटल लेनदेन को प्रोत्साहित करना है, जिससे कि समाज के सभी वर्ग, विशेष रूप से गरीब और मध्यम वर्ग इलेक्ट्रॉनिक भुगतानों को अपना सकें.

यूनियन बैंक ऑफ इंडिया द्वारा डिजिटल भुगतान हेतु सरकारी योजनाओं में तथा एनपीसीआई द्वारा किए गए विभिन्न डिजिटल उत्पादों के उपयोग में सक्रिय सहभागिता द्वारा नकदी विहीन अर्थव्यवस्था की दिशा में अपना महत्वपूर्ण योगदान दिया जा रहा है.

डिजिटल भुगतान के विभिन्न तरीकों ने जहां एक ओर बैंकिंग सेवा प्रदान करने में लगने वाले समय तथा लागत को कम कर दिया है तथा लोगों का जीवन आसान बना दिया है, वहीं दूसरी ओर भुगतान के इन तरीकों ने साइबर जोखिम को भी बढ़ा दिया है. जरा सी लापरवाही ग्राहक और बैंकों को भारी नुकसान पहुंचा सकती है. अतः उपयोगकर्ता को डिजिटल भुगतान के तरीकों के साथ साइबर सुरक्षा संबंधित जानकारी देना भी आवश्यक है.



ई-कॉमर्स

डिम्पल कौर
सहायक प्रबन्धक
क्षे. का. आगरा

आजकल लोग प्राचीन तरीकों को बहुत कम अपनाते हैं. पुराने तरीकों से काम बहुत अधिक समय में होता है लेकिन आधुनिक तरीकों से काम बहुत जल्दी हो जाता है. ऐसे ही कुछ आधुनिक तरीकों में से एक 'ई-कॉमर्स' है. ई-कॉमर्स का अर्थ होता है "ईलेक्ट्रॉनिक कॉमर्स" या हम कह सकते हैं कि इंटरनेट द्वारा व्यापार करना. ई-कॉमर्स के अंतर्गत वस्तुओं या सेवाओं की खरीद या बिक्री "ईलेक्ट्रॉनिक कॉमर्स" जैसे - इंटरनेट के माध्यम से की जाती है. ई-कॉमर्स में कंपनियाँ इंटरनेट पर स्टोर स्थापित करती हैं और उपयोगकर्ता इंटरफेस प्रदान करती हैं, जिस पर व्यापारिक वस्तुओं की खरीद और बिक्री की अनुमति होती है. विक्रेताओं और क्रेताओं के बीच कोई भौतिक संपर्क नहीं होता है. यह एक ऐसा क्षेत्र है जिसके माध्यम से, ग्राहकों को सुविधाएं देकर उनसे आर्थिक मूल्य लिया जाता है तथा इसमें सीधे धन का आदान प्रदान नहीं होता है. 'ई-कॉमर्स' ग्राहकों की मांग को पूरा करने और लेन-देन को व्यवस्थित करने के लिए प्रौद्योगिकी का उपयोग करता है. इस व्यवसाय के मॉडल में किसी व्यापारी को, भौतिक आधार की जरूरत नहीं है. आज के समय में, इंटरनेट के व्यापार में, बहुत तेजी से वृद्धि हो रही है. सन् 1998 में इस मीडिया से लगभग 43 अरब डॉलर का व्यापार हुआ था. इसका जाल आज बहुत तेजी से फैल रहा है. ई-कॉमर्स उपभोक्ताओं को समय और दूरी संबंधी कई बाधाओं के बावजूद वस्तुओं और सेवाओं को, इलेक्ट्रॉनिक रूप से, आदान-प्रदान करने की अनुमति देता है.

ई-कॉमर्स की शुरुआत 1960 के दशक से हुई थी, जब संस्थाओं ने अन्य कंपनियों के साथ बिजनेस डॉक्यूमेंट को शेयर करने के लिए इलेक्ट्रॉनिक् डाटा इंटरचेंज का प्रयोग शुरू किया था. 1979 में, अमेरीकन नेशनल स्टैंडर्ड इंस्टीट्यूट ने ASCX12 को इलेक्ट्रॉनिक नेटवर्क के माध्यम से डाक्यूमेंट को आपस में शेयर करने के लिए, एक यूनिवर्सल स्टैंडर्ड के रूप में विकसित किया था. ई-कॉमर्स के इतिहास को, ई-बे (ebay) और अमेजन (Amazon) के बिना सोचना असंभव है, जो इलेक्ट्रॉनिक ट्रांज़ैक्शन को शुरू करने वाली पहली इंटरनेट कंपनियों में से थे. 1990 के दशक में ebay और amazon के उदय से ई-कॉमर्स उद्योग में क्रांतिकारी बदलाव आया था.

कार्य-प्रणाली : ई-कॉमर्स की व्यापार प्रणाली बहुत ही सरल होती है. अगर कोई व्यापारी, कुछ खरीदना चाहता है तो वह वेबसाइट से व्यापारी के इलेक्ट्रॉनिक स्टोर में से उत्पादों को चुन लेता है. उस समय वह ऑर्डर फॉर्म को भर देता है. चीज़ों का चुनाव करने के बाद साइट में हरकत होती है और वह खरीददार के अकाउंट की सूचना देता है. साइट से 'खरीदने और बेचने' वाले की सुरक्षा और प्रामाणिकता का मापदंड होता है. यह संदेश को सुरक्षित भेजने के लिए गुप्त संदेश की विधि को अपनाता है. जब बेचने वाले को ऑर्डर मिल जाता है तो वह खरीददार के बैंक को कीमत देने के लिए इज़ाजत दे देता है. जब उसे इसकी स्वीकृति मिल जाती है तो वह कार्डधारक को इसकी पुष्टि की खबर देने के बाद माल भेज देता है.

प्रकार : ई-कॉमर्स कुल छः प्रकार के होते हैं:

1. **बिजनेस टू कंज्यूमर - बी टू सी {(Business to Consumer (B2C)} :** यह सबसे ज्यादा प्रचलित ई-कॉमर्स का प्रकार है. यहाँ पर विक्रेता अपने उत्पादों को वेबसाइट पर डालता है, जहां से ग्राहक सीधे खरीद सकते हैं. इसमें किसी डिस्ट्रीब्यूटर की जरूरत नहीं होती है. जैसे - फ्लिपकार्ट (Flipkart) व अमेजन (Amazon) आदि.

2. **बिजनेस टू बिजनेस (बी टू बी) (Business to Business (B2B)) :** इसके अंतर्गत एक संस्था अपने उत्पादों को दूसरी संस्थाओं को बेचती है. जैसे manufacturer अपना सामान wholesaler को बेचता है और होलसेलर (थोक विक्रेता) अपना सामान अंतिम विक्रेताओं को बेचता है.

3. **कंज़्यूमर टू बिजनेस (सी टू बी) {Consumer to Business (C2B)} :** इसमें ग्राहक अपने उत्पादों या सर्विस को कंपनी को बेचता है. जैसेः आप अपने ग्राफिक्स को डिज़ाइन करके कुछ कंपनियों जैसेः fiverr तथा freelancer वेबसाइटस के माध्यम से बेच सकते हैं.

4. **कंज़्यूमर टू कंज़्यूमर (सीटूसी) {Consumer to Consumer (C2C)} :** इस माध्यम के अंतर्गत एक कस्टमर दूसरे कस्टमर को अपना सामान बेचता है. जैसे ओएलएक्स (OLX) व क्विकर (quicker) आदि.

5. **बिजनेस टू एडमिनिस्ट्रेशन (बी टू ए) {(Business to Administration (B2A)}:** इसमें बिजनेस संस्था तथा सरकारी एजेंसियों (government agency) की वेबसाईटों के द्वारा सूचनाओं का आदान-प्रदान किया जाता हैं.

6. **कंज़्यूमर टू एडमिनिस्ट्रेशन (सीटूए) {Consumer to Administration (C2A)) :** इसमें कस्टमर तथा सरकारी एजेंसियों (government agency) के मध्य सूचनाओं का आदान प्रदान वेबसाईट के माध्यम से होता हैः

लाभ : ई-कॉमर्स के कुछ लाभ निम्न हैं:

1. उत्पाद एवं मूल्य की तुलना कर सकते हैं.
2. तुरंत भुगतान विकल्प
3. नकदी की जरूरत नहीं
4. देश तथा विदेश में खरीददारी के विकल्प
5. विभिन्न कंपनी के उत्पादों की एक जगह 24*7 उपलब्धता
6. बेहतर सुविधा उपलब्ध कराना
7. आसान फंड स्थापना (निधियों का निर्माण) शुरुआती उपक्रमों के लिए.

हानियाँ : ई-कॉमर्स की कुछ हानियाँ निम्न हैं:

1. इन्टरनेट की जानकारी आवश्यक है.
2. नई वेबसाईटों पर भरोसा नहीं कर सकते
3. बदलते प्रतियोगी वातावरण में उपयुक्त नहीं
4. इंटरनेट स्कैम का खतरा
5. आवेग में खरीद
6. बिक्री के बाद समर्थन का अभाव
7. मानवीय मूल्यों एवं व्यक्तिगत भावनाओं की कमी

उल्लेखनीय है कि भारत सरकार विदेश के बाज़ारों की क्षमता पर नकारात्मक प्रभाव डालने के उद्देश्य से ई-कॉमर्स क्षेत्र का विस्तार करने हेतु एक नई नीति पर कार्य कर रही है. इस पहल की शुरुआत, ट्रिलियन डॉलर की अर्थव्यवस्था बनने के लक्ष्य को प्राप्त करने के लिए की जा रही है.

प्रमुख बिन्दु :

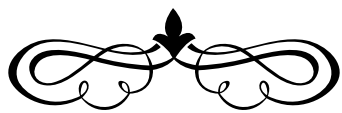
1. हमारा देश ई-कॉमर्स का विस्तार करने हेतु एक नीतिगत ढांचे तैयार कर रहा है. इसके निम्न दो पहलू होंगे- देश के अंदर ही ई-कॉमर्स के विस्तार को बढ़ावा देना व ई-कॉमर्स का विस्तार देश के बाहर करना. तात्पर्य यह है कि भारत की 'ई-कॉमर्स अर्थव्यवस्था' सीमापारीय भी होनी चाहिए तथा इसे विदेशी बाज़ारों से भी पूंजी का सृजन करना चाहिए.

2. वर्तमान में, भारत का ई-कॉमर्स बाज़ार 30 बिलियन डॉलर का है और सरकार यह अपेक्षा रखती है कि वर्ष 2024-25 तक यह लगभग 150 बिलियन डॉलर का हो जाएगा.

3. मंत्रालय के अनुसार, देश में डिजिटल अर्थव्यवस्था की शुरुआत, वर्ष 2024-25 तक लगभग, 30 मिलियन लोगों के लिए रोजगार का सृजन करने के उद्देश्य से की गई थी.

4. भारत में 'ई-कॉमर्स' अभूतपूर्व दर से बढ़ रहा है, जो हर महीने लगभग छः मिलियन नए सदस्यों को जोड़ता है. एक अनुमान के अनुसार इस वित्त वर्ष में भारत के ई-कॉमर्स बाज़ार में ₹ 2 लाख करोड़ का इजाफा होगा.

प्रौद्योगिकी निश्चित रूप से अच्छी बात है क्योंकि इससे संचार और सूचनाओं तक पहुँचना आसान हो गया है. इसने दुनिया को एक वैश्विक गाँव बना दिया है और उन उद्यमियों के लिए यह एक अद्भुत मंच बन गया है जो अपने उद्यमों का विस्तार करना चाहते हैं. ई-कॉमर्स आधुनिक दुनिया के लिए एक व्यवसाय मॉडल है और सही रणनीतियों को अपनाने के साथ, यह एक छोटे व्यवसाय को एक साम्राज्य में बदल सकता है. आज के युवा के लिए इस क्षेत्र में कई स्वर्णिम अवसर मौजूद हैं. देश के युवा ई-कॉमर्स में प्रशिक्षण प्राप्त करके अपना भविष्य सुनहरा बनाएं एवं देश हित में अपना महत्वपूर्ण योगदान दें.



क्लाउड कम्प्यूटिंग का बढ़ता बाज़ार

अर्पित जैन
प्रबंधक (राजभाषा)
स्टाफ प्रशिक्षण केन्द्र, भोपाल

दिव्या दीक्षित
प्रबंधक
क्षे. का. इलाहाबाद

जब हम प्रौद्योगिकी में बढ़ते हुए प्रचलन की बात करते हैं तब क्लाउड कंप्यूटिंग सबसे अधिक चर्चा का विषय होता है. यह अकेले ही वैश्विक स्तर पर बड़े परिवर्तन को करने में सक्षम है. विविध बाज़ार सर्वेक्षणों के आधार पर क्लाउड कम्प्यूटिंग का वैश्विक बाज़ार वर्ष 2014 में 209.90 मिलियन डॉलर का था, जो कि वर्ष 2020 तक $411 मिलियन तक पहुँचने का अनुमान है (श्रोत फोर्ब्स पत्रिका). जॉन हैगेल, को-चेयरमैन, डिलॉइट सेंटर ऑफ एज, के अनुसार "क्लाउड कंप्यूटिंग में विशेष क्षमता है जो कि टेक्निकल इंडस्ट्री से निकल कर अन्य कई इंडस्ट्री को सफलता की ऊंचाइयों तक ले जा सकती है."

परिचयः

कम्प्यूटर की कार्य-निष्पादन क्षमता को बढ़ाने हेतु विविध नई विधाएं एवं प्रौद्योगिकी हैं. क्लाउड कम्प्यूटिंग या मेघ संरचना इसमें प्रमुखता से प्रयोग में आ रही हैं. क्लाउड कम्प्यूटिंग एक लाइसेन्सधारी सेवा है, जो कि अलग-अलग कंपनियों के द्वारा इंटरनेट प्रयोक्ता को प्रदान किया जा रहा है. क्लाउड प्रौद्योगिकी एवं इंटरनेट पूर्णतः समागमित है. क्लाउड शब्द को इंटरनेट का "रुपक" भी कहा जा सकता है.

क्लाउड का अर्थ है बादल अथवा मेघ अर्थात् डाटा एवं सॉफ्टवेर से भंडारित सर्वर को " क्लाउड" कहा जाता है, ऐसा प्रतीत होता है कि समस्त डाटा व प्रोग्राम प्रयोक्ता के कम्प्यूटर पर ही उपलब्ध है. यह वास्तव में इंटरनेट-आधारित प्रक्रिया और कंप्यूटर ऐप्लीकेशन का इस्तेमाल है, जो बिजनेस ऐप्लीकेशन ऑनलाइन मुहैया कराता है तथा वेब ब्राउजर का इस्तेमाल कर इस तक पहुंचा जा सकता है.

जन-साधारण के द्वारा प्रयोग किए जा रहे कम्प्यूटर, लैपटाप, मोबाइल अथवा टेबलेट की भंडारण क्षमता सीमित है, इसको बढ़ाने के लिए हार्ड ड्राइव का प्रयोग किया जा सकता है किन्तु हार्ड ड्राइव के प्रयोग से अधिक व्यय होगा. अतः यदि किसी प्रयोक्ता को इस संबंध में अधिक प्रोसेसिंग स्पेस या भंडारण क्षमता की आवश्यकता है तो प्रयोक्ता

अपनी आवश्यकता अनुसार किसी कंपनी की कम्प्यूटिंग अवसंरचना का प्रयोग निर्धारित शुल्क देकर कर सकता है. अतः यह सामान्य संग्रहण यंत्र की तरह काम करता है, जिससे सर्वर पर संग्रहित डाटा या जानकारी का प्रयोग सर्वर पर जुड़े सभी अभियंत्र (कम्प्यूटर, लैपटाप, मोबाइल अथवा टेबलेट) कर सकते हैं.

सोशल नेटवर्किंग साइट इसका प्रमुख उदाहरण है. सोशल मीडिया पर तस्वीरें या ईमेल पर डाटा अपलोड करने पर वह हमारे व्यक्तिगत कम्प्यूटर या मोबाइल पर जगह नहीं लेता और उस वेबसाइट या एप के क्लाउड पर जा कर संग्रहित हो जाता है. अपने व्यक्तिगत कम्प्यूटर या मोबाइल से उसको मिटाने के बाद भी वह सोशल मीडिया के क्लाउड पर संग्रहित रहता है.

इस प्रकार क्लाउड कम्प्यूटिंग हमारे दिन-प्रतिदिन की जीवनचर्या पर विविध आयामों में प्रभाव डाल रही है. इस प्रौद्योगिकी ने जन साधारण ही नहीं अपितु व्यवसाय करने की प्रणालियों में भी परिवर्तन किया है 'जैसे ग्राहकों तक पहुंचाना या प्रमुख व्यवसाय संबन्धित डाटा को संग्रहित करना आदि'.

क्लाउड की व्यवसायिक महत्ता को समझने से पूर्व, क्लाउड कम्प्यूटिंग के विविध प्रकारों को समझना अनिवार्य है. वैश्विक क्लाउड सेवा संस्था को सेवा, प्रकार, अंतिम प्रयोक्ता या भौगोलिक संरचना के आधार पर विभाजित किया जा सकता है, विविध प्रकार की क्लाउड सेवाएं बाज़ार में अपना एक विशेष महत्व रखती हैं.

संयुक्त राज्य अमेरिका के राष्ट्रीय मानक एवं परीक्षण संस्थान (NIST) के अनुसार क्लाउड कम्प्यूटिंग में निम्नांकित विशेषताएं होनी चाहिए.

मांग पर उपलब्ध एवं स्व सेवा : इच्छुक उपयोगकर्ता को क्लाउड कम्प्यूटिंग सेवाएं प्रदान की जाती है. जितनी मांग होती है उतनी ही सेवा प्रदान की जाती है.

व्यापक नेटवर्क तक पहुंच : क्लाउड का उपयोग केवल एक अहाते में बैठकर ही नहीं किया जाता बल्कि इसे 7/24/365 यानि कहीं भी, कभी भी की तर्ज पर उपयोग किया जा सकता है. कार्यालय को घर पर तथा घर को कार्यालय में ला पाना क्लाउड कम्प्यूटिंग के माध्यम से संभव हुआ है.

संसाधनों का साझा उपयोग : क्लाउड पर रखी सामग्री को किसी के साथ भी साझा किया जा सकता है अर्थात् क्लाउड पर रखी फाइलों व साफ्टवेयरों को औरों के साथ लिंक द्वारा साझा किया जा सकता है. इस तरह से लाइसेंस तथा कॉपीराइट जैसे मुद्दों से बचकर संसाधनों का अधिकतम उपयोग किया जा सकता है.

त्वरितता लचीलापन : क्लाउड पर आधारित कम्प्यूटर बहुत अधिक शक्तिशाली होते हैं. इनकी क्षमता किसी सुपर कम्प्यूटर की तरह ही होती है. ऐसे में यदि कोई क्लाउड का उपयोग कर रहा है तो इसका अभिप्राय है कि वह तुरंत किसी साधन तक अपनी पहुंच बना लेगा तथा वह अपनी सुविधा से उसका जैसे चाहे उपयोग कर सकता है.

सेवा का मापन : किसी उपयोगकर्ता ने कितनी सेवा प्राप्त की है इसका स्वतः मापन हो जाता है. ऐसे में उपयोगकर्ता एवं सेवा प्रदाता के मध्य किसी भी प्रकार का विवाद होने की संभावना नहीं रहती है.

क्लाउड कम्प्यूटिंग की कुछ अन्य विशेषताएं

क्लाउड कम्प्यूटिंग सेल्फ सर्विस वाले किसी रेस्त्राँ की भाँति है. इसमें किसी से भी अनुमोदन अथवा स्वीकृति प्राप्त करने की आवश्यकता नहीं है. उपयोगकर्ता को अपनी आवश्यकता के अनुसार क्लाउड का चयन करना होता है तथा यदि काम में अधिक गुणवत्ता एवं कम्प्यूटर क्षमता की आवश्यकता होती है तो भुगतान आधारित सेवा प्राप्त की जा सकती है. यदि काम सामान्य किस्म का है तो ऐसी स्थिति में निःशुल्क क्लाउड सेवाएं ली जा सकती हैं. कम्प्यूटर प्रणाली के सबसे विस्तृत कम्प्यूटर नेटवर्क को उपयोग किया जा सकता है. संसाधनों का साझा उपयोग भी इसके द्वारा संभव है. यह ठीक वैसा ही है जैसे किसी एक कार में 3 या 4 यात्री जो कि अलग-अलग स्थान पर जाने वाले होते हैं एक कार पूल करते हैं तथा समय एवं खर्च बचाते हैं. क्लाउड सर्वरों के पास बहुत बड़ी क्षमता होती है जिसका साझा उपयोग करने से कम्प्यूटर क्षमता एवं आर्थिक संसाधनों का समुचित दोहन किया जा सकता है. तेजी से उपयोग में परिवर्तन किया जा सकता है. उपयोग की जाने वाली क्षमता एवं संसाधनों को मापा जा सकता है जिससे ठीक-ठीक आवश्यकताओं को पहचानना संभव है.

क्लाउड कम्प्यूटिंग के प्रकारः-

क्लाउड कम्प्यूटिंग को संरचना के आधार पर मुख्यतः 4 प्रकारों में वर्गीकृत किया जा सकता है;

1. **कम्यूनिटी क्लाउड :** इस तरह के क्लाउड का प्रयोग उन व्यवसायों या संस्थाओं द्वारा किया जाता है जो कि किसी सम्मिलित प्रोजेक्ट, खोज या अन्य संयुक्त क्रियाकलापों को एक साथ या एक दिशा में पूर्ण करने में अग्रसर होती हैं. अतः यह एक संकरित मेघ संरचना का निजी क्लाउड है, जो कि निश्चित प्रयोक्ताओं द्वारा प्रयोग किया जाता है.

2. **संकरित क्लाउड :** यह विविध निजी एवं सार्वजनिक क्लाउड का समागम है. जब कोई संस्था आंतरिक प्राइवेट क्लाउड कम्प्यूटिंग डोमेन का प्रयोग करते हुए पब्लिक क्लाउड कम्प्यूटिंग डोमेन का भी प्रयोग करती है तो उसे हाइब्रिड या संकरित क्लाउड कहते हैं. एक संकरित क्लाउड पर्यावरण में कई आंतरिक और/या बाहरी प्रदाता शामिल होते हैं, "जो अधिकांश उद्यमों के लिए प्रारूपिक होगा".

3. **निजी क्लाउड :** इस प्रकार की क्लाउड संरचना संस्था के अंतर्गत उसके आंतरिक कार्यों में प्रयोग होती है. अतः यह स्वयं संस्था की आंतरिक संरचना है.

गार्टनर, अनुसंधान एवं सलाहकार कंपनी, के पूर्वानुमान के अनुसार, वर्ष 2018 में वैश्विक पब्लिक क्लाउड सेवा का मार्केट 21.4% तक बढ़ना अनुमानित किया गया. वर्ष 2017 की तुलना में $153.5 बिलियन से बढ़कर वर्ष 2018 में $186.4 बिलियन तक पहुँचने का अनुमान लगाया गया.

सेवा के आधार पर क्लाउड सेवा संस्था का विभाजन निम्नवत है;

क) बुनियादी सुविधाएं एक सेवा के रूप में (IaaS): यह बाज़ार का सबसे अधिक तीव्रता से बढ़ने वाला भाग है, जो कि 35.9% की वृद्धि के साथ $ 40.8 बिलियन तक अनुमानित की गयी.

ख) प्लेटफार्म एक सेवा के रुप में (PaaS): पीएएएस का बाज़ार वर्ष 2021 तक $10.00 बिलियन तक पहुँचना अनुमानित है.

ग) सॉफ्टवेयर एक सेवा के रुप में (SaaS): यह क्लाउड कम्प्यूटिंग का सबसे बड़ा भाग है, वर्ष 2018 में 22.2% की वृद्धि के साथ इसका कुल बाज़ार $ 73.6 बिलियन तक अनुमानित था. **गार्टनर की रिपोर्ट के अनुसार वर्ष 2021 तक एसएएएस बाज़ार 45% तक पहुँचने का पूर्वानुमान है.**

उत्पत्ति, विकास एवं बाज़ार:

21 वीं शताब्दी के अंत तक, शब्द "क्लाउड कंप्यूटिंग" अधिक व्यापक रूप से प्रकट होने लगा,यद्यपि इन सेवाओं का प्रयोग मूलतः SaaS (क्लाउड कम्प्यूटिंग का एक प्रकार) तक सीमित था.

क्लाउड अवस्था : 2000 के दशक के प्रारंभ में, माइक्रोसॉफ्ट ने सेवाओं के विकास के माध्यम से Saas की अवधारणा को विस्तृत किया. आईबीएम कंपनी ने 2001 में ऑटोनोमिक कम्प्यूटिंग घोषणा पत्र में इन अवधारणाओं का विवरण दिया, जिसने विषमांगी भंडारण, सर्वर, अनुप्रयोग, नेटवर्क, सुरक्षा तंत्र और ऐसे अन्य तत्वो के साथ जटिल IT (सूचना प्रोद्योगिकी) प्रणाली के प्रबंधन में उन्नत ऑटोमेशन तकनीकों जैसे स्व-नियंत्रण, स्व-चिकित्सा, स्व-विन्यास और स्व-अनुकूलन का वर्णन किया जिन्हें एक उद्यम में प्रयोग किया जा सकता है. अमेजन ने नयी क्लाउड सरंचना के परिणाम स्वरुप महत्वपूर्ण आंतरिक प्रभाविता सुधार पाए जाने और डॉट-कोम बबल के बाद अपने डाटा केन्द्रों के आधुनिकीकरण के द्वारा क्लाउड कम्प्यूटिंग के विकास में महत्वपूर्ण भूमिका निभायी, इसके लिए उसने एक यूटिलिटी कम्प्यूटिंग आधार पर 2005 में अमेजन वेब सेवाओं के माध्यम से अपने सिस्टम उपलब्ध कराए.

क्लाउड कम्प्यूटिंग अनुमान एवं बाज़ार मूल्यांकन 2018:

(श्रोत क्लाउड बिजनस ड्राईवस अमेजोन प्रोफिट्स, स्टेस्टिस्टा जुलाई 27, 2018 फोब्स पत्रिका)

कंपनियां जैसे ड्रॉपबॉक्स फेसबुक आदि ने जनसाधारण के लिए नए आयाम दिए हैं, जहां कोई भी अपना व्यक्तिगत डाटा संग्रहित कर सकता है तथा कहीं फिर भी उसका प्रयोग कर सकता है. मार्केट सर्वे के आधार पर 95% व्यवसाय आज क्लाउड का प्रयोग कर रहे हैं एवं वर्ष 2019 में कुल उपलब्ध डाटा का लगभग 90% क्लाउड पर ही उपलब्ध होगा इस प्रकार क्लाउड हमारे जीवन का अभिन्न अंग बन चुका है.

क्लाउड प्रौद्योगिकी के विविध उदाहरणों की हम दिन प्रतिदिन अपनी जीवन चर्या में प्रयोग कर रहे हैं तथा विभिन्न कंपनीयां इससे अच्छा राजस्व अर्जित कर रही हैं, जो कि निम्न वत हैं;

नेविगेशन प्रोग्राम : जो की बहुत अधिक डेटा को संचालित करने के साथ उसको रियल टाइम आधार पर अपडेट भी करता है इस तरह आप विश्व में किसी भी देश में भ्रमण करते हुए वहां की रास्तों से सुपरिचित रह सकते हैं.

ऑनलाइन शॉपिंग : सांख्यिकी गणना के आधार पर कुल ऑनलाइन खरीदी करने वाले ग्राहकों में लगभग 32% ग्राहक सत्ता में कम से कम एक बार खरीदी करते ही हैं यह ऑनलाइन स्टोर अपनी जानकारी एवं तस्वीरों को संचालित करने के लिए क्लाउड का ही प्रयोग करते हैं

सोशल मीडिया इसके विविध उदाहरण है तथा हम आज के समय में सोशल मीडिया के माध्यम से जानकारी एवं मनोरंजन दोनों को ही प्राप्त कर रहे हैं फेसबुक, ट्विटर, इंस्टाग्राम, व्हाट्सएप एवं गूगल ड्रॉपबॉक्स इसका प्रचलित स्वरूप है.

व्यवसाय सहयोग : विविध व्यवसाय नये एसएमई एक्सपोर्ट आदि क्लाउड संरचना का प्रयोग वैश्विक मंच पर अपनी सेवा एवं वस्तुओं को प्रचारित करने में कर रहे हैं आजकल क्लाउड का प्रयोग ऑनलाइन मीटिंग विचारों के आदान-प्रदान सांख्यिकी तुलना के लिए किया जाता है जो की कार्यप्रणाली को संतुलित एवं उत्पादकता के अनुपात को बेहतर कर रहा है.

वर्तमान में क्लाउड कम्प्यूटिंग के क्षेत्र की दस शीर्ष सबसे अधिक शक्तिशाली, सशक्त एवं प्रभावशाली वितरक माइक्रोसॉफ़्ट, अमेजन, आईबीएम, सेलफोर्स, एस ए पी, ओरेकल, गूगल, सर्विस नाओ, वर्क दे, वीएम वेयर हैं. वर्ष 2016 में यह आईएएएस क्लाउड के कुल बाज़ार का 50% था जो कि 2021 तक 70% होने का अनुमान है.

पिछले दो वर्षों में वैश्विक क्लाउड पब्लिक सेवा में तीव्र व्रद्धि हुई है. वर्ष 2017 में यह लगभग $ 1.8 बिलियन तक पहुँच गयी तथा वर्ष 2020 तक यह $4.1 बिलियन तक की अप्रत्याशित वृद्धि का अनुमान है. एशिया पैसिफिक भाग में भारत, चीन के बाद सबसे अधिक तीव्रता से बढ़ने वाला बाज़ार है.

वित्त वर्ष 2018 की तृतीय तिमाही में 7.2% की जीडीपी वृद्धि के साथ भारत इंटरनेट के बाज़ार में आने के लिए तथा अप्रत्याशित वृद्धि के लिए तैयार है.

पिछले कुछ महीनो में गूगल, अलीबाबा, अमेजन तथा माइक्रोसॉफ़्ट ने देश में अपने डाटा सेंटर प्रारम्भ कर दिये हैं. भारत के निजी बाज़ार में नैक्सटजेन नामक कंपनी अपने "देव क्लाउड" नामक सुविधा के साथ बाज़ार में अपना स्थान बना रही है.

भारत के स्मार्ट शहरों में "ईएसडीएस" इन सुविधाओं का प्रबंधन कर रही है. साथ ही CntrlS ने वैश्विक पटल पर, एशिया के सबसे बड़े टियर 4 डाटा सेंटर के साथ, अपना स्थान बना लिया है.

अपने आकार से इतर भारतीय कंपनियों ने डाटा सेंटर की जटिलता को समझते हुए "क्लाउड" की तरफ अपना रुख कर लिया है. माइक्रोसॉफ़्ट इंडिया एवं थॉट अर्बिट्रेज रिसर्च इंस्टीट्यूट (TARI) के एक सर्वेक्षण के अनुसार "क्लाउड के प्रयोग के साथ लघु एवं मध्यम उध्योग, व्यवसायों में धन के प्रवाह को 308% तक बढ़ा सकते हैं तथा वर्तमान में 96% लघु एवं मध्यम व्यवसायों ने अपने परिचालन व्यय पर दो वर्षों में ही सकारात्मक प्रभाव डाला है."

भारत में क्लाउड कम्प्यूटिंग को आत्मसात करने के दो प्रमुख प्रचलन देखने को मिलते हैं;

प्रथम सह-स्थान सेवा एवं सुनिश्चित या बंदी डाटा सेंटर जो कि अत्यधिक विनयमित ऊर्ध्वाधर जैसे बैंकिंग, वित्तीय सेवा विभाग, बीमा, स्वास्थ्य सेवा उद्योंग एवं सरकारी विभागों द्वारा प्रयोग की जा रही है. बंदी (capative) डाटा सेंटर एन उद्योंगों कि "सप्रभुत" की आवश्यकता को पूर्ण करते हुए, कम विलंब तथा अधिक तीव्र गति जैसी सुविधा के साथ अत्यधिक उत्पादक साबित हो रही है.

द्वितीय, संकरित क्लाउड संरचना सम्पूर्ण भारत में अत्यधिक लोकप्रिय हो रही है. क्लाउड जगत में विविध क्रम परिवर्तन एवं संयोजन संभव हैं, जिससे कि क्लाउड को किसी भी संस्थान के व्यवसाय या अन्य आवश्यकताओं के अनुसार संरचित किया जा सकता है. एनएसई इसका प्रमुख उदाहरण है. एनएसई ने अपनी सूचना प्रौद्योगिकी की आधारभूत संरचना को उन्नत करते हुए, पूर्णतः स्वचालित स्क्रीन- आधारित ट्रेडिंग सिस्टम को विकसित किया, जिससे एनएसई में होने वाले लेनदेन की संख्या 8 मिलियन प्रतिदिन से बढ़कर लगभग 12 मिलियन प्रतिदिन हो गयी है, साथ ही इसकी क्षमता 60% तक उन्नत हो गयी है.

क्लाउड कम्प्यूटिंग के बढ़ते बाज़ार को विविध घटक प्रभावित कर रहे हैं. इनमें सबसे प्रमुख है लागत- प्रभावशीलता, क्लाउड का प्रयोग करते हुए संस्थाएं अपनी परिचालन लागत का 35% व्यय कम कर सकती हैं. इसके अन्य तथ्य कार्यात्मक क्षमता पर आधारित हैं जो कि किसी भी मूलतः व्यवसाय की उत्पादकता को बढ़ाता है. यद्यपि भारतीय प्रायद्वीप अभी भी तीव्र गति इंटरनेट सेवा, विद्युत आपूर्ति, ऑप्टिकल फाइबर स्थापित इंटरनेट जैसी समस्याओं से उबर रहा है तथापि व्यवसाय व उद्योंगों में बढ़ते नवोन्मेष एवं चपलता तथा सरकार के 'डिजिटल इंडिया' मिशन के साथ भारत क्लाउड कम्प्यूटिंग का विशाल बाज़ार है, तथा क्लाउड सेवाओं को आत्मसाध करते हुए वैश्विक पटल पर अपनी छाप छोड़ने में अग्रसर है.

जीपीएस

अमित कुमार
प्रबंधक,
सरल क्षे. का. मुंबई (पश्चिम)

मान लीजिए कि आपका तबादला किसी नए शहर में हो गया है और आप पहली बार घर से अपने कार्यालय के लिये निकल रहे हैं. यह बड़ी सामान्य सी बात है कि नए शहर में आपको अपने घर से कार्यालय की न तो दूरी मालूम होगी, न ही कार्यालय पहुंचने में लगने वाला समय. ऐसी स्थिति में आप क्या करते हैं? ज़्यादातर लोगों का जवाब होगा कि मोबाइल में नक्शा (मैप) खोलते हैं और उसमें कार्यालय का पता डालते हैं, मैप बता देता है कि आपका कार्यालय आपके घर से कितना दूर है और आप कितनी देर में अपने कार्यालय पहुंच जाएंगे. आप जब भी मोबाइल या कंप्यूटर पर ऐसे किसी भी मैप का प्रयोग कर रहे होते हैं तब आप जिस क्रांतिकारी तकनीक के सहारे सारी जानकारी अपने मोबाइल पर पा जाते हैं, उसे ग्लोबल पोज़ीशनिंग सिस्टम (जीपीएस) कहते हैं.

जीपीएस वह तकनीक है, जो केवल लोकेशन और समय ही नहीं बताती, बल्कि किसी भी जगह के मौसम के विषय में भी सटीक जानकारी उपलब्ध कराती है. आइए जानते हैं कि वह तकनीक जो हमें घर, कार्यालय या किसी दूसरे की लोकेशन का पता बताती है, तेज़ गति से भागती गाड़ी की भी लोकेशन बता देती है, रास्ता, गलियां, घर, दफ्तर सबका पता देती है, वह काम कैसे करती है.

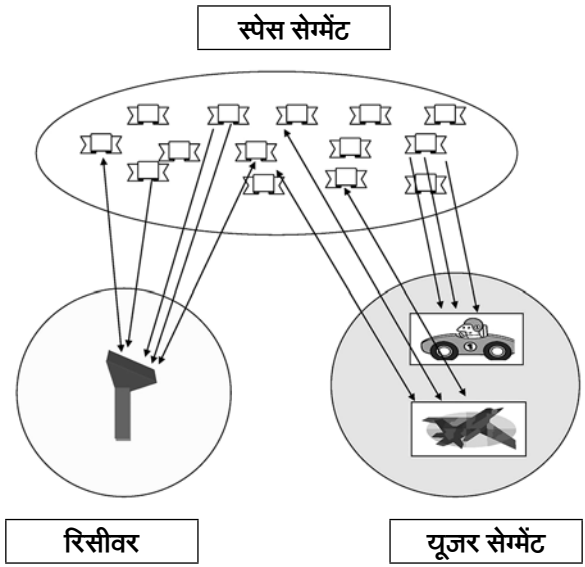
कैसे काम करता है जीपीएस

जीपीएस एक बहु-उद्देशीय, स्पेस-आधारित रेडियो नेविगेशन सिस्टम है, यह अमेरिकी सरकार के स्वामित्व में है और संयुक्त राज्य अमेरिका की वायु सेना द्वारा संचालित है. वर्तमान में जीपीएस सेवा के दो स्तर हैं :

स्टैंडर्ड पोज़ीशनिंग सर्विस (एसपीएस) Standard Positioning Service (SPS) जो आम नागरिकों द्वारा प्रयोग में लाई जाती है क्योंकि इस सेवा के द्वारा 100 मीटर के दायरे में स्थिति का पता चलता है. ये सेवा L1 फ्रीक्वेंसी पर coarse acquisition (C/A) कोड का इस्तेमाल करती है.

प्रिसाइज़ पोज़ीशनिंग सर्विस (पीपीएस) Precise Positioning Service (PPS) इस सेवा में L1 और L2 दोनों फ्रीक्वेंसी पर P(Y) कोड का इस्तेमाल होता है और इसका प्रयोग सामान्यतः सैन्य गतिविधियों के लिए किया जाता है. क्योंकि इस सेवा के द्वारा किसी भी व्यक्ति या स्थान के बारे में 10 मीटर के दायरे तक की सटीक जानकारी ली जा सकती है.

पीपीएस केवल अमेरिकी सेना, अमेरिकी संघीय यूएस फेडरल एजेंसीज और सिलेक्टेड आर्म्ड फोर्स और सरकार के द्वारा इस्तेमाल किया जाता है जबकि एसपीएस का प्रयोग पूरे विश्व के लिये खुला है. जिन सैटेलाइट्स का उपयोग हम करते हैं वह दरअसल 32 सैटेलाइट्स का एक समूह है जो पृथ्वी के ऊपर लगभग 20,000 किमी की ऊंचाई पर ऑर्बिट में स्थित है. इन सभी सैटेलाइट्स का स्वामित्व अमेरिका के पास है और कोई भी इन सैटेलाइट्स के सिग्नल का उपयोग कर सकता है, बशर्ते उसने इसके अधिकार ख़रीदे हों और उनके पास एक रिसीवर हो, जो चार उपग्रहों से मिली सूचनाओं को प्राप्त करने में सक्षम हो. यह रिसीवर ही सेटेलाइट से मिले डाटा की गणना करता है और हमें तक जानकारियां उपलब्ध कराता है, इस प्रक्रिया को ट्रायंगुलेशन कहते हैं. सरल भाषा में समझना हो तो यह कहा जा सकता है कि जीपीएस की बुनियादी संरचना में तीन सेगमेंट्स होते हैं, जिसे आप नीचे दिये गए चित्र के माध्यम से समझ सकते हैं.



स्पेस सेग्मेंट (Space Segment) : जैसा कि आपको पता है, जीपीएस 32 अमेरिकी उपग्रहों का समूह है और इन समूहों ने पृथ्वी को 8 ऑर्बिट्स में बांट रखा है. प्रत्येक ऑर्बिट में 4 उपग्रह होते हैं और यह उपग्रह लगभग 20,000 किलोमीटर की दूरी पर अंतरिक्ष में पृथ्वी के चारों ओर लगभग 1 घंटे के अंतराल पर पृथ्वी का चक्कर लगाते रहते हैं और कंट्रोल सेगमेंट को लगातार सिगनल्स और सूचनाएं प्रेषित करते रहते हैं.

कंट्रोल सेग्मेंट (Control Segments) : कंट्रोल सेगमेंट्स में लगे मॉनीटर इन उपग्रहों से मिली सूचनाओं को नियंत्रित करते हैं और व्यवस्थित करते रहते हैं ताकि यह सुनिश्चित किया जा सके कि प्रत्येक ऑर्बिट में स्थित उपग्रहों के विचलन से जुड़े सिगनल्स को लगातार प्राप्त करके उसकी सही गणना कर समय और दूरी का सही ऑकलन कर वांछित सूचनाएं यूज़र सेगमेंट तक पहुंचायी जा सके.

यूज़र सेग्मेंट- जीपीएस रिसीवर (User Segment- GPS Receivers):

यूज़र सेगमेंट में लगा रिसीवर सेटेलाइट से मिले डाटा की गणना करता है. किसी भी पोजीशन की सही जानकारी के लिए कम से कम एक बार में तीन सेटेलाइट्स की मदद ली जाती है. ये पोजीशन लांगीट्यूड (Longitude) और लैटिट्यूड (Latitude) से दर्शाए जाते हैं और 2 डी (2 Dimensional) जानकारी देते हैं. 3 डी (जिसमें कि ऊंचाई भी शामिल है) अवस्थिति पता करने के लिए कम से कम चार उपग्रहों की सहायता ली जाती है. एक बार ये सभी जानकारियां मिलने के बाद जीपीएस रिसीवर, उपग्रह से सिंक हो जाता है एवं गति, दूरी, ऊंचाई और किसी जगह पर पहुंचने में लगने वाले समय की गणना कर लेता है. यह 10 मीटर से 100 मीटर तक के सीमा की सटीक जानकारी देता है.

आज विश्व के सभी विकसित देश इस वैश्विक दिशा निर्धारण प्रणाली का उपयोग अपनी जरूरतों और क्षमताओं के अनुसार कर रहे हैं. अमेरिका द्वारा शुरू की गई वैश्विक दिशा निर्धारण प्रणाली को जीपीएस के नाम से जाना जाता है तो वहीं रूस की वैश्विक दिशा निर्धारण प्रणाली ग्लोनॉस(GLONASS), यूरोपियन यूनियन की गैलीलियो(GALLILEO), चीन की बिडू (BEIDU) और जापान की QZSS के नाम से जानी जाती है. भारत में वैश्विक दिशा निर्धारण प्रणाली का इतिहास एक दशक पुराना है लेकिन ये पूरी तरह से अमेरिकी सूचनाओं पर आधारित था. वैश्विक दिशा निर्धारण प्रणाली के उपयोग पर, अमेरिकी एकाधिकार का नतीजा यह निकला है कि अमेरिका न तो किसी देश की सभी नागरिक की जरूरतों के लिए अपने जीपीएस के इस्तेमाल की इजाजत देता था और न ही भारत को संवेदनशील जानकारियां मुहैया कराता था. साल 1999 में करगिल युद्ध में ऑपरेशन विजय के दौरान जब भारत ने अमेरिका से जीपीएस

के आधार पर सूचनाओं के आदान-प्रदान के लिये अनुरोध किया तो अमेरिका ने यह सूचनाएं साझा करने से इनकार कर दिया था. यही वो समय था जब भारत को अपनी आवश्यकताओं के अनुकूल एक वैश्विक स्थान निर्धारण प्रणाली की जरूरत महसूस हुई और इसे विकसित करने का ज़िम्मा हमारे देश की सबसे प्रतिष्ठित एजेंसियों में से एक भारतीय अंतरिक्ष अनुसंधान संगठन को सौंपा गया.

भारतीय अंतरिक्ष अनुसंधान संगठन एवं इसके वैज्ञानिकों ने इसे एक चुनौती के रूप में लिया और 2013-16 के दौरान कुल 7 उपग्रह इसी अभियान के अंतर्गत भेजे गए और अंततः 28 अप्रैल 2016 को देश की सामरिक एवं नागरिक जरूरतों की आत्मनिर्भरता के दिशा में एक महत्त्वपूर्ण उपलब्धि हासिल हुई. इसरो ने देश के पहले नेविगेशन उपग्रह इंडियन रीजनल नेवीगेशन सैटलाइट सिस्टम (IRNSS) अर्थात भारतीय क्षेत्रीय दिशा सूचक उपग्रह प्रणाली की श्रृंखला में उपग्रह IRNSS-1-I को सफलतापूर्वक कक्षा में स्थापित कर दिया. यह उपग्रह सन 2013 से सन 2016 के बीच छोड़े गए कुल 7 उपग्रहों की कड़ी में आख़िरी था. इस उपग्रह के अंतरिक्ष में स्थापित होने के बाद, भारत की अपनी वैश्विक दिशा निर्धारण प्रणाली है, जिसका उपयोग सरकारी एवं सैन्य कार्यों के लिये शुरु भी हो चुका है. भारतीय प्रधानमंत्री ने भारतीय संदर्भ में इसे "नाविक" (NAVIC) नाम दिया जिसका शाब्दिक अर्थ है नेविगेशन विद इंडियन कांस्टेलेशन. भारतीय उपग्रहों की आई आर एन एस एस श्रृंखला के 7 उपग्रहों में से 4 उपग्रह जियोस्टेशनरी कक्षा में स्थापित किए गए हैं. इस कक्षा में स्थापित उपग्रहों को जमीन से देखने पर लगता है, जैसे वे आकाश में एक ही जगह पर स्थिर हों. इसके अतिरिक्त 3 उपग्रह जियोसिंक्रोनस कक्षा में स्थापित किए गए हैं, जो पृथ्वी के ऊपर अंतरिक्ष में, अंग्रेजी के 8 के आकार में चक्कर काटते दिखाई देते हैं. दो अलग-अलग कक्षाओं में स्थापित होने के कारण, इन 7 उपग्रहों की मदद से भारतीय उपमहाद्वीप में सैन्य गतिविधियों और नागरिक जरूरतों की पूर्ति हो सकेगी. फिलहाल इस क्षमता का व्यवसायिक उपयोग सीमित मात्रा में ही हो रहा है, लेकिन जैसे-जैसे भारत के अपने उपग्रहों की संख्या बढ़ती जाएगी वैसे-वैसे भारत इस दिशा में आत्मनिर्भर होता जाएगा और अमेरिकी जीपीएस प्रणाली पर उसकी निर्भरता ख़त्म होती जाएगी. जीपीएस में आत्मनिर्भरता भारत को दुनिया के अग्रिम पंक्ति के देशों की कतार में ला खड़ी करती है. अगर भारत भी अपने जीपीएस में उपग्रहों की संख्या को बढ़ाता जाए तो ना सिर्फ यह वर्तमान में भारतीय उपमहाद्वीप एवं आसपास के 1500 वर्ग किलोमीटर के इलाके की चौकसी भी कर सकेगा किंतु पूरी पृथ्वी को अपने देसी जीपीएस के तहत ले आएगा. ऐसी सेवाओं से ना सिर्फ़ जरूरतों के वक्त हम अपने विमानों, जहाजों और लोगों की दुनिया के किसी भी कोने में स्थिति का पता लगा सकते हैं बल्कि, अपने देश से बाहर की जमीनों पर होने वाले सैन्य और नागरिक गतिविधियों से जुड़ी जानकारी अपनी सुविधानुसार बेचकर भारी मात्रा में विदेशी मुद्रा भी अर्जित कर सकते हैं.

अब तक हम जीपीएस के सामान्य उपयोगों से तो वाकिफ़ हो चुके हैं लेकिन अब जबकि 'मोबाइल फोन' प्रत्येक मनुष्य के जीवन का हिस्सा बन चुका है ऐसे में जीपीएस आधारित मोबाइल सेवा अत्यंत लोकप्रिय हैं. जीपीएस के ऐसे बहुत से उपयोग हैं, जिसके बारे में इसे विकसित करते समय भी सोचा नहीं गया था.

अवस्थिति का पता लगाना (Locating Positions) : GPS से किसी लोकेशन का पता लगता इसका मुख्य और सबसे आम उपयोग है. मान लीजिए कि आप अपने दोस्तों के साथ लंबी यात्रा कर रहे हैं और आप अलग हो जाते हैं, तो जीपीएस आपको एक दूसरे के लोकेशन को ढूंढने में मदद कर सकता है. हालांकि ये आम नागरिक के द्वारा नहीं किया जा सकता, इसके लिये हमें प्रिसाइज़ पोज़ीशनिंग सर्विस का सहारा लेना होगा जो कि आम नागरिकों के लिए निषिद्ध है.

यातायात के दौरान आपातकालीन सहायता : यदि आपके साथ कोई सड़क दुर्घटना हो गई है या आप किसी आपात स्थिति में हैं तथा आपको तत्काल सहायता की आवश्यकता है तो आप अपने स्मार्टफ़ोन पर पहले से प्रोग्राम किय गए इमरजेंसी नंबर पर कॉल कर सकते हैं. अवस्थिति का विवरण दिये बिना भी, आपातकालीन दल आपकी वर्तमान अवस्थिति का पता लगाकर, आपको सहायता पहुंचाने में, सक्षम होगा.

वाहन चोरी रोकना : जीपीएस ट्रैकर एक उत्कृष्ट एंटी-थेफ़्ट डिवाइस है जो आपका वाहन चोरी हो जाने की स्थिति में, उसकी लोकेशन का पता लगाने में मदद करता है.

मैपिंग एवं सर्वेक्षण : मैपिंग और सर्वेक्षण के कार्यों में भी, जीपीएस का प्रयोग किया जाता है. सर्वेक्षण में GPS का इस्तेमाल, कंपनियों के समय और लागत को बचाता है. यह राजमार्गों, बिजली लाइनों, फसलों, मिट्टी के प्रकार तथा नदियों आदि के मैपिंग कार्यों में भी, इस्तेमाल किया जा सकता है.

ट्रैकिंग अपराधियों का पीछा करने में, पुलिस और जांचकर्ताओं द्वारा भी, जीपीएस का उपयोग किया जाता है.

पालतू जानवरों का पता लगाना: अक्सर पालतू जानवरों के खोने की ख़बरें मिलती हैं. जीपीएस तकनीक पालतू जानवरों का पता लगाने के लिये भी इस्तेमाल में लायी जा सकती है. अमेरिका में तो अधिकतर पालतू जानवरों के गले में, जीपीएस कॉलर होती है, और उनके मालिक, उनके पालतू जानवरों के खो जाने की स्थिति में, जीपीएस तकनीक की सहायता से ही उनका पता लगाते हैं.

वृद्ध लोगों की स्थिति को ट्रैक करना : जीपीएस ट्रैकिंग डिवाइस, आपको परिवार के विशेष सदस्य या बुजुर्ग की देखभाल करने में मदद करता है. वे कभी कभी अकेले

घूमते हैं और फिर उन्हें घर वापस जाने में कठिनाई होती है. इन GPS ट्रैकिंग डिवाइस में एक बटन होता है जिसे दबाने पर, बुजुर्ग तक तुरंत चिकित्सा सहायता पहुंचाने के लिए या आपात कालीन कॉल करने के लिए इस्तेमाल किया जाता है. कुछ स्वास्थ्य सुविधा देने वाली संस्थाएं, अपने मरीजों की देखभाल के लिए, भी इनका उपयोग करती हैं.

खनन उद्योग : जीपीएस ट्रैकिंग सिस्टम खनन उद्योग में भी बहुत उपयोगी है. जीपीएस डिवाइस की सहायता से पृथ्वी की सतह के विभिन्न परतों में, खनिजों की स्थिति का पता लगाया जाता है.

एंटीक एवं बहुमूल्य कलाकृतियों की सुरक्षा : पेंटिंग और कलाकृतियों की कीमतें कई बार लाखों और करोड़ों में होती हैं. जब किसी कला दीर्घा या संग्रहालय में इनका प्रदर्शन किया जाता है तो कई बार इन्हें बदलने या चोरी करने के मामले सामने आते हैं. इन कलाकृतियों की सुरक्षा भी जीपीएस के द्वारा की जा रही है.

जीपीएस का इस्तेमाल, प्रकृतिक आपदाओं से हुए नुकसान का जल्द से जल्द आकलन और सुदूर इलाकों में मदद पहुंचाने के लिए भी किया जा सकता है. भारत जैसे विविधतापूर्ण देश में मिट्टी की गुणवत्ता, मौसम और किस जगह कैसी फसल उगाई जाए इसके लिए आवश्यक सलाह किसानों को दी जा सकेगी, साथ ही जानवरों की लुप्त होती प्रजातियों को ट्रैक करने और उसमें सुधार लाने में भी जीपीएस की मदद मिल सकेगी.

आज उपरोक्त में से ज़्यादातर सुविधाएं जीपीएस आधारित मोबाइल फोन के द्वारा हर एक नागरिक को उपलब्ध हैं, जिससे उनका जीवन और आसान हुआ है. आधुनिक दौर में जीपीएस मनुष्य के जीवन के प्रत्येक क्षेत्र को प्रभावित कर रहा है एवं इसकी आवश्यकता सभी जगह महसूस की जा रही है. एस्ट्रोनॉमी, कार्टोग्राफी, फ्लाइट-ट्रैकिंग, जिओफेसिंग, जियो टैगिंग, जीपीएस आधारित एयरक्राफ्ट ट्रैकिंग एवं डिजास्टर मैनेजमेंट के क्षेत्र में जीपीएस का सफलतापूर्वक उपयोग हो रहा है. फिर भी इस दिशा में नए आयामों की निरंतर खोज की जा रही है.

ई-वालेट

नेहा कुमारी
सहायक प्रबंधक
नोडल क्षे. का. बेंगलुरु

सुभाष चन्द्र
राजभाषा अधिकारी
क्षे. का.मदुरै

ई-वालेट या डिजिटल वालेट जिसे आप ई-बटुआ या डिजिटल बटुआ भी कह सकते हैं. यह एक इलेक्ट्रॉनिक डिवाइस है, जो एक व्यक्ति को इलेक्ट्रॉनिक लेनदेन करने की अनुमति देता है. ई वालेट वस्तुओं को खरीदने के लिए पैसे की जगह इस्तेमाल किया जाने वाला एक प्रीपेड खाते का एक प्रकार है. आसान शब्दों में अगर कहा जाये तो आपका मोबाइल फोन ही आपका ई-वालेट हैं. ई वालेट एक तरह से बटुए का प्रतिस्थापन है. भारत सरकार ने देश को 'कैशलेश' बनाने की मुहिम चला रखी हैं. सरकार की इस मुहिम में ई वालेट, लोगों के लिए सबसे कारगर साबित हो रहा है. ई-वालेट कैशलेश भुगतान का ऑनलाइन और आसान तरीका हैं. यह सबसे तेज और सुविधाजनक भी है. एक रुपये से लेकर किसी भी राशि के लिए अब बिना कैश के, डिजिटल भुगतान किया जा सकता है. हम 24 घंटे डिजिटल लेन-देन कर सकते हैं, यहां तक कि छुट्टियों के दौरान भी.

आज बाजार में पेटीएम, फ्रीचार्ज, ऑक्सीज़न, मोबिक्विक, पेयू मनी, ओला मनी आदि अनेकों ई-वालेट अपना नाम स्थापित कर चुके हैं. आज जिस गति से प्रौद्योगिकी का विकास हो रहा है, उसी गति से बाज़ार में भी बदलाव हो रहे हैं. आज से कुछ 15 वर्ष पहले तक हम तकनीकी रूप से इतने सक्षम नहीं थे कि हम बैंक डिटेल्स को मोबाइल पर देखने, ऑनलाइन भुगतान करने या ई-वालेट आदि के बारे में भी सोच सकें. परंतु, निरंतर विकास करते तकनीकी युग में आज कुछ भी असंभव नहीं है. बैंकों में घंटों लाइन लगाकर टोकन ले कर अपना लेन देन करना अब बीते जमाने की बात हो चुकी है. आज पासबुक में लेनदेनों की प्रविष्टि कराने के बारे में कोई सोचता ही नहीं क्योंकि सारे स्टेटमेंट अब ईमेल पर ही मिल जाते हैं.

मोबाइल वालेट में अपनी आवश्यकतानुसार पैसे रखे जा सकते हैं, जिससे डेबिट या क्रेडिट कार्ड डिटेल्स को बार-बार सार्वजनिक नहीं करना पड़ता है. इससे आपके कार्ड की सुरक्षा बढ़ जाती है. आज अधिकतर सेवाओं/वस्तुओं के भुगतान हेतु मोबाइल-वालेट

प्रभावी रूप से कार्य करता है, अतः अपने साथ ज्यादा कैश लेकर चलने की आवश्यकता नहीं है. इस प्रकार की सेवाएं डेबिट या क्रेडिट कार्ड की तुलना में अधिक सुरक्षित हैं, क्योंकि इन सेवाओं के प्रयोग के दौरान मोबाइल पर हर बार एक नया पासवर्ड प्राप्त होता है, जो सिर्फ एक ट्रांजेक्शन हेतु बहुत सीमित अवधि तक के लिए ही मान्य होता है.

उपभोक्ताओं को भी कैशलेस व्यवस्था का हिस्सा बनने पर अनेकों लाभ हैं. एक रुपए से लेकर कितना भी पैसा नकदी लेनदेन के बिना डिजिटली भुगतान किया जा सकता है. केवल फंड अंतरण ही नहीं ई-वालेट द्वारा बिजली बिल का भुगतान, केबल टी. वी. रीचार्ज, रेल व हवाई जहाज टिकट बुकिंग, मोबाइल रीचार्ज, सिनेमा टिकट बुकिंग, क्रेडिट कार्ड बिल पेमेंट, गैस बुकिंग व उसका भुगतान आदि सुविधाओं का लाभ भी प्राप्त होता है. सबसे बड़ी बात यह है कि ये सुविधाएं चौबीसों घंटे और यहाँ तक की छुट्टियों के दिन भी उपलब्ध रहती हैं. सरकार ने भी देश में डिजिटल भुगतान को बढ़ावा देने हेतु कई प्रोत्साहन योजनाएं घोषित कर रखी हैं.

इसके अतिरिक्त, पेट्रोल की खरीद पर छूट, बीमा प्रीमियम व सेवाकर में छूट तथा अन्य कैश बैक भी शामिल हैं. ये सेवाएँ सुरक्षित, तेज व ग्राहकों के अनुकूल भी हैं. आज भीम एप और यूएसएसडी जैसे डिजिटल माध्यमों की भी शुरुआत हो चुकी है. इन सब के लिए बड़ी संख्या में जागरूकता अभियान भी चलाये जा रहे हैं ताकि लोग डिजिटल भुगतान के प्रति शिक्षित हो और इसे आसानी से अपना सकें.

ई वालेट का उपयोग कैसे करें :-

1. स्मार्टफोन पर ई-वालेट का उपयोग करने के लिए मोबाइल वालेट या ई-वालेट को डाउनलोड करें.
2. कंप्यूटर पर ई-वालेट का उपयोग करने के लिए संबंधित वालेट की आधिकारिक साइट पर जाएं.
3. उपलब्ध जानकारी डाल कर पंजीयन (Register) करें और नया वालेट ID बनाएं.
4. पासवर्ड सेट करें. पासवर्ड ऐसा हो कि कोई अन्य व्यक्ति अनुमान न लगा सके.
5. अपने बैंक खाते से BHIM, IMPS Fund Transfer, क्रेडिट कार्ड, डेबिट कार्ड या इंटरनेट बैंकिंग का उपयोग कर अपने ई-वालेट में पैसा जमा करें.
6. ई-वालेट का उपयोग कर भुगतान करें.

ई-वालेट के प्रकार :-

- **क्लोज्ड वालेट** - यह एक ऐसा वालेट है, जो कि आपको विशिष्ट कंपनी से फुटकर खरीदी करने की अनुमति देता है. उदाहरण के लिए अमेज़न, जबाँग, फ्लिपकार्ट आदि.
- **सेमी क्लोज्ड वालेट** - सेमी क्लोज्ड वालेट आपको कई स्थानों पर खरीद और भुगतान करने की अनुमति देता है. पेटीएम, ऑक्सीज़न, पेयू मनी, मोबिक्विक आदि सेमी क्लोज्ड के उदाहरण हैं. ये सभी वालेट भारतीय रिजर्व बैंक (RBI) द्वारा अनुमोदित किये जाते हैं. इनसे कैश को भौतिक रूप से निकालने की अनुमति नहीं होती हैं.
- **ओपन वालेट** - ओपन वालेट बैंक द्वारा प्रदान किये जाने वाले वालेट हैं. इस तरह के वालेट में सेमी क्लोज्ड वालेट की सभी विशेषताएं तो विद्यमान होती ही हैं, इसके अलावा यह ATM से कैश निकालने की भी अनुमति देता है. एसबीआई बड्डी और एचडीएफ़सी चिल्लर आदि ओपन वालेट के ही उदाहरण हैं.

ई वालेट के उपयोग के फायदे -

1. किसी भी प्रकार के भुगतान के लिए आपको क्रेडिट कार्ड या डेबिट कार्ड का प्रयोग करने की जरूरत नहीं होती है. तुरंत प्रभाव से आप भुगतान कर सकते हैं.
2. ई-भुगतान के लिए आपको अपने बैंक खाते का उपयोग करने की कोई ज़रूरत नहीं है.
3. ई-वालेट एक प्रीपेड खाते की तरह कार्य करता हैं अतः भुगतान के फेल होने की कोई संभावना नहीं रहती हैं.
4. ई-वालेट का उपयोग कर, हर राशि के भुगतान पर आपको अतिरिक्त कैशबैक मिलता है.
5. ई-वालेट का उपयोग कर हर खरीद पर आपको रिवार्ड और अतिरिक्त छूट मिलती हैं.
6. लेनदेन में विफलता (transaction failure) के मामले में पूरे पैसे वापस किये जाते हैं.
7. ई-वालेट से ई-वालेट पर पैसे अंतरण किए जा सकते हैं.
8. घर बैठे ही भुगतान का विकल्प मिल जाता है.
9. किसी तरह की लाइन में लगने की आवश्यकता नहीं होती हैं. आपका अमूल्य समय बचाता है.

ई-वालेट का उपयोग करने पर जोखिम और कमियां -

1. ई-वालेट के पैसों को आप वापस नहीं ले सकते इस पैसे का उपयोग आप वस्तुओं को खरीदने में ही कर सकते हैं. यह पैसा पास होते हुए भी पैसे की अनुपलब्धता का कारक बन सकता है.
2. आप ई-वालेट का उपयोग तब तक कर सकते हैं, जब तक आपका मोबाइल चालू अवस्था में है.
3. मोबाइल में नेटवर्क न होने की स्थिति में आपका कार्य रुक सकता है.
4. ऐसा संभव हो सकता है कि आप वालेट में जमा पैसों से ज्यादा राशि खर्च करना चाहते हैं, तब ई-वालेट का विकल्प उपलब्ध नहीं होगा.
5. यदि किसी सरकारी कार्य के लिए पैसे खर्च कर रहें हो तो आपको बिल और अन्य औपचारिकताओं की ज्यादा आवश्यकता पड़ेगी.

ई-वालेट के प्रयोग में बरती जाने वाली सावधानियां -

आज आवश्यकता इस बात की है कि हम अपने ई-वालेट, एटीएम व नेट-बैंकिंग का सुरक्षित प्रयोग सुनिश्चित करें. इसके लिए कुछ बातों का ध्यान रखना अति आवश्यक हैः

- मोबाइल ओटीपी किसी को न बताए.
- अपने फोन व ई-वालेट में अलग-अलग पासवर्ड लगा कर रखें, ताकि यदि फोन चोरी भी हो जाए तो कोई इसका इस्तेमाल न कर सके अन्यथा आपके फोन पर ही ओटीपी मंगा कर खाता खाली किया जा सकता है.
- ई-वालेट को कभी भी दूसरे के फोन में लॉगिन न करें. इसे हमेशा अपने फोन से ही लॉगिन करें.
- फर्जी मैसेज व कॉल से सावधान रहें. यदि आपके पास खाते से संबंधित कोई मैसेज या कॉल आता है तो उसपर आँख बंद कर भरोसा न करें तथा उसकी वास्तविकता जानने का प्रयास करें.

भारत में प्रयोग होने वाले ई-वॉलेट और भुगतान बैंक -

बदलते समय के साथ भारत में बैंकिंग का स्वरूप बदलता गया. बैंकिंग की पहुँच बहुत आसान हो गई है. एक सामान्य व्यक्ति भी अब भारत के किसी बैंक में केवाईसी नियम पूरे करके खाता खोल सकता है. इनमें एयरटेल भुगतान बैंक, पेटीएम भुगतान बैंक, आइडिया पेमेंट बैंक और जियो भुगतान बैंक शामिल हैं, जो ई-वॉलेट की सुविधा प्रदान करते हैं.

'ई-वॉलेट' कैसे मील का पत्थर साबित होगा-

भारत डिजिटल भुगतान के माध्यम से कैशलेस अर्थव्यवस्था में परिवर्तन के दौर से गुजर रहा है. यह देखते हुए कि हमारे देश में बहुत ही कम लोग डिजिटल भुगतान कर रहे हैं, इसलिए बैंकिंग और भुगतान जितना अधिक डिजिटल होगा, देश की अर्थव्यवस्था उतनी ही मजबूत और पारदर्शी होगी, साथ ही इससे सार्वजनिक जीवन व शासन में भ्रष्टाचार को दूर करने में भी मदद मिलेगी. इससे नकदी के मुद्रण पर होने वाले भारी भरकम खर्च को भी बचाया जा सकता है.

जब देश में नोटबंदी की घोषणा हुई, तब पूरे देश में एकाएक करेंसी की कमी पड़ गयी. अधिकांश नागरिकों को बहुत परेशानी झेलनी पड़ी, परंतु जो व्यक्ति पहले से डिजिटल माध्यमों का प्रयोग करते थे, वे काफी हद तक परेशानी से बच गए. इसके बाद सब ने ई-वालेट जैसे माध्यमों के बारे में सोचना व उपयोग करना सीखा. आज यह काफी प्रचलित माध्यम है. आज डिजिटल भुगतान बहुत तेजी से हमारे जीवन का अभिन्न हिस्सा बन रहा है. अर्थशास्त्रियों का मानना है कि डिजिटल भुगतान प्रणाली यानि ई-वालेट भविष्य में सबसे ज़्यादा इस्तेमाल होने वाली भुगतान प्रणाली बन जाएगी.

भारत दिन-प्रतिदिन बदल रहा है. भारत को प्रगति की डगर पर तेजी से आगे बढ़ने के लिए, डिजिटल की दौर अपनाना ही होगा. नकदी लेन-देन कम कर या बंद कर डिजिटल भुगतान या कैशलेस ट्रांजेक्शन अपना कर ही हम डिजिटल इंडिया का सपना साकार कर सकते हैं.

इंटरनेट ऑफ़ थिंग्स (IOT)

अनिर्बान कुमार विश्वास
प्रबंधक (राजभाषा)
डीआईटी, पवई

चार दशक पहले, कम्प्यूटर के प्रादुर्भाव से अब तक मानव जीवन की सभी गतिविधियों में तकनीक ने द्रुत गति से पदार्पण किया है. पत्थरों से शिकार करने से लेकर आग जलाकर उसे पकाने और आग के माध्यम से जानवरों को डराकर उनका शिकार करना सीखने में इंसान को लगभग 12 लाख वर्ष लग गए. लेकिन अब इस तकनीकी दुनिया में लगभग हर वर्ष नई तकनीक हमारे जीवन को पूरी तरह से बदलती जा रही है. जैसे वर्ष 1996 में पेजर का पदार्पण हुआ किंतु 1 वर्ष बाद ही मोबाइल फोन आया, जिसकी वजह से पेजर का वजूद समाप्त हो गया. अब हमारे सामने हैं इंटरनेट इनेबल्ड डिवाइस, स्मार्टवॉच, स्मार्टटीवी तथा स्मार्टफ़ोन है. इसके अलावा हम बात कर रहे हैं उन डिवाइसों की, जो खुद सोच सकती हैं और अपने मन से कोई काम कर सकती हैं और इनके साथ ही उदय हुआ इंटरनेट ऑफ़ थिंग्स का.

इस विचार का उदय सन 1982 में कार्नेगी मेलन यूनिवर्सिटी के एक लैब में हुआ था, जब वहां के शोधार्थियों ने एक कोक मशीन को इंटरनेट से जोड़ा था. यह मशीन अपने भीतर रखे पेय पदार्थ की बोतलों की संख्या का हिसाब रख सकती थी व उनके तापमान को माप लेती थी. वहाँ से चलकर हम अब एक ऐसे मुकाम पर खड़े हैं, जहाँ 2020 तक ऐसे समझदार डिवाइसों की संख्या 30 अरब पार करने का अनुमान है, जो स्वयं अपना संचालन करेंगी.

क्या है इंटरनेट ऑफ़ थिंग्स?

सरल शब्दों में इंटरनेट ऑफ थिंग्स, जिसे हम आईओटी कहते हैं, स्मार्ट डिवाइसेस हैं, जो इंटरनेट से जुड़कर एक दूसरे से संवाद करती हैं और डाटा भेजती हैं.

"इंटरनेट ऑफ थिंग्स" नेटवर्किंग को कहा जाता है. अब आपके मन में सवाल होगा कि यह किस तरह की नेटवर्किंग है? इस नेटवर्किंग में आपके उपयोग के सभी गैजेट्स और इलेक्ट्रॉनिक डिवाइसेज एक-दूसरे से जुड़ी होती हैं. यह तो हम सभी जानते ही हैं

कि टेक्नोलॉजी ने हमारी रोजमर्रा की जिन्दगी को कितना आसान बना दिया है. इसे सरल शब्दों में एक उदहारण के जरिए समझा जा सकता है - जैसे आपकी एक डिवाइस आपके घर, किचन आदि में मौजूद अन्य डिवाइसेस को कमांड देती है. इस तरह से एक डिवाइस को इंटरनेट के साथ लिंक करके बाकी डिवाइसेस से अपने अनुसार कुछ भी कार्य करवाया जा सकता है. उदाहरण के लिए बीमा कंपनी अपने पालिसी धारको को सेंसर के माध्यम से किसी ऐसे क्षेत्र में जाने से रोकती है या चेतावनी दे सकती है, जहां चक्रवात या कोई अन्य आपदा आने की आशंका है.

आमतौर पर, आईओटी में डिवाइसों, सिस्टम, मशीन से मशीन (M2M) संचार सेवाओं, प्रोटोकॉल, डोमेन और एप्लिकेशन को शामिल कर उन्नत कनेक्टिविटी प्रदान की जाती है. इन सभी डिवाइसों को अलग-अलग पहचानने और इंटरनेट से जोड़ने के लिए इंटरनेट प्रोटोकॉल वर्जन 6(IPv6) का उपयोग किया जाता है. इसे तकनीकी दुनिया का नॉन-स्क्रीन कम्प्यूटिंग भी कहा जा रहा है, क्योंकि ये डिवाइसें एक कम्प्यूटर की तरह सोच तो सकती हैं, लेकिन इनमें कम्प्यूटर की तरह कोई स्क्रीन नहीं होती है.

इंटरनेट ऑफ़ थिंग्स हमारे जीवन में क्या बदलाव ला रही है? उदाहरण के लिए कितना अच्छा होगा, यदि कोई फ्रिज अपने भीतर रखे हुए सामान के समाप्त होने पर या समाप्त हो रहे सामान का ऑर्डर स्वयं किसी स्टोर को दे दे या फिर सिक्योरिटी कैमरा आपकी गाड़ी को देखकर आपके मकान के सिक्योरिटी सिस्टम को गैराज का ताला खोल देने और शटर के मैकेनिज़्म को शटर खोलने तथा गैराज की बत्तियों को ऑन हो जाने का आदेश दे दे. ऐसी कारों के प्रोटोटाइप तो बन ही गए हैं, जो आपके ऑफ़िस के दरवाज़े पर उतरने पर खुद ही पार्किंग स्पेस में जाकर कार को पार्क हो जाते है और आपके मोबाइल के एक संकेत पर कार वहाँ से आकर आपकी सेवा में हाज़िर हो जाए; एक ऐसी एम्बुलेंस, जो किसी सड़क दुर्घटना का शिकार हुए व्यक्ति को लेने जाते समय, पहले तो सबसे कम समय लेने वाले रास्ते का चयन कर सके और फिर घायल का पूरा चिकित्सकीय विवरण ऑनलाइन खंगालकर उसकी प्राथमिक चिकित्सा व दवाएँ सुझा सके. चौंकिए मत! सूचना प्रौद्योगिकी हमारी दुनिया को कहाँ ले जाएगी, कोई नहीं जानता. इंटरनेट ऑफ़ थिंग्स एक ऐसे ही युग का आगाज़ है, जिसमें समझदार डिवाइसें आपकी हर ज़रूरत को समय से पहले पूरा करेंगी.

बैंकिंग सेवाओं में आईओटीः

आईओटी में अरबों डिवाइसें एक दूसरे से जुडी होती हैं, जिससे सिस्टम एक स्मार्ट सिस्टम बन जाता है. जब ये डिवाइसें और सिस्टम क्लाउड पर डाटा साझा करते हैं और इसका विश्लेषण करना शुरू करते हैं, तो वे अनगिनत तरीके से हमारे व्यापार, हमारे जीवन और हमारी दुनिया को बदलने की क्षमता रखते हैं. हम ग्राहक तक डाटा

पहुँचाने के लिए स्मार्ट डिवाइसों का उपयोग करते हैं, जो बैंकों को रीयल टाइम ग्राहक वित्त का पूरा दृश्य प्रदान करने में सहायक होती है. बैंक एकत्रित डाटा के माध्यम से ग्राहकों की जरूरतों की पूर्ति कर सकते हैं, समाधान एवं सलाह भी प्रदान कर सकते हैं; जिससे ग्राहकों को स्मार्ट वित्तीय निर्णय लेने में भी मदद हो. बैंकिंग क्षेत्र में आईओटी के सबसे महत्वपूर्ण लाभों में से एक है ग्राहकों तक आसानी से क्रेडिट और डेबिट कार्ड पहुंचाना. बैंक विशिष्ट क्षेत्रों में एटीएम कियोस्क के उपयोग का विश्लेषण कर, उपयोग मात्रा के आधार पर एटीएम की स्थापना में वृद्धि या कमी कर सकते हैं. बैंक एटीएम और कियोस्क से ग्राहक तक ऑन-डिमांड सेवाओं तथा सेवाओं की पहुंच बढ़ाने में आईओटी डाटा का उपयोग कर सकते हैं. आईओटी के माध्यम से उपलब्ध ग्राहक डाटा बैंकों को अपने ग्राहकों की व्यावसायिक जरूरतों की पहचान करने में मदद करेगा. इस तरह, "बैंक ऑफ थिंग्स" ग्राहक वफादारी बढ़ाने में एक सशक्त माध्यम बन सकती है और बदले में, बैंकों के व्यवसाय में वृद्धि हो सकती है.

इंटरनेट ऑफ थिंग्स के फायदे :

इंटरनेट ऑफ थिंग्स के जरिए हर काम को आसानी से किया जा सकता है. आने वाले समय में इंटरनेट ऑफ थिंग्स के जरिए लोगों के जीवन स्तर में बहुत बदलाव आएगा. इस तकनीक की मदद से आप एक साथ कई काम कर सकते हैं. इसके अलावा अगर आप अपने दफ्तर या घर से दूर हैं, तो आप स्मार्ट डिवाइसों की मदद से घर या दफ्तर की जानकारी आसानी से प्राप्त कर सकते हैं.

इंटरनेट ऑफ थिंग्स के नुकसानः

इंटरनेट ऑफ थिंग्स से जुड़ा सबसे बड़ा नुकसान सुरक्षा को लेकर है. आज के दौर में इंटरनेट की सुरक्षा को लेकर तरह-तरह के सवाल उठते रहे हैं. ऐसे में चीजों को इंटरनेट से जोड़ने पर उनकी सुरक्षा को लेकर भी खतरा बना रहेगा. वहीं आने वाले समय में इंटरनेट ऑफ थिंग्स मानव आवश्यकता को कम कर लोगों की नौकरियां भी खतरे में डाल सकती है. दुनिया में ऐसी कई तरह की डिवाइसें बनायी जा रही हैं, जो कि हमारे लिए काफी फायदेमंद तो साबित हो रही हैं, परंतु तकनीक पर हमारी निर्भरता को बढ़ाती जा रही है, जिसे देख कर लगता है कि आने वाले समय में हम धीरे-धीरे पूरी तरह से इन तकनीकों के गुलाम बनने वाले हैं, जो कि मानव जीवन के लिए अच्छा संकेत नहीं है. इससे हमारी अपनी जीवन शैली खतरे में पड़ती जा रही है.

आईओटी की प्रमुख-सुरक्षा चुनौतियां :

आईओटी की प्रत्येक डोमेन में हजारों एप्लिकेशन्स हैं और दिन-प्रतिदिन नई-नई डिवाइसें जुड़ती जा रही हैं, सिर्फ इन डिवाइसों के बीच एक मजबूत अंतःक्रिया की

आवश्यकता है. यह अंतःक्रिया न केवल एक तकनीकी मुद्दा है बल्कि गोपनीयता, मानकीकरण और कानूनी मुद्दा भी है. क्योंकि आईओटी सिस्टम अक्सर अनियंत्रित, जटिल और शत्रुतापूर्ण वातावरण में ही स्थापित होता है,जिस कारण इसे सुरक्षित रखने में कई चुनौतियां होती है. आईओटी का प्रमुख उद्देश्य स्मार्ट वातावरण एवं स्थान और सेल्फ-अवेयर थिंग्स का निर्माण करना है. आईओटी की कुछ प्रमुख सुरक्षा चुनौतियां निम्न हैं :

1. **सुरक्षा बाधित डिवाइस / Secure constrained devices:**

   कई आईओटी डिवाइसों में भंडारण, मेमोरी और प्रासेसिंग क्षमता सीमित मात्रा में होती है तथा ये कम बिजली पर काम करने में भी सक्षम नहीं हैं. उदाहरण के लिए, सुरक्षा दृष्टिकोण एन्क्रिप्शन पर निर्भर हैं, जो बैटरी से चलते समय इन डिवाइसों के लिए उपयुक्त नहीं हैं; क्योंकि वे वास्तविक समय में सुरक्षित डाटा संचारण में जटिल एन्क्रिप्शन एवं डीक्रिप्शन करने में सक्षम नहीं होते. आईओटी सिस्टम की सुरक्षा कई परतों में की जाती है.

2. **तकनीकी और अर्थपूर्ण अंतःक्रियाशीलता / Technological & Semantic Interoperability:**

   अंतःक्रियाशीलता आईओटी की लिए काफी चुनौतीपूर्ण है क्योंकि यह न केवल लोगों को लोगों से जोड़ने का कार्य करती है बल्कि डिवाइसों के साथ लोगों को परस्पर निर्बाध अंतःक्रिया करती है.इन डिवाइसों की तकनीकी क्षमताओं में भिन्नता हो सकती है, पर अर्थपूर्ण अंतःक्रियाशीलता के लिए आवश्यक है कि वह डिवाइसों द्वारा साझा की गई सूचनाओं को समझ कर तदनुसार प्रतिक्रिया करे.

3. **स्मार्ट थिंग्स / Smart Things :** अल्ट्रा लो पावर सर्किट एवं कठोर वातावरण सहन करने में सक्षम डिवाइसों को विकसित करना चाहिए. इसके अलावा, आईओटी डिवाइसों में कम ऊर्जा वाले मल्टी प्रोसेसर सिस्टम में समानांतर प्रसंस्करण, अनुकूलन, ट्रस्ट, गोपनीयता, सुरक्षा गारंटी, स्वायत्त व्यवहार, बैटरी, ऊर्जा उत्पन्न करना और स्टोरेज टेक्नोलॉजी आदि जैसी कई चुनौतियां हैं.

4. **डिवाइसों को प्राधिकृत और प्रमाणीकृत करना / Authorize and authenticate devices:**

   आईओटी सिस्टम में विफलता के संभावित बिंदुओं की पेशकश करने वाले कई डिवाइसों के साथ, आईओटी सिस्टम को सुरक्षित करने के लिए डिवाइस को प्रमाणीकृत और प्राधिकृत करना आवश्यक है. गेटवे, अपस्ट्रीम सेवाओं और एप्स

तक पहुंचने से पहले डिवाइसों को अपनी पहचान स्थापित करनी होगी. हालांकि, ऐसे कई आईओटी डिवाइस हैं, जो डिवाइस प्रमाणीकरण के समय फॉल डाउन हो जाते हैं. उदाहरण के लिए, कमजोर मूल पासवर्ड का उपयोग या अपने डिफ़ॉल्ट मानों से अपरिवर्तित पासवर्ड का उपयोग. डिफ़ॉल्ट रूप से सुरक्षा प्रदान करने वाले आईओटी प्लेटफ़ॉर्म को अपनाने से इन समस्याओं को हल करने में मदद मिलती है. उदाहरण के लिए, दो कारक प्रमाणीकरण (2FA) सक्षम करना और मजबूत पासवर्ड या प्रमाणपत्रों का उपयोग करना. आईओटी प्लेटफार्म डिवाइस प्राधिकृत सेवाएं भी प्रदान करती है, जो यह निर्धारित करती है कि कौन सी सेवाओं, एप्स या संसाधनों को डिवाइस से पूरे सिस्टम में एक्सेस प्रदान किया जाएगा.

5. डिवाइस अपडेट प्रबंधन करना / Manage device updates:

आईओटी डिवाइसों और गेटवे पर चलने वाले फर्मवेयर या सॉफ़्टवेयर के लिए सुरक्षा पैच सहित अपडेटों को लागू करना बड़ी चुनौतीपूर्ण कार्य है. उदाहरण के लिए, आपको यह ट्रैक रखने की आवश्यकता है कि कौन सी अपडेट वर्तमान में उपलब्ध है और अलग-अलग नेटवर्किंग प्रोटोकॉल की श्रृंखला में संचारित विषम डिवाइसों के साथ वितरित वातावरण में लगातार अपडेट्स लागू करना है. सभी डिवाइस ओवर-द-एयर अपडेट्स या डाउनटाइम के बिना अपडेट का समर्थन नहीं करते हैं, इसलिए अपडेट को लागू करने के लिए डिवाइसों को भौतिक रूप से एक्सेस या अस्थायी रूप से एक्सेस करने की आवश्यकता है. इसके अलावा अपडेट्स सभी डिवाइसों, विशेष रूप से पुराने डिवाइसों या उन डिवाइसों के लिए उपलब्ध नहीं हैं जो अब उनके निर्माता द्वारा समर्थित नहीं हैं.

6. डाटा गोपनीयता और अखंडता सुनिश्चित करना / Ensure data privacy and integrity:

डाटा नेटवर्क पर प्रसारित होने के बाद समाप्त हो जाता है और यह सुरक्षित रूप से संग्रहित और संसाधित हो जाता है तथा अनावश्यक डाटा को सुरक्षित रूप से रखा जाता है, संग्रहित डाटा का कानूनी और नियामक ढांचे में अनुपालन भी एक महत्वपूर्ण चुनौती है. डाटा अखंडता जिसमें डाटा से कोई छेड़छाड़ न की जा सके, यह सुनिश्चित करने के लिए चेकसम या डिजिटल हस्ताक्षर को शामिल करना चाहिए. ब्लॉकचैन-आईओटी डाटा के लिए एक विकेन्द्रीकृत वितरित लेजर है, जो आईओटी डाटा की अखंडता सुनिश्चित कर उसे स्केलेबल और लचीला दृष्टिकोण प्रदान करती है.

7. सुरक्षित संचरण / Secure communication:

एक बार डिवाइस के स्वयं सुरक्षित हो जाने के बाद, अगली आईओटी सुरक्षा चुनौती यह सुनिश्चित करना है कि डिवाइस और क्लाउड सेवाओं या एप्स के बीच नेटवर्क में सुरक्षित संचार हो रहा है कि नहीं. कुछ आईओटी डिवाइसें नेटवर्क पर संदेश भेजने से पहले संदेशों को एन्क्रिप्ट नहीं करती है. हालांकि, संदेश भेजने का सबसे अच्छा तरीका ट्रांसपोर्ट एन्क्रिप्शन और टीएलएस जैसे मानकों को अपनाना है. डिवाइसों को अलग करने के लिए अलग-अलग नेटवर्क का उपयोग करने से उसकी सुरक्षा एवं निजी संचार सुविधा स्थापित करने में मदद मिलती है तथा संचारित डाटा की गोपनीयता एवं अखंडता बनी रहती है.

8. सुरक्षित वेब, मोबाइल और क्लाउड एप्लिकेशन / Secure web, mobile, and cloud applications:

वेब, मोबाइल और क्लाउड एप्स सेवाओं का उपयोग कर आईओटी डिवाइसों और डाटा को प्रबंधित, एक्सेस और संसाधित किया जाता है, इसलिए इसे आईओटी सुरक्षा के बहु-स्तरीय दृष्टिकोण से सुरक्षित किया जाना आवश्यक है. आईओटी एप्लिकेशन को विकसित करते समय, OWASP टॉप 10 भेद्यता जैसी कमजोरियों से बचने के लिए सुरक्षित इंजीनियरिंग अभ्यासों को लागू करें ताकि डिवाइसों की तरह एप्स को भी 2FA और सुरक्षित पासवर्ड पुनः प्राप्ति विकल्पों जैसे विकल्प से एप और एप्लिकेशन यूजर्स के लिए सुरक्षित प्रमाणीकरण प्रदान किया जा सके.

9. उच्च उपलब्धता सुनिश्चित करें/ Ensure high availability:

औद्योगिक वातावरण या आपातकालीन परिस्थिति में सिस्टम की अस्थायी रुकावट भी स्वीकार नहीं की जाती. चूंकि हम अपने दैनिक जीवन में आईओटी पर अधिक भरोसा करने लगे हैं, अतः आईओटी डेवलपर्स को आईओटी डाटा, वेब और मोबाइल एप की उपलब्धता पर विचार करना चाहिए जो उस डाटा पर भरोसा करते हों, साथ ही साथ उस तक उनकी भौतिक पहुंच भी हो. कनेक्टिविटी आउटेज या डिवाइस फेल्योर के परिणामस्वरूप व्यवधान की संभावना denial of service attacks से उत्पन्न होने वाली असुविधा से भी अधिक असुविधाजनक है. कुछ एप्लिकेशन में, उपलब्धता की कमी के प्रभाव का मतलब राजस्व नुकसान, डिवाइस की क्षति या यहां तक कि जीवन की हानि भी हो सकती है. उदाहरण के लिए, आईओटी से जुड़े शहर में आवश्यक सेवाओं के लिए आधारभूत संरचना जैसे यातायात नियंत्रण और स्वास्थ्य सेवा जैसे पेसमेकर या इंसुलिन पम्प शामिल हैं. आईओटी डिवाइसों की उपलब्धता सुनिश्चित करने के लिए साइबर हमलों के

साथ-साथ भौतिक छेड़छाड़ को भी संरक्षित करना होगा. बिन्दु मात्र की फेल्योर को रोकने के लिए आईओटी सिस्टम रिडंडेन्सी को शामिल करना होगा.

10. भेद्यता और उल्लंघनों का पता लगाना या प्रबंधन करना/ Detect and Manage Vulnerabilities and Incidents:

सर्वोत्तम प्रयासों के बावजूद, सुरक्षा भेद्यता और उल्लंघन अपरिहार्य है. आप कैसे पता लगाएंगे कि आपके आईओटी सिस्टम से समझौता किया गया है या नहीं? बड़े पैमाने पर आईओटी सिस्टम से जुड़ी डिवाइसों की संख्या के मामले में सिस्टम की जटिलता और विभिन्न प्रकार की डिवाइसों, ऐप्स, सेवाओं और संचार प्रोटोकॉल शामिल होने पर, भेद्यता और उल्लंघनों को पहचानना मुश्किल हो सकता है. सुरक्षा भेद्यता और उल्लंघनों का पता लगाने की रणनीतियों में नेटवर्क संचार एवं एक्टिविटी लॉग की निगरानी, भेद्यता या कमजोरियों का पता लगाने के लिए पेनीट्रेशन टेस्टिंग और एथिकल हैकिंग को शामिल करना और इंसिडेंट्स की पहचान कर उसे सूचित करने के लिए सेक्युरिटी इंटेलिजेंस और एनालेटिक्स सिस्टम को लागू करना चाहिए. आईओटी सिस्टम की भेद्यता या उल्लंघनों की सीमाओं का आकलन करना भी चुनौतीपूर्ण कार्य है. "डिवाइस मैनेजर" डिवाइसों का एक रजिस्टर बनाएं, जिसका उपयोग अस्थायी रूप से प्रभावित डिवाइसों को अक्षम या अलग करने के लिए किया जा सकता है, जब तक कि इसे पैच न कर लिए जाए. यह सुविधा गेटवे डिवाइसों जैसी प्रमुख डिवाइसों के लिए विशेष रूप से महत्वपूर्ण है ताकि उनकी नुकसान या व्यवधान पैदा करने की अपनी क्षमता को सीमित किया जा सके. भेद्यता और उल्लंघन प्रबंधन नीतियों के आधार पर रुल्स इंजन का उपयोग कर प्रबंधन कार्य को स्वचालित किया जा सकता है.

निष्कर्ष : वर्तमान में आईओटी के लिए चिन्हित प्रमुख डोमेन जैसे ऊर्जा, स्मार्ट सिटी, परिवहन, स्मार्ट होम, पर्यावरण, आपूर्ति श्रृंखला और स्वास्थ देखभाल है. आईओटी विकास के लिए बहु-स्तरीय सुरक्षा दृष्टिकोण को अपनाने के लिए डिवाइसों, डाटा, मोबाइल और क्लाउड-आधारित आईओटी एप्स और सेवाओं को सुरक्षित प्रबंधन के साथ-साथ खतरे या मुद्दों से निपटने की आवश्यकता है. जहां सुरक्षा सुविधाओं को सबसे सुरक्षित सेटिंग्स पर कॉन्फ़िगर किया गया हो, वहां डिफ़ॉल्ट सुरक्षा सुविधाओं को शामिल करना चाहिए; ताकि आरंभ और विकास के बाद आपको डाटा की गोपनीयता, अखंडता और उपलब्धता (CIA) को बनाए रखा जा सके.

डिजिलॉकर, भारत सरकार की दस्तावेज संरक्षण हेतु पेपरलेस पहल

राज कुमार सिंह
वरिष्ठ प्रबंधक
स्टाफ प्रशिक्षण केंद्र, भोपाल

(छायाचित्रः www.india.gov.in)

देश को विश्वपटल पर ज्ञानाधारित अर्थव्यवस्था के रूप में स्थापित करने हेतु भारत सरकार द्वारा शुरू की गयी एक बदलावकारी पहल है, डिजिलॉकर. यह देश को डिजिटल आधार पर सशक्त बनाने का प्रमुख प्रयास है. यह भारत सरकार के इलेक्ट्रानिक्स एवं डिजिटल प्रौद्योगिकी विभाग द्वारा शुरू की गई केन्द्रीयकृत प्रणाली है, जिसके द्वारा दस्तावेजों एवं प्रमाणपत्रों को डिजिटल रूप में न केवल ऑनलाइन सुरक्षित रखा जा सकता है, बल्कि इन्हें डिजिटल स्वरूप में विभिन्न विभागों की आवश्यकतानुसार उपयोग भी किया जा सकता है. इस प्रकार दस्तावेजों को भौतिक रूप से लाने-ले जाने के जोखिम से बचा जा सकता है. कार्यालयों में कागजों की भरमार को भी इस नयी पहल से दूर किया जा सकता है. इसके साथ ही काम की गति को भी कई गुना बढ़ाया जा सकता हैं.

कौन से दस्तावेज सुरक्षित रखे जा सकते हैं?

भारत के नागरिक डिजिलॉकर सुविधा का लाभ उठाकर अपना पैन कार्ड, वोटर कार्ड, अकादमिक प्रमाणपत्र, इत्यादि सुरक्षित रख सकते हैं. इसमें ई-दस्तावेज जारीकर्ता के द्वारा उपलब्ध करवाया गया संयुक्त श्रोत प्रदर्शक (यूआरआई) भी उपलब्ध होता है. भारतीय अद्वितीय पहचान प्राधिकरण (यूआईडीएआई) द्वारा एक जीबी का डाटा

डिजिलॉकर में संबद्ध किया जाता है. डिजिलॉकर में प्रदान किया गया स्थान व्यक्तिगत होता है. दस्तावेजों को सुरक्षित रखने का यह उत्तम तथा ऑनलाइन माध्यम है.

डिजिलॉकर का उद्देश्य है, दस्तावेजों की भौतिक प्रतियों के उपयोग में कमी लाना तथा विभिन्न एजेंसियों के मध्य दस्तावेजों के इलेक्ट्रानिक वर्जन के आदान-प्रदान को सुदृढ़ करना. डिजिलॉकर भारत सरकार द्वारा अपने नागरिकों को प्रदान की गयी क्लाउड आधारित व्यवस्था है, जो दस्तावेजों को आनलाइन सुरक्षित रखने की सुविधा प्रदान करता है. यहाँ पर दस्तावेजों की स्कैन प्रतियाँ सुरक्षित रख उन्हें किसी भी समय उपयोग में लाया जा सकता है. इतना ही नहीं शासकीय सेवाओं का त्वरित लाभ उठाने के लिए यहाँ पर सुरक्षित रखे गये दस्तावेजों को किसी भी सरकारी विभाग के साथ आसानी से साझा भी किया जा सकता है. यह शासकीय सेवाओं को आनलाइन प्रदान करने में भी सहायक है. इसके साथ ही इस प्लेटफार्म के माध्यम से विभिन्न सरकारी विभाग दस्तावेज जारी कर सकते हैं तथा उन्हें सत्यापित भी कर सकते हैं.

इस पोर्टल के द्वारा ई-दस्तावेजों को पंजीकृत कोड द्वारा साझा किया जाता है, जिससे दस्तावेज की ऑनलाइन प्रामाणिकता को भी सुनिश्चित किया जा सकता है. भारतीय नागरिक अपने दस्तावेजों को इलेक्ट्रानिक फार्म में अपलोड कर उन्हें ई-हस्ताक्षर सुविधा द्वारा हस्ताक्षरित भी कर सकते हैं. इस प्रकार डिजिटल तौर पर उन्हें सत्यापित भी किया जा सकता है. ऐसे दस्तावेजों को शासकीय अथवा अन्य उपक्रमों में मांग किये जाने पर प्रदान भी किया जा सकता है तथा सभी कार्यालय द्वारा स्वीकार्य भी है. भारतीय नागरिक अपने वसीयती दस्तावेजों को भी स्कैन कर यहाँ पर अपलोड कर सकते हैं, ऐसे दस्तावेजों को ई-हस्ताक्षरित भी किया जा सकता है.

उद्देश्य

डिजिलॉकर एक बहुेशीय पोर्टल है, इसके निम्नांकित उद्देश्य है :

- क्लाउड के जरिये डिजिटल लॉकर सुविधा उपलब्ध करवाकर नागरिकों का डिजिटल सशक्तिकरण करना
- ई-हस्ताक्षर सुविधा प्रदान कर, उसे उपलब्ध करवाना
- भौतिक दस्तावेजों के उपयोग में कमी लाना
- ई-दस्तावेजों की प्रामाणिकता सुनिश्चित करना तथा फर्जी दस्तावेजों के प्रचलन को रोकना
- नागरिकों को वेबसाइट एवं मोबाइल एप के जरिये शासकीय दस्तावेज उपलब्ध करवाना
- प्रशासनिक भार को कम कर नागरिकों को शासकीय सुविधाएं प्राप्त करने में सहयोग प्रदान करना

- गोपनीयता बनाए रखना तथा नागरिकों का डाटा पर प्राधिकार सुनिश्चित करना
- नागरिकों की कहीं भी और कभी भी दस्तावेजों तक पहुंच

डिजिलॉकर का स्वरूप

डिजिलॉकर को निम्नांकित भागों में वर्गीकृत किया जा सकता हैं -

माई सर्टिफिकेट - इसके 2 उपभाग होते हैं -

(i) **डिजिटल दस्तावेज :** इसमें उपयोगकर्ता को शासकीय विभाग अथवा अन्य एजेंसी द्वारा जारी दस्तावेजों की यूआरआई होती है.

(ii) **अपलोडेड दस्तावेज :** इसमें वे दस्तावेज सम्मिलित होते हैं, जिन्हें उपयोगकर्ता द्वारा अपलोड किया जाता है. अपलोड किये जाने वाले दस्तावेज का फाइल साइज 1 एमबी से अधिक नहीं होना चाहिए तथा पीडीएफ, जेपीजी, जेपीईजी, पीएनजी, बीएमपी व जीआईएफ प्रकार के फाइल को ही अपलोड किया जाना चाहिए.

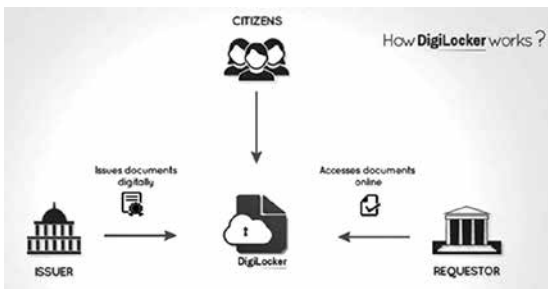
माई प्रोफाइल - इसमें उपयोगकर्ता की यूआईडीएआई में उपलब्ध जानकारी प्रदर्शित होती है.

माई इश्यूअर्स - इसमें उपयोगकर्ता को जारी किये गये दस्तावेजों के जारी करने वाले विभाग अथवा एजेंसियों की जानकारी तथा उनके द्वारा जारी किये दस्तावेजों की संख्या प्रदर्शित होती है.

माई रिक्वेस्टर्स - इसमें उपयोगकर्ता से दस्तावेजों की मांग करने वाले निकायों की सूची होती है.

डाइरेक्ट्री - यहाँ पर पंजीकृत रिक्वेस्टर्स एवं इश्यूअर्स (जारीकर्ताओं) की सूची उनके यूआरएल (URL) के साथ दी जाती है.

मुख्य घटक



(छायाचित्रः www.digilocker.gov.in)

डिजिलॉकर के मुख्य घटक है -

रिपोजिटरी - यह ई-दस्तावेजों का संग्रह है जिसमें दस्तावेज एपीआई के जरिये तुरंत उपलब्ध होते हैं.

एक्सेस गेटवे - यह दस्तावेज चाहने वाली इकाइयों हेतु सुरक्षित तौर पर विभिन्न रिपोजिटरी से ई-दस्तावेज प्राप्त करने हेतु एक प्रणाली है, जिसमें यूआरआई के माध्यम से दस्तावेज साझा किये जाते हैं.

डिजिलॉकर का पोर्टल - यह क्लाउड आधारित व्यक्तिगत साइबर स्पेस है, जो उपयोगकर्ता के ई-दस्तावेजों को सुरक्षित रखने के लिए आधार अथवा यूआरआई द्वारा जुड़ा होता है. डिजिलॉकर में पंजीकृत दस्तावेज जारीकर्ताओं की सूची भी होती है साथ ही इसमें विभिन्न गेटवे, रिपोजिटरी, से जुड़े हुए दिशानिर्देश भी होते हैं. डैशबोर्ड, तत्काल ई-दस्तावेजों के लेनदेन हेतु होता है, जिसे उपयोगकर्ता द्वारा उपयोग में लाया जा सकता है.

हितधारक

डिजिलॉकर प्रणाली के मुख्य रूप से तीन हितधारक है -

नागरिक - भारतीय नागरिक इसमें अपने दस्तावेज रखकर उनका उपयोग कर सकते हैं. इसमें अपलोड किये हुए अथवा जारी किये हुए दस्तावेजों को सुरक्षित रखा जा सकता है -

(i) **अपलोड किये गये दस्तावेज** - भारतीय नागरिक अपने महत्वपूर्ण दस्तावेजों की स्कैन प्रति को अपलोड कर सकते हैं. इन दस्तावेजों में पैन कार्ड, ईपीआईसी, पासपोर्ट, स्कूल के प्रमाणपत्र, इत्यादि हो सकते हैं. यदि किसी शासकीय एजेंसी

द्वारा मांग की जाती है तो वे ई-हस्ताक्षरित प्रति को भी मांगकर्ता एजेंसी को प्रेषित कर सकते हैं. यह आवश्यक है कि मांग करने वाली एजेंसी को दस्तावेज प्राप्तकर्ता अर्थात प्रार्थी के रूप में पंजीकृत होना चाहिए.

(ii) **जारी किये गये दस्तावेज** - ऐसे दस्तावेज, जिन्हें जारीकर्ता विभाग अथवा एजेंसी द्वारा डिजिलॉकर पर जारी किया गया हो. जारीकर्ता उपयोगकर्ता के आधार क्रमांक पर दस्तावेज की यूआरआई प्रदान करेगा. ये यूआरआई केन्द्रीय रिपोजिटरी में संग्रहित होती हैं तथा उपयोगकर्ता इन्हें देख सकता है अथवा इनकी लिंक को साझा कर सकता है.

जारीकर्ता - विभिन्न शासकीय एजेंसियां ई-दस्तावेज जारी कर्ता के रूप में पंजीकृत होकर इलेक्ट्रानिक स्वरूप में दस्तावेज जारी कर सकती हैं. ऐसी एजेंसियों में सीबीएसई, रजिस्ट्रार कार्यालय, आयकर विभाग और इसी तरह के अन्य विभाग, जो किसी भी प्रकार के दस्तावेज जारी करते हैं, इसमें सम्मिलित किये जा सकते हैं. 2016 में सीबीएसई द्वारा कक्षा 12वीं के परीक्षा परिणाम डिजिलॉकर पर जारी किये गये हैं. आगे से सभी सीबीएसई परीक्षाफल डिजिलॉकर पर भी जारी किये जाएंगे. जारीकर्ताओं के लिए इसमें विरासत संबंधी कानूनी दस्तावेज (Legacy data) जारी करने की सुविधा भी प्रदान की गयी है. ऐसे दस्तावेजों के मामले में जारी कर्ता के डाटा के साथ आधार का जुड़ा होना आवश्यक है.

प्रार्थी/मांगकर्ता - डिजिलॉकर के संदर्भ में प्रार्थी से अभिप्राय उस शासकीय विभाग से है, जो नागरिकों को सेवा प्रदान करता है. इसमें राजस्व विभाग, पासपोर्ट कार्यालय, अथवा स्थानीय प्रशासन जैसे विभाग सम्मिलित हो सकते हैं. अन्य संगठन जिन्हें दस्तावेजों की आवश्यकता होती है, जैसे बैंक, दूरसंचार से जुड़ी सेवा प्रदाता कंपनियाँ इत्यादि. शासकीय सेवा प्रदान करने हेतु किसी शासकीय एजेंसी को किसी व्यक्ति विशेष की निजी जानकारी यथा आयु, राष्ट्रीयता को ज्ञात करने के लिए विभिन्न शासकीय विभागों/एजेंसियों द्वारा जारी किये गये मानक एवं सहायक दस्तावेजों की आवश्यकता होती है. सेवा प्रदान करने के लिए एजेंसियों के द्वारा दस्तावेजों की ई-प्रति की मांग की जा सकती है. डिजिलॉकर की सहायता से ई-प्रति लाभार्थी द्वारा प्रदान की जा सकती है. यह प्रक्रिया डिजिलॉकर पर त्वरित गति से बहुत आसानी से संभव है.

सुरक्षा उपाय

डिजिलॉकर एक पूर्णतः सुरक्षित प्लेटफार्म है. इसमें सुरक्षा के पर्याप्त उपाय किये गये हैं जो नीचे दिए गए चित्र में प्रदर्शित है.

भारत सरकार के सूचना एवं आईटी विभाग द्वारा प्रबन्धित यह लॉकर एसएसएलके द्वारा एचटीटीपीएस सुरक्षा प्रणाली द्वारा सुरक्षित है, जो कि फिलहाल वेबसाइट सुरक्षा के लिए सबसे सुरक्षित प्रणाली है. वेबसाइट के यूआरएल (https:// digitallocker.gov.in) में noclick_https:// और उसके आगे एक हरा ताला इसकी सुरक्षा का द्योतक है. यहाँ 's' का मतलब अंग्रेजी का शब्द secure से है.

कैसे करें पंजीयन

पंजीयन हेतु आपके पास इन्टरनेट कनेक्शन के साथ लैपटाप, पीसी अथवा स्मार्ट फोन होना चाहिए तथा एक सक्रिय मोबाइल नंबर भी होना चाहिए-

- पंजीयन के लिए वेब www.digilocker.gov.in के **'register'** पृष्ठ में जायें.
- स्क्रीन के दाईं ओर बने बॉक्स में अपना मोबाइल नंबर दर्ज करें और आगे दिये गए **'जारी'** (Continue) बटन पर क्लिक करें.
- आपको अपने मोबाइल पर ओटीपी (One Time Password) प्राप्त होगा.
- दूसरे टेक्स्ट बाक्स में ओटीपी दर्ज कर, **'वेरिफ़ाई'** बटन दबाकर अपना नंबर सत्यापित करें.
- सत्यापन होने पर आपको **यूजर आईडी** तथा **पासवर्ड** बनाने हेतु अवसर मिलता है. आपका पासवर्ड 8 से 30 अक्षरों वाला पासवर्ड होना चाहिए जिसमें कम से कम एक अक्षर, एक अंक तथा एक विशेष चिह्न होना अनिवार्य है.
- यहाँ पर आधार की जानकारी भी मांगी जाती है, जिसे आप भर सकते हैं या बिना भरे भी छोडकर आगे बढ़ सकते हैं.

- डिजिलॉकर तैयार होने की प्रक्रिया के दौरान स्क्रीन पर एक संदेश मिलता है, **'इस दौरान स्क्रीन को रीफ्रेश न करें'**. कुछ मिनट प्रतीक्षा कर पेज को रीफ्रेश करें.
- तत्पश्चात आप **'लॉगिन पेज'** पर पहुंचते है, जहाँ पर **यूज़र आईडी** एवं **पासवर्ड** की सहायता से **लॉगिन** किया जा सकता है. लॉगिन करने पर एक बधाई संदेश प्राप्त होता है. अब आप अपने डिजिलॉकर का उपयोग आरंभ कर सकते हैं.
- अपने ई-मेल को यहाँ दिये गये बाक्स में दर्ज कर सत्यापित कर सकते हैं. आपके ई-मेल बॉक्स में सत्यापन हेतु एक ई-मेल आता है और यहाँ पर दी गयी हाइपर लिंक पर क्लिक कर ई-मेल को सत्यापित किया जा सकता है.
- अब आप को डिजिलॉकर की वेबसाइट पर रीडाइरेक्ट कर दिया जाता है. यहाँ आप **साइन-इन** कर अपने दस्तावेजों को अपलोड कर सकते हैं.

दस्तावेजों एवं प्रमाणपत्रों का अपलोड किया जाना

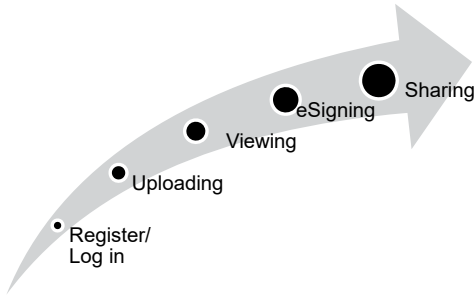
- **साइन-इन** करने के पश्चात **'अपलोडेड डाक्यूमेंट'** बटन पर क्लिक करें और अब डॉक्युमेंट्स अपलोड करने के लिए **'अपलोड'** बटन पर क्लिक करके, लोकेशन व फ़ाइल का चयन करें.
- एक समय पर एक से अधिक दस्तावेजों को अपलोड किया जा सकता है.
- **'अपलोडेड सेक्शन'** में जाकर अपलोड किये गये दस्तावेजों को देखा जा सकता है. यहाँ पर फाइल के नाम तथा प्रकार को सुधारा या बदला जा सकता है. यहाँ से फाइल को डाउनलोड तथा साझा भी किया जा सकता है.

e-Sign/ई-साइन दस्तावेज या प्रमाणपत्र

- 'अपलोडेड दस्तावेजों' के फोल्डर में प्रत्येक दस्तावेज के साथ ई-साइन (e-Sign) का लिंक दिया गया है, इस लिंक पर क्लिक करें.
- क्लिक करने पर उपयोगकर्ता के मोबाइल पर ओटीपी आता है, जिसे दिये गये स्थान पर दर्ज करना होता है.
- इसके पश्चात ई-साइन के बटन पर क्लिक करना होता है और चयनित दस्तावेज के साथ ई-साइन जुड़ जाएगा. यदि दस्तावेज पीडीएफ नहीं है तो वह पीडीएफ में परिवर्तित हो जाएगा.
- एक समय पर केवल एक ही दस्तावेज ई-साइन किया जा सकता है.

दस्तावेज या प्रमाणपत्र को साझा करना

- **'अपलोडेड दस्तावेजों'** सेक्शन में उपलब्ध करवाई गयी 'शेयर' लिंक पर क्लिक करें.
- प्रत्येक दस्तावेज के साथ इस तरह की लिंक उपलब्ध है.
- एक पॉप-अप विंडो खुलेगी, जिसमें उपयोगकर्ता वह ई-मेल दर्ज करेगा, जिस पर उसे दस्तावेज प्रेषित करना है.
- ई-मेल आईडी दर्ज करने के पश्चात 'सेंड' (send) बटन पर क्लिक करना होता है.
- चयनित दस्तावेज संबंधित संस्था/व्यक्ति के साथ साझा हो जाएगा.
- एक बार में केवल एक ही दस्तावेज साझा किया जा सकता है.



दस्तावेज/ प्रमाणपत्र जारी करना

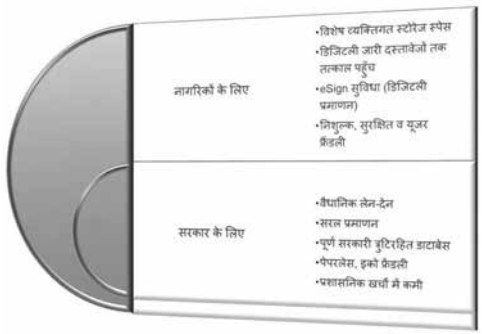
- किसी जारीकर्ता को प्रमाणपत्र जारी करने हेतु स्वयं को अपनी अद्वितीय पहचान संख्या (Unique Issuer ID) लेने हेतु पंजीयन करवाना होता है.
- जब आईडी बन जाता है, तो जारीकर्ता दस्तावेज को रिपोजिटरी में एक्सएमएल (XML) प्रारूप में अपलोड करता है. इसमें रिपोजिटरी सर्विस प्रोवाइडर API की निर्दिष्ट रिपोजिटरी इस्तेमाल की जाती है.
- रिपोजिटरी में अपलोड प्रत्येक दस्तावेज की भिन्न यूआरआई (Unique URI) होती है, जिसमें जारीकर्ता आईडी दस्तावेज प्रकार तथा दस्तावेज आईडी शामिल रहता है.
- दस्तावेज यूआरआई मांगकर्ता के आधार से जुड़े डिजिलॉकर में चला जाता है.

जारी दस्तावेजों को देखना

- समस्त जारी दस्तावेजों को देखने के लिए **'लॉगिन'** करने के पश्चात "**इश्यूड डाक्यूमेंट**" पर क्लिक करें.
- यहाँ पर जारीकर्ता के साथ साझा किए हुए समस्त दस्तावेजों की यूआरआई प्रदर्शित होती है.
- **'यूआरआई'** पर क्लिक करके वास्तविक दस्तावेजों को जारी कर्ता के डाटाबेस सिस्टम से डाउनलोड किया जा सकता है या देखा जा सकता है.

लाभ

डिजिलॉकर से दोनों ही पक्षों यथा जन सामान्य एवं सरकार दोनों को ही लाभ हैं -



डिजिलॉकर पोर्टल की सफलता को यहां पर पंजीकृत उपयोगकर्ताओं की संख्या से भलीभांति समझा जा सकता है. फरवरी 2015 में शुरू होने के पश्चात सितंबर 2018 तक 1.57 करोड़ लोग इस पर पंजीयन करवा चुके हैं. 2 करोड़ से अधिक दस्तावेज यहाँ पर अपलोड किये जा चुके हैं तथा 3 करोड़ से अधिक दस्तावेज विभिन्न जारीकर्ताओं द्वारा जारी किये जा चुके हैं. हालाँकि प्रथम दृष्ट्या ये आँकड़े अच्छे प्रतीत हो सकते हैं, किंतु इसमें बहुत कुछ किया जाना आवश्यक है.

देश को विकसित अर्थव्यवस्था बनाने तथा देश में काम-काज की गति को बढ़ावा देने के लिए आवश्यक है कि डिजिलॉकर जैसी सुविधा को अधिकाधिक उपयोग में लाया जाए. आज देश में सक्रिय इंटरनेट उपयोगकर्ताओं की संख्या बढ़ी है, 2020 तक यह 73 करोड़ व्यक्ति हो जाएगी. ऐसे में यह आवश्यक है कि डिजिलॉकर के विषय में जानकारी एवं जागरूकता को बढ़ावा मिले.

संदर्भः

1. www.digilocker.gov.in
2. www.wikipedia.org/wiki/DigiLocker
3. www.internetlivestats.com
4. www.india.gov.in

चैटबॉट

विश्वास कुमार आनंद
प्रबंधक
डिजिटल बैंकिंग विभाग, कें. का., मुंबई

मित्रों आपने अक्सर ऐसा देखा होगा, जब हम किसी सहायता के लिए ग्राहक सेवा केंद्र को फोन करते हैं, तो हमें यह सुनाई देता है "आप कतार में हैं" या आपसे प्रतीक्षा करने के लिए कहा जाता है. यह अनुभव किसी प्रकार से भी आनंदायक नहीं होता. दूसरी ओर अगर आप कॉल सेंटर अधिकारी के कार्यकलाप को देखें, तो पाएंगे कि वह पूरे दिन एक ही तरह की प्रश्नावली का उत्तर बार-बार देते रहते हैं. यह प्रक्रिया समय और संसाधन दोनों की बर्बादी है.

इस स्थिति में गुणात्मक बदलाव के लिए टेक्नोलॉजी हमारी सहायता कर सकती है. चैटबॉट इस समस्या का बेहतरीन समाधान है. आर्टिफिशियल इंटेलिजेंस का विकास अब अपने अंतिम चरण में पहुंच गया है और तकनीक की इस महारत का इस्तेमाल चैटबॉट में व्यापक रूप से होने लगा है. ग्राहक सेवा को अधिक सुगम और सटीक तथा उनके अनुभव को आनंदमय बनाने के लिए, सूचनाओं को उन तक त्वरित गति से पहुंचाना आवश्यक है. इसी कारण चैटबॉट सेवा का इस्तेमाल व्यावसायिक रूप से होने लगा है. बातचीत करने में समर्थ, पहला चैटबॉट अमेरिका के एक कंप्यूटर साइंस इंजीनियर जोसफ वेइजेनबॉम ने 1966 ईस्वी में बनाया और उसका नाम एलिजा रखा गया. कुछ ही दिनों में एलिजा बातचीत करने में इतनी सक्षम हो गई कि उसका प्रयोग करने वालों को उसमें और मानव एजेंटों में कोई फर्क महसूस नहीं होता था.

आज के समय में मैसेजिंग एप जैसे व्हाट्सएप, फेसबुक मैसेंजर आदि की मांग बहुत तेजी से बढ़ रही है. एक अनुमान के मुताबिक, पूरी दुनिया में आज 100 करोड़ से ज्यादा लोग इन सुविधाओं का इस्तेमाल कर रहे हैं. विश्व प्रसिद्ध व्यवसायिक परामर्शदात्री संस्था गार्टनर के अनुसार निकट भविष्य में 84% संवाद चैटबॉट के माध्यम से किए जाएगें.

आज चैटबॉट सुविधाओं का इस्तेमाल अनेक क्षेत्रों में किया जा रहा है, जैसे बैंकिंग, ग्राहक सेवा, मेडिकल तथा शिक्षा. डिजिटल मार्केटिंग की दुनिया में चैटबॉट

सिर्फ सूचनाओं के आदान-प्रदान तक ही सीमित नहीं है बल्कि उनका इस्तेमाल मार्केटिंग गतिविधियों में बहुतायत में किया जा रहा है. इन के माध्यम से एकत्रित एनालिटिक्स ग्राहकों के बारे में बहुत सारी सूचनाएं एकत्रित करने में मदद करता है. इन जानकारियों के आधार पर हम ग्राहक केंद्रित कई नई सेवाओं का आरंभ कर सकते हैं. इस प्रकार चैटबॉट ना सिर्फ ग्राहक सेवा की गुणवत्ता बढ़ाने बल्कि ब्रांड के संबंध में ग्राहकों की अवधारणा को मजबूत करने में मदद करता है.

चैटबॉट क्या है और यह किस प्रकार हमारी सहायता करता है?

चैटबॉट एक विशेष प्रकार का कंप्यूटर प्रोग्राम है, जो यूज़र के साथ बातचीत से संपर्क स्थापित करने के लिए डिजाइन किया जाता है. विशेष तौर पर यह संपर्क, इंटरनेट के माध्यम से स्थापित होता है. यह एक प्रकार का वर्चुअल सहायक है, जो हमें वांछित सूचनाएं प्रदान करने में मदद करता है. चैटबॉट एक खास तरह की तकनीक है, जिसे नेचुरल लैंग्वेज प्रोसेसिंग (NLP) कहा जाता है. इसका इस्तेमाल यूज़र की भाषा और उसकी भावना या इंटेंट (intent) पता करने में करते हैं. फिर अपने डेटाबेस में सर्च कर सटीक जानकारी उत्तर के रूप में प्रदान करते हैं. ऐसा करने के लिए सॉफ्टवेयर डेवलपर लगातार चैट ट्रांसक्रिप्ट (transcript) का विश्लेषण करता रहता है. फिर इन विश्लेषण का उपयोग कर बॉट को प्रशिक्षित किया जाता है. इस प्रक्रिया को बॉट ट्रेनिंग प्रोसेस कहा जाता है.

यह सवाल उठ सकता कि हमें इसकी आवश्यकता क्यों?

हर व्यवसाय या सेवा क्षेत्र में कुछ ऐसे कार्य होते हैं, जो रूटीन किस्म के होते हैं. रूटीन क्रियाओं के संपादन के लिए हमें काफी धन और मानव श्रम का उपयोग करना पड़ता है. चैटबॉट के प्रयोग से रूटीन क्रियाओं के संपादन में गुणवत्ता बढ़ाई जा सकती है तथा मानव श्रम तथा धन दोनों की बचत हो सकती है. आर्टिफिशियल इंटेलिजेंस के सहयोग से चैटबॉट बहुत ही कम समय में वार्तालाप के क्रम में ही नई जानकारियों को सीखते रहते हैं तथा कुछ समय पश्चात बिना किसी निगरानी के सूचनाओं के निष्पादन में सक्षम हो जाते हैं. रूटीन क्रियाओं को करने में ना सिर्फ समय की बचत होती है बल्कि एक साथ कई चैनलों के माध्यम से ग्राहकों से संपर्क स्थापित करना संभव हो पाता है. इस तरीके से हमारी उत्पादकता कई गुना बढ़ जाती है और ऑपरेटिंग कॉस्ट बहुत ही कम हो जाता है.

चैटबॉट के विभिन्न प्रकारः

1. **मेनू आधारित (menu based) चैटबॉट**

   यह सबसे साधारण किस्म के चैटबॉट होते हैं. यूज़र को स्क्रीन पर दर्शाए गए कई ऑप्शन में से किसी एक को क्लिक करना होता है. यूज़र क्लिक और बटन के माध्यम से सूचना प्राप्त कर सकते हैं. सामान्यता इस तरह के चैटबॉट में प्रश्न

पहले से तय होते हैं तथा यूज़र के सलेक्शन के अनुसार रिस्पांस दिया जाता है. इस तरह के चाटबॉट रूटीन किस्म के सवालों के जवाब देने के लिए सक्षम होते हैं, लेकिन जटिल संवादों में इनकी उपयोगिता इतनी अच्छी नहीं है. इनका इस्तेमाल बड़े पैमाने पर काफी महंगे आईवीआर के विकल्प की तरह किया जा रहा है. फॉरेस्टर के मुताबिक ग्राहक सेवा के क्षेत्र में इस तरह के रूटीन प्रश्नों का प्रतिशत 80% के आसपास है. अतः यह साधारण किंतु बहुत ही सटीक समाधान है.

2. की-वर्ड आधारित चैटबॉट

मेनू बेस्ड चैटबॉट के पृथक, यह चैटबॉट यूज़र के टाइपिंग को लगातार देखते रहते हैं. टाइप किए गए शब्दों के अनुसार यूज़र के प्रश्न को समझते हैं या समझने की कोशिश करते हैं. पूछे गए शब्दों में से कीवर्ड्स के आधार पर उपयुक्त उत्तर देने की कोशिश करते हैं. इस प्रकार के चैटबॉट यूज़र को मनचाही जानकारी प्रदान करने के लिए customizable की-वर्ड का प्रयोग करते हैं.

उदाहरण के लिए यदि कोई यूज़र पूछता है, "मैं डेबिट कार्ड का पिन कैसे जनरेट कर सकता हूं?" तो चैटबॉट कुछ कीवर्ड जैसे "डेबिट कार्ड" "पिन जनरेशन" इत्यादि के कॉन्बिनेशन से यह पता कर लेता है कि यूज़र डेबिट कार्ड का पिन सेट करना चाहता है. इसके उपरांत यह अपने डेटाबेस में इसका ठीक-ठीक उत्तर सर्च करता है तथा यूज़र को पिन जनरेशन की प्रक्रिया साझा करता है.

3. कंटेक्सटुअल चैटबॉट

कंटेक्सटुअल चैटबॉट सबसे उन्नत हैं. ये बॉट मशीन लर्निंग (ML) और आर्टिफिशियल इंटेलिजेंस (AI) का उपयोग यूज़र के साथ बातचीत को याद रखने और उसका इंटेंट समझने के लिए करते हैं. की-वर्ड-आधारित चैटबॉट के विपरीत, यह बॉट्स उपयोगकर्ता जो पूछ रहा है और वे इसे कैसे पूछ रहा है, इसे समझने में सक्षम होता है. सेल्फ लर्निंग के आधार पर उत्तरों में पर्याप्त परिवर्तन करने के लिए प्रोग्राम बनाए जाते हैं. हर वार्तालाप के साथ इनकी क्षमता में गुणात्मक सुधार होता रहता है.

उदाहरण के लिए, एक कंटेक्सटुअल चैटबॉट, जो उपयोगकर्ता को पिज्जा ऑर्डर करने की अनुमति देता है, डेटा को प्रत्येक वार्तालाप के दौरान स्टोर करेगा और यह जानने का प्रयास करता है कि उपयोगकर्ता किस तरह ऑर्डर करना पसंद करता है. नतीजतन जब कोई उपयोगकर्ता अगली बार इस बॉट के साथ चैट करता है, तो बॉट उपयोगकर्ता का नवीनतम आदेश, उनके डिलीवरी पते और उनकी भुगतान संबंधी जानकारी याद रखता है और केवल यह पूछता है कि क्या वे इस आदेश को दोहराना चाहते हैं. कई सवालों के जवाब देने के बजाय उपयोगकर्ता को सिर्फ 'हां' जवाब देना है और पिज्जा डिलीवरी के लिए तैयार है!

हालांकि यह एक बहुत ही बुनियादी उदाहरण है. यह टेक्नोलॉजी अभी विकास की प्रक्रिया में है. यह देखना रोचक है कि एआई(AI) और एमएल(ML) के उपयोग से भविष्य में कितना सटीक वार्तालाप संभव हो सकता है. यह सॉल्यूशन लगातार बातचीत के क्रम में एकत्रित सूचना तथा पूछने के तरीके, उसके हाव-भाव, यूज़र के मूड इत्यादि के आधार पर, डेटा का संवर्धन करता रहता है. इन सूचनाओं को लाइब्रेरी में संग्रहित किया जाता है तथा भविष्य की वार्तालाप में इसका इस्तेमाल किया जाता है. भविष्य में इस टेक्नोलॉजी की उपयोगिता, समस्या के समाधान में लिए गए समय और सटीकता में होने वाले सुधार से तय होगी.

चैटबॉट काम कैसे करता है?

बॉट की पूरी संरचना तीन भागों में बटी होती है. पहला भाग ऍप, दूसरा नॉलेज बेस तथा तीसरा लॉजिक इंजन कहलाता है. एक बार पूर्णतया डेवलप हो जाने के बाद इन्हे रेप्लिकेट करना बहुत आसान होता है. बॉट एक साथ कई सेशन में यूज़र से बातचीत कर सकता है. इसी मॉड्यूलर डिजाइन के कारण विभिन्न प्लेटफार्म पर इसे स्थापित करना आसान होता है. खर्च को कम रखने के उद्देश्य से हम क्लाउड कंप्यूटिंग का लाभ लेते हुए, बॉट के विभिन्न हिस्सों को क्लाउड में भी रख सकते हैं. ऍप को अपनी जरूरत के हिसाब से विभिन्न प्लेटफार्म जैसे वेबसाइट, मोबाइल एप, सोशल मीडिया तथा मोबाइल मैसेंजर के रूप में भी प्रयोग किया जा सकता है. इस तरह एक ही क्लाउड सोल्यूशन से संचार के सारे चैनलों पर बॉट की गतिविधि को नियंत्रित करना संभव है.

चैटबॉट की विशेषताएं :

चैटबॉट की क्षमता उनमें प्रोग्राम की गई कुछ विशेषताओं पर निर्भर करती है. आइए इन विशेषताओं को एक-एक कर समझते हैं :

- इंटेंट पहचानने की क्षमता : यूज़र किस तरह की जानकारी मांग रहा है, इसका सही अंदाज़ा लगाना बहुत ही आवश्यक है. इसी अंदाज़ के भरोसे बॉट सही प्रतिक्रिया दे पाता है. अगर बॉट यूज़र को बिना खिन्न किए वार्तालाप जारी रखना चाहता है और कम से कम चरणों में यूज़र को उत्तर से संतुष्ट करना चाहता है तो बॉट में उन्नत किस्म की इंटैक्ट रिकॉग्निशन तकनीक का होना अति आवश्यक हैं.
- डायलॉग मैनेजमेंट : साधारण प्रश्न और उत्तर के वार्तालाप से अलग हटकर चैटबॉट में कठिन और इमोशनल शब्द और वाक्य समझने की क्षमता होना अति आवश्यक है.
- इंटरेक्शन चैनल : चैटबॉट हर तरह के प्लेटफार्म में कंपैटिबल होने चाहिए. जैसे वेबसाइट, फेसबुक, मोबाइल एप आदि. ताकि यूज़र को हर प्लेटफार्म पर एक

समान संवाद का अनुभव हो.

- सिक्योरिटी एंड कंप्लायंस : सूचना प्रौद्योगिकी एक दो धारी तलवार है. यहां हर सुविधा एक चुनौती लेकर आती है. इस संदर्भ में चाटबॉट का साइबर सिक्योरिटी के सारे मानकों पर खरा उतरना अति आवश्यक है. यदि कार्ड या पेमेंट सिस्टम का प्रयोग किया जा रहा है तो उसका पीसीआई डीएसएस कंप्लायंट होना अनिवार्य है. विभिन्न ऑडिट मानकों पर खरा उतरना भी उसकी स्वीकार्यता के लिए अति आवश्यक है.

एआई(AI) और एमएल(ML) एक शक्तिशाली टेक्नोलॉजी है. चूंकि बॉट यूज़र के वार्तालाप से लगातार सीखता रहता है, अतः इस प्रक्रिया में वह सकारात्मक और नकारात्मक दोनों तरह की बातों को ग्रहण करता है. इसके नकारात्मक और दूरगामी परिणाम भी हो सकते हैं. कई परिस्थितियों में यूज़र द्वारा की गई अभद्र टिप्पणियों को भी वह सामान्य भाषा का हिस्सा बना लेता है. यह डेवलपर के सामने एक बड़ी चुनौती है. इस तरह का गलत रिस्पांस संस्थान की ब्रांड इमेज को बहुत चोट पहुंचा सकता है. माइक्रोसॉफ्ट के चैटबॉट Tay का उदाहरण हमारे सामने हैं. ट्विटरबॉट Tay को 2016 में माइक्रोसॉफ्ट द्वारा लॉन्च किया गया था, जिसमें बातचीत की मानवीय आदतों को समझ, प्रत्युत्तर के स्तर में सुधार करना शामिल था. इसके रिलीज के 24 घंटों से भी कम समय में इसे बंद करना पड़ा, क्योंकि इसने नस्लवादी, लिंगवादी भाषा सहित अनुचित ट्वीट्स किए. माइक्रोसॉफ्ट ने ट्विटर में चैटबॉट की दौड़ जीतने की कोशिश की, लेकिन वह बुरी तरह असफल रहा, क्योंकि बॉट उपयोगकर्ता के जानबूझकर नस्ल भेदी टिप्पणियां को अलग करने में सक्षम नहीं था. यह नमूना भविष्य में मौजूदा आईटी फर्मों के लिए एक चेतावनी हो सकता है. अतः टेक्नोलॉजी के इस्तेमाल में सावधानी बरतना भी अति आवश्यक है.

चैटबॉट बहुत ही कम खर्च में स्थापित किए जा सकते हैं और उनके रखरखाव पर भी बहुत कम खर्च आता है. एक और जहां चैटबॉट सूचनाओं की गुणवत्ता, निरंतरता तथा गति में सहायक हैं, वहीं दूसरी ओर ग्राहक सेवा के क्षेत्र में होने वाले भारी भरकम खर्च को भी कम करने में यह प्रभावकारी सिद्ध हो सकता है.

आपको जानकर हर्ष होगा कि हमारा बैंक भी चैटबॉट की सुविधा अपने ग्राहकों को उपलब्ध करा रहा है. हमारे मुख्य वेबसाइट तथा फेसबुक चैनल पर यह सुविधा उपलब्ध है. हमारे बैंक का चैटबॉट कीवर्ड और कंटेक्सटुअल बेस्ट चैटबॉट का कांबिनेशन है.

27 वें आशीर्वाद पुरस्कार वितरण समारोह में माननीय सांसद
श्री सत्यनारायण जटिया जी से श्रेष्ठ राजभाषा कार्यान्वयन का द्वितीय पुरस्कार
प्राप्त करते हुए बैंक के चेयरमैन श्री केवल हांडा जी,
श्री डी. चिरंजीवी, उप महा प्रबंधक एवं अन्य अधिकारीगण.

58 वें एबीसीआई पुरस्कार वितरण समारोह में अध्यक्ष श्री योगेश जोशी से
बैंक की गृह पत्रिका यूनियन धारा को प्रदत्त चैंपियन ऑफ चैंपियन पुरस्कार
प्राप्त करती हुई यूनियन बैंक टीम.