Union Bank of India

Cyber Security Customer Awareness Guide – Vol. II

Page Index

UPI Scam	1~2
Online Rental Scam	3~4
Customer Care Scam	5~6
Online job fraud	7~8
Fake Video Advertise Scam	9~10
SIM Swap Fraud	11~12
Pig Butchering Scam	13~14
Online Gift Card & Lottery Fraud	15~16
Downloading of Malicious App	17~18

Cyber Security is Everyone's Responsibility

संदेश
सुश्री ए मणिमेखलै
प्रबंध निदेशक एवं सीईओ

डिजिटल उत्कृष्टता की दिशा में यूनियन बैंक ऑफ इंडिया ने विभिन्न डिजिटल चैनलों के माध्यम से साइबर सुरक्षा जागरूकता फैलाकर अपने हितधारकों के बीच सुदृढ़ साइबर सुरक्षा संस्कृति का सृजन कर रहा है। एक अग्रसक्रिय पहल के रूप में, बैंक साइबर सुरक्षा धोखाधड़ी से ग्राहकों को सुरक्षित रखने के लिए साइबर सुरक्षा ग्राहक जागरूकता गाइड श्रृंखला प्रकाशित कर रहा है।

साइबर सुरक्षा जागरूकता श्रृंखला की यह दूसरी पुस्तिका है। मैं सभी पाठकों से पुस्तिका का पुर्ण सदुपयोग करने तथा जागरूकता ज्ञान हासिल करने का आग्रह करती हूं।

संदेश
श्री निधु सक्सेना,
कार्यपालक निदेशक

यूनियन बैंक ऑफ इंडिया डिजिटल क्षेत्र में अपनी बढ़ती मौजूदगी के साथ ही अपने हितधारकों के डिजिटल हितों की रक्षा में साइबर सुरक्षा जागरूकता फैलाकर ठोस कदम उठा रहा है। साइबर सुरक्षा ग्राहक जागरूकता गाइड श्रृंखला का नवीन अंक आपके समक्ष प्रस्तुत है जो नवीनतम साइबर सुरक्षा धोखाधड़ी की व्यापक जानकारी प्रदान करने में सक्षम है।

मैं सभी पाठकों से आग्रह करता हूं कि वे स्वयं को जागरूक करने के साथ-साथ अपने मित्रों व परिवारजनों के बीच भी जागरूकता फैलाने का सुकार्य करें।

संदेश
श्री आर पी सिंह,
सीआईएसओ

यूनियन बैंक ऑफ इंडिया "सुरक्षित और विश्वसनीय" बैंक की अपनी प्रतिबद्धता के प्रति सजग है। अपने हितधारकों को साइबर धोखाधड़ी से बचाने के लिए ही साइबर सुरक्षा जागरूकता गाइड श्रृंखला की शुरूआत की गई है ताकि उन्हें प्रासंगिक रूप से शिक्षित किया जा सके।

इस दूसरी पुस्तिका का उद्देश्य घोटालेबाजों द्वारा अपनाई जाने वाली कार्यप्रणाली के बारे में जागरूकता पैदा करना और ऐसी घटनाओं से बचने के लिए सुरक्षा युक्तियाँ प्रदान करना है। मैं सभी से इसका सर्वोत्तम उपयोग करने का आग्रह करता हूं।
#साइबरजागरूक बनें #साइबर सुरक्षित रहें

Message from
Ms. A. Manimekhalai
MD&CEO

Union Bank of India in its journey towards digital excellence is creating a robust cyber security culture among its stakeholders by spreading cyber security awareness through various digital channels. As a proactive initiative, Bank is publishing cyber security customer awareness guide series, for the benefit of customers for protection from Cyber Security frauds.

This is the 2nd booklet in the cyber security awareness series. I urge all readers to make full use of the booklet to gain awareness.

Message from
Shri Nidhu Saxena,
Executive Director

Union Bank of India with its increasing digital presence is undertaking conclusive steps for creating cyber security awareness for safeguarding digital interest of its stakeholders. Cyber security customer awareness guide series is one such step in providing comprehensive information about latest cyber security frauds.

I urge all readers to make themselves aware and to spread the awareness among their friends & family.

Message from
Shri R P Singh,
CISO

Union Bank of India being true to its commitment of “Safe & Trusted” Bank is proactively educating its stakeholders to safeguard them against cyber frauds by introducing cyber security awareness guide series.

This 2nd booklet is intended to create awareness about the modus operandi adopted by the scammers & to provide safety tips to avoid such incidents. I urge everyone to make the best use of it.

#BeCyberAware #BeCyberSafe

क्या आप क्यूआर कोड स्कैन कर रहे हैं या यूपीआई लिंक पर क्लिक कर रहे हैं?

यूपीआई धोखाधड़ी से सावधान रहें।

कार्यप्रणाली:

- अविश्वसनीय छूट पर वांछित उत्पाद पेश करने के लिए घोटालेबाज द्वारा नकली वेबसाइटें बनाई जाती हैं।
- घोटालेबाज इंटरनेट पर फर्जी कॉल सेंटर नंबर पोस्ट करते हैं। जब उपयोगकर्ता इन टोल-फ्री नंबरों पर कॉल करता है, तो उपयोगकर्ता की समस्या को हल करने के बहाने शुल्क के रूप में कम राशि की मांग के साथ क्यूआर कोड/यूपीआई लिंक भेजा जाता है।
- घोटालेबाज ग्राहकों को एसएमएस/व्हाट्सएप संदेशों के माध्यम से कैश बैक/डिस्काउंट ऑफर का प्रलोभन देते हैं।
- पैसे प्राप्त करने के लिए क्यूआर कोड भेजे जाते हैं।
- घोटालेबाज उपयोगकर्ताओं को यूपीआई अनुरोध लिंक स्वीकार करने और उपयोगकर्ता के खाते/वॉलेट में पैसे/कैशबैक प्राप्त करने के लिए यूपीआई पिन दर्ज करने के लिए लुभाते हैं।
- एक बार यूपीआई पिन दर्ज करने के बाद राशि उपयोगकर्ता के खाते में जमा होने के बजाय खाते से नामे (डेबिट) हो जाता है।

सुरक्षा टिप्स:

- अनजान व्यक्तियों के साथ यूपीआई आईडी साझा न करें।
- अपना यूपीआई पिन नियमित रूप से बदलें।
- अपनी लेनदेन सीमा नियमित रूप से समीक्षा करें और दैनिक लेनदेन सीमा निर्धारित करें।
- अज्ञात स्रोतों से प्राप्त लिंक को न खोलें।
- हमेशा प्रेषक की पहचान सत्यापित करें।
- याद रखें, यूपीआई से जुड़े खाते में "धन प्राप्ति" के लिए यूपीआई पिन की आवश्यकता नहीं होती है।

साइबर अपराध की रिपोर्ट करने के लिए 1930 (टोल-फ्री) पर कॉल करें या www.cybercrime.gov.in पर पंजीकरण करें।

Scanning a QR code or clicking on UPI link?

Beware of UPI frauds.

Modus Operandi:

- Fake websites are created by the scammer to offer desired products at unbelievable discounts containing links and QR Codes for debiting victim's account.
- Scammers post fake Customer Care Numbers in internet and promote them through search engines. When the user calls on these Toll-Free numbers, on the pretext of solving user's problem, QR code/UPI link is sent to collect information or steal money.
- Scammers tricks customers through cash back/discount offers via SMS/WhatsApp messages.
- Scammers send QR codes to collect money in pretext of making payments/refunds. Once the QR Code is scanned and Pin is entered, the money is debited from account.
- Scammers entice users to accept UPI collect request link and to enter UPI pin for receiving money/Cash back in user's account/wallet.
- Once the UPI PIN is entered users account is debited instead of being credited.

Safety Tips:

- Don't share UPI id with unknown persons.
- Reset your UPI PIN regularly.
- Review your transaction limit & set a daily transaction limit.
- Don't open link received from unknown sources.
- Always verify the identity of the sender.
- Remember, UPI does not require PIN to "Receive money" in UPI linked account.

To report cybercrime call 1930 (Toll-Free)

Or register @ www.cybercrime.gov.in.

क्या आप किराए के लिए अपना फ्लैट पोस्ट कर रहे हैं?

प्रतिरूपण घोटाला से सावधान रहें।

कार्यप्रणाली:

- घोटालेबाज वास्तविक समय में नई संपत्ति को किराये हेतु सूचीबद्ध किए जाने की ऑनलाइन निगरानी करते हैं।
- सूचीबद्ध संपत्ति पर तत्काल प्रतिक्रिया भेजी जाती है।
- घोटालेबाज मालिक का विश्वास हासिल करने के लिए सेना/सीआरपीएफ ड्रेस कोड के साथ प्रतिरूपित पारिवारिक तस्वीरें/आधार कार्ड/पैन कार्ड साझा करते हैं।
- पट्टा करार (Lease Agreement) के निष्पादन पर जोर दिए बिना और सूचीबद्ध संपत्ति की तत्काल आवश्यकता बताते हुए तत्काल भुगतान की पेशकश की जाती है।
- मालिक को पैसे भेजने के लिए एसएमएस/व्हाट्सएप लिंक/क्यूआर कोड भेजे जाते हैं।
- एक बार यूपीआई पिन दर्ज कर देने के बाद मालिक के खाते से पैसा नामे (डेबिट) हो जाता है।
- घोटालेबाज मालिकों को कॉल करते हैं और दोबारा एसएमएस/व्हाट्सएप लिंक/क्यूआर कोड भेजकर पैसे वापस करने की पेशकश करते हैं जिसके कारण ग्राहक के खाते से पैसे दोबारा नामे (डेबिट) हो जाता है।
- एक बार पैसा निकल जाने के बाद, घोटालेबाज का मोबाइल नंबर बंद हो जाता है।

सुरक्षा टिप्स:

- संभावित किरायेदारों को हमेशा व्यक्तिगत रूप से संपत्ति को देखने और पट्टा करार (Lease Agreement) निष्पादित करने के लिए कहें।
- पहचान प्रमाण दस्तावेजों की जांच करते समय सतर्क रहें।
- हमेशा याद रखें, क्यूआर कोड स्कैनिंग का उद्देश्य पैसे भेजना है न कि पैसे प्राप्त करना।
- यूपीआई से जुड़े खाते में "धन प्राप्ति" के लिए यूपीआई पिन की आवश्यकता नहीं होती है।
- एक बार खाते से राशि नामे (डेबिट) हो जाने के बाद, धन वापसी के लिए घोटालेबाज द्वारा भेजे गए नए क्यूआर कोड को कभी भी स्कैन न करें। जालसाज़ पीड़ित की भावनाओं से खेलते हैं और आपके खाते से दोबारा पैसे निकाले जा सकते हैं।

साइबर अपराध की रिपोर्ट करने के लिए 1930 (टोल-फ्री) पर कॉल करें या www.cybercrime.gov.in पर पंजीकरण करें।

Posting your Flat for Rent?

Beware of Impersonation Scam.

Modus Operandi:

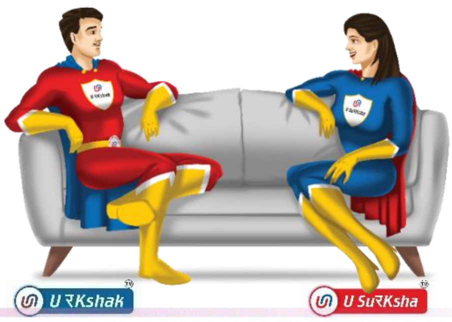
- Scammers monitor new property rental listings online in real time.
- Immediate response is sent on listed property.
- Scammers share fake family photographs/Aadhaar card/PAN card with Army/CRPF dress code to gain confidence of the owner.
- Immediate payment is offered without insisting for execution of lease agreement & an urgent occupation requirement is expressed for the listed property.
- Link/QR Codes for collecting money is sent to owner through SMS/Social media messaging apps in pretext of sending money.
- Once the UPI PIN is entered the account of the owner is debited.
- Sometimes Scammers call the owners and offer to refund the money by sending a separate link/QR codes through SMS/Social media messaging app and debits customers account once again.

Safety Tips:

- Always ask the prospective tenants to visit the property in person and execute lease agreements.
- Be cautious while checking the Identity proof documents.
- Always remember that, QR code scanning is to send money & not to receiving money.
- Remember, UPI does not require PIN to “Receive money” in UPI linked account.
- Once the account is debited, never scan the new QR code sent by the scammer to get refund as this may lead to further loss.

To report cybercrime call 1930 (Toll-Free)

Or register @ www.cybercrime.gov.in.



क्या आप सर्च इंजन में टोल-फ्री नंबर खोज रहे हैं ?

ग्राहक सेवा घोटाले से सावधान रहें।

कार्यप्रणाली:

- घोटालेबाज नकली ग्राहक सेवा नंबर बनाते हैं और सर्च इंजन के माध्यम से प्रचारित करते हैं।
- ग्राहकों को संपर्क करने के लिए जानीमानी कंपनियों तथा वित्तीय संस्थानों की नकली वेबसाइटें बनाई जाती - हैं।
- जब इन फर्जी टोलफ्री नंबरों पर संपर्क किया जाता है-, तो घोटालेबाज ग्राहकों से कम राशि के साथ सेवा प्रभार वसूलने के बहाने विद्वेषपूर्ण)malicious) ऐप डाउनलोड करनेक्यूआर स्कैन /लिंक क्लिक करने/ करने और बैंक खाते के विवरण सहित व्यक्तिगत पहचान संबंधित जानकारी साझा करने के लिए राजी कर लेते हैं।
- इसके बाद ग्राहक के खाते में से धोखे से राशि निकाल ली जाती है।

सुरक्षा टिप्स:

- सर्च इंजिनयों की सहायता से प्राप्त उपभोगता सहायता केंद्र संपर्क विवरणों के उपयोग में सावधानी बरतें।
- हमेशा कंपनी की आधिकारिक वेबसाइट/ऐप में दिए गए संपर्क विवरण का उपयोग करें।
- संदिग्ध ईमेल/एसएमएस/व्हाट्सएप संदेश के माध्यम से प्राप्त अज्ञात लिंक पर कभी भी क्लिक न करें।
- कभी भी अज्ञात व्यक्तियों अथवा असुरक्षित वेबसाइटों पर मोबाइल नंबर, खाता संख्या या पासवर्ड, ओटीपी, पिन साझा न करें।
- बैंक जैसे वित्तीय संस्थान ग्राहकों से कभी भी व्यक्तिगत पहचान योग्य सूचना (PII), ओटीपी, पिन आदि की मांग नहीं करते हैं।
- यूनियन बैंक ऑफ इंडिया टोल-फ्री ग्राहक सेवा नंबर बैंक की आधिकारिक वेबसाइट: www.unionbankofindia.bank.in बैंक पासबुक तथा मोबाइल बैंकिंग ऐप पर उपलब्ध है।

साइबर अपराध की रिपोर्ट करने के लिए 1930 (टोल-फ्री) पर कॉल करें या www.cybercrime.gov.in पर पंजीकरण करें।

Looking for Toll-Free No. in Search Engine?

Beware of Customer Care Scam.

Modus Operandi:

- Scammers post fake customer care numbers and promote them through search engines.
- Fake websites of known companies & financial institutions are created for customers to make contact.
- When these fake toll-free numbers are contacted, scammers trick the customers to download malicious apps/click links/scan QR and share personal identifiable information including bank account details in the pretext of collecting small service charges.
- Subsequently scammers siphon off customer account with the help of details obtained.

Safety Tips:

- Be Cautious in using Customer Care Contact details obtained by directly searching through Search Engines.
- Always use contact details provided in official website/App of the company.
- Never click on unknown links received through suspicious email/SMS/WhatsApp message.
- Never share/submit mobile number, account number or password, OTP, PIN to unknown persons or unsecured websites.
- Financial institutions like Bank never asks for any Personal Identifiable Information Data, OTP, PIN etc. from customers.
- Union Bank Of India Toll – Free Customer care number is available in Bank's official website: www.unionbankofindia.bank.in, Banks Passbook and Mobile banking App.

To report cybercrime call 1930 (Toll-Free)

Or register @ www.cybercrime.gov.in.

क्या आप नौकरी की तलाश कर रहे हैं? ऑनलाइन नौकरी धोखाधड़ी से सावधान रहें।

कार्यप्रणाली:

- घोटालेबाज नकली नौकरियों के लिए वेबसाइट बनाते हैं और उन्हें सर्च इंजन के माध्यम से प्रचारित करते हैं।
- अत्यंत आकर्षक दिखने वाले ऑफर को एसएमएस/व्हाट्सएप संदेशों के माध्यम से प्रसारित किए जाते हैं।
- घोटालेबाज ईमेल के माध्यम से प्रतिष्ठित कंपनियों के लिए व्यक्ति विशेष के अनुरूप नौकरी का प्रस्ताव भेजते हैं।
- आधार/पैन/बैंक खाता विवरण जैसी व्यक्तिगत जानकारी एकत्र की जाती है, जिसका उपयोग करके उम्मीदवारों के खाते में धोखाधड़ी की जाती है।
- उम्मीदवारों /नौकरी चाहने वालों को विश्वास दिलाने के लिए फर्जी साक्षात्कार आयोजित किए जाते हैं।
- उम्मीदवारों/नौकरी चाहने वालों को एजेंसी शुल्क, पंजीकरण, प्रशिक्षण, साक्षात्कार आयोजित करने, वीज़ा प्रसंस्करण शुल्क आदि के बहाने धन अंतरित करने के लिए प्रेरित किया जाता है।
- धन प्राप्त हो जाने पर घोटालेबाज कारोबारी गतिविधि बंद कर देता है और अपना मोबाइल फोन बंद कर लेता है।

सुरक्षा टिप्स:

- हमेशा वास्तविक नौकरी वेबसाइटों/पोर्टलों के माध्यम से आवेदन करें।
- उपलब्ध नौकरी के लिए आवेदन करते समय कंपनी की आधिकारिक वेबसाइट पर जाएं।
- नौकरी देते समय कंपनियां कभी भी पैसे नहीं मांगती हैं।
- अत्यंत आकर्षक दिखने वाली नौकरी के प्रस्ताव ज्यादातर घोटाले होते हैं।
- कभी भी ऐसी आकर्षक नौकरी की पेशकश स्वीकार न करें जिसके लिए न्यूनतम प्रयास की आवश्यकता होती है और बिना अनुभव के दी जाती है।
- वास्तविक कंपनियाँ अपने आधिकारिक ईमेल के माध्यम से नौकरी के प्रस्ताव साझा करती हैं, न कि पब्लिक ईमेल के माध्यम से।

साइबर अपराध की रिपोर्ट करने के लिए 1930 (टोल-फ्री) पर कॉल करें या www.cybercrime.gov.in पर पंजीकरण करें।

Looking for a Job?

Beware of Online Job Frauds.

Modus Operandi:

- Scammers create fake job websites and promote them through search engines.
- Too good to be true offers are circulated through SMS/WhatsApp messages.
- Scammers send personalised job offers of reputed companies through email.
- Personal information like Aadhaar/PAN/Bank account details are collected, which results in compromise of job seekers account.
- Fake interviews are organized to convince the job seekers.
- Candidates/Job seekers are induced to transfer funds on the pretext of agency fees, registration, training, organizing interviews, VISA processing charges etc.
- On receipt of fund scammers shut shop and switch off their mobile phones.

Safety Tips:

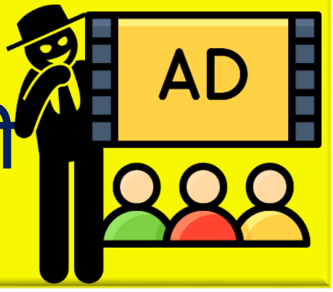
- Always apply through genuine job websites/portals.
- Visit the company's official website to apply for available job opportunities.
- Companies never ask for money while offering jobs.
- Too good to be true job offers are mostly scams.
- Never accept lucrative job offers which require minimal efforts and are offered without experience.
- Genuine companies share job offers through their official email and not through public email.

To report cybercrime call 1930 (Toll-Free)

Or register @ www.cybercrime.gov.in.

क्या आप उत्पाद जानकारी के लिए ऑनलाइन प्लेटफ़ॉर्म का उपयोग कर रहे हैं?

ऑनलाइन विडियो फर्जी संपर्क नंबर धोखाधड़ी से सावधान रहें।



कार्यप्रणाली:

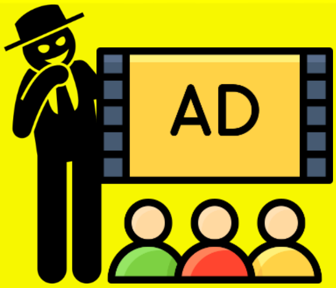
- घोटालेबाज उपयोगकर्ताओं की सहायता के लिए वीडियो तैयार करते हैं और उन्हें ऑनलाइन प्रसारित करते हैं।
- वीडियो प्रतिष्ठित कंपनियों के नाम पर उनके लोगो, ब्रांड नाम और सामग्री का उपयोग करके तैयार किए जाते हैं।
- ये जानकारीपूर्ण वीडियो वास्तविक प्रक्रिया और उपयोग संबंधित दिशानिर्देश साझा करते हैं जो वास्तविक कंपनियों के द्वारा जारी किए गए दिशानिर्देशों के समान होते हैं।
- हालाँकि, वीडियो में संपर्क के लिए प्रदर्शित नंबर घोटालेबाज के होते हैं।
- जब उपयोगकर्ता इन नंबरों पर संपर्क करते हैं, तो पंजीकरण, सत्यापन और सेवा शुल्क के नाम पर उपयोगकर्ताओं को मलिशियस (malicious) लिंक/क्यूआर और .apk फ़ाइलें भेजी जाती हैं।
- इसके उपरांत उपयोगकर्ताओं के खातों में से धोखे से पैसे निकाल लिए जाते हैं।

सुरक्षा टिप्स:

- हमेशा कंपनी की आधिकारिक वेबसाइट/ऐप में दिए गए संपर्क विवरण का उपयोग करें।
- ऑनलाइन प्लेटफॉर्म, सोशल मीडिया के वीडियो विज्ञापनों एवं सर्च इंजिनयों से प्राप्त कंपनियों के संपर्क नंबर के इस्तेमाल से बचें।
- कभी भी अनजान व्यक्तियों या असुरक्षित वेबसाइटों/लिंक में मोबाइल नंबर, खाता संख्या या पासवर्ड, ओटीपी, पिन साझा न करें।
- कभी भी थर्ड पार्टी या अनौपचारिक ऐप स्टोर / लिंक या APK फ़ाइल के सहायता से ऐप इन्स्टाल न करें।

साइबर अपराध की रिपोर्ट करने के लिए 1930 (टोल-फ्री) पर कॉल करें या www.cybercrime.gov.in पर पंजीकरण करें।

Searching Online for Product information?



Beware of fake Contact in online Video.

Modus Operandi:

- Scammers prepare awareness videos to assist the users and circulate them online.
- The videos are prepared in the name of reputed companies using their Logos, brand names and usage content.
- These informative videos share the genuine process and usage guidelines which are similar to service guidelines issued by real companies.
- However, the contact details displayed in videos are of scammers.
- When users contact these numbers, malicious link/QR & .apk files are sent in the name of registration, verification and collection of service fee.
- Subsequently Accounts of users are compromised and money is siphoned off.

Safety Tips:

- Always use contact details provided in official website/App of the company.
- Avoid usage of customer care contact numbers of companies obtained from online platforms, social media video ads and search engines.
- Never share/submit mobile number, account number or password, OTP, PIN to unknown persons or unsecured websites/link.
- Never install mobile apps from 3rd party or unofficial stores/links or using apk files.

To report cybercrime call 1930 (Toll-Free)

Or register @ www.cybercrime.gov.in.

क्या मोबाइल में नेटवर्क नहीं है?

सिम स्वैप धोखाधड़ी से सावधान रहें।

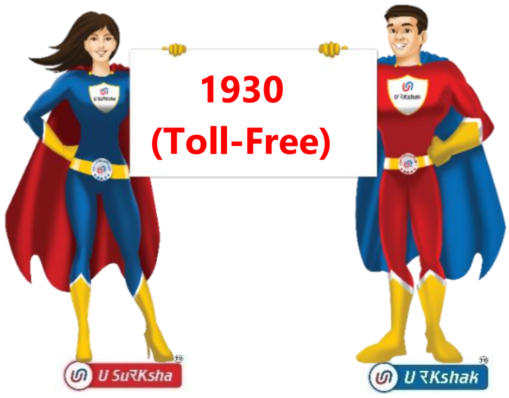
कार्यप्रणाली:

- घोटालेबाज सोशल मीडिया, फ़िशिंग ईमेल, एसएमएस एवं व्हाट्सएप संदेशों के माध्यम से लोगों के व्यक्तिगत बैंक खाता विवरण एवं पंजीकृत मोबाइल नम्बर प्राप्त करते हैं।
- पीड़ित व्यक्ति के व्यक्तिगत पहचान दस्तावेजों का उपयोग करके, घोटालेबाज टेलीकॉम ऑपरेटर के पास जाते हैं और ग्राहक का सिम ब्लॉक करने का अनुरोध करते हैं।
- वास्तविक ग्राहक के सिम निष्क्रियकरण के बाद, सिम घोटालेबाज पीड़ित व्यक्ति के व्यक्तिगत पहचान योग्य सूचना (PII) दस्तावेजों की सहायता से टेलीकॉम ऑपरेटर से डुप्लिकेट सिम कार्ड प्राप्त कर लेता है।
- उसके बाद प्रतिरूपित (डुप्लिकेट) सिम में प्राप्त ओटीपी का उपयोग अनधिकृत लेनदेन को अंजाम देने के लिए किया जाता है और पीड़ित के बैंक खाते से पैसे निकाल लिए जाते हैं।

सुरक्षा टिप्स:

- सोशल मीडिया पर कभी भी निजी जानकारी साझा न करें। घोटालेबाज व्यक्तिगत डेटा चुराने के लिए विशिंग, फ़िशिंग, स्मिशिंग जैसी सोशल इंजीनियरिंग तकनीकों का उपयोग करते हैं।
- ईमेल या मैसेजिंग प्लेटफॉर्म में कभी भी संदिग्ध अटैचमेंट या लिंक को न खोलें या क्लिक न करें।
- अपने वित्तीय रिकॉर्ड की नियमित रूप से निगरानी करें।
- यदि आपका मोबाइल नंबर लंबे समय तक निष्क्रिय बना हुआ है या बिना नेटवर्क के है, तो अपने दूरसंचार ऑपरेटर से संपर्क करें।
- बैंकिंग लेनदेन के लिए हमेशा एसएमएस के साथ-साथ ई-मेल अलर्ट के लिए भी पंजीकरण करें।
- वित्तीय धोखाधड़ी के मामले में, आगे के लेनदेन को रोकने के लिए तत्काल बैंक के ग्राहक सहायता सेंटर से संपर्क करें एवं अपने खाते को ब्लॉक कराएं।

साइबर अपराध की रिपोर्ट करने के लिए 1930 (टोल-फ्री) पर कॉल करें या www.cybercrime.gov.in पर पंजीकरण करें।



No Network in Mobile?

Beware of SIM Swap Fraud.

Modus Operandi:

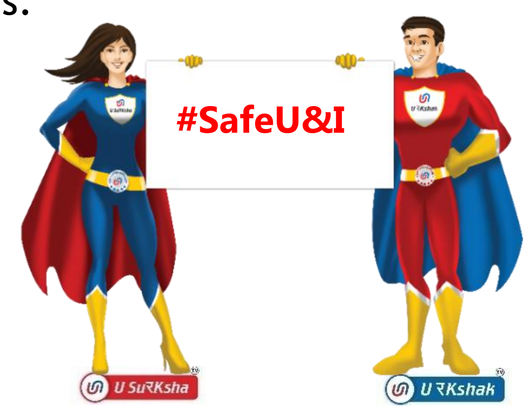
- Scammers gather individual's bank account details and registered mobile number through social media, phishing emails, SMS & WhatsApp messages.
- Using the personal identity documents of the victim, scammers visit the telecom operator with a request to block the SIM.
- After deactivation of the genuine customer's SIM, scammers obtain a duplicate SIM card from telecom operator with the Personal Identifiable information documents of the victim.
- The OTP received in the duplicate SIM is then used to execute unauthorized transactions and siphon off money from victim's bank account.

Safety Tips:

- Never share your personal information with anyone. Scammers use social engineering techniques like vishing, phishing, smishing to steal personal data.
- Never open/click suspicious attachments or link in email or messaging platforms.
- Monitor your financial records regularly.
- In case of your mobile number is inactive or without network for a longer period, contact your telecom operator.
- Always register for SMS as well as e-mail alerts for banking transactions.
- In case of a financial fraud, contact customer support team immediately to have your account blocked to avoid further transactions.

To report cybercrime call 1930 (Toll-Free)

Or register @ www.cybercrime.gov.in.



क्या आप ऑनलाइन निवेश कर रहे हैं ?

पिग बुचरिंग घोटाले से सावधान रहें।

कार्यप्रणाली:

- पिग बुचरिंग में पीड़ित को धीमी और संयमित तरीके से गुमराह किया जाता है।
- घोटालेबाज फर्जी निवेश योजनाओं के वीडियो पोस्ट करते हैं और ऐप डाउनलोड के लिए टेलीग्राम जैसे सोशल मीडिया मेसेजिंग ऐप या अन्य स्ट्रीमिंग प्लेटफॉर्म के माध्यम से लिंक साझा करते हैं।
- ये फर्जी ऐप्स निवेश पर अच्छे रिटर्न का वादा करते हैं एवं पीड़ित को पैसे निवेश करने के लिए गुमराह करते है ।
- पीड़ितों को शुरुआत में छोटी रकम अंतरण करने के लिए मनाया जाता है। निवेश ऐप्स प्रारंभिक छोटे निवेशों पर अच्छा रिटर्न दिखाते हैं जिससे पीड़ित को ज्यादा रकम निवेश करने के लिए प्रोत्साहन मिलता है।
- एक बार जब पीड़ित अपना निवेश काफी हद तक बढ़ा लेता है, तो धोखेबाज सारा निवेश लेकर फरार हो जाता है एवं उपयोगकर्ता को पूरी तरह से ब्लॉक कर देता है।

सुरक्षा टिप्स:

- अत्यंत आकर्षक दिखने वाले प्रस्ताव अधिकतर घोटाले होते हैं।
- संवेदनशील व्यक्तिगत जानकारी और वित्तीय विवरण कभी भी अनजान लोगों के साथ साझा न करें।
- निवेश के बारे में सम्पूर्ण जानकारी प्राप्त किए बिना धन का निवेश न करें।
- व्यक्ति विशेष के बारे में जाने बिना कभी भी ऑनलाइन मित्र अनुरोध स्वीकार न करें।
- हमेशा कंपनी की आधिकारिक वेबसाइट, गूगल प्ले या ऐप्पल ऐप स्टोर से ही ऐप डाउनलोड करें। कभी भी अन्य पक्ष ऐप/वेबसाइटों से ऐप डाउनलोड न करें।

साइबर अपराध की रिपोर्ट करने के लिए 1930 (टोल-फ्री) पर कॉल करें या www.cybercrime.gov.in पर पंजीकरण करें।

Are you Investing online?

Beware of Pig Butchering Scam.

Modus Operandi:

- Pig Butchering involves slow & steady brain washing of the targets.
- Scammers post videos of fake investment schemes & share links for downloading app through social messaging platforms such as Telegram & other streaming platforms.
- These fake investment apps promise good return against investment and victims are persuaded to transfer amount for investing.
- Victims are convinced initially to transfer small amounts. The investment apps displays good return for the initial small investments which encourages victims to invest more amount.
- Once the victim substantially increase their investment, all the savings are cleaned out by fraudster in one go and the user is blocked completely.

Safety Tips:

- Too good to be true offers are mostly scams.
- Never share sensitive personal information and financial details with unknown people.
- Never invest funds before conducting through background checks.
- Never accept online friend requests without knowing about the individual.
- Always download apps from company's official website, Google play or Apple App store only. Never download apps from 3rd party Apps/Websites/links.

To report cybercrime call 1930 (Toll-Free)

Or register @ www.cybercrime.gov.in.

क्या आपको ऑनलाइन मुफ़्त उपहार कार्ड /लॉटरी टिकट प्राप्त हुई है?

गिफ्ट कार्ड/लॉटरी धोखाधड़ी से सावधान रहें।

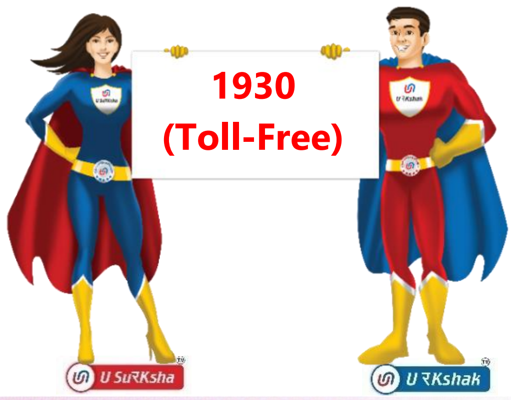
कार्यप्रणाली:

- घोटालेबाज सोशल मीडिया प्लेटफॉर्म/ऐप के माध्यम से ईमेल, संदेश भेजकर पीड़ितों को मुफ्त उपहार कार्ड और लॉटरी जीतने के बारे में सूचित करते हैं।
- ग्राहकों को गुमराह करके जल्द निवेश करने के लिए प्रेरित किया जाता है।
- ग्राहकों को उपहार वाउचर खरीदने और व्यक्तिगत पहचान योग्य जानकारी (PII)/खाता विवरण/कार्ड नंबर/पिन/ओटीपी आदि साझा करने के लिए बहलाया जाता है।
- पीड़ितों को क्यूआर कोड या गलत भुगतान लिंक भेजे जाते हैं। तत्काल खरीद या सदस्यता की सीमित उपलब्धता/एकबारगी अवसर होने पर जोर दिया जाता है।
- एक बार पीड़ित जब अपनी जानकारी साझा कर देता है या नकली उपहार कार्ड खरीद लेता है, तो घोटालेबाज पीड़ित को पूरी तरह से ब्लॉक कर देता है और उनके पैसे निकाल लेता है।

सुरक्षा टिप्स:

- ईमेल/एसएमएस में अनचाहे अनुरोधों पर कभी भी व्यक्तिगत या वित्तीय जानकारी साझा न करें।
- इस दुनिया में कुछ भी मुफ़्त नहीं है। अत्यधिक आकर्षक दिखने वाले प्रस्ताव अधिकतर घोटाले होते हैं।
- उचित सत्यापन या प्रमाणीकरण के बिना कभी भी संदेश, लिंक, ई-मेल अग्रेषित न करें।
- अपने डिजिटल उपकरणों में कभी भी अज्ञात लिंक पर क्लिक न करें या अज्ञात सॉफ़्टवेयर डाउनलोड न करें।

साइबर अपराध की रिपोर्ट करने के लिए 1930 (टोल-फ्री) पर कॉल करें या www.cybercrime.gov.in पर पंजीकरण करें।



Have you received/Won an online free Gift Card/Lottery?

Beware of Gift Card/Lottery Fraud.

Modus Operandi:

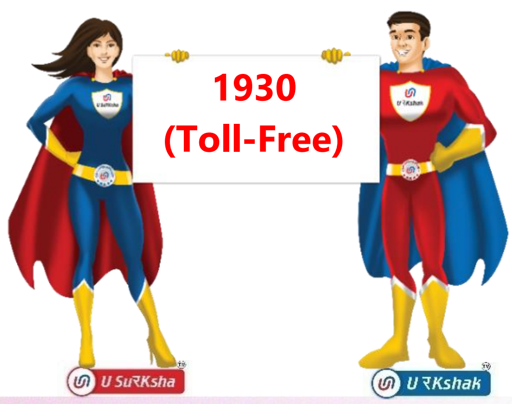
- The scammers sends emails, messages through social media platforms/App informing victims about free gift cards and lottery winnings.
- Scammers use persuasive techniques to create a sense of urgency among victims.
- They exploit emotional triggers for purchasing gift vouchers and submission of Personal Identifiable Information (PII)/account details/Card No/PIN/OTP etc.
- QR code or malicious payment links are sent to victims. Immediate purchase or subscription are pressed showing limited availability/one-time opportunity.
- Once the victim enters their credentials or purchase fake gift cards, the scammer blocks the victim completely and siphon off their money.

Safety Tips:

- Never share personal or financial information in response to unsolicited requests in email/SMS.
- Nothing is free in this world. Too good to be true offers are mostly scams.
- Never forward messages, links, E-mails without proper verification or authentication.
- Never click on unknown links or download unknown software on your digital devices.

To report cybercrime call 1930 (Toll-Free)

Or register @ www.cybercrime.gov.in.



क्या आप अनाधिकारिक ऐप स्टोर/लिंक से ऐप्स डाउनलोड कर रहे हैं?

फर्जी ऐप घोटाले से सावधान रहें।

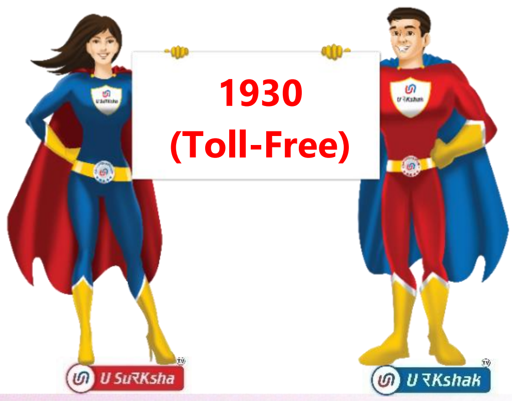
कार्यप्रणाली:

- घोटालेबाज सोशल मीडिया, व्हाट्सएप संदेश, टेलीग्राम चैनल व एसएमएस जैसे विभिन्न चैनलों के माध्यम से फर्जी मोबाइल ऐप को डाउनलोड करने का लिंक भेजते हैं।
- फर्जी ऐप वास्तविक ऐप जैसा दिखता है और मैलवेयर के जरिए आपकी व्यक्तिगत जानकारी इकठ्ठा कर लेता है।
- जब पीड़ित ऐसे ऐप को डाउनलोड कर लेता है, तो घोटालेबाज परोक्ष रूप से डिजिटल हमले प्रारंभ कर देता है।
- घोटालेबाज द्वारा उपयोगकर्ताओं की व्यक्तिगत पहचान योग्य सूचना (PII) प्राप्त करने के बाद खाते में से धोखे से सारे पैसे निकाल लेता है।

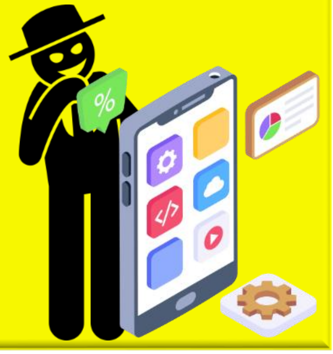
सुरक्षा टिप्स:

- हमेशा आधिकारिक ऐप स्टोर (जैसे गुगल प्ले स्टोर, एप्पल ऐप स्टोर एवं ऑफिशियल ऐप स्टोर) से ही ऐप डाउनलोड करें क्योंकि वे सख्त सुरक्षा नियम का पालन करते हैं।
- फर्जी या विद्वेषपूर्ण (malicious) ऐप को परखने के लिए, डाउनलोड करने से पहले हमेशा ऐप विवरण की जांच करें - देखें कि डेवलपर कौन है, उपयोगकर्ता रिव्यू, डाउनलोड की संख्या आदि के माध्यम से ऐप का सत्यापन करें।
- किसी भी ऐप/वेबसाइट में संदिग्ध लिंक पर कभी भी क्लिक न करें।
- हमेशा एप्लिकेशन द्वारा मांगी गई अनुमतियों के अनुरोध की समीक्षा करें।
- अपने मोबाइल में हमेशा एंटीवायरस या एंटीमैलवेयर सॉफ़्टवेयर का उपयोग करें और इसे नियमित रूप से स्कैन करें।

साइबर अपराध की रिपोर्ट करने के लिए 1930 (टोल-फ्री) पर कॉल करें या www.cybercrime.gov.in पर पंजीकरण करें।



Downloading apps from unofficial app store/link?



Beware of Fake App Scam.

Modus Operandi:

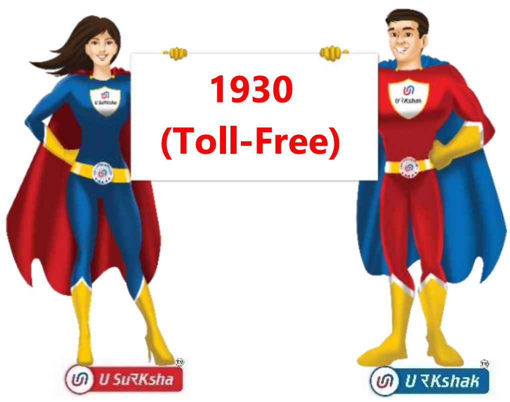
- Scammers distribute Fake Mobile App download links through various channels like social media, WhatsApp messages, Telegram channels & SMS.
- The fake apps resemble legitimate apps and undertakes malicious activities like installing malware or stealing your personal information.
- When the victim downloads these Apps, the scammer initiates hidden background activities and launches further attacks.
- Once the Personally identifiable information (PII) data and accounts of users are compromised and money is siphoned off & the user account is blocked by the scammer.

Safety Tips:

- Always download apps from official app stores (such as Google Play Store, Apple App Store & Govt. App Store) as they have stringent security checks in place.
- Always check the app details before you download to filter out fake or malicious apps – Look at who the developer is, User reviews, Number of downloads etc.
- Never click on suspicious links in any app/website.
- Always review permissions that are requested by the application.
- Always use an antivirus or Antimalware software in your mobile & scan it regularly.

To report cybercrime call 1930 (Toll-Free)

Or register @ www.cybercrime.gov.in.



यूनियन बैंक ऑफ इंडिया
भारत सरकार का उपक्रम

Union Bank of India
A Government of India Undertaking

CYBERSECURITY CENTRE of XCELLENCE
Innovate. Digitize. Excel. Automate.

Report Cyber Crime incidents at www.cybercrime.gov.in or call 1930 (Toll Free)

Report phishing incidents to our 24x7 anti phishing help desk:

antiphishing.ciso@unionbankofindia.bank.in