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.

Union Bank of India

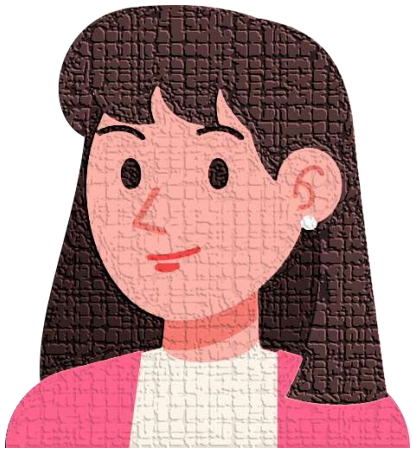
साइबर सुरक्षा
ग्राहक जागरूकता मार्गदर्शिका - अंक V

Cyber Security
Customer Awareness Guide – Vol. V
for
Senior Citizen | Women | Children

To report any cyber crime incident call 1930 or visit www.cybercrime.gov.in
To report suspected fraud communications received through Call/SMS/WhatsApp Messages visit https://sancharsaathi.gov.in/sfc/

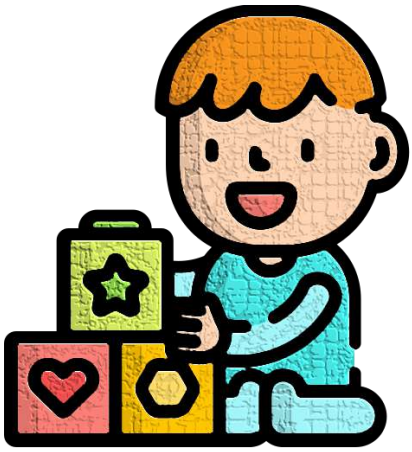
About the Book

Cyber fraudsters target Senior Citizens as they are more vulnerable to online financial frauds in the present digital era. This booklet aims to enable senior citizens to recognize scams, protect personal information and emphasizes usage of strong passwords, multi-factor authentication. The aim is to make senior citizens aware regarding not to share sensitive information like PINs or OTPs over the phone or internet.



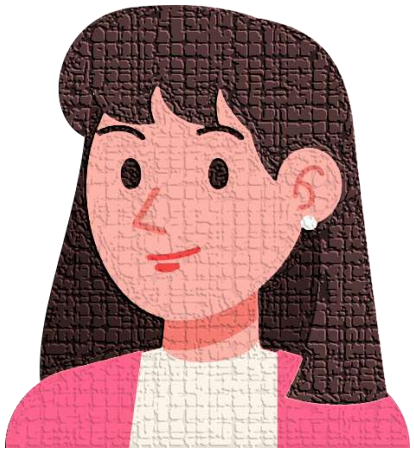
This booklet for Women provides guidance on how to stay safe online and covers topics like social media safety, avoiding cyber frauds, protecting personal information, safeguarding themselves against cyber bullying & reporting cybercrimes. The aim is to empower women folk with knowledge and best practices to navigate the digital world securely.

For Children, this booklet aims to educate regarding safe online practices, creating strong passwords and being cautious about what they share online, and recognizing potential dangers of phishing and cyberbullying.



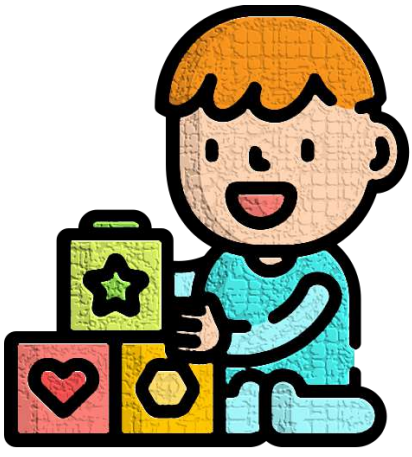
पुस्तक परिचय

साइबर धोखेबाज वरिष्ठ नागरिकों को निशाना बनाते हैं क्योंकि वर्तमान डिजिटल युग में ऑनलाइन वित्तीय धोखाधड़ी के गिरफ्त में आने की उनकी संभावना सबसे अधिक होती है। इस पुस्तिका का उद्देश्य वरिष्ठ नागरिकों को घोटालों को पहचानने, व्यक्तिगत जानकारी की रक्षा करने और मजबूत पासवर्ड, बहुस्तरीय प्रमाणीकरण के उपयोग पर जोर देना है। इसका उद्देश्य वरिष्ठ नागरिकों को फोन या इंटरनेट पर पिन या ओटीपी जैसी संवेदनशील जानकारी साझा न करने के बारे में जागरूक करना है।



महिलाओं के लिए यह पुस्तिका ऑनलाइन सुरक्षित रहने के बारे में मार्गदर्शन प्रदान करती है और सोशल मीडिया सुरक्षा, साइबर धोखाधड़ी से बचने, व्यक्तिगत जानकारी की रक्षा करने, साइबर बुलिंग के खिलाफ खुद को सुरक्षित रखने और साइबर अपराधों की रिपोर्ट करने जैसे विषयों को शामिल करती है। इसका उद्देश्य डिजिटल दुनिया को सुरक्षित रूप से नेविगेट करने के लिए ज्ञान और सर्वोत्तम प्रथाओं के साथ महिलाओं को सशक्त बनाना है।

बच्चों के लिए, इस पुस्तिका का उद्देश्य सुरक्षित ऑनलाइन आदतों के बारे में शिक्षित करना, मजबूत पासवर्ड बनाना और जो वे ऑनलाइन साझा करते हैं, उसके बारे में सतर्क रहना और फ़िशिंग और साइबर बुलिंग के संभावित खतरों को पहचानना है।



Message From:

Shri Sanjay Rudra,
Executive Director

As our lives become increasingly integrated with the digital ecosystem, cybercrime has emerged as a formidable challenge—impacting individuals, businesses, and institutions alike. At Union Bank of India, we recognize the critical importance of cybersecurity and have taken proactive steps to mitigate risks and raise awareness about evolving cyber threats.

Cybercrime remains an ever-present danger, and financial scams targeting customers are a growing concern. We are committed to empowering our customers with the knowledge and tools they need to protect themselves, avoid falling prey to fraudsters, and navigate the digital world safely.

This booklet is part of our initiative to build cybersecurity awareness. It provides valuable insights into the tactics used by cybercriminals, particularly those targeting Senior Citizens, Women, and Children, and shares effective online safety tips to help prevent mishaps.

I encourage all customers to read this booklet thoroughly, understand the risks, and take the recommended precautions to stay protected.

Message From:

Shri Anil Kuril,
CGM & CISO

Union Bank of India has implemented strong security measures to protect customer data and defend against emerging cyber threats. In today's hyper connected world, even a single vulnerability can have widespread consequences—affecting not only individuals but entire digital ecosystems.

This booklet is the fifth in our cybersecurity awareness series, aimed at simplifying the complexities of the digital world. It provides readers with essential knowledge to safeguard their online presence and financial transactions. By highlighting specific types of cyber threats—including Digital Arrest Fraud, Investment Fraud, Matrimonial Fraud, Cyber Stalking, and Cyber Bullying—it serves as a practical guide for individuals, particularly Senior Citizens, Women, and Children.

Additionally, the booklet outlines strategies for both prevention and incident response. By staying informed, customers can significantly reduce their risk of falling victim to cybercrime and better protect their financial and emotional well-being.

I urge all customers to go through this booklet and follow the cyber safety tips to ensure a secure digital experience.

संदेश:

श्री संजय रुद्र,
कार्यपालक निदेशक

जैसे-जैसे हमारा जीवन डिजिटल तंत्र के साथ तेजी से एकीकृत होता जा रहा है, साइबर अपराध एक विकट चुनौती के रूप में उभरा है - जो व्यक्तियों, व्यवसायों और संस्थानों को समान रूप से प्रभावित कर रहा है। यूनियन बैंक ऑफ इंडिया में, हम साइबर सुरक्षा के महत्व को पहचानते और समझते हैं। हमने जोखिमों को कम करने और साइबर खतरों के बारे में जागरूकता बढ़ाने के लिए सक्रिय कदम भी उठाए हैं।

साइबर अपराध एक सदैव विद्यमान खतरे के रूप में बना हुआ है, और ग्राहकों को लक्षित करने वाले वित्तीय घोटाले अत्यंत चिंता का विषय है। हम अपने ग्राहकों को उन ज्ञान और उपकरणों के साथ सशक्त बनाने के लिए प्रतिबद्ध हैं जिनकी उन्हें खुद को बचाने के लिए आवश्यकता है। धोखेबाजों का शिकार होने से बचें और डिजिटल दुनिया की सुविधाओं का सुरक्षित रूप से लाभ उठाएँ।

यह पुस्तिका साइबर सुरक्षा जागरूकता पैदा करने की हमारी पहल का हिस्सा है। यह साइबर अपराधियों द्वारा उपयोग की जाने वाली रणनीति में मूल्यवान अंतर्दृष्टि प्रदान करती है। यह विशेषकर वरिष्ठ नागरिकों, महिलाओं और बच्चों के लिए अत्यंत महत्त्वपूर्ण है। साथ ही, इसमें दुर्घटनाओं को रोकने में मदद करने के लिए प्रभावी ऑनलाइन सुरक्षा युक्तियाँ भी साझा की गयी हैं।

मैं सभी ग्राहकों को इस पुस्तिका को अच्छी तरह से पढ़ने, जोखिमों को समझने और सुरक्षित रहने के लिए अनुशंसित सावधानी बरतने के लिए प्रोत्साहित करता हूं।

संदेश:

श्री अनिल कुरील,
सीजीएम और
सीआईएसओ

यूनियन बैंक ऑफ इंडिया ने ग्राहक डेटा की सुरक्षा और उभरते साइबर खतरों से बचाव के लिए मजबूत सुरक्षा उपाय लागू किए हैं। संचार माध्यमों से आज की सिकुड़ती हुई दुनिया में, एक भी भेद्यता के व्यापक परिणाम हो सकते हैं – यह न केवल व्यक्तियों को बल्कि पूरे डिजिटल तंत्र को प्रभावित करते हैं।

यह पुस्तिका हमारी साइबर सुरक्षा जागरूकता श्रृंखला में पांचवीं पुस्तिका है, जिसका उद्देश्य डिजिटल दुनिया की जटिलताओं को सरल बनाना है। यह पाठकों को उनकी ऑनलाइन उपस्थिति और वित्तीय संव्यवहार की सुरक्षा के लिए आवश्यक ज्ञान प्रदान करती है। डिजिटल गिरफ्तारी धोखाधड़ी, निवेश धोखाधड़ी, वैवाहिक धोखाधड़ी, साइबर स्टाकिंग और साइबर बुलिंग सहित विशिष्ट प्रकार के साइबर खतरों को उजागर करके - यह व्यक्तियों, विशेष रूप से वरिष्ठ नागरिकों, महिलाओं और बच्चों के लिए एक व्यावहारिक मार्गदर्शिका के रूप में ग्राहकों के लिए सहायक सिद्ध होता है।

इसके अतिरिक्त, यह पुस्तिका साइबर धोखाधड़ी के रोकथाम और घटना प्रतिक्रिया दोनों के लिए रणनीतियों की रूपरेखा तैयार करती है। सूचित रहकर, ग्राहक साइबर अपराध के शिकार होने के अपने जोखिम को काफी कम कर सकते हैं। साथ ही, अपनी वित्तीय और भावनात्मक भलाई की बेहतर सुरक्षा कर सकते हैं।

मैं सभी ग्राहकों से इस पुस्तिका को पढ़ने और अपने सुरक्षित डिजिटल अनुभव सुनिश्चित करने के लिए साइबर सुरक्षा युक्तियों का पालन करने का आग्रह करता हूं।

Page Index

Senior Citizen

Women

Children

अनुक्रमणिका

वरिष्ठ नागरिक

महिला

बच्चे

Investment Fraud:

Scammers target senior citizens through Calls, SMS & Email in the pretext of investment schemes. Fraudsters pose as financial advisors/insurance agents & try to convince senior citizens to buy fake policies or invest in fraudulent schemes through malicious Links/APKs to steal their lifelong savings.

Fraudsters offer high returns and too good to be true offers with little to no risk.

Safety Tips:

- Research the investment scheme independently through official websites or trusted sources.
- Always verify the caller's credentials with the official insurance/investment company before making any investment.
- Always download mobile banking apps from official app stores only (Google Play store for Android & Apple App store for Apple devices).
- Never Click on unknown links/APKs received from unverified sources.
- Never Share mobile number, account number, password, OTP, PIN or any other confidential details with anyone.
- Always remember, too good to be true offers are mostly scams.

#SabkoBataoo

निवेश धोखाधड़ी:

धोखेबाज़ निवेश योजनाओं के बहाने कॉल, एसएमएस और ईमेल के माध्यम से वरिष्ठ नागरिकों को लक्षित करते हैं। धोखेबाज वित्तीय सलाहकार/बीमा एजेंट के रूप में वरिष्ठ नागरिकों को नकली पॉलिसी खरीदने या उनकी आजीवन बचत को चोरी करने के उद्देश्य से दुर्भावनापूर्ण लिंक/एपीके के माध्यम से धोखाधड़ी युक्त योजनाओं में निवेश करने के लिए झांसा देने की कोशिश करते हैं।

धोखेबाज़ उच्च प्रतिलाभ का प्रस्ताव देते हैं। ये प्रस्ताव कम से कम जोखिम के साथ बिलकुल सत्य प्रतीत होते हैं।

सुरक्षा युक्तियाँ:

- आधिकारिक वेबसाइटों या विश्वसनीय स्रोतों के माध्यम से स्वतंत्र रूप से निवेश योजना के बारे में जाँच-पड़ताल करें।
- कोई भी निवेश करने से पहले हमेशा आधिकारिक बीमा/निवेश कंपनी के साथ कॉलर की सत्यता को सत्यापित करें।
- केवल आधिकारिक ऐप स्टोर से ही मोबाइल बैंकिंग ऐप डाउनलोड करें (एंड्रॉइड के लिए गूगल प्ले स्टोर और ऐप्पल डिवाइस के लिए ऐप्पल ऐप स्टोर)।
- असत्यापित स्रोतों से प्राप्त अज्ञात लिंक/एपीके पर कभी भी क्लिक न करें।
- कभी भी मोबाइल नंबर, खाता संख्या, पासवर्ड, ओटीपी, पिन या कोई अन्य गोपनीय विवरण किसी के साथ साझा न करें।
- हमेशा याद रखें, ज़्यादा अच्छे और सच्चे प्रतीत होने वाले प्रस्ताव ज्यादातर घोटाले होते हैं।

Digital Arrest Fraud:

The scammers call the victims over video calls in Skype, WhatsApp or any Social Media Apps in the pretext of usage of victim's Aadhaar/mobile numbers/Bank Accounts for illegal activities registered in their name and intimidate them to share sensitive financial information or to send money in lieu of avoiding digital arrest.

Fraudsters create law enforcement office setup & impersonate law enforcement officials such a Police, Narcotics Bureau, CBI etc.

Safety Tips:

- Never join any video call request received from strangers for any investigation or arrest.
- Avoid sharing personal information with unknown people on social media.
- Never make any payment to strangers claiming to be from investigating agencies.
- If you receive any calls about arrest or investigation, visit the nearest police station.
- Always remember, No Government investigating agency will interrogate or arrest you through online calls/Skype.
- Always remember, there is no provision of Digital Arrest in Indian law.

#SabkoBataoo

डिजिटल अरेस्ट धोखाधड़ी:

धोखेबाज़ पीड़ितों को स्काइप, व्हाट्सएप या किसी भी सोशल मीडिया ऐप में वीडियो कॉल के माध्यम से उनके नाम पर पंजीकृत अवैध गतिविधियों में संलिप्त पीड़ित के आधार/मोबाइल नंबर/बैंक खातों के दुरुपयोग के बहाने कॉल करते हैं और उन्हें संवेदनशील वित्तीय जानकारी साझा करने या डिजिटल अरेस्ट से बचने के बदले पैसे भेजने के लिए धमकाते हैं।

धोखेबाज विधि प्रवर्तन कार्यालय जैसा सेटअप बनाते हैं और पुलिस, नारकोटिक्स ब्यूरो, सीबीआई आदि विधि प्रवर्तन अधिकारियों को प्रतिरूपित करते हैं।

सुरक्षा युक्तियाँ:

- किसी भी जांच या गिरफ्तारी के लिए अपरिचितों से प्राप्त वीडियो कॉल अनुरोध का उत्तर न दें।
- सोशल मीडिया पर अनजान लोगों से निजी जानकारी साझा करने से बचें।
- जांच एजेंसियों से होने का दावा करने वाले अजनबियों को कभी भी कोई भुगतान न करें।
- यदि आपको गिरफ्तारी या जांच के बारे में कोई कॉल आता है, तो ऐसी स्थिति में निकटतम पुलिस थाना से संपर्क करें।
- हमेशा याद रखें, कोई भी सरकारी जांच संस्था ऑनलाइन कॉल / स्काइप के माध्यम से आपसे पूछताछ या आपको गिरफ्तार नहीं करेगी।
- हमेशा याद रखें, भारत में डिजिटल अरेस्ट का कोई कानूनी प्रावधान नहीं है।

#SabkoBataoo

U SuRKsha

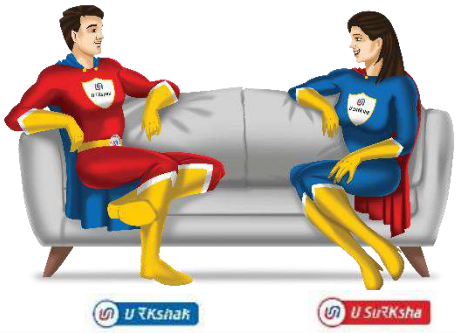
OnlineRental Fraud:

The rental scam targets elderly property owners by monitoring popular real estate online platforms and contacting the owners through immediate offer for possession.

Scammers pose as army officers/Govt. officials to establish an initial level of trust. After gaining the trust, scammers send a UPI QR code collect request and convince the owner to scan the code and enter their UPI pin to receive the rental advance payment. Once the pin is entered money is siphoned off funds from the account instead of crediting. Often in the name of returning money, additional collect request is sent to further defraud the victim.

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.



#SabkoBataoo

ऑनलाइन किराया धोखाधड़ी:

धोखेबाज़ प्रसिद्ध रियल एस्टेट प्लेटफॉर्म्स पर निगरानी रखकर उन वरिष्ठ नागरिकों को लक्षित करते हैं जो सम्पत्तियों के मालिक होते हैं। ये धोखेबाज़ संपत्ति मालिकों से तुरंत परिग्रह के ओट में संपर्क करते हैं।

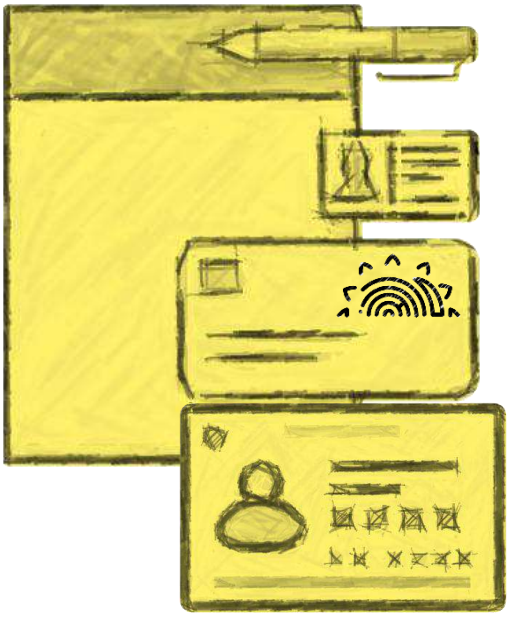
धोखेबाज़ प्रथम दृष्टया विश्वास स्थापित करने के लिए सेना का अधिकारी/सरकारी अधिकारी को प्रतिरूपित करते हैं। विश्वास हासिल करने के बाद, धोखेबाज़ एक यूपीआई क्युआर कोड कलेक्ट रिक्वेस्ट भेजते हैं और मालिक को कोड स्कैन करने और किराया अग्रिम (रेंटल एडवांस) भुगतान प्राप्त करने के लिए अपना यूपीआई पिन दर्ज करने के लिए मनाते हैं. एक बार पिन दर्ज करने के बाद पैसे जमा करने के बजाय खाते से धन निकाल लिया जाता है। अक्सर पैसे लौटाने के नाम पर पीड़ित को और ठगने के लिए अतिरिक्त राशि एकत्रित करने के उद्देश्य से अनुरोध भेजा जाता है।

सुरक्षा युक्तियाँ:

- हमेशा संभावित किरायेदारों को व्यक्तिगत रूप से संपत्ति का दौरा करने और पट्टा समझौतों (लीज़ अग्रीमेंट) को निष्पादित करने के लिए कहें।
- पहचान प्रमाण पत्रों की जांच करते समय सतर्क रहें।
- हमेशा याद रखें कि, क्यूआर कोड स्कैनिंग पैसे भेजने के लिए उपयोग किया जाता है न कि पैसे प्राप्त करने के लिए।
- याद रखें, यूपीआई से सम्बद्ध खाते में "पैसे प्राप्त करने" के लिए यूपीआई को पिन की आवश्यकता नहीं होती है।
- एक बार खाता से पैसा निकल जाने के बाद, फिर से पैसा प्राप्त करने के लिए धोखेबाज़ द्वारा भेजे गए नए क्यूआर कोड को कभी भी स्कैन न करें क्योंकि इससे आपका और अधिक नुकसान हो सकता है।

KYC /Aadhaar Update Fraud:

KYC (Know Your Customer) and Aadhaar update frauds are carried out through SMS, WhatsApp, phone calls, APKs or phishing websites.

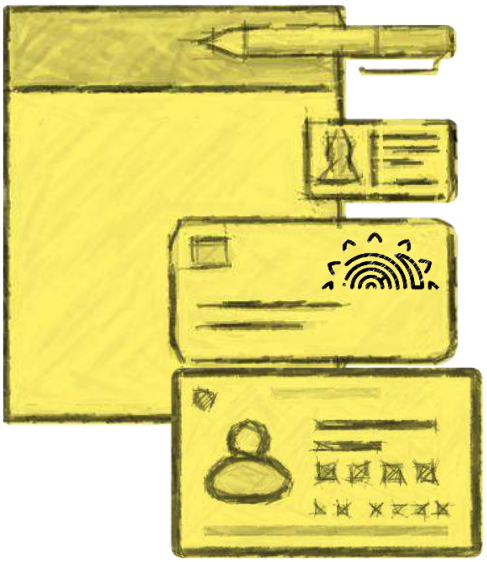


Fraudsters send messages & pretend to be from Financial Institutions, Telecom Companies or Govt. Agencies. Victims are intimidated regarding blockage of bank account, SIM cards and discontinuation of services linked to Aadhaar number & incomplete KYC. Fraudster convinces victim to visit the phishing site, download malicious APKs to gains control of the victim's phone and access sensitive data like SMS (for OTPs), banking apps, etc. to siphon off victims money.

Safety Tips:

- Always update KYC via Bank branches, official bank apps and official websites only.
- Always update Aadhaar details through authorized Aadhaar centres or UIDAI official website.
- Subscribe to Bank's SMS service to receive real time updates related to Bank account.
- Never share OTPs, Aadhaar numbers, or any other sensitive banking details with anyone over call or SMS.
- Never click on links/or install applications (APKs) received through social media messaging platforms like WhatsApp, Telegram etc.
- Always download mobile banking apps from official app stores only (Google Play store for Android & Apple App store for Apple devices).

केवाईसी/आधार अद्यतन धोखाधड़ी:



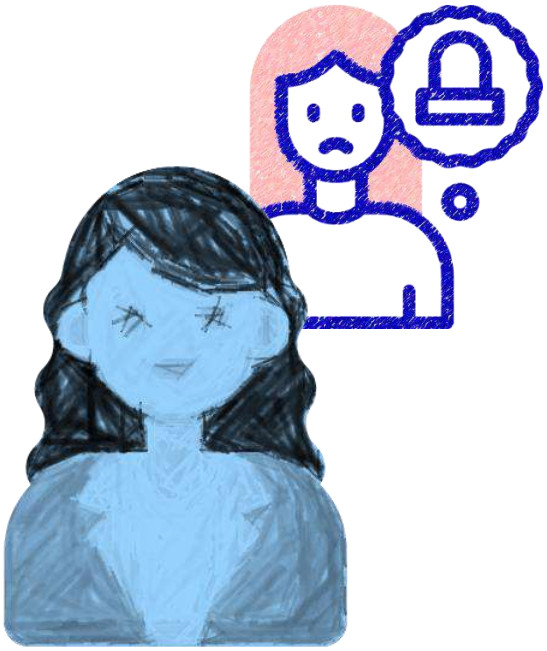
केवाईसी (अपने ग्राहक को पहचाने) और आधार अद्यतन (अपडेट) धोखाधड़ी एसएमएस, व्हाट्सएप, फोन कॉल, एपीके या फ़िशिंग वेबसाइटों के माध्यम से किया जाता है।

धोखेबाज संदेश भेजते हैं और वित्तीय संस्थानों, दूरसंचार कंपनियों या सरकारी संस्थाओं से होने का दावा करते हैं। पीड़ितों को बैंक खाते, सिम कार्ड को बंद करने और आधार नंबर और अधूरे केवाईसी से जुड़ी सेवाओं को बंद करने के बारे में डराया जाता है। जालसाज पीड़ित के फोन पर नियंत्रण पाने के उद्देश्य से उसे फ़िशिंग साइट पर जाने और दुर्भावनापूर्ण एपीके डाउनलोड करने के लिए विवश करते हैं ताकि पीड़ितों के पैसे निकालने के लिए एसएमएस (ओटीपी के लिए), बैंकिंग ऐप आदि जैसे संवेदनशील डेटा तक पहुँच सके।

सुरक्षा युक्तियाँ:

- हमेशा केवाईसी को बैंक शाखाओं, आधिकारिक बैंक ऐप और आधिकारिक वेबसाइटों के माध्यम से ही अद्यतित करें।
- हमेशा अधिकृत आधार केंद्रों या यूआईडीएआई की आधिकारिक वेबसाइट के माध्यम से ही आधार विवरण अद्यतित करें।
- बैंक खाते से संबंधित तुरंत अपडेट प्राप्त करने के लिए बैंक की एसएमएस सेवा सुविधा सक्रिय करें।
- कभी भी ओटीपी, आधार नंबर या कोई अन्य संवेदनशील बैंकिंग विवरण कॉल या एसएमएस पर किसी के साथ साझा न करें।
- व्हाट्सएप, टेलीग्राम आदि जैसे सोशल मीडिया मैसेजिंग प्लेटफॉर्म के माध्यम से प्राप्त लिंक/या इंस्टॉल एप्लिकेशन (एपीके) पर कभी भी क्लिक न करें।
- हमेशा मोबाइल बैंकिंग ऐप केवल आधिकारिक ऐप स्टोर से डाउनलोड करें (एंड्रॉइड के लिए गूगल प्ले स्टोर और ऐप्पल डिवाइस के लिए ऐप्पल ऐप स्टोर)।

Morphing & Deepfake AI Frauds:



Scammers use morphing and Deepfake AI tools to alter images of women/young girls available in social media, job application sites etc. to blend facial features and create fake videos/photographs.

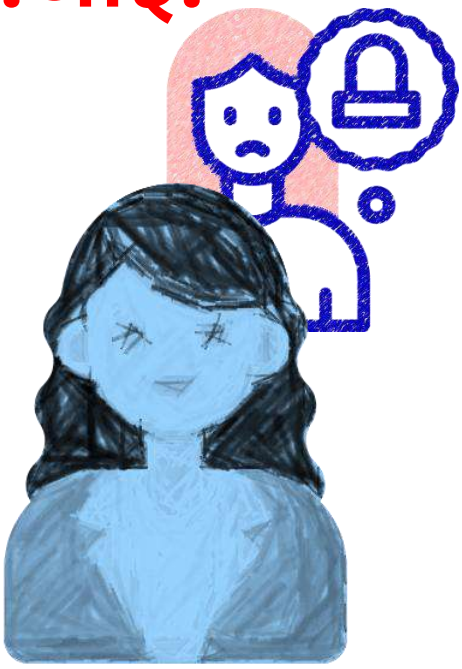
The morphed pictures are used by scammers for blackmailing the victims, creating fake online profile, sexting, sex chats, pornographic content, nude pictures etc., Morphing damages the victim's online reputation and can cause emotional trauma. Gullible victims often fall prey to blackmailing by fraudsters.

Safety Tips:

- Avoid sharing personal pictures/content in social media accounts.
- Always enable your security and privacy features on social media accounts.
- Always enable multi-factor authentication with strong passwords for all social media accounts.
- Never accept friend request from unknown, suspicious people on social media.
- Report any instances of fake profile or any such objectionable posts in social media to the social media platforms (Instagram, YouTube, etc.) and law enforcement agencies.
- Don’t be silent, always reach out and seek help from trusted family members and friends.
- Always save the evidence and screen shots for reporting the incident.

#SabkoBataoo

मॉर्फिंग और डीपफेक ए.आई. धोखाधड़ी:



धोखेबाज़ नकली वीडियो/तस्वीरें बनाने के लिए सोशल मीडिया, नौकरी आवेदन साइटों आदि पर उपलब्ध महिलाओं/युवा लड़कियों की तस्वीरों में उनके नयन-नक्श में परिवर्तन करने के लिए मॉर्फिंग और डीपफेक एआई टूल का उपयोग करते हैं।

मॉर्फ्ड तस्वीरों का उपयोग धोखेबाज़ द्वारा पीड़ितों को धमकाने-डराने के लिए, नकली ऑनलाइन प्रोफाइल बनाने, सेक्सटिंग, सेक्स चैट, अश्लील सामग्री, नग्न चित्र आदि बनाने के लिए किया जाता है। मॉर्फिंग पीड़ित की ऑनलाइन प्रतिष्ठा को हानि पहुंचाता है और यह भावनात्मक स्तर पर भी पीड़ित को आहत करता है। मासूम लोग अक्सर धोखेबाजों द्वारा ब्लैकमेलिंग का शिकार हो जाते हैं।

सुरक्षा युक्तियाँ:

- सोशल मीडिया अकाउंट में व्यक्तिगत तस्वीरें/सामग्री साझा करने से बचें।
- सोशल मीडिया खातों पर हमेशा अपनी सुरक्षा और गोपनीयता के विकल्प को सक्षम करें।
- सभी सोशल मीडिया खातों के लिए हमेशा मजबूत पासवर्ड के साथ बहु-स्तरीय प्रमाणीकरण को सक्रिय रखें।
- सोशल मीडिया पर कभी भी अज्ञात, संदिग्ध लोगों से मित्रता का अनुरोध (फ्रेंड रिक्वेस्ट) स्वीकार न करें।
- सोशल मीडिया में नकली प्रोफ़ाइल या ऐसी किसी भी आपत्तिजनक पोस्ट की रिपोर्ट सोशल मीडिया प्लेटफॉर्म (इंस्टाग्राम, यूट्यूब, आदि) और विधि प्रवर्तन संस्थाओं को करें।
- चुप न रहें, हमेशा विश्वसनीय परिवार के सदस्यों और दोस्तों से मदद लें।
- घटना की रिपोर्ट करने के लिए हमेशा सबूत और स्क्रीन शॉट को अपने पास सुरक्षित रखें।

Matrimonial Fraud:

Matrimonial fraud involves scammers who create fake profiles on popular matrimonial websites or social media to con women seeking partners. These fraudsters fabricate stories to build emotional connect and exploit women victims for financial gain.

Fraudsters then use various pretext like medical emergencies, Jewellery purchase, marriage expenses etc. to requests urgent money transfers. In some cases victims are blackmailed with private photos/videos creating emotional trauma, financial loss and social stigma.

Safety Tips:

- Avoid sharing personal pictures/content in social media accounts.
- Always use reputed matrimonial sites with good privacy policies and use platforms that offer ID-verified profiles only.
- Avoid sharing intimate photos, ID documents, Bank account details etc.
- Always use privacy settings to control who can view your profile.
- Never transfer money to someone you've never met.
- In case of doubt, always reach out to the platform and seek help from trusted family members and friends.
- Report any instances of fraud to the law enforcement agencies.

#SabkoBataoo

वैवाहिक धोखाधड़ी:

वैवाहिक धोखाधड़ी में धोखेबाज़ लोकप्रिय वैवाहिक वेबसाइटों या सोशल मीडिया पर नकली प्रोफाइल बनाते हैं ताकि साथी की तलाश में महिलाओं को धोखा दिया जा सके। ये जालसाज भावनात्मक जुड़ाव बनाने के लिए कहानियाँ गढ़ते हैं और वित्तीय लाभ उठाने के लिए पीड़ित महिला का शोषण करते हैं। जालसाज चिकित्सा की आपात स्थिति, आभूषणों की खरीद, शादी के खर्च आदि जैसे विभिन्न बहाने से तत्काल पैसा भेजने के लिए कहते हैं। कुछ मामलों में पीड़ितों को निजी फोटो/वीडियो के साथ ब्लैकमेल किया जाता है, जिससे भावनात्मक आघात, वित्तीय नुकसान और समाज में बदनामी का डर पैदा होता है।

सुरक्षा युक्तियाँ:

- सोशल मीडिया अकाउंट पर व्यक्तिगत तस्वीरें/जानकारी साझा करने से बचें।
- हमेशा सुदृढ़ गोपनीयता नीतियों का अनुपालन करने वाली प्रतिष्ठित वैवाहिक साइटों का उपयोग करें और ऐसे प्लेटफार्मों का उपयोग करें जो केवल आईडी-सत्यापित प्रोफाइल प्रदान करते हैं।
- अंतरंग फोटो, आईडी दस्तावेज, बैंक खाता विवरण आदि साझा करने से बचें।
- आपकी प्रोफ़ाइल कौन देख सकता है, इसे नियंत्रित करने के लिए हमेशा गोपनीयता सेटिंग (प्राइवेसी सेटिंग) का उपयोग करें.
- कभी भी किसी ऐसे व्यक्ति को पैसे न भेजे, जिससे आप कभी नहीं मिले हैं।
- संदेह के मामले में, हमेशा मदद के लिए आगे आए और परिवार के विश्वसनीय सदस्यों और दोस्तों से मदद लें।
- धोखाधड़ी के किसी भी मामले की रिपोर्ट विधि प्रवर्तन संस्थाओं को करें।

Cyber Stalking:

Cyber Stalkers send friend request through fake social media accounts of people known to the women victims. After acceptance of the request, they repeatedly bully the victim through unwanted contact request via email, texts, messages etc. Stalkers often ask inappropriate questions, send posts or share sexual or offensive content, abusive comments, or false accusations to the victim. Sometimes they track victim's movements by following their social media posts.

Safety Tips:

- Avoid sharing personal pictures/content/vacation plans/address/location through social media accounts.
- Never accept online friend requests of unknown people through social media.
- Always use privacy settings to control who can view your profile on social media.
- Report instances of stalking to the law enforcement agencies.
- Don't suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.

#SabkoBataoo

साइबर स्टॉकिंग:

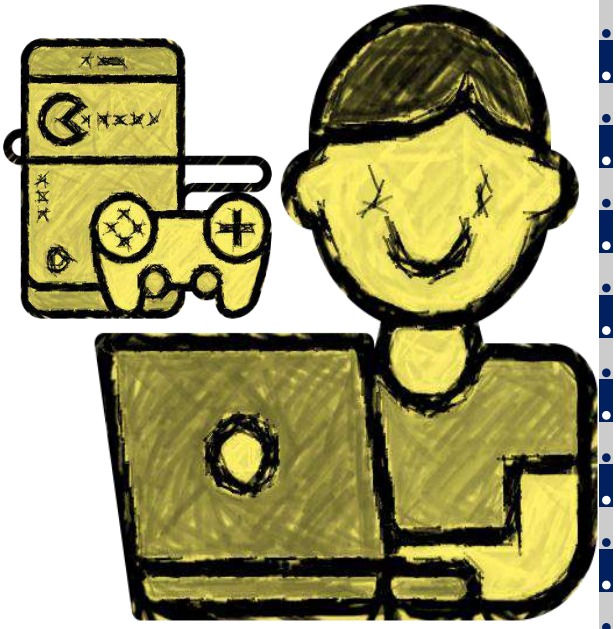
साइबर स्टॉकर्स पीड़ित महिलाओं के परिचित लोगों के नाम पर फर्जी सोशल मीडिया अकाउंट से फ्रेंड रिक्वेस्ट भेजते हैं। अनुरोध स्वीकार करने के बाद, अवांछित संपर्क करने के उद्देश्य से वे ईमेल, संदेशों आदि के माध्यम से पीड़ित को बार-बार धमकाते हैं। पीछा करने वाले (स्टॉकर) अक्सर अनुचित प्रश्न पूछते हैं, पोस्ट भेजते हैं या पीड़ित को आपत्तिजनक सामग्री भेजते हैं। अपमानजनक टिप्पणियां करते हैं या झूठे आरोप भी लगाते हैं। कभी-कभी वे सोशल मीडिया पोस्ट का अनुसरण करते हुए पीड़ितों की गतिविधियों को भी ट्रैक करते हैं।

सुरक्षा युक्तियाँ:

- सोशल मीडिया अकाउंट के माध्यम से व्यक्तिगत तस्वीरें/जानकारी/अवकाश योजना/पता/स्थान साझा करने से बचें।
- सोशल मीडिया पर अनजान लोगों के ऑनलाइन मित्रता का अनुरोध (फ्रेंड रिक्वेस्ट) कभी भी स्वीकार न करें।
- सोशल मीडिया पर आपकी प्रोफ़ाइल कौन देख सकता है, इसे नियंत्रित करने के लिए हमेशा गोपनीयता सेटिंग्स (प्राइवेसि सेटिंग्स) का उपयोग करें।
- विधि प्रवर्तन संस्थाओं को पीछा करने के मामलों की रिपोर्ट करें।
- चुप रहकर परेशान न हों, यह समझे कि आप अकेले नहीं हैं और परिवार के विश्वसनीय सदस्यों और दोस्तों से अवश्य मदद लें।

Online Gaming Fraud:

Kid access games via mobile apps, gaming consoles, or Personal Computers. These games are free-to-play, with option of in-app purchases. The gaming apps always obtain access for photos, videos, files, SMS and other sensitive information. Children are also incentivized to continue playing through rewards, leader boards, and levelling up which leads to excessive screen time and addiction.

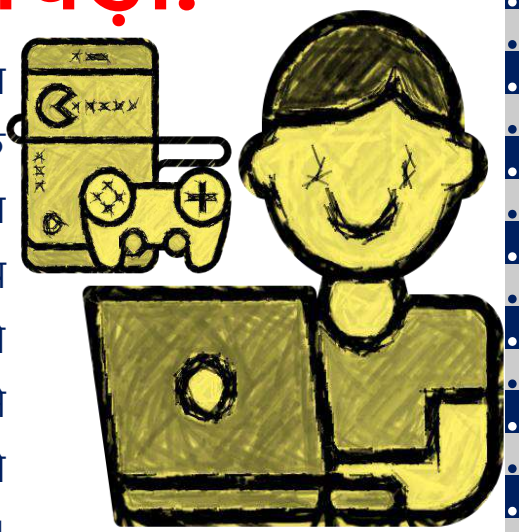


Safety Tips:

- If children request to purchase game subscription always make sure to use official platforms only.
- Never save card details to accounts while purchasing online gaming subscription.
- Always ensure that your child's accounts are enabled with multifactor authentication and protected with strong unique passwords.
- Always use parental controls for content & screen time limitation.
- Always check permissions requested by apps and games. Be cautious if the app/game asks for unnecessary permissions.
- Educate your children not to share personal information such as name, age, address, phone number, or school name with other online players.
- Always monitor kids/bank accounts for unusual/unauthorized transactions.
- Regularly update system/mobile software which include security patches to prevent hacking or data breaches and enhances security.

#SabkoBataoo

ऑनलाइन गेमिंग धोखाधड़ी:



बच्चे मोबाइल ऐप, गेमिंग कंसोल या पर्सनल कंप्यूटर के माध्यम से गेम एक्सेस करते हैं। ये गेम इन-ऐप खरीदारी के विकल्प के साथ आते हैं और इन्हें मुफ्त में खेला भी जा सकता है। यह गेमिंग ऐप्स हमेशा फोटो, वीडियो, फाइल, एसएमएस और अन्य संवेदनशील जानकारी के लिए पहुंच प्राप्त करते हैं। बच्चों को पुरस्कार, लीडर बोर्ड और खेल के स्तर को बढ़ाने के माध्यम से खेलना जारी रखने के लिए प्रोत्साहित किया जाता है जिससे अत्यधिक स्क्रीन समय बढ़ जाता है और अंतत: लत लग जाती है।

सुरक्षा युक्तियाँ:

- यदि बच्चे खेल की सदस्यता खरीदने का अनुरोध करते हैं, तो हमेशा आधिकारिक प्लेटफार्मों का उपयोग करना सुनिश्चित करें।
- ऑनलाइन खेल की सदस्यता खरीदते समय कभी भी कार्ड विवरण को खातों में न सहेजें।
- हमेशा सुनिश्चित करें कि आपके बच्चे का खाता बहु-स्तरीय प्रमाणीकरण के साथ सक्षम है और विशिष्ट मजबूत पासवर्ड के साथ सुरक्षित हो।
- सामग्री और स्क्रीन समय सीमा के लिए हमेशा माता-पिता के नियंत्रण (परेंटल कंट्रोल) फीचर का उपयोग करें।
- हमेशा ऐप्स और गेम द्वारा अनुरोधित अनुमतियों की जांच करें। यदि ऐप/गेम अनावश्यक अनुमति मांगता है तो सतर्क रहें।
- अपने बच्चों को शिक्षित व जागरूक करें कि वे अन्य ऑनलाइन खिलाड़ियों के साथ व्यक्तिगत जानकारी जैसे नाम, आयु, पता, फोन नंबर या विद्यालय का नाम साझा न करें।
- असामान्य/अनाधिकृत लेनदेन के लिए हमेशा बच्चों/बैंक खातों की जाँच करें।
- सिस्टम/मोबाइल सॉफ्टवेयर को नियमित रूप से अद्यतन करें जिसमें हैकिंग या डाटा उल्लंघनों को रोकने और सुरक्षा बढ़ाने के लिए सुरक्षा पैच शामिल हो।

Cyber Bullying:

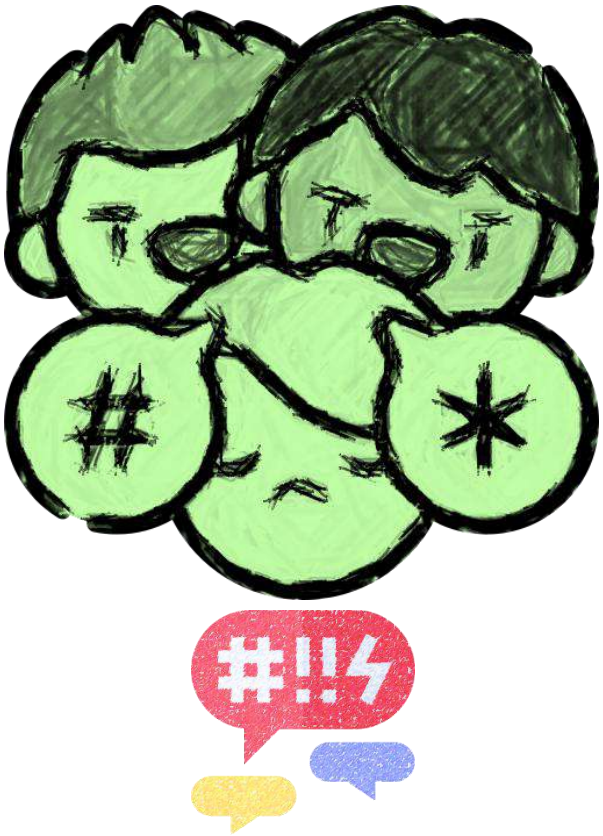
Cyber Bullying is a form of harassment which includes sending, posting, or sharing negative, harmful, fake or mean content about kids by peers & friends. It may include sharing personal or private information about someone else related to kids causing embarrassment or humiliation.

Safety Tips:

- Always talk to Parents, Teacher or Guardian if someone is bothering you online.
- Use the block or report feature on apps and platforms to stop harassment.
- Always ensure that your profile is private and connect to known people only.
- Never share personal information like your Name, School, Address, Phone Number, Bank Details, Photos or Videos online.
- Always Keep accounts safe with strong passwords and don't share them with friends.
- Always use parental controls for content & screen time limitation for your kids.
- Report any incident of blackmailing promptly to your parents/guardians and the law enforcement agencies.

#SabkoBataoo

साइबर बुलिंग:



साइबर बुलिंग उत्पीड़न का एक ऐसा रूप है जिसमें साथियों और दोस्तों द्वारा बच्चों के बारे में नकारात्मक, हानिकारक, नकली या मतलबी सामग्री भेजना, पोस्ट करना या साझा करना शामिल है। इसमें बच्चों से संबंधित शर्मिंदगी या अपमान पैदा करने वाले किसी और के बारे में व्यक्तिगत या निजी जानकारी साझा करना शामिल हो सकता है।

सुरक्षा युक्तियाँ:

- हमेशा माता-पिता, शिक्षक या अभिभावक से बात करें यदि कोई आपको ऑनलाइन परेशान कर रहा है।
- उत्पीड़न को रोकने के लिए ऐप्स और प्लेटफ़ॉर्म पर ब्लॉक या रिपोर्ट सुविधा का उपयोग करें।
- हमेशा सुनिश्चित करें कि आपकी प्रोफ़ाइल निजी (प्राइवेट) हो और केवल ज्ञात लोगों से ही जुड़ी हुई हो।
- कभी भी अपना नाम, विद्यालय, पता, फोन नंबर, बैंक विवरण, फोटो या वीडियो जैसी व्यक्तिगत जानकारी ऑनलाइन साझा न करें।
- हमेशा मजबूत पासवर्ड के साथ खातों को सुरक्षित रखें और उन्हें दोस्तों के साथ साझा न करें।
- हमेशा अपने बच्चों के लिए विषय-वस्तु की जानकारी (कंटैंट) और स्क्रीन समय सीमा के लिए माता-पिता के नियंत्रण (पैरेंटल कंट्रोल) फीचर का उपयोग करें।
- डराने-धमकाने (ब्लैकमेल) की किसी भी घटना की सूचना तुरंत अपने माता-पिता/अभिभावकों और विधि प्रवर्तन संस्थाओं को दें।

भारत दूरसंचार
DOT
INDIA TELECOM

SANCHAR SAATHI

AN INTEGRATED SPACE FOR CITIZEN CENTRIC SERVICES

REPORT
- Suspected Fraud Communication & Unsolicited Commercial Communication/SPAM
- International Call with Indian Number

TRACK
- Your Lost or stolen mobile handset
- Your Mobile connections
- Your wireline internet service provider

ACCESS NOW

Web Portal
https://sancharsaathi.gov.in

Mobile App
GET IT ON Google Play
Download on the App Store

STOP
THINK
TAKE ACTION
STAY CYBERSAFE

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

REPORT ANY
CYBERCRIME AT
1930

OR

REGISTER
ONLINE
COMPLAINT ON
CYBERCRIME.GOV.IN

!! Be Cyber Aware, Be Cyber Safe !!