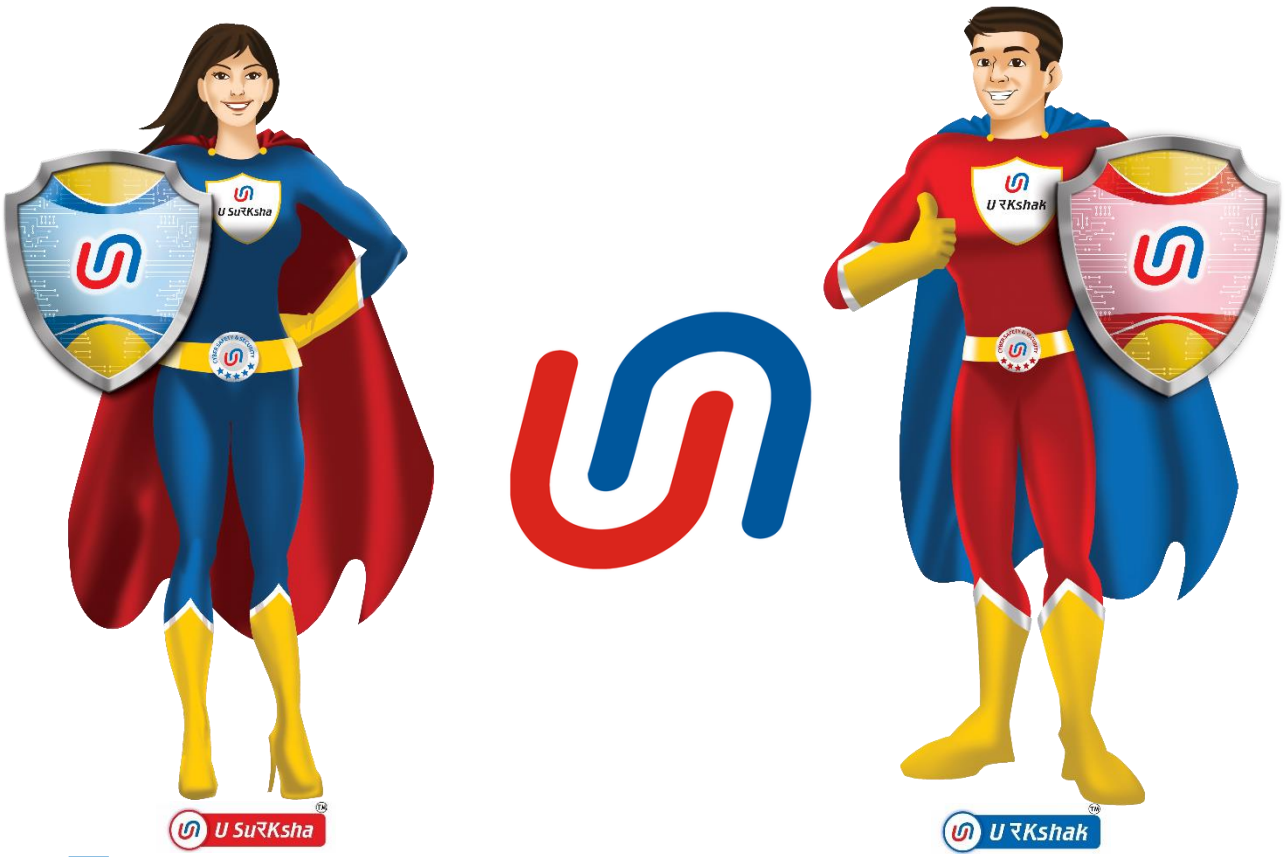
यूनियन बैंक ऑफ इंडिया
भारत सरकार का उपक्रम

Union Bank of India
A Government of India Undertaking

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

Union Bank of India

Cyber Security Customer Awareness Guide



Page Index

Cyber Security is Everyone's Responsibility

संदेश

सुश्री ए मणिमेखलै

प्रबंध निदेशक एवं सीईओ

यूनियन बैंक ऑफ इंडिया ने ग्राहकों को सुरक्षित और उन्नत डिजिटल अनुभव प्रदान करने के लिए हमेशा ही अत्याधुनिक तकनीक को अपनाया है ताकि डिजिटल सुरक्षा सुनिश्चित किया जा सके। हमारा बैंक नए डिजिटल उत्पादों और सेवा क्षेत्रों में निरंतर अभिनव पहल करते हुए सभी हितधारकों के हितों की रक्षा हेतु मजबूत साइबर सुरक्षा संस्कृति विकसित कर रहा है।

यह पुस्तिका उसी दिशा में एक पहल है। मैं सभी पाठकों से इस पुस्तिका का भरपूर उपयोग करने एवं जागरूकता ज्ञान हासिल करने का आग्रह करती हूं।

संदेश

श्री निधु सक्सेना,

कार्यपालक निदेशक

यूनियन बैंक ग्राहक अनुभूति में सतत वृद्धि और ग्राहक संतुष्टि प्रदान करने की मंशा से बैंकिंग सेवा के विभिन्न पहलुओं में डिजिटलीकरण को तेजी से अपना रहा है। हमेशा "सुरक्षित और विश्वसनीय" बने रहने के लिए बैंक विभिन्न डिजिटल चैनलों के माध्यम से अपने हितधारकों के बीच साइबर सुरक्षा जागरूकता पैदा करने पर अत्यधिक महत्व दे रहा है। मैं सभी पाठकों से इस बुकलेट के माध्यम से स्वयं को जागरूक करने और अपने मित्र एवं परिवारजनों के बीच भी जागरूकता फैलाने का आह्वान करता हूं।

संदेश

श्री आर पी सिंह,

सीआईएसओ

यूनियन बैंक अपने ग्राहकों को सुरक्षित डिजिटल सेवाएं देने के लिए प्रतिबद्ध है। सर्वोत्तम साइबर स्वच्छता प्रथाओं का पालन करने से किसी भी साइबर धोखाधड़ी का शिकार होने का जोखिम कम हो जाता है। बैंक अपने विभिन्न हितधारकों को साइबर दुनिया के खतरों से बचाने की दिशा में काम कर रहा है। यह पुस्तिका पाठकों के बीच साइबर जागरूकता बढ़ाने की दृष्टि से तैयार की गई है। मैं सभी पाठकों से पुस्तिका का इष्टतम उपयोग करने की गुजारिश करता हूं।

Message from
Ms. A. Manimekhalai
MD&CEO

Union Bank of India has adopted state-of-art technology to deliver safe and enhanced digital experience to customers ensuring safety and security. Bank in its continuous journey of innovating new digital products and services is developing a robust cyber security culture for safeguarding interest of all stakeholders.

This booklet is an initiative in the same direction. I urge all readers to make full use of the booklet to gain awareness.

Message from
Shri Nidhu Saxena,
Executive Director

Union Bank is increasingly adopting digitization in various aspects of Banking service to enhance customer experience and achieve customer delight. To always remain "Safe & Trusted", Bank is giving utmost importance in creating Cyber Security Awareness among its stakeholders through various digital channels. I urge all readers to make themselves aware and to spread the awareness among their friends & family through this booklet.

Message from
Shri R P Singh,
CISO

Union Bank is committed to deliver digital services to its customers with safety and security. Following best Cyber Hygiene practices reduces the risk of falling victim to any cyber fraud. Bank is working towards protecting its various stakeholders from dangers of Cyber World. This booklet has been designed to enhance the cyber awareness among the readers. I urge all readers to make the best use of it.

मनी म्यूल धोखाधड़ी:

मनी म्यूल्स ऐसे असंदेही व्यक्ति होते हैं जो साइबर अपराध, तस्करी, ड्रग्स आदि से सृजित अवैध धन की आवाजाही को सुगम बनाने के लिए मध्यस्थ के रूप में काम कर रहे हैं। एक व्यक्ति अनजाने में "मनी म्यूल" बन जाता है, जो गलत तरीके से कमाए गए धन की आवाजाही को सुविधाजनक बनाता है, जबकि इसमें लिप्त अपराधी अदृश्य रहते हैं। मनी म्यूल गतिविधियों में भाग लेना आपराधिक कृत्य है, भले ही व्यक्ति लेनदेन की वास्तविक प्रकृति से अनजान है।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- पूरा नाम
- पैन
- आधार नंबर

बैंकिंग जानकारी

- खाता संख्या
- इंटरनेट बैंकिंग लॉगिन पासवर्ड
- इंटरनेट बैंकिंग लेनदेन पासवर्ड
- मोबाइल बैंकिंग पिन

कार्यप्रणाली:

- जालसाज़ विभिन्न संचार माध्यमों जैसे ईमेल, सोशल मीडिया, नौकरी वेबसाइट, डेटिंग प्लेटफ़ॉर्म आदि के माध्यम से छद्म पहचान के साथ संपर्क शुरू करते हैं, आकर्षक या लुभावने प्रस्ताव देते हैं, नकली नौकरी के अवसर प्रदान करते हैं, आसानी से पैसे कमाने की पेशकश करते हैं, रोमांटिक संबंधों का दिखावा करते हैं और मनगढ़ंत कहानियों के साथ संबंध बनाते हैं।
- जालसाज़ पीड़ित को अपने खातों में पैसे स्वीकार करने के लिए मना लेता है और पीड़ित के बैंक खाते में चोरी या धोखाधड़ी से अर्जित धनराशि भेजता है। वे पीड़ित को धन की वास्तविक आगम और लेनदेन की अवैध प्रकृति के बारे में अंधेरे में रखते हैं।
- पीड़ित जो मनी म्यूल बन जाता है, उसे निर्देश दिया जाता है कि वह धनराशि को अन्य खातों में अंतरित कर दे या राशि को अन्य खातों में अंतरित करने के लिए अपने इंटरनेट/मोबाइल बैंकिंग क्रेडेंशियल्स को साझा कर दे, जो संभवतः किसी अन्य मनी म्यूल का खाता हो सकता है - यह श्रृंखला की शुरूआत है जिसके परिणामस्वरूप अंततः धन जालसाज़ के खाते में अंतरित हो जाता है।

सुरक्षा टिप्स:

- दूसरों के लिए धनराशि अंतरित करने हेतु बैंक खाते का उपयोग करने के किसी भी अनुरोध से सावधान रहें।
- उन वित्तीय लेनदेन के लिए मध्यस्थ बनने से बचें जिनमें स्पष्ट और वैध उद्देश्य का अभाव है।
- अवास्तविक रिटर्न या अत्यधिक अच्छे दिखने वाले प्रस्तावों का दावा करने वाले किसी भी व्यक्ति को प्रारंभिक जमा, कमीशन या अंतरण शुल्क के रूप में पैसे न भेजें।
- ऐसे ऑनलाइन रिश्तों से सावधान रहें जो तेजी से पनपते हैं और जिनमें वित्तीय लेनदेन शामिल होता है।
- कभी भी संवेदनशील व्यक्तिगत या वित्तीय जानकारी किसी के साथ साझा न करें।

Money Mule Fraud:

Money mules are unsuspecting individuals who are working as intermediaries to facilitate the movement of illicit finds generated from cybercrimes, smuggling, drugs etc. A person unknowingly becomes a “Money Mule”, facilitating the movement of ill-gotten funds, while the criminals behind the scenes remain concealed. Participation in money mule activities is a criminal offense, even if one is unaware of the true nature of the transactions.

Information being harvested:

Personal Information

- Full Name
- Pan
- Aadhaar Number

Banking Information

- Account Number
- Internet Banking Login password
- Internet Banking Transaction password
- Mobile Banking Pin

Modus Operandi:

- Fraudster Initiate contact through various communication channels like email, social media, job websites, dating platforms etc. with fake identities, making attractive or lucrative offers fake job opportunities, offering easy money, pretending romantic connection and building rapport with fabricated stories.
- Fraudster convinces the victim to accept money into their accounts and sends stolen or fraudulent funds to the victim’s bank account. They keep victim in dark about the actual origin of the funds and the illegal nature of the transaction.
- The victim who becomes a money mule is instructed to transfer the funds to other accounts or share their internet/mobile banking credentials for transferring the amount to other accounts which can possibly be another money mule’s account – starting a chain that ultimately results in the money transferred to fraudster’s account.

Safety Tips:

- Be wary of any requests to use bank account for receiving of transferring funds for others.
- Avoid becoming an intermediary for financial transactions that lacks clear and legitimate purpose.
- Don’t send money as initial deposit, commission or transfer fee to anyone claiming unrealistic returns or offers too good to be true.
- Be cautious of online relationships that evolve quickly and involve financial transactions.
- Never share sensitive personal or financial information with anyone.
- Be cautious of requests to encash cheques for someone else. Scammers often use fake cheques to involve victims in their schemes.

आधार सक्षम भुगतान प्रणाली (एईपीएस) धोखाधड़ी

एईपीएस धोखाधड़ी उंगलियों के निशान आदि के साथ लीक हुए बायोमेट्रिक क्रेडेंशियल्स को इकट्ठा करके की जाती है। इन क्रेडेंशियल्स का उपयोग पीड़ितों के खाते तक पहुंचने और पैसे निकालने के लिए किया जाता है।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- आधार नंबर
- बायोमेट्रिक क्रेडेंशियल

बैंकिंग जानकारी

- बैंक का नाम

कार्यप्रणाली:

- जालसाज विभिन्न स्रोतों जैसे वेबसाइट/दुकान/सिम कार्ड आउटलेट या नकली मोबाइल ऐप के माध्यम से बायोमेट्रिक डेटा एकत्र करते हैं।
- एक बार बायोमेट्रिक डेटा प्राप्त हो जाने के बाद, धोखेबाज आधार से जुड़े बैंक खातों से पैसे चुराने के लिए उनका उपयोग करते हैं।

सुरक्षा टिप्स:

- यदि आवश्यक न हो तो, आधार आधारित सेवाओं के लिए अपने बायोमेट्रिक को निम्न तरीके से लॉक करें:
  - एमआधार ऐप के माध्यम से
  - यूआईडीएआई वेबसाइट के माध्यम से
  - 1947 पर संदेश भेजकर
- किसी भी लेनदेन के संबंध में बैंक द्वारा भेजे गए एसएमएस और ईमेल को ठीक से जांचें और किसी भी संदेह के मामले में तत्काल अपने बैंक से संपर्क करें।
- अपना बायोमेट्रिक डेटा शेयर करते समय सावधान रहें।
- मोबाइल ऐप्स को बायोमेट्रिक एक्सेस की अनुमति देने में सावधानी बरतें।
- हमेशा सर्वोत्तम साइबर स्वच्छता प्रथाओं का पालन करें।

Aadhaar Enabled Payment System (AePS) Fraud

AePS frauds are carried out by collecting leaked biometric credentials including fingerprints etc. These credentials are then used to access victims account and siphon money.

Information being harvested:

Personal Information

- Aadhaar Number
- Biometric Credential

Banking Information

- Name of the Bank

Modus Operandi:

- Fraudsters are collecting biometric data through various means like websites/shops/ SIM card outlets or fake mobile apps.
- Once the biometric data is obtained, fraudsters are using them to steal money from Aadhaar linked bank accounts.

Safety Tips:

- Use any of the below methods to lock your biometrics for Aadhaar based services, when not required:
  - Using mAadhaar App
  - Using UIDAI website
  - Sending SMS to 1947
- Properly check the SMS and email sent by bank regarding any transactions and contact your bank immediately in case of any suspicion.
- Be careful while sharing your biometric data.
- Be careful in giving biometric access permission to mobile apps.
- Always follow best cyber hygiene practices.

नकली ऐप के माध्यम से केवाईसी धोखाधड़ी

केवाईसी अद्यतन धोखाधड़ी में पीड़ित को यह विश्वास दिलाया जाता है कि उनका बैंक खाता अवरुद्ध हो जाएगा और उन्हें चालू रखने के लिए तत्काल कार्रवाई की आवश्यकता है। फिर पीड़ितों से ऐप डाउनलोड करने या लिंक पर क्लिक करने और खाते का सुचारू रूप से संचालन करने के लिए संवेदनशील डेटा प्रस्तुत करने का आग्रह किया जाता है। इस प्रकार प्रस्तुत किए गए डेटा का उपयोग पीड़ितों के खाते तक पहुंचने और पैसे निकालने के लिए किया जाता है।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- पूरा नाम
- पैन
- आधार नंबर
- फ़ोन में सेव फ़ाइलें
- पता
- संपर्क

बैंकिंग जानकारी

- खाता संख्या
- आईएफएससी कोड
- डेबिट/क्रेडिट कार्ड नंबर
- डेबिट/क्रेडिट कार्ड पिन
- सीवीवी
- मोबाइल बैंकिंग पिन

कार्यप्रणाली:

- बैंक अधिकारी बनकर घोटालेबाज फर्जी एसएमएस/संदेशों के माध्यम से पीड़ित से संपर्क करते हैं और सेवा जारी रखने के लिए बैंक खाते में केवाईसी विवरण अद्यतन करने की तत्काल आवश्यकता बताते हैं।
- फिर पीड़ित को मोबाइल ऐप डाउनलोड करने (आमतौर पर स्क्रीन शेयरिंग) / लिंक पर क्लिक करने और केवाईसी जानकारी प्रस्तुत करने के लिए बरगलाया जाता है।
- मोबाइल में संग्रहित व्यक्तिगत जानकारी/स्क्रीन में दर्ज डेटा को घोटालेबाज द्वारा कैप्चर कर लिया जाता है।
- एकत्रित जानकारी का उपयोग घोटालेबाज द्वारा पीड़ित के बैंक खाते तक पहुंचने और पैसे निकालने के लिए किया जाता है।

सुरक्षा टिप्स:

- ऐसे दावों की वास्तविकता सत्यापित करने के लिए हमेशा सीधे बैंक से संपर्क करें। संपर्क करने हेतु हमेशा बैंक की आधिकारिक वेबसाइट/पासबुक पर दिए गए संपर्क विवरण का उपयोग करें।
- असत्यापित स्रोतों से प्राप्त अज्ञात लिंक पर कभी भी क्लिक न करें।
- अनजान कॉल करने वालों के अनुरोध पर कभी भी मोबाइल ऐप डाउनलोड न करें।
- कभी भी मोबाइल नंबर, खाता नंबर, पासवर्ड, ओटीपी, पिन या कोई अन्य गोपनीय जानकारी किसी से साझा न करें।
- रिमोट एक्सेस सुविधा प्रदान करने वाले एप्लिकेशन इंस्टॉल करके कभी भी अपने डिवाइस का एक्सेस किसी को न दें।

KYC Fraud through fake app

KYC updation fraud are carried out by tricking the victim to believe that their bank account will get blocked and urgent action is needed to keep them functioning. Victims are then urged to download apps or click on links and submit sensitive data for unblocking the account. The data submitted is then used to access victims account and siphon money.

Information being harvested:

Personal Information

- Full Name
- Pan
- Aadhaar Number
- Files in phone
- Address
- Contacts

Banking Information

- Account Number
- IFSC Code
- Debit/Credit Card Number
- Debit/Credit Card Pin
- CVV
- Mobile Banking Pin

Modus Operandi:

- Scammers impersonating as Bank officials contact victim through fake SMS/Messages informing urgent need for updation of KYC details in Bank account for continuation of service.
- Victim is then tricked to download mobile app (generally screen sharing) / Click link and submit KYC information.
- Personal information stored in mobile / Data entered in screen is then captured by Scammer.
- Information gathered is used by the scammer to access Bank account of the victim and siphon off money.

Safety Tips:

- Always verify the genuineness of such claims by contacting the Bank directly. Always use the contact details provided in official website/passbook provided by the bank.
- Never Click on unknown links received from unverified sources.
- Never download mobile apps on request from unknown callers.
- Never Share mobile number, account number, password, OTP, PIN or any other confidential details to anyone.
- Never give access of your device to anyone by installing applications supporting remote access features.

फर्जी ग्राहक सेवा/संपर्क केंद्र घोटाला

ग्राहक सेवा घोटाला को नकली वेबपेज बनाकर, इंटरनेट पर किसी वास्तविक कंपनी की ग्राहक सेवा संपर्क जानकारी को बदलकर या सर्च इंजन के माध्यम से उपलब्ध जानकारी को संपादित करके किया जाता है।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- पूरा नाम
- पैन
- आधार नंबर
- फ़ोन में सुरक्षित फ़ाइलें
- पता
- संपर्क

बैंकिंग जानकारी

- खाता संख्या
- आईएफएससी कोड
- डेबिट/क्रेडिट कार्ड नंबर
- डेबिट/क्रेडिट कार्ड पिन
- सीवीवी
- मोबाइल बैंकिंग पिन

कार्यप्रणाली:

- सर्च इंजन में उपलब्ध मौजूदा जानकारी को संपादित करके या नकली वेबपेज बनाकर वास्तविक कंपनी का ग्राहक सेवा नंबर बदल देते हैं और पीड़ित के संपर्क करने का इंतजार करते हैं।
- जब कोई पीड़ित इन फर्जी नंबरों पर संपर्क करता है, तो ग्राहक सेवा एजेंट के छद्म रूप में मौजूद धोखेबाज उन्हें विद्वेशक मोबाइल ऐप डाउनलोड करने / लिंक पर क्लिक करने और व्यक्तिगत एवं बैंकिंग जानकारी प्रस्तुत करने का झांसा देता है।
- एकत्रित जानकारी का उपयोग घोटालेबाज द्वारा पीड़ित के बैंक खाते तक पहुंचने और पैसे निकालने के लिए किया जाता है।

सुरक्षा टिप्स:

- संपर्क करने के लिए हमेशा बैंक की आधिकारिक वेबसाइट/पासबुक पर दिए गए संपर्क विवरण का उपयोग करें।
- असत्यापित स्रोतों से प्राप्त अज्ञात लिंक पर कभी भी क्लिक न करें।
- अनजान कॉल करने वालों के अनुरोध पर कभी भी मोबाइल ऐप डाउनलोड न करें।
- मोबाइल नंबर, खाता संख्या, पासवर्ड, ओटीपी, पिन या कोई अन्य गोपनीय विवरण कभी भी किसी को/असुरक्षित वेबसाइट पर साझा/प्रस्तुत न करें।
- रिमोट एक्सेस सुविधा प्रदान करने वाले एप्लिकेशन इंस्टॉल करके कभी भी अपने डिवाइस का एक्सेस किसी को न दें।

Fake Customer Care/Contact Centre Scam

Customer Care Scam are carried out by changing customer care contact information of a genuine company in internet by creating fake webpages or editing the information available through search engines.

Information being harvested:

Personal Information

- Full Name
- Pan
- Aadhaar Number
- Files in phone
- Address
- Contacts

Banking Information

- Account Number
- IFSC Code
- Debit/Credit Card Number
- Debit/Credit Card Pin
- CVV
- Mobile Banking Pin

Modus Operandi:

- Fraudsters Change the customer Care number of a genuine company in internet by editing the existing information available in the search engines or creating fake webpages and wait for victim to make contact.
- When any victim contact these fake numbers, Fraudster impersonating as customer care agent tricks them in downloading malicious mobile apps / Click link and submit Personal and Banking Information.
- Information gathered is then used by the scammer to access Bank account of the victim and siphon off money.

Safety Tips:

- Always use the contact details provided in Bank's official website/Passbook.
- Never Click on unknown links received from unverified sources.
- Never download mobile apps on request from unknown callers.
- Never Share/submit mobile number, account number, password, OTP, PIN or any other confidential details to anyone/unsecured websites.
- Never give access of your device to anyone by installing applications supporting remote access features.

यूपीआई कलेक्ट रिक्वेस्ट घोटाला

यूपीआई कलेक्ट रिक्वेस्ट घोटाला में पीड़ित को क्यूआर कोड स्कैन करने और पैसे प्राप्त करने के लिए यूपीआई पिन दर्ज करने के लिए बरगलाया जाता है।

सूचना संग्रहण:

इस घोटाले में कोई भी व्यक्तिगत या बैंकिंग जानकारी प्राप्त नहीं की जाती है।

कार्यप्रणाली:

- जालसाज पीड़ितों से तब संपर्क करते हैं जब वे अपने मोबाइल, फर्नीचर, बाइक आदि बेचने या अपना घर किराए पर देने के लिए वेबसाइटों पर विज्ञापन देते हैं।
- पीड़ित का विश्वास हासिल करने के लिए, जालसाज़ आम तौर पर बैंक खाते के विवरण की सत्यता परखने के बहाने कम राशि का भुगतान भेजता है।
- फिर जालसाज पीड़ित को यूपीआई कलेक्ट रिक्वेस्ट क्यूआर कोड भेजता है और उसे पैसे प्राप्त करने के लिए क्यूआर स्कैन करने के लिए मना लेता है।
- क्यूआर स्कैन करने और यूपीआई पिन दर्ज करने पर पीड़ित के बैंक खाते से पैसे नामे हो जाते हैं।

सुरक्षा टिप्स:

- हमेशा याद रखें, पैसे प्राप्त करने के लिए यूपीआई पिन की आवश्यकता नहीं होती है।
- अपना यूपीआई पिन किसी के साथ साझा न करें, यहां तक कि अपने दोस्तों और परिवारजनों के साथ भी नहीं।
- किसी भी यूपीआई क्यूआर कोड को स्कैन करने के बाद हमेशा लाभार्थी के विवरण को सत्यापित करें।
- किसी अनजान व्यक्ति द्वारा भेजे गए लिंक पर क्लिक न करें।
- साइबर अपराध की रिपोर्ट करने के लिए **1930 (टोल फ्री)** डायल करें या www.cybercrime.gov.in पर दर्ज करें। साथ ही अपने नजदीकी साइबर अपराध पुलिस स्टेशन में भी रिपोर्ट करें।

UPI Collect Request Scam

UPI Collect Request Scam are carried out by tricking the victim to scan QR codes and entering UPI pin for receiving money.

Information being harvested:

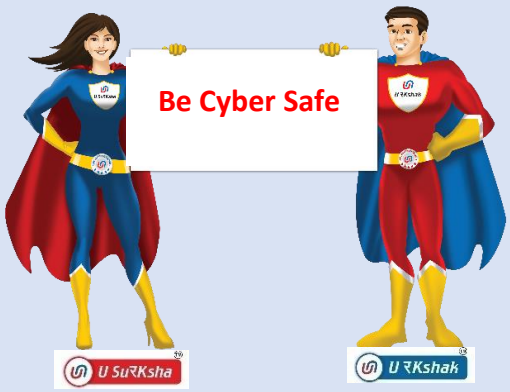
No personal or banking information is harvested in this scam.

Modus Operandi:

- Fraudsters contact victims when they advertise on websites to sell their mobiles, furniture, bikes etc. or to rent their house.
- To gain trust of the victim, fraudster generally sends a small payment in the pretext of testing the correctness of bank account details.
- Then the fraudster sends UPI collect request QR code to the victim & convinces him/her to scan the QR to receive the money.
- On scanning the QR & entering the UPI Pin, Money from the victim's bank account is debited.

Safety Tips:

- Always remember, UPI Pin is not required to receive money.
- Don't share your UPI Pin with anyone, not even with your friends and family.
- Always verify the beneficiary details after scanning any UPI QR code.
- Don't click on link(s) sent by unknown person.
- To report a cyber crime dial 1930 (Toll free) or register on www.cybercrime.gov.in. Also report at your nearest cyber crime police station.



रिमोट एक्सेस ऐप घोटाला

इन घोटालों में पीड़ित को रिमोट एक्सेस ऐप डाउनलोड करने के लिए कहा जाता है फिर दर्ज किए गए विवरणों को कैप्चर करने या पीड़ित के मोबाइल फोन को पूरी तरह से अपने कब्जे में लेने के लिए धोखा दिया जाता है।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- फ़ाइलें
- तस्वीर
- संपर्क विवरण

बैंकिंग जानकारी

- डेबिट/क्रेडिट कार्ड नंबर
- बैंकिंग ऐप्स लॉगिन पिन
- खाता संख्या/आईएफएससी कोड
- लेनदेन ओ.टी.पी.

कार्यप्रणाली:

- धोखेबाज किसी कंपनी के ग्राहक सेवा एजेंट के छद्म रूप में धन-वापसी, कैशबैक दावा, बैंक खाता संक्रियण, डेबिट/क्रेडिट कार्ड संक्रियण, केवाईसी अद्यतन आदि के बहाने पीड़ित को कॉल करते हैं।
- वे पीड़ित को ऐप स्टोर से रिमोट एक्सेस सॉफ्टवेयर डाउनलोड करने के लिए कहते हैं ताकि वे प्रक्रिया पूरी करने में मदद कर सकें।
- एक बार कनेक्ट होने के बाद, धोखेबाज का पीड़ित के मोबाइल पर पूरा नियंत्रण हो जाता है, जिसमें फाइलों तक पहुंचना, प्रोग्राम चलाना, ओटीपी पढ़ना और पैसे निकालना शामिल है।

सुरक्षा टिप्स:

- किसी भी अनजान व्यक्ति के अनुरोध या सलाह पर कभी भी कोई ऐप इन्स्टाल न करें।
- किसी जेन्युइन कंपनी का सेवा एजेंट कभी भी पासवर्ड या पिन जैसी व्यक्तिगत जानकारी का अनुरोध नहीं करेगा। ऐसे किसी भी अनुरोध से हमेशा बचें।
- ऐसी सेवा या तकनीकी सहायता कभी स्वीकार न करें जिसका आपने अनुरोध नहीं किया है।
- किसी भी ऐप को अनुमति देने से पहले हमेशा सतर्क रहें। केवल वही अनुमति दें जो ऐप को काम करने के लिए आवश्यक हों।
- किसी भी घोटाले के प्रयास की सूचना स्थानीय कानून प्रवर्तन और किसी अन्य संबंधित प्राधिकारी को दें।

Remote Access App Scam

These scams are carried out by tricking the victim to download remote access apps and capturing the details entered or completely taking over victim's mobile phone.

Information being harvested:

Personal Information

- Files
- Photos
- Contacts

Banking Information

- Debit/Credit Card No
- Banking Apps Login Pin
- Account Number/IFSC Code
- Transaction OTP

Modus Operandi:

- Fraudsters impersonate customer care of a company & call the victim in the pretext of refund, cashback claim, activation of bank account, Debit/credit card unblocking, KYC updation etc.
- They ask the victim to download a remote access software from app store so that they can help to get the process completed.
- Once connected, the fraudster has complete control over the victim's mobile, including accessing files, running programs, reading OTP and siphon off money.

Safety Tips:

- Never install any application in your phone on request or suggestion of unknown people.
- Service agent of a genuine company will never request personal information like password or pin. Always avoid any such request.
- Never accept service or technical support that you have not requested.
- Always be cautious before giving permission to any app. Only allow permissions which are required for the app to work.
- Report any scam attempts to the local law enforcement and any other relevant authorities.

कूरियर या पार्सल घोटाले

कूरियर घोटाले पुलिस/आरबीआई/नारकोटिक्स विभाग के अधिकारियों का रूप धारण करके किए जाते हैं। फिर पीड़ितों पर संवेदनशील व्यक्तिगत विवरण साझा करने के लिए दबाव डाला जाता है, जिसका उपयोग पैसे हड़पने के लिए किया जाता है।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- पैन
- आधार नंबर
- मतदाता पहचान पत्र

बैंकिंग जानकारी

- बैंक विवरणी
- खाता विवरण
- खाता संख्या

कार्यप्रणाली:

- घोटालेबाज पीड़ित को यह कहते हुए कॉल करते हैं कि पीड़ित के नाम का पार्सल पुलिस/नारकोटिक्स विभाग आदि ने रोक लिया है। फिर पीड़ित को फर्जी अधिकारी से संपर्क कराया जाता है जो पुलिस/नारकोटिक्स विभाग आदि से होने का दावा करता है।
- घोटालेबाज कूरियर के जाली दस्तावेज़ और पुलिस/नारकोटिक्स विभाग आदि के कुछ नकली पहचान प्रमाण साझा करते हैं। ताकि पीड़ित को यह विश्वास दिलाया जा सके कि मामला दर्ज किया जा रहा है।
- घोटालेबाज पीड़ित को कानूनी उलझनों की धमकी देकर पैसे जमा करने के लिए मजबूर करते हैं। एक बार पैसा जमा हो जाने के बाद इसे निकाल लिया जाता है।

सुरक्षा टिप्स:

- कार्रवाई में जल्दबाजी न करें। घोटालेबाज अक्सर पीड़ितों पर जल्दबाजी में निर्णय लेने के लिए दबाव डालने हेतु तात्कालिकता और घबराहट की भावना पैदा करते हैं। कोई भी लेन-देन करने या व्यक्तिगत जानकारी साझा करने से पहले अपना समय लें, जानकारी इकट्ठा करें और विश्वसनीय व्यक्तियों से परामर्श करें।
- कूरियर सेवाओं या कानून प्रवर्तन एजेंसियों से होने का दावा करने वाले अप्रत्याशित कॉल या संदेशों से सावधान रहें।
- आधिकारिक स्रोतों से जानकारी सत्यापित करें। यदि आपको कोई संदिग्ध संचार प्राप्त होता है, तो सीधे कूरियर कंपनी से संपर्क करके जानकारी को व्यक्तिगत रूप से सत्यापित करें।
- व्यक्तिगत विवरण, जैसे कि आपका आधार नंबर, बैंक खाता जानकारी, या कोई अन्य संवेदनशील डेटा, विशेष रूप से फ़ोन पर या अपरिचित वेबसाइटों या लिंक के माध्यम से साझा न करें।

Courier or Parcel Scams

Courier Scams are carried by impersonating Police/RBI/Narcotics department officials. Victims are then pressurized to share sensitive personal details which are then used to siphon off money.

Information being harvested:

Personal Information

- Pan
- Aadhaar Number
- Voter ID

Banking Information

- Bank Statement
- Account Details
- Account Number

Modus Operandi:

- Scammers call the victim saying that a parcel in victim's name has been intercepted by police/narcotics dept. etc. The victim is then connected to fake official who claim to be from police/narcotics dept. etc.
- The scammers share forged documents of the courier and some fake identity proofs of police/narcotics dept. etc. to convince the victim that a case has being booked.
- Scammers threaten the victim of legal implications and force them to deposit money. Once the money is deposited it is siphoned off.

Safety Tips:

- Do not rush into action. Scammers often create a sense of urgency and panic to pressure victims into making hasty decisions. Take your time, gather information, and consult with trusted individuals before making any transactions or sharing personal information.
- Be aware of unexpected calls or messages claiming to be from courier services or law enforcement agencies.
- Verify the information with official sources. If you receive any suspicious communication, independently verify the information by contacting the courier company directly.
- Do not share personal details, such as your Aadhaar number, bank account information, or any other sensitive data, especially over the phone or through unfamiliar websites or links.

लॉटरी घोटाला

घोटालेबाज पीड़ित को यह विश्वास दिलाते हैं कि उन्होंने लॉटरी जीत ली है। फिर पीड़ितों से पुरस्कार राशि का दावा करने के लिए अपना डेटा प्रस्तुत करने के लिए ऐप डाउनलोड करने या लिंक पर क्लिक करने का आग्रह किया जाता है। प्रस्तुत किए गए डेटा का उपयोग पीड़ितों के खाते तक पहुंचने और पैसे निकालने के लिए किया जाता है।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- पूरा नाम
- पैन
- आधार नंबर
- फ़ोन में सेव फ़ाइलें
- पता
- संपर्क

बैंकिंग जानकारी

- खाता संख्या
- आईएफएससी कोड
- क्रेडिट कार्ड नंबर
- समाप्ति तिथि
- सीवीवी
- पिन नंबर

कार्यप्रणाली:

- जालसाज संभावित पीड़ितों को थोक संदेश (Bulk SMS) का उपयोग करके विद्वेशक ऐप का लिंक भेजते हैं।
- पीड़ित लिंक पर क्लिक करता है जिसके परिणामस्वरूप उसके मोबाइल में विद्वेशक ऐप स्थापित हो जाता है।
- इंस्टॉल किए गए एप्लिकेशन का उपयोग खाते तक पहुंचने और पैसे निकालने के लिए किया जाता है।

सुरक्षा टिप्स:

- कभी भी ईमेल/एसएमएस में प्रसारित ऐसे ऑफ़र/छूट का शिकार न बनें जो अत्यधिक लुभावने लगते हैं।
- उचित सत्यापन या प्रमाणीकरण के बिना कभी भी फर्जी संदेश, लिंक, ई-मेल अग्रेषित न करें।
- अपने डिजिटल उपकरणों पर कभी भी अज्ञात लिंक पर क्लिक न करें या अज्ञात सॉफ़्टवेयर डाउनलोड न करें।
- हमेशा आधिकारिक स्टोर/साइट से ऐप्स/सॉफ्टवेयर डाउनलोड करें।

Lottery Scam

Scammers trick the victim to believe that they have won a lottery. Victims are then urged to download apps or click on links to submit their data for claiming the prize money. The data submitted is then used to access victims account and siphon money.

Information being harvested:

Personal Information

- Full Name
- Pan
- Aadhaar Number
- Files in phone
- Address
- Contacts

Banking Information

- Account Number
- IFSC Code
- Credit Card Number
- Expiry Date
- CVV
- PIN Number

Modus Operandi:

- Fraudsters send link of malicious App using bulk SMS to potential victims.
- Victim clicks on the link which result in malicious App getting installed in his/her mobile.
- Application installed is then used to access account and siphon money

Safety Tips:

- Never fall prey to offers/discounts circulated in emails/SMS which are too good to be true.
- Never forward fake messages, links, E-mails without proper verification or authentication.
- Never click on unknown links or download unknown software on your digital devices.
- Always download apps/software from the official stores/sites.

आयकर वापसी (आईटी रिटर्न) धोखाधड़ी

आयकर वापसी (आईटी रिफंड) धोखाधड़ी में पीड़ित को यह विश्वास दिलाया जाता है कि वे भारी आयकर रिफंड प्राप्त करने के पात्र हैं। फिर पीड़ितों से ऐप डाउनलोड करने या लिंक पर क्लिक करने और संवेदनशील डेटा प्रस्तुत करने का आग्रह किया जाता है। प्रस्तुत किए गए डेटा का उपयोग पीड़ितों के खाते तक पहुंचने और पैसे निकालने के लिए किया जाता है।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- पूरा नाम
- पैन
- आधार नंबर

बैंकिंग जानकारी

- खाता संख्या
- आईएफएससी कोड
- क्रेडिट कार्ड नंबर
- समाप्ति तिथि
- सीवीवी
- डेबिट/क्रेडिट कार्ड पिन

कार्यप्रणाली:

- घोटालेबाज करदाता को फ़िशिंग संदेश भेजते हैं, यह दिखावा करते हुए कि वे आयकर विभाग से हैं और कर राशि वापसी की पेशकश करते हैं।
- संदेश में एक लिंक होता है जो करदाता को नकली वेबसाइट पर पुनर्निर्देशित करता है, जहां करदाता को घन-वापसी के लिए बैंक खाते का विवरण अद्यतन करने के लिए कहा जाता है।
- एक बार जब करदाता अपनी बैंकिंग जानकारी दर्ज कर देता है, तो घोटालेबाज अवैध रूप से उस तक पहुंच प्राप्त कर लेते हैं और पैसे निकाल लेते हैं।

सुरक्षा टिप्स:

- किसी भी लिंक पर क्लिक करने से बचें और अपने कर-वापसी की स्थिति जांचने के लिए सीधे आयकर विभाग की आधिकारिक वेबसाइट पर जाएं।
- व्यक्तिगत जानकारी मांगने वाले संदेशों में सावधानी बरतें। यदि कोई संदेश ऐसी जानकारी मांगता है, तो इसे घोटाला मानें।
- यदि आप किसी वेबसाइट की वैधता के बारे में अनिश्चित हैं तो यह सुनिश्चित करने के लिए यूआरएल सत्यापित करें कि यह आधिकारिक साइट से मेल खाता है या नहीं।
- उन सभी कॉल करने वालों पर नज़र रखें जो बातचीत की शुरुआत किसी धमकी या ऐसी किसी चीज़ से करते हैं जो अतिवादी लगती है।
- किसी भी घोटाले के प्रयास की सूचना स्थानीय कानून प्रवर्तन एजेंसी को दें।

IT Return Fraud

IT Refund Fraud are carried out by tricking the victim to believe that are eligible to receive huge income tax refunds. Victims are then urged to download apps or click on links and submit sensitive data. The data submitted is then used to access victims account and siphon money.

Information being harvested:

Personal Information

- Full Name
- Pan
- Aadhaar Number

Banking Information

- Account Number
- IFSC Code
- Credit Card Number
- Expiry Date
- CVV
- Debit/Credit Card Pin

Modus Operandi:

- Scammer send phishing messages to a taxpayer, pretending to be from the Income Tax Department offering tax refunds.
- The message includes a link that redirects the taxpayer to a fake website, where the taxpayer is asked to update details of bank account to get refund.
- Once the taxpayer enters their banking information, scammers illicitly gain access to it and siphon off money.

Safety Tips:

- Avoid clicking any links and directly visit the official Income Tax Department website to check your refund status.
- Exercise caution with messages requesting personal information. If any message demands such information, treat it as a scam.
- Verify the URL to ensure it matches the official site if you are uncertain about a website's legitimacy.
- Hang up on all callers who begin the conversation with a threat or anything that seems extreme.
- Report any scam attempts to the local law enforcement agency.

बिजली बिल धोखाधड़ी

बिजली बिल धोखाधड़ी में पीड़ित को यह विश्वास दिलाया जाता है कि बकाया भुगतान न करने के कारण उनकी बिजली आपूर्ति बंद की जा रही है और उसके समाधान के लिए तत्काल कार्रवाई की आवश्यकता है।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- पूरा नाम
- पैन
- आधार नंबर
- फ़ोन में सेव फ़ाइलें
- पता
- संपर्क

बैंकिंग जानकारी

- खाता संख्या
- आईएफएससी कोड
- क्रेडिट कार्ड नंबर
- डेबिट/क्रेडिट कार्ड पिन
- सीवीवी
- मोबाइल बैंकिंग पिन

कार्यप्रणाली:

- बिजली कंपनी के अधिकारी या ग्राहक सेवा एजेंट के छद्म रूप में धोखेबाज पीड़ित से संपर्क कर सूचित करते हैं कि बकाया राशि का भुगतान न करने के कारण बिजली आपूर्ति रोकी जा रही है और इस हेतु तत्काल निपटान की आवश्यकता है।
- इसके बाद पीड़ित को मोबाइल ऐप डाउनलोड करने/लिंक पर क्लिक करने और जानकारी प्रस्तुत करने या भुगतान करने के लिए बरगलाया जाता है।
- फिर पीड़ित की व्यक्तिगत/बैंकिंग जानकारी हासिल कर ली जाती है और बैंक खाते तक पहुंच बनाई जाती है और पैसे निकाल लिए जाते हैं।

सुरक्षा टिप्स:

- हमेशा सीधे बिजली विभाग/कंपनी से संपर्क करके ऐसे दावों की वास्तविकता की पुष्टि करें।
- असत्यापित स्रोतों से प्राप्त अज्ञात लिंक पर कभी भी क्लिक न करें।
- अनजान कॉल करने वालों के अनुरोध पर कभी भी मोबाइल ऐप डाउनलोड न करें।
- कभी भी मोबाइल नंबर, खाता नंबर, पासवर्ड, ओटीपी, पिन या कोई अन्य गोपनीय जानकारी किसी से साझा न करें।
- रिमोट एक्सेस सुविधा प्रदान करने वाले एप्लिकेशन इंस्टॉल करके कभी भी अपने डिवाइस का एक्सेस किसी को न दें।

Electricity Bill Fraud

Electricity Bill Fraud are carried out by tricking the victim to believe that their power supply is being disconnected due to non-payment of dues and urgent action is required for resolving the same.

Information being harvested:

Personal Information

- Full Name
- Pan
- Aadhaar Number
- Files in phone
- Address
- Contacts

Banking Information

- Account Number
- IFSC Code
- Credit Card Number
- Debit/Credit Card Pin
- CVV
- Mobile Banking Pin

Modus Operandi:

- Scammers impersonating as electricity company official or Customer care agent contact victim informing impending disconnection due to non-payment of dues and urgent need for settlement.
- Victim is then tricked to download mobile app / Click link and submit information or make payment.
- Personal/Banking details of victim is then captured and Bank account is accessed and money is siphoned off.

Safety Tips:

- Always verify the genuineness of such claims by contacting the electricity dept. /company directly.
- Never Click on unknown links received from unverified sources.
- Never download mobile apps on request from unknown callers.
- Never Share mobile number, account number, password, OTP, PIN or any other confidential details to anyone.
- Never give access of your device to anyone by installing applications supporting remote access features.

अवैध ऋण ऐप घोटाला

अवैध ऋण ऐप धोखेबाजों द्वारा मोबाइल ऐप के माध्यम से धोखाधड़ी की जाती है, जिसमें वे पीड़ितों को बिना किसी दस्तावेज के तुरंत बिना प्रतिभूति के ऋण प्राप्त करने का लालच देते हैं।

सूचना संग्रहण:

व्यक्तिगत जानकारी

- पूरा नाम
- पैन
- आधार नंबर
- फ़ोन में सेव फ़ाइलें
- पता
- संपर्क

बैंकिंग जानकारी

- खाता संख्या
- आईएफएससी कोड
- यूपीआई आईडी

कार्यप्रणाली:

- धोखेबाज पीड़ितों को बिना दस्तावेज के तत्काल ऋण देने का लालच देते हैं।
- पीड़ितों से मोबाइल ऐप डाउनलोड करने और ऋण प्राप्त करने के लिए ऐप को सभी अनुमतियां प्रदान करने का आग्रह किया जाता है।
- फिर पीड़ित के फ़ोन में उपलब्ध सभी संपर्क, फ़ोटो, फ़ाइलें जालसाज़ द्वारा एक्सेस कर ली जाती हैं।
- पीड़ित पर अत्यधिक ब्याज और शुल्क लगाया जाता है और फिर रिकवरी एजेंट उपयोगकर्ता को कॉल करते हैं और कॉल सेंटर से संचालन करके उनकी मॉर्फ्ड तस्वीरों का उपयोग करके पैसे वसूलते हैं।
- समाज के डर से उपयोगकर्ता पैसे दे देता है।

सुरक्षा टिप्स:

- ऋण लेने से पहले हमेशा आरबीआई की वेबसाइट से ऋणदाता का लाइसेंस/पंजीकरण जांच लें।
- कभी भी अनापेक्षित ऐप्स डाउनलोड न करें।
- मोबाइल ऐप को अनुमति प्रदान करते समय हमेशा सावधानी बरतें। केवल वही अनुमति दें जो ऐप को काम करने के लिए आवश्यक हो।
- किसी भी धोखाधड़ी के प्रयास की रिपोर्ट स्थानीय कानून प्रवर्तन एजेंसी को करें।

Illegal Loan App Scam

Illegal Loan app Frauds are carried out by fraudsters through mobile apps, wherein they lure victims to receive instant unsecured loans without any documentation.

Information being harvested:

Personal Information

- Full Name
- Pan
- Aadhaar Number
- Files in phone
- Address
- Contacts

Banking Information

- Account Number
- IFSC Code
- UPI ID

Modus Operandi:

- Fraudsters are luring victims with promise of instant loan without documentation.
- Victims are urged to download mobile apps and provide all permissions to the app for availing the loan.
- All contacts, photos, files, of the victim's phone are then accessed by the fraudster.
- Exorbitant interest & charges are levied on the victim and the recovery agents, would then call the user and extort money using their morphed photos by operating from call centres.
- Due to fear of society, the user pays the money.

Safety Tips:

- Always check the license/registration of the lender from RBI website before availing the loan.
- Never download unsolicited apps.
- Always be careful in giving permission to mobile app. Only allow permission that are required for the app to work.
- Report any fraud attempt to the local law enforcement agency.

Follow Cyber Hygiene To Build Robust Cyber Security Culture

मजबूत साइबर सुरक्षा संस्कृति के निर्माण के लिए साइबर स्वच्छता का पालन करें

Never click on unknown link or download any attachment in emails received from unknown sources

Never share your sensitive and confidential informaton with anyone

Always refer Banks official website or Passbook for Customer Care number

Never share your KYCdetails with anyone
Bank never asks such details over phone

यूनियन बैंक ऑफ इंडिया
भारत सरकार का उपक्रम

Union Bank of India
A Government of India Undertaking

CYBERSECURITY CENTRE XCELLENCE
Innovate. Digitize. Excel. Automate.

VYOM

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