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 IV

Cyber Security
Customer Awareness Guide – Vol. IV

MINISTRY OF HOME AFFAIRS
Indian Cyber Crime Coordination Centre

आधुनिक टेक्नोलॉजी के इस्तेमाल के कारण साइबर सुरक्षा
वर्तमान जीवन का अभिन्न अंग बन गया है

साइबर स्वच्छ प्रथाओं का पालन करें
और साइबर क्राइम से बचें

ऑनलाइन वित्तीय धोखाधड़ी
की रिपोर्ट करने के लिए
1930
पर कॉल करें

cybercrime.gov.in
पर अपनी शिकायत दर्ज करें

चक्षु – Report Suspected Fraud Communication
(Received Through Call/SMS/WhatsApp)

(Report any suspected fraud communication received within last 30 days)

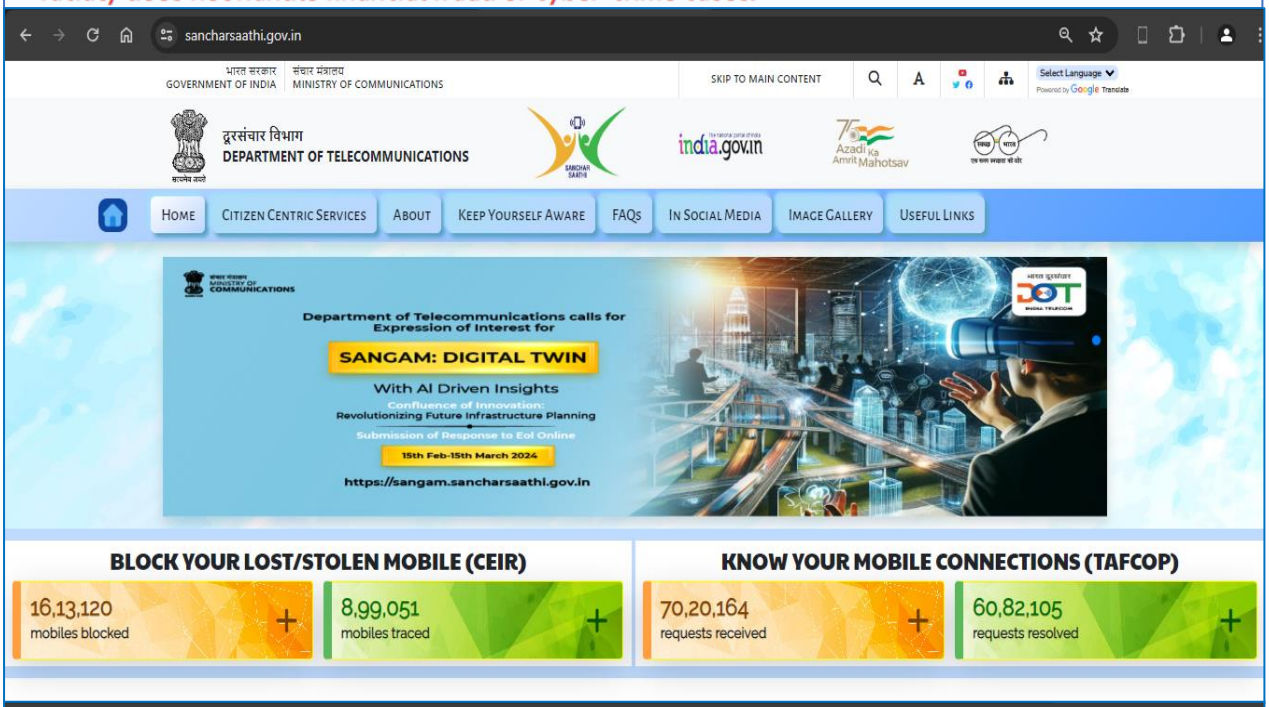
https://www.sancharsaathi.gov.in/sfc/

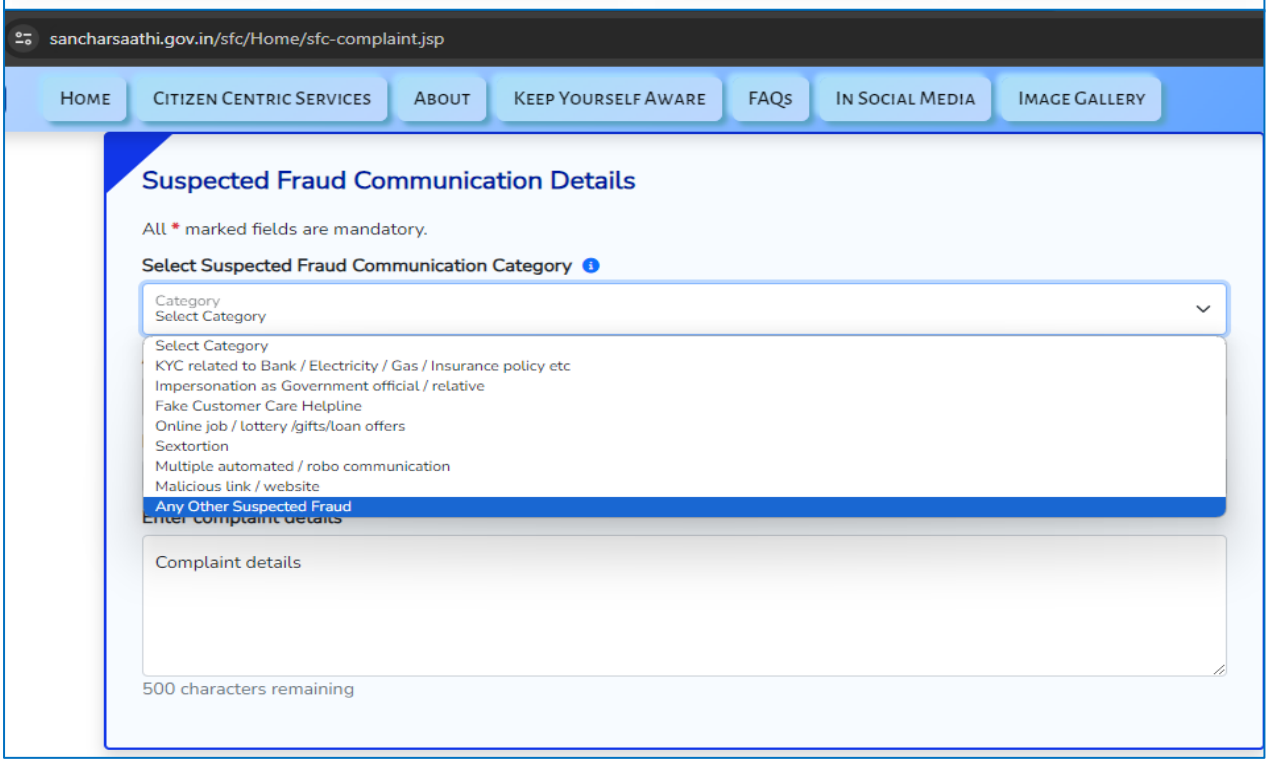
Chakshu

Chakshu facilitates citizens to report the suspected fraud communications with the intention of defrauding telecom service users for cyber-crime, financial frauds, non-bonafide purpose like impersonation or any other misuse through Call, SMS or WhatsApp.

Few examples of suspected fraud communications are communication related to Bank Account / Payment Wallet / SIM / Gas connection / Electricity connection / KYC update / expiry / deactivation, impersonation as Government official / relative, sextortion related etc.

Note: If you have already lost money due to financial fraud or are a victim of cyber-crime, please report at cyber crime helpline number 1930 or website https://www.cybercrime.gov.in. Chakshu facility does not handle financial fraud or cyber-crime cases.





Message From:

A. Manimekhalai
Managing Director & CEO

प्रिय ग्राहको,

वर्तमान समय में डिजिटल प्रगति बैंकिंग और वित्तीय सेवाओं को सरल बना रही है, और इसके साथ ही कई तरह की चुनौतियाँ और जोखिम भी सामने आ रहे हैं, जिनसे सतर्क रहना और पहले से ही सजग रहना आवश्यक है। यूनियन बैंक ऑफ इंडिया आपके वित्तीय सुरक्षा को सुनिश्चित करने के प्रति पूर्णतः प्रतिबद्ध है।

यह "साइबर सुरक्षा ग्राहक जागरूकता मार्गदर्शिका" आपको नवीनतम साइबर खतरों को पहचानने और अपने खाते को सुरक्षित रखने के सर्वोत्तम उपाय अपनाने में अवश्य सहायक सिद्ध होगी। आज के दौर में धोखेबाज़ लोग नए और परिष्कृत तरीकों का उपयोग कर रहे हैं, इसलिए सतर्क रहना और संभावित खतरों की समय रहते पहचान करना अत्यंत आवश्यक है। साइबर सुरक्षा एक सामूहिक ज़िम्मेदारी है, और हम आपसे अनुरोध करते हैं कि साइबर धोखाधड़ी के खिलाफ सतर्क रहें और जानकार बनें।

आपकी सुरक्षा हमारी सर्वोच्च प्राथमिकता है। हम आपको सुरक्षित बैंकिंग सेवाएँ प्रदान करने के साथ-साथ साइबर सुरक्षा संबंधी जागरूकता को निरंतर बढ़ाने के लिए भी प्रतिबद्ध हैं। यह मार्गदर्शिका हमारे ग्राहकों को सतर्क और सुरक्षित रखने की हमारी सतत पहल का एक अभिन्न अंग है। यदि हम सतर्क, जागरूक और सजग रहेंगे, तो हम सभी के लिए एक सुरक्षित एवं अभेद्य डिजिटल वातावरण बना सकते हैं।

यूनियन बैंक ऑफ इंडिया में आपके निरंतर विश्वास के लिए धन्यवाद। हम आपको उच्चतम स्तर की सुरक्षा और सहायता प्रदान करने के लिए सदैव प्रतिबद्ध हैं।

डिजिटल रहें, सुरक्षित रहें!

Dear Valued Customers,

As digital advancements continue to simplify banking and financial services, they also introduce new risks that require vigilance and proactive measures. At Union Bank of India, we are committed to ensuring your safety in this evolving landscape.

This Customer Awareness Guide on Cyber Security is designed to help you recognize the latest threats and adopt best practices to safeguard your accounts. Fraudulent tactics are becoming increasingly sophisticated, making it essential to stay informed and recognize potential risks before they strike. Cyber security is a shared responsibility, and we urge you to remain updated and vigilant against cyber fraud.

Your safety remains our top priority. We are dedicated to providing secure banking services while empowering you with the knowledge to protect yourself. This magazine is part of our ongoing commitment to keeping our customers informed and safe. By staying proactive, informed, and vigilant, we can work together to create a safer digital ecosystem for all.

Thank you for your continued trust in Union Bank of India. We remain committed to providing you with the highest level of security and support.

Stay Digital, Stay Safe!

Message From:

Pankaj Dwivedi
Executive Director,

प्रिय ग्राहको,

सभी को मेरा हार्दिक नमस्कार। आशा करता हूं कि आप कुशलता से होंगे, हम आपके स्वस्थ और खुशहाल जीवन की कामना करते हैं।

आज की डिजिटल दुनिया में, ऑनलाइन गतिविधियों से जुड़ी जोखिम लगातार बढ़ रहे हैं, और संभावित खतरों से आगे रहना महत्वपूर्ण है। यूनियन बैंक ऑफ इंडिया में, हम आपको इन चुनौतियों से आत्मविश्वास के साथ निपटने में सहायता करने के लिए आवश्यक उपाय और जानकारी प्रदान करके आपकी सुरक्षा सुनिश्चित करने हेतु प्रतिबद्ध हैं। यह गाइड आपको कुछ नवीनतम धोखाधड़ी रणनीतियों के बारे में सूचित करने और इन जोखिमों को कम करने के लिए प्रभावी सुरक्षा उपाय प्रदान करने हेतु सावधानीपूर्वक तैयार किया गया है।

जैसे-जैसे तकनीक उन्नति करती है, धोखेबाज अपने नये नये तरीकों को बदलना जारी रखते हैं, जिससे आपके लिए सतर्क रहना और भी महत्वपूर्ण हो जाता है। इस गाइड में, आपको अपनी व्यक्तिगत और वित्तीय जानकारी की सुरक्षा के लिए व्यावहारिक सलाह प्राप्त होगी, जिसमें संदिग्ध गतिविधि की पहचान करने और अपने खातों की सुरक्षा करने के उपाय शामिल हैं। इस गाइड में बताए गए उपायों को लागू करके, आप ऑनलाइन धोखाधड़ी का शिकार होने के जोखिम को काफी कम कर सकते हैं।

हम आशा करते हैं कि यह गाइड आपको एक विश्वसनीय और सुरक्षित ऑनलाइन अनुभव बनाए रखने में सहायता करने हेतु एक बहुमूल्य संसाधन साबित होगा।

बहुत बहुत शुभकामनाएँ!

Dear Valued Customers,

My greetings to all. I hope this message finds you well and in good spirits.

In today's digital world, the risks associated with online activities are constantly evolving, and it is crucial to stay ahead of potential threats. At Union Bank of India, we are committed in ensuring your safety by providing the necessary tools and knowledge to help you navigate these challenges with confidence. This guide has been carefully crafted to inform you about the some of the latest fraudulent tactics and to provide effective safety tips to mitigate these risks.

As technology advances, fraudsters continue to adapt their newer methods, making it even more important for you to stay vigilant. In this guide, you will find practical advices to protect your personal and financial information, including steps to identify suspicious activity and safeguard your accounts. By applying the tips outlined in this guide, you can significantly reduce risk of falling victim to online scams.

We hope this guide will serve as a valuable resource in helping you maintain a safe and secure online experience.

All the very best!

Message From:

Tajvinder Kaur
Chief Information Security Officer

प्रिय ग्राहको,

यूनियन बैंक ऑफ इंडिया में, हम मानते हैं कि तकनीकी उन्नति की तीव्र गति कई अवसर उपलब्ध कराती है, किंतु इसके साथ ही कुछ जोखिम भी आती है। संभावित खतरों के संकेतों की पहचान करना और निवारक उपाय अपनाने से ऑनलाइन धोखाधड़ी के खतरों को काफी हद तक कम किया जा सकता है।

तदनुसार, बैंक अपने ग्राहकों/हितधारकों को बाजार में प्रचलित साइबर घटनाओं से अवगत रखने हेतु नियमित आधार पर जागरूकता बिट्स साझा कर रहा है। सभी की सुविधा के लिए यूनियन बैंक ऑफ इंडिया की वेबसाइट unionbankofindia.bank.in/en/common/cyber-security) पर जागरूकता सुरक्षा उपायों को उपलब्ध कराया गया है।

यह मार्गदर्शिका धोखाधड़ी के संचालन के तरीकों सहित, नवीनतम धोखाधड़ी के संबंध में जानकारी में वृद्धि करने के लिए डिज़ाइन की गई है, और हमारे पाठकों के व्यक्तिगत और वित्तीय जानकारी की सुरक्षा में सहायता करने के लिए महत्वपूर्ण सुरक्षा उपायों की जानकारी प्रदान करती है। इस पुस्तिका में उल्लिखित धोखाधड़ी के विभिन्न तौर-तरीके उदाहरण के रूप में दिए गए हैं, और सुविस्तृत नहीं हैं।

इस गाइड के नवीनतम संस्करण में, डिजिटल गिरफ्तारी, फर्जी एपीके, व्हाट्सएप हाइजैकिंग आदि जैसे कुछ नवीनतम धोखाधड़ी की पहचान करने और इस हेतु निवारक उपाय करने में आपकी सहायता करने के लिए हमने आवश्यक जानकारी का संकलन किया है।

मैं सभी पाठकों को यूनियन बैंक ऑफ इंडिया की वेबसाइट पर उपलब्ध इन पुस्तिकाओं सहित विभिन्न स्रोतों से प्राप्त जानकारी का प्रयोग करने और अपने डिजिटल लेनदेन के हर पहलू में सीख को अपनाने के लिए प्रोत्साहित करती हूँ।

Dear Valued Customers,

At Union Bank of India, we recognize that the rapid pace of technological advancement brings opportunities, but it also comes with certain risks. Recognizing the signs of potential threats and adopting preventive measures can significantly reduce susceptibility to online frauds.

Accordingly, Bank is sharing awareness bits on regular basis to keep our customers/stakeholders abreast of the cyber incidents prevalent in the market. Awareness safety tips are made available in Union Bank of India website (www.unionbankofindia.bank.in/en/common/cyber-security) for convenience of all.

This guide is designed to enhance the knowledge of our readers about the latest scams, including their methods of operation, and offers key safety tips to help protect personal and financial information. The modus operandi of the various frauds outlined in this booklet are intended to serve as illustrative examples, and are not exhaustive.

In the latest edition of this guide, we've compiled essential information to help you identify some of the latest frauds such as Digital Arrest, Fake APK, and WhatsApp Hijacking etc. and take preventive measures.

I encourage all readers to apply the insights gained from various sources including these booklets available in Union Bank of India website and adopt the learnings into every aspect of their digital transactions. I urge upon all our esteemed stakeholders to remain vigilant and stay safe by adopting smart cyber security practices.

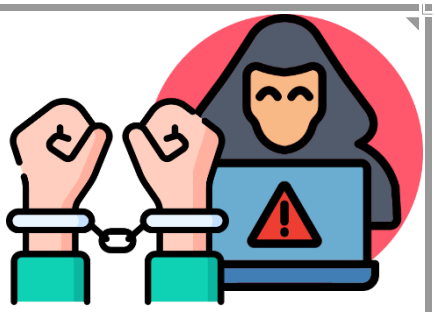
Page Index

"Training today, security forever"

अनुक्रमणिका

"वर्तमान प्रशिक्षित, भविष्य सुरक्षित"

Digital Arrest Fraud



Modus Operandi:

The victims receive calls, email or message claiming they are under investigation as their name or mobile number has been found to be connected with criminal activities like pornography, drug trafficking, or money laundering. The scammer threatens the victim with arrest or legal consequences unless they take immediate action.

The victim is then instructed to call a specific number urgently to avoid a 'digital arrest.' Once the victim calls the provided number, fraudsters impersonate officials from law enforcement agencies such as Police, CBI, Narcotics Control Bureau or Customs. They wear official looking uniforms similar to these law enforcement agencies and set up backgrounds with flags, logos, and make the experience highly convincing.

Scammers then make the victim to stay on the video call in pretext of 'monitoring' and force them to transfer large sums of money in to specified accounts.

Safety Tips:

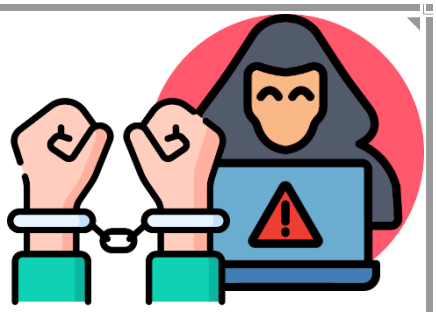
- Avoid sharing your personal information with unknown people on social media.
- Never accept to join any video call requests received from strangers for any investigation or arrest.
- Never make any payment to strangers claiming to be from investigating agencies.
- If you receive any calls about arrest or investigation visit the nearest police station.
- Always remember, no Govt. investigating agency will interrogate or arrest you on online calls/Skype.

#SabkoBataoo

#CyberSurakshitBharat

#SatarkNagrik

डिजिटल गिरफ्तारी धोखाधड़ी



कार्यप्रणाली:

पीड़ितों को कई बार ऐसे फोन कॉल, ईमेल या संदेश प्राप्त होते हैं जो यह दावा करते हैं कि उनका नाम या मोबाइल नंबर पोर्नोग्राफी, मादक पदार्थों की तस्करी या धन-शोधन (मनी लॉन्ड्रिंग) जैसी आपराधिक गतिविधियों से संबन्धित होने के कारण वे जांच के अधीन हैं। पीड़ित व्यक्ति के डर का फायदा उठाते हुए धोखेबाज़ पीड़ित को गिरफ्तारी या कानूनी परिणामों की धमकी देता है, जब तक कि वे तत्काल कार्रवाई नहीं करते।

धोखेबाज़ फिर पीड़ित को 'डिजिटल गिरफ्तारी' से बचने के लिए तत्काल एक विशिष्ट नंबर पर कॉल करने का निर्देश देता है। जब पीड़ित दिए गए नंबर पर कॉल करता है, तो धोखेबाज पुलिस, सीबीआई, नारकोटिक्स कंट्रोल ब्यूरो या सीमा शुल्क जैसी विधि प्रवर्तन एजेंसियों के अधिकारियों का प्रतिरूपण करते हैं। वे वीडियो कॉल पर विधि प्रवर्तन एजेंसियों के अधिकारियों के समान वर्दी पहने हुए और झंडे, चिन्ह (लोगो) के साथ व्यवस्थित पृष्ठभूमि बनाकर बैठते हैं, और इस प्रकार वे पीड़ितों के अनुभव को अत्यधिक वास्तविक बनाते हैं।

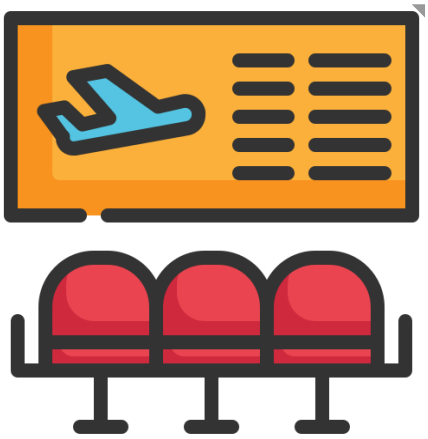
माहौल को और अधिक वास्तविक बनाने के लिए धोखेबाज़ पीड़ित पर 'निगरानी' रखने के बहाने वीडियो कॉल पर बने रहने की मांग करते हैं और उनके नाम को समाज में ख़राब होने से बचाने के नाम पर निर्दिष्ट खातों में बड़ी रकम स्थानांतरित करने के लिए उन्हें मजबूर करते हैं।

सुरक्षा युक्तियाँ:

- सोशल मीडिया पर अनजान लोगों के साथ अपनी निजी जानकारी साझा करने से बचें।
- अंजान व्यक्तियों द्वारा किसी भी प्रकार की जांच या गिरफ्तारी से संबंधित वीडियो कॉल ज्वाइन करने के अनुरोध को कभी भी स्वीकार न करें।
- यहां तक कि अगर आप इस तरह के कॉल में अपने प्रियजनों की आवाज सुनते हैं, तो उन्हें व्यक्तिगत रूप से कॉल करें और उनके ठिकाने की जांच करें।
- जांच एजेंसियों से होने का दावा करने वाले अजनबियों को कभी भी, किसी भी तरह का भुगतान न करें।
- यदि आपको गिरफ्तारी या जांच के बारे में कोई कॉल आती है, तो निकटतम पुलिस स्टेशन पर जाएं।
- हमेशा याद रखें, कोई भी सरकारी जांच एजेंसी ऑनलाइन कॉल / स्काइप पर आपसे पूछताछ या आपको गिरफ्तार नहीं करेगी।

#सबकोबताओ
#साइबरसुरक्षितभारत
#सतर्कनागरिक

Fake Airport Lounge Pass App/APK Fraud



Modus Operandi:

Scammers in the name of assisting air travellers for lounge access circulate fake lounge pass App/APK through WhatsApp at airports directing users to malicious domains such as loungepass.in, loungepass.info, loungepass.online which are linked to scam.

Victims are tricked into downloading the app, which request for access to SMS permissions during installation. Once installed scammers intercept victim's sensitive text messages such as OTP which enable them to steal money.

As these apps are not available on official app stores, it makes the take down of these malicious apps difficult.

Safety Tips:

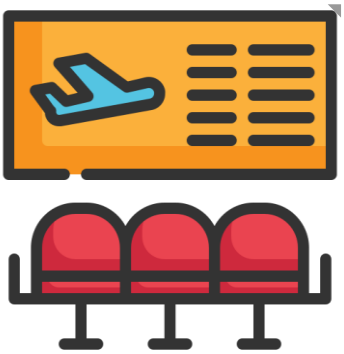
- Never install Apps from links, websites or APKs received through message or WhatsApp.
- Always download apps from authorized app stores only (Google Play store for Android & Apple App store for Apple devices).
- Enable Two-Factor Authentication (2FA) wherever possible to add an extra layer of security to your accounts.

#SabkoBataoo

#CyberSurakshitBharat

#SatarkNagrik

फ़र्जी एयरपोर्ट लाउंज पास ऐप/एपीके धोखाधड़ी



कार्यप्रणाली:

लाउंज एक्सेस के लिए हवाई यात्रियों की सहायता करने के नाम पर धोखेबाज़ हवाई अड्डों पर व्हाट्सएप के माध्यम से नकली लाउंज पास ऐप/एपीके प्रसारित करते हैं, जो उपयोगकर्ताओं को loungepass.in, loungepass.info, loungepass.online जैसे दुर्भावनापूर्ण डोमेन पर निर्देशित करते हैं जो घोटालों से जुड़े होते हैं।

पीड़ितों को ऐप डाउनलोड करने के लिए झांसा दिया जाता है, जिसके बाद एसएमएस अनुमतियां भी प्राप्त कर लिया जाता है। नकली ऐप / .एपीके फाइल के माध्यम से धोखेबाज़ पीड़ित के संवेदनशील टेक्स्ट संदेशों जैसे ओटीपी को प्राप्त करते हैं जो उन्हें पैसे चुराने में सक्षम बनाते हैं।

चूंकि ये ऐप आधिकारिक ऐप स्टोर पर उपलब्ध नहीं होते हैं, इसलिए इन दुर्भावनापूर्ण ऐप्स को हटाना या डिलीट करना मुश्किल होता है।

सुरक्षा युक्तियाँ:

- कभी भी लिंक, वेबसाइट या मैसेज अथवा व्हाट्सएप के माध्यम से प्राप्त एपीके से ऐप्स इंस्टॉल न करें।
- हमेशा केवल अधिकृत ऐप स्टोर से ऐप डाउनलोड करें (एंड्रॉइड के लिए गूगल प्ले स्टोर और ऐप्पल डिवाइस के लिए ऐप्पल ऐप स्टोर का प्रयोग करें)।
- अपने खातों की सुरक्षा को सुदृढ़ करने हेतु यथासंभव टू-फैक्टर ऑथेंटिकेशन (2FA) का प्रयोग करें।

#सबकोबताओ
#साइबरसुरक्षितभारत
#सतर्कनागरिक

Reward Point Redemption Fraud

Modus Operandi:

Scammers send fake text SMS/Email messages to the victims urging them to click on the link to redeem loyalty/reward points before they expire. The group icons and senders names in the messages is changed by scammers to make them appear legitimate. These messages claim that the victim's reward points are about to lapse, creating a sense of urgency.

When the victim clicks on the link, they are prompted to download an APK file, which is disguised as an official application or update related to reward points. By downloading and installing these files, the victim unknowingly installs malware on their device. These malwares then steal sensitive financial information including banking credentials, passwords, and OTPs and help scammers siphon off money from victim's account.

Fake Message

Dear Customer
Your ,I Net-Banking
reward point INR 9987 Due to
Expire Today Immediately Self
Redeem your Cash deposited now
https://t.ly/ceINn

Safety Tips:

- Never click on links received from unknown sources without verifying their source.
- Regularly change and keep a strong, unique bank account password.
- Never share your personal information with unknown people over phone, SMS or through any website if you are not sure about it.
- Always activate two-step verification on your social media & bank accounts. This adds an extra layer of security. 2FA requires a PIN in addition to the OTP sent to the phone for verification.

#SabkoBataoo
#CyberSurakshitBharat
#SatarkNagrik

रिवॉर्ड पॉइंट रिडेम्पशन धोखाधड़ी

कार्यप्रणाली:

धोखेबाज़ पीड़ित को फर्जी टेक्स्ट एसएमएस/ईमेल संदेश भेजते हैं जिसमें पीड़ितों से आग्रह किया जाता है कि वे लॉयल्टी/रिवॉर्ड पॉइंट का लाभ उठाने के लिए लिंक पर क्लिक करें। धोखेबाज़ों द्वारा समूह चिन्ह एवं संदेश भेजने वाले का नाम बदल दिया जाता है ताकि वो पीड़ित को वैध प्रतीत हो। इस प्रकार के संदेशों में तात्कालिकता की भावना पैदा करने के लिए यह दावा किया जाता है कि पीड़ित के रिवॉर्ड पॉइंट की वैध तिथि समाप्त होने वाली है।

जब पीड़ित लिंक पर क्लिक करता है, तो उन्हें एक एपीके फ़ाइल डाउनलोड करने के लिए निर्देशित किया जाता है, जो आधिकारिक एप्लिकेशन या रिवॉर्ड पॉइंट से संबंधित अपडेट के रूप में छिपी होती है। इस फाइल को डाउनलोड और इंस्टॉल करके पीड़ित अनजाने में अपने डिवाइस में मालवेयर इंस्टॉल कर लेता है। और यह मैलवेयर बैंकिंग क्रेडेंशियल, पासवर्ड और ओटीपी सहित संवेदनशील वित्तीय जानकारी को चुराता है और इस तरह धोखेबाज़, पीड़ित की मेहनत की कमाई और जमा पूंजी को निकाल लेता है।

नकली संदेश

Dear Customer
Your ,I Net-Banking
reward point INR 9987 Due to
Expire Today Immediately Self
Redeem your Cash deposited now
https://t.ly/celNn

सुरक्षा युक्तियाँ:

- अज्ञात स्रोतों से प्राप्त लिंक के स्रोत को सत्यापित किए बिना कभी भी उन पर क्लिक न करें।
- नियमित रूप से पासवर्ड बदलें और एक मजबूत व अलग पासवर्ड बनाए।
- यदि आप किसी फोन कॉल, एसएमएस या वेबसाइट पर बताए गए, लिखे गए अथवा दिखाए गए विषयवस्तु के बारे में नहीं जानते हैं तो कभी भी अपनी व्यक्तिगत जानकारी साझा न करें।
- हमेशा अपने सोशल मीडिया और बैंक खातों पर टू-फ़ैक्टर आथेंटीकेशन प्रक्रिया को सक्रिय रखें। यह आपकी सुरक्षा को अधिक मजबूत और सुदृढ़ बनाता है। टू-फ़ैक्टर आथेंटीकेशन में सत्यापन के लिए फोन पर भेजे गए ओटीपी के अलावा एक पिन की भी आवश्यकता होती है।

#सबकोबताओ
#साइबरसुरक्षितभारत
#सतर्कनागरिक

WhatsApp Hijacking Fraud

Modus Operandi:

WhatsApp hijacking refers to unauthorized access to a person's WhatsApp account, often through methods like SIM swapping, phishing or malware. Once someone hijacks an account, they can read messages, send texts & access personal information. This creates a privacy & security concern as it can lead to identity theft or other malicious activities.

Scammers call victim from unknown numbers pretending to be from WhatsApp for account verification asking the victim to verify personal information. Simultaneously the scammer starts WhatsApp registration process for the same mobile number.

Call based account activation option is selected by the scammer and the victim is asked to merge the call for some security reason. As soon as the victim merges the call which is a verification call from WhatsApp for OTP, the fraudster enters the OTP and activates the account and the victim gets logged off from WhatsApp.

Safety Tips:

- Be cautious while receiving calls from unknown number, in case of suspicious behaviour such as call merger, adding other people in call, hang up immediately for your safety.
- Always set up 2 factor authentication in your WhatsApp.
- Never share OTP, PIN, CVV, Password or any other confidential details with anyone.
- Never give access of your device to anyone by installing applications supporting remote access features.
- Turn off auto download feature in WhatsApp.

#SabkoBataoo

#CyberSurakshitBharat

#SatarkNagrik

व्हाट्सएप हाईजैक धोखाधड़ी

कार्यप्रणाली:

व्हाट्सएप हाईजैकिंग से तात्पर्य किसी व्यक्ति के व्हाट्सएप अकाउंट तक अनाधिकृत पहुंच से है, अक्सर सिम स्वैपिंग, फ़िशिंग या मैलवेयर जैसे तरीकों के माध्यम से इसे अंजाम दिया जाता है। एक बार जब कोई व्यक्ति किसी व्हाट्सएप अकाउंट को हाईजैक कर लेता है, तो वे संदेश पढ़ सकते हैं, एसएमएस भेज सकते हैं और व्यक्तिगत जानकारी तक भी पहुंच सकते हैं। यह व्यक्ति की निजी जानकारी और सुरक्षा के सन्दर्भ में गंभीर चिंता का विषय बन जाता है क्योंकि इसके द्वारा प्रतिरूपण, पहचान की चोरी या अन्य दुर्भावनापूर्ण गतिविधियों को अंजाम दिया जा सकता है।

धोखेबाज़ अज्ञात नंबरों से पीड़ित को खाता सत्यापन के लिए कॉल करता है और व्हाट्सएप से होने का दावा करते हुए पीड़ित को अपनी व्यक्तिगत जानकारी सत्यापित करने के लिए कहता है। इसी के समानांतर धोखेबाज़ उसी मोबाइल नंबर के लिए व्हाट्सएप पंजीकरण प्रक्रिया शुरू कर देता है।

धोखेबाज़, कॉल आधारित व्हाट्सएप अकाउंट सक्रिय करने के विकल्प को चुनता है और पीड़ित को कुछ सुरक्षा कारणों से कॉल को मर्ज करने के लिए निर्देशित करता है। ओटीपी के लिए व्हाट्सएप से किए हुए सत्यापन कॉल को पीड़ित जैसे ही पीड़ित कॉल को मर्ज करता है, तुरंत जालसाज की पहुँच ओटीपी तक हो जाती है और धोखेबाज़ द्वारा व्हाट्सएप अकाउंट को सक्रिय कर लिया जाता है जिसके परिणाम स्वरूप पीड़ित अपने व्हाट्सएप से लॉग ऑफ हो जाता है।

सुरक्षा युक्तियाँ:

- अनजान नंबर से कॉल का उत्तर देते समय सतर्क रहें। संदिग्द्ध गतिविधियों जैसे कॉल मर्जर या कॉल में अन्य लोगों को जोड़ने की स्थिति में अपनी सुरक्षा को ध्यान में रखते हुए फोन कॉल को तुरंत रख दें या कॉल डिसकनेक्ट करे दें।
- अपने व्हाट्सएप में हमेशा 2 फैक्टर ऑथेंटिकेशन सेट करें।
- कभी भी ओटीपी, पिन, सीवीवी, पासवर्ड या कोई अन्य गोपनीय विवरण किसी के साथ साझा न करें।
- रिमोट एक्सेस सुविधाओं का समर्थन करने वाले एप्लिकेशन इंस्टॉल करके कभी भी अपने डिवाइस का एक्सेस किसी को भी न दें।
- व्हाट्सएप में ऑटो डाउनलोड फीचर को बंद रखें।

#सबकोबताओ
#साइबरसुरक्षितभारत
#सतर्कनागरिक

Credit Card Application Fraud

Modus Operandi:

Scammers lure victims to apply for a free credit card without any charges and higher spent limits on social media messaging platforms and also through unsolicited SMS.

Victims are tricked to click on links received through SMS or WhatsApp messages from unsolicited mobile number or email to apply for a free credit card. The group icons and senders names in the messages are changed by the scammers to make them appear legitimate. Once the link is clicked, the victim is asked to apply for a life time free credit card by filling out sensitive personal information or by downloading APK which are then used by the scammer to read all messages and OTP on victim's phone and to siphon off money.

Check Your EMI Card- 7mq5.com

G00D NEWS 94391xxxxx, Your EMI card XXXX9953 Can be Appr0ved. CHECK N0W- 7ky1.com/bel01nxlnm

Fake Messages

Safety Tips:

- Beware of unsolicited SMS & WhatsApp messages as scammers often mimic numbers of trusted sources. Always verify the sender's authenticity before responding or clicking any links
- For applying any credit card always visit bank's official website/Branch.
- Never share your OTP, PIN or any sensitive financial information with anyone.
- Scam text messages often create a sense of greed & urgency, prompting immediate action. Never fall for it. Always go through the official channels.

#SabkoBataoo

#CyberSurakshitBharat

#SatarkNagrik

क्रेडिट कार्ड आवेदन धोखाधड़ी

कार्यप्रणाली:

धोखेबाज़ पीड़ितों को सोशल मीडिया मैसेजिंग प्लेटफॉर्म पर और अवांछित एसएमएस के माध्यम से अधिक खर्च-सीमा वाले एवं निःशुल्क क्रेडिट कार्ड के लिए आवेदन करने का लालच देते हैं।

धोखेबाज़ों द्वारा पीड़ितों को मुफ्त क्रेडिट कार्ड हेतु आवेदन करने के लिए अवांछित मोबाइल नंबर या ईमेल से, एसएमएस या व्हाट्सएप संदेशों के माध्यम से प्राप्त लिंक पर क्लिक करने के लिए झांसा दिया जाता है। धोखेबाज़ों द्वारा समूह चिन्ह एवं संदेश भेजने वाले का नाम बादल दिया जाता है ताकि वो पीड़ित को वैध प्रतीत हो। एक बार लिंक पर क्लिक करने के बाद, पीड़ित को संवेदनशील व्यक्तिगत जानकारी भरने या किसी भी एपीके को डाउनलोड करके आजीवन मुफ्त क्रेडिट कार्ड के लिए आवेदन करने के लिए कहा जाता है, जिसका उपयोग धोखेबाज़ द्वारा पीड़ित के फोन पर सभी संदेशों और ओटीपी को पढ़ने और पैसे निकालने के लिए किया जाता है।

Check Your EMI Card- 7mq5.com

G00D NEWS 94391xxxxx, Your EMI card XXXX9953 Can be Appr0ved. CHECK N0W- 7ky1.com/bel01nxlnm

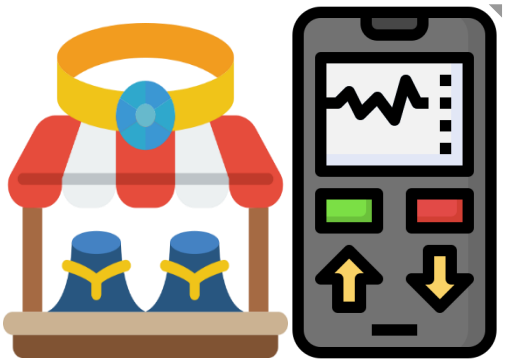
नकली संदेश

सुरक्षा युक्तियाँ:

- अवांछित एसएमएस और व्हाट्सएप संदेशों से सावधान रहें क्योंकि धोखेबाज़ अक्सर विश्वसनीय स्रोतों के नंबरों की नकल करते हैं। किसी भी लिंक पर क्लिक करने से पहले हमेशा प्रेषक की प्रामाणिकता को सत्यापित करें।
- किसी भी क्रेडिट कार्ड हेतु आवेदन करने के लिए हमेशा बैंक की आधिकारिक वेबसाइट / शाखा पर जाएं।
- कभी भी अपना ओटीपी, पिन या किसी भी तरह की संवेदनशील वित्तीय जानकारी किसी के साथ साझा न करें।
- धोखाधड़ी युक्त संदेश अक्सर लालच एवं तात्कालिकता की भावना पैदा करते हैं और तत्काल कार्रवाई को प्रेरित करते हैं। इनके जाल में कभी भी न फसें। हमेशा आधिकारिक चैनलों का प्रयोग करें।

#सबकोबताओ
#साइबरसुरक्षितभारत
#सतर्कनागरिक

Forex & Jewellery Investment Fraud



Modus Operandi:

Fraudsters are increasingly targeting unsuspecting investors with **Fake Forex Trading** and **Jewellery Investment App**s promising high returns.

The scammer contact victims through WhatsApp, SMS & Telegram channel. They lure victims with high return on investments in forex apps and show fake profit screen shots. Once the unsuspecting victim makes an investment, the app shows high returns on investment, but when the victim attempts to withdraw funds, the app asks to pay additional amount for tax purposes and doesn't allow withdrawal. Once bigger investment is done, the victim is blocked by the scammer and the money is siphoned off.

Similarly in case of Jewellery scam, the scammer lure the victims with daily return on investment app. The profits are also credited in the victim's account for initial few days. Eventually, when high value investment is done by the victim, payments are stopped immediately by the scammer, resulting in a total loss for victim.

Gold price is soaring! Earn Rs. 19,500 today with smart investment moves. Stay ahead with daily updates. https://dub.sh/BfPZk6	Rs 10,300 profit booked today from forex trading. Stay informed with real-time insights. https://dub.sh/hTsym5	Group profit this month Rs 33,800, join for daily analysis. https://goo.su/U3DZrF

Fake Messages

Safety Tips:

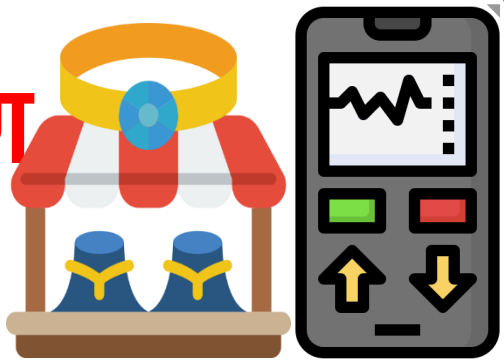
- Always verify the credibility of any trading or investment app before engaging.
- Always check RBI alert list of unauthorized forex trading platforms/apps.
- Never disclose personal financial details to unknown individuals. Always exercise caution while engaging with people online.
- Always be skeptical of investments promising high returns and low risk. Mostly these are scams.

#SabkoBataoo

#CyberSurakshitBharat

#SatarkNagrik

विदेशी मुद्रा व आभूषण निवेश धोखाधड़ी



कार्यप्रणाली:

धोखेबाज **नकली विदेशी मुद्रा व्यापार और आभूषण निवेश एप्प** पर उच्च प्रतिलाभ (हाई रिटर्न) को दिखाकर, फर्जीवाड़े से अनजान निवेशकों को तेजी से लक्षित कर रहे हैं।

धोखेबाज व्हाट्सएप, एसएमएस और टेलीग्राम चैनल के द्वारा पीड़ितों से संपर्क करता है। वे विदेशी मुद्रा ऐप्स में निवेश पर उच्च रिटर्न का दावा करके और फर्जी लाभ से संबंधित स्क्रीन शॉट दिखाकर पीड़ितों को लुभाते हैं। फर्जीवाड़े से अंजान पीड़ित जब निवेश करता है, तो ऐप निवेश पर उच्च रिटर्न दिखाता है, लेकिन जब वे पैसा निकालने के लिए प्रयास करते हैं, तो ऐप कर (टैक्स) संबंधी उद्देश्यों का झांसा देकर अतिरिक्त राशि का भुगतान करने के लिए कहता है और पैसा निकालने की अनुमति नहीं देता है। एक बार बड़ा निवेश हो जाने के बाद, पीड़ित को धोखेबाज़ द्वारा ब्लॉक कर दिया जाता है और पैसे निकाल लिए जाते हैं।

इसी तरह आभूषण फर्जीवाड़े के मामले में, धोखेबाज़ पीड़ितों को निवेश-ऐप पर दैनिक रिटर्न के साथ लुभाता है। शुरुआती कुछ दिनों के लिए लाभ पीड़ित के खाते में भी जमा किया जाता है। आखिरकार, पीड़ित द्वारा जब उच्च मूल्य का निवेश किया जाता है, तो धोखेबाज द्वारा भुगतान तुरंत रोक दिया जाता है, जिसके परिणामस्वरूप निवेशक के पूरे पैसे डूब जाते हैं।

Gold price is soaring! Earn Rs. 19,500 today with smart investment moves. Stay ahead with daily updates. https://dub.sh/BfPZk6

Rs 10,300 profit booked today from forex trading. Stay informed with real-time insights. https://dub.sh/hTsym5

Group profit this month Rs 33,800, join for daily analysis. https://goo.su/U3DZrF

नकली संदेश

सुरक्षा युक्तियाँ:

- निवेश करने से पहले हमेशा किसी भी ट्रेडिंग या निवेश-ऐप की विश्वसनीयता को अवश्य सत्यापित करें।
- हमेशा अनाधिकृत विदेशी मुद्रा व्यापार प्लेटफार्मों / ऐप्स के बारे में आरबीआई अलर्ट सूची में जांच अवश्य करें।
- कभी भी अनजान लोगों को व्यक्तिगत वित्तीय विवरण न बताएं। ऑनलाइन माध्यमों द्वारा लोगों से निवेश संबंधी मामलों में सम्मिलित होते समय हमेशा सावधानी बरतें।
- हमेशा उच्च प्रतिलाभ (हाई-रिटर्न) और कम जोखिम का वादा करने वाले निवेशों को संदेहास्पद निगाह से देखें, उनके बारे में जांच करें। अधिकतर ये धोखाधड़ी से जुड़े होते हैं।

#सबकोबताओ
#साइबरसुरक्षितभारत
#सतर्कनागरिक

Fake WhatsApp DP Fraud

Modus Operandi

In a new trend fraudsters are using fake WhatsApp profiles to scam unsuspecting individuals.

Initially scammers research their targets, collecting details about the victim. After careful study, research and social engineering of targeted victims, scammers upload fake DP in WhatsApp of Senior officers or head of the department/Organisations to whom the victims report as subordinates in real life and who commands authority over them. Messages are framed to demand immediate action, often under the guise of confidentiality and urgency. As soon as these messages are received by the employees, many of them see the WhatsApp DP of their Senior Officials/ Dept Heads and assume that the messages have been sent by their senior/boss/supervisor from his/her personal mobile number. Victims who fail to verify the authenticity of the message end up getting conned and losing their hard-earned wealth or vital information to cyber criminals.

Safety Tips:

- Always confirm any message received from an unfamiliar number by contacting the individual on their known number.
- Before initiating any transaction, verify the request with your supervisor or the concerned person directly.
- Regularly educate yourself about cybersecurity practices and emerging fraud techniques.
- Never disclose personal financial details to unknown individuals. Always exercise caution while engaging with people online.

#SabkoBataoo

#CyberSurakshitBharat

#SatarkNagrik

नकली व्हाट्सएप डीपी धोखाधड़ी

कार्यप्रणाली

आजकल धोखेबाज नकली व्हाट्सएप प्रोफाइल का उपयोग कर रहे हैं ताकि फर्जीवाड़े से, अनभिज्ञ व्यक्तियों को जाल में फसाया जा सके।

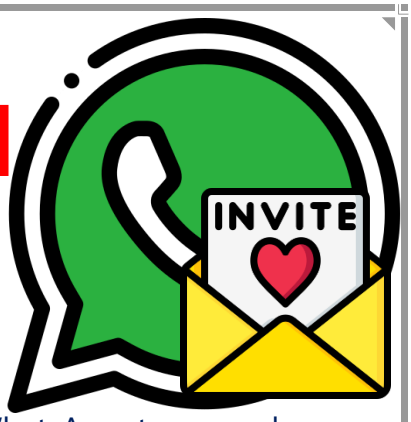
पहले धोखेबाज अपने लक्षित पीड़ितों के बारे में जानकारी एकत्रित करते हैं। उनके बारे में सावधानीपूर्वक सोशल इंजीनियरिंग का इस्तेमाल करने के बाद, धोखेबाज वरिष्ठ अधिकारियों या विभाग/संगठनों के प्रमुख का व्हाट्सएप पर नकली डीपी अपलोड करते हैं, जिन्हें पीड़ित वास्तविक जीवन में अधीनस्थ के रूप में रिपोर्ट करते हैं और जो उनकी गतिविधियों पर प्रशासनिक अधिकार रखते हैं। संदेशों को अक्सर गोपनीयता और तात्कालिकता की आड़ में तुरंत कार्रवाई की मांग करने जैसा बनाया जाता है। जैसे ही कर्मचारियों द्वारा ये संदेश प्राप्त किया जाता है, उनमें से कई अपने वरिष्ठ अधिकारियों / विभाग प्रमुखों की व्हाट्सएप डीपी देखते हैं और यह मान लेते हैं कि संदेश उनके वरिष्ठ / बॉस / पर्यवेक्षक द्वारा उनके व्यक्तिगत मोबाइल नंबर से भेजा गया है। जो पीड़ित संदेश की प्रामाणिकता को सत्यापित करने में विफल रहते हैं, वे अंत में ठग लिए जाते हैं और अपनी मेहनत की कमाई खो देते हैं या अज्ञात लोगों को महत्वपूर्ण जानकारी साझा करने की गलती कर बैठते हैं।

सुरक्षा युक्तियाँ:

- किसी अपरिचित नंबर से प्राप्त किसी भी संदेश की हमेशा उस व्यक्ति से उसके ज्ञात नंबर पर संपर्क करके पुष्टि करें।
- कोई भी बड़ा अंतरण (ट्रांज़ैक्शन) शुरू करने से पहले, अपने पर्यवेक्षक या सम्बद्ध व्यक्ति से सीधे इस बारे में बात करें और मामले को सत्यापित करें.
- नियमित रूप से साइबर सुरक्षा प्रथाओं और उभरती धोखाधड़ी तकनीकों के बारे में स्वयं को शिक्षित करें और सतर्क रहें।
- कभी भी अनजान लोगों को व्यक्तिगत वित्तीय विवरण न बताएं। अंजान लोगों से ऑनलाइन माध्यम से बात करते समय हमेशा सावधानी बरतें।

#सबकोबताओ
#साइबरसुरक्षितभारत
#सतर्कनागरिक

Wedding Invite Fraud



Modus Operandi:

Fraudsters are using fake digital wedding invitations sent via WhatsApp to spread malware through Apk files and steal personal information.

Fraudsters are sending digital wedding invitations on WhatsApp to spread malicious APK files disguised as wedding invitations via WhatsApp and compromise personal data.

Downloading these files infects phones with malware and grant hackers full access to the device. This allows them to send messages, steal personal information, and even extort money from the victim's phone without their knowledge.

Safety Tips:

- Never click on links received from unknown sources on messaging apps like WhatsApp, SMS etc.
- Never download software applications/APKs from links received in WhatsApp as it could download malicious APK file disguised as some useful application.
- Always download Apps from authorized app stores only (Google Play store for Android & Apple App store for Apple phones).
- Never disclose personal financial details to unknown individuals. Always exercise caution while engaging with people online.
- Never download wedding invitations if you received from unsolicited WhatsApp numbers.

#SabkoBataoo

#CyberSurakshitBharat

#SatarkNagrik

वैवाहिक निमंत्रण-पत्र धोखाधड़ी

कार्यप्रणाली:

जालसाज एपीके फाइलों के माध्यम से मैलवेयर फैलाने और व्यक्तिगत जानकारी चुराने के उद्देश्य से व्हाट्सएप पर शादी के नकली डिजिटल निमंत्रण-पत्र का प्रयोग कर रहे हैं।

जालसाज व्हाट्सएप पर शादी के निमंत्रण-पत्र के रूप में दुर्भावनापूर्ण एपीके फाइलों को व्हाट्सएप के माध्यम से फैलाने और व्यक्तिगत डाटा चुराने के उद्देश्य से शादी के डिजिटल निमंत्रण-पत्र भेज रहे हैं।

इन फ़ाइलों को डाउनलोड करने से फोन मैलवेयर से संक्रमित हो जाता है और हैकर्स को डिवाइस तक पूर्ण पहुंच प्रदान करते हैं। यह संदेश भेजने, व्यक्तिगत जानकारी चुराने और यहां तक कि पीड़ित के फोन से उनकी जानकारी के बिना पैसे निकालने की अनुमति देता है। जैसे-जैसे लग्न का शुभ समय चरम पर होता है, ये डिजिटल निमंत्रण ज़्यादा तेज़ी से लोगों के बीच प्रसारित किए जाते हैं।

सुरक्षा युक्तियाँ:

- कभी भी मैसेजिंग ऐप जैसे व्हाट्सएप, एसएमएस आदि पर अज्ञात स्रोतों से प्राप्त लिंक पर क्लिक न करें।
- व्हाट्सएप में प्राप्त लिंक से कभी भी सॉफ़्टवेयर एप्लिकेशन/एपीके डाउनलोड न करें क्योंकि यह कुछ उपयोगी एप्लिकेशन के रूप में प्रच्छन्न दुर्भावनापूर्ण एपीके फ़ाइल डाउनलोड कर सकता है।
- हमेशा केवल अधिकृत ऐप स्टोर से ऐप्स डाउनलोड करें (एंड्रॉइड के लिए गूगल प्ले स्टोर और ऐप्पल फोन के लिए ऐप्पल ऐप स्टोर)।
- कभी भी अनजान लोगों को व्यक्तिगत वित्तीय विवरण न बताएं। ऑनलाइन माध्यमों से लोगों से बात करते समय हमेशा सावधानी बरतें।
- अगर आपको अनचाहे व्हाट्सएप नंबरों से वैवाहिक निमंत्रण पत्र प्राप्त हुआ है तो कभी भी उन्हें डाउनलोड न करें।

#सबकोबताओ
#साइबरसुरक्षितभारत
#सतर्कनागरिक

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.

MINISTRY OF HOME AFFAIRS

REPORT ONLINE FINANCIAL FRAUD AT THE NATIONAL CYBERCRIME HELPLINE NO

1930

FILE COMPLAINT OF ANY CYBERCRIME AT NCRP:

www.cybercrime.gov.in

Report Suspected Fraud Communication (Received Through Call/SMS/WhatsApp in last 30 days) on https://www.sancharsaathi.gov.in/sfc

FOLLOW US !

@unionbankofindia @UnionBankTweets unionbankinsta @UnionBankofIndiaUtube @unionbankofIndia @unionbankinsta