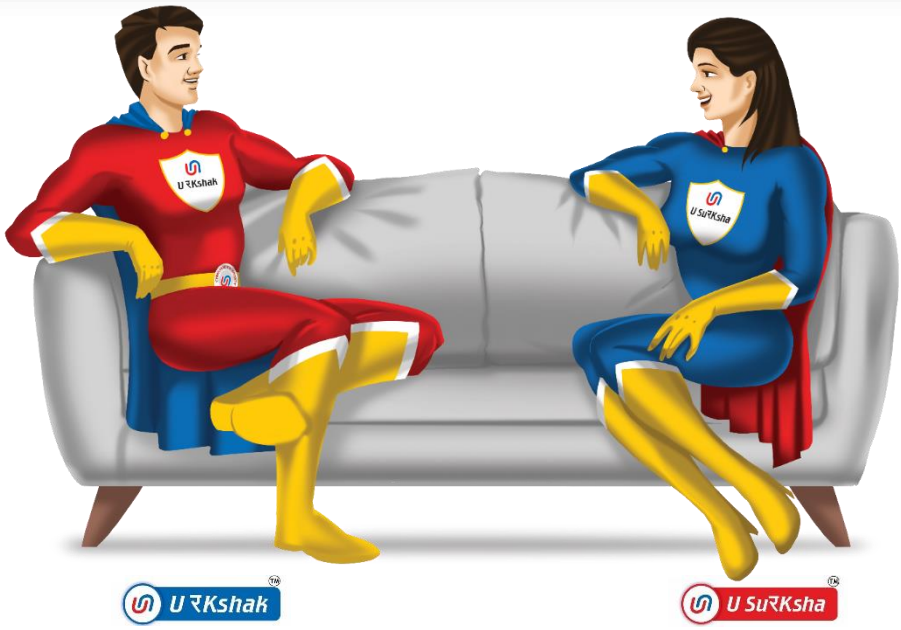
यूनियन बैंक ऑफ इंडिया
भारत सरकार का उपक्रम

Union Bank of India
A Government of India Undertaking

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

Union Bank of India

Cyber Security
Customer Awareness Guide – Vol. III



Facilities through Customer Care for Mitigating Cyber Frauds:

Below are the list of helpful services available to customers through banks Call Centre/IVR:

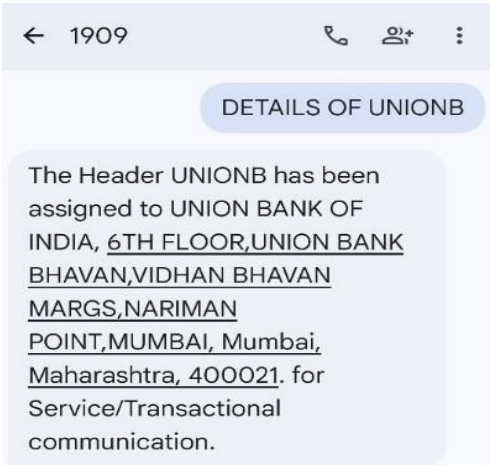
Request for Account Statement	Balance Enquiry	Details of last 5 Transactions	Suspension of Mobile Banking	Suspension of Internet Banking
Speak to Customer Care Executive	Request for SMS Alert	Hotlisting of debit card through IVR/customer care executive's assistance		

!! Beware!!

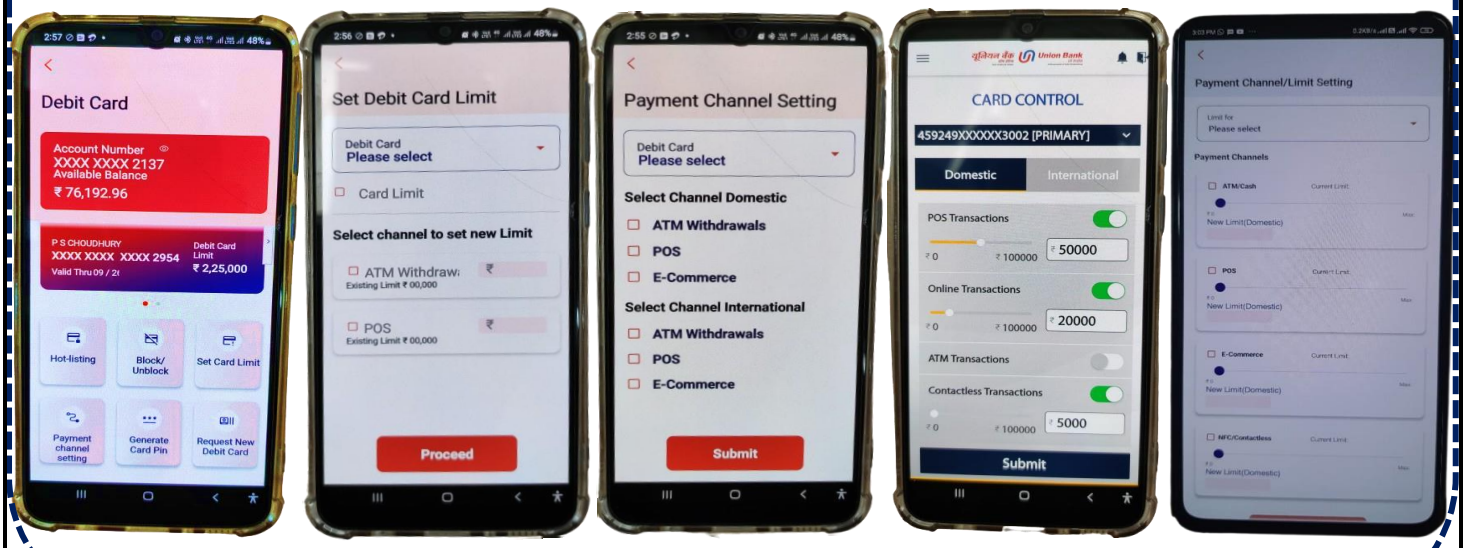
Never click or download any .apk/.ipa files, links, etc. impersonating Banks's name and logo received via WhatsApp/Telegram/SMS for redeeming rewards point, KYC update or account reactivation. **Bank never sends such messages.**

How to know SMS Header Information?

Send SMS to 1909 with following SMS content
"DETAILS OF <SMS Header>"
Example: DETAILS OF UNIONB



Debit/Credit Card Safety Features Available in our Bank's App:



Page Index

“Don’t wait for the breach to teach.”

चक्षु - Report Suspected Fraud Communication

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

To Report suspected fraud communications received through Call/SMS/WhatsApp messages related to Bank Account / Payment Wallet / SIM / Gas connection / Electricity connection / KYC update / expiry / deactivation, impersonation as Government official / relative, sextortion related etc. at: https://sancharsaathi.gov.in/sfc/

Message from
Ms. A. Manimekhalai
MD&CEO

Union Bank of India is committed to empower customers with enhanced digital experiences through various customer friendly digital products. In today's digital world, where financial transactions breach and cyber threats loom large, cybersecurity awareness is the first line of defence.

Through this book "The Cyber Security awareness guide" one can learn to prioritize cybersecurity awareness and education to mitigate risks, strengthen defences, and contribute to a safer and more secure digital ecosystem.

Message from
Shri Sanjay Rudra,
Executive Director

In today's ever-evolving digital landscape, cybersecurity is no longer an afterthought – it's the foundation of trust. At Union Bank, we're committed to providing a safe and secure banking experience for all our stakeholders. This magazine serves as a crucial step in that journey.This issue delves into the latest threats and empowers you with the knowledge to protect yourself and your loved ones.

I encourage you to not only educate yourselves but also share this knowledge with your loved ones. By staying informed, we can navigate the digital landscape with confidence.

Message from
Shri R P Singh,
CISO

As one of the largest Banks in the country, we need to empower our Customers with latest knowledge on cybersecurity best practices. By prioritizing cybersecurity awareness and education, individuals can mitigate risks, strengthen defences, and contribute to a safer and more secure digital ecosystem.

Remember, when it comes to cybersecurity, awareness is the first line of defence. This book is published in view of educating our Staff and Customers to safeguard them from the hazards of Cyber fraud tactics. I urge all readers to make the best use of it.

संदेश

सुश्री ए मणिमेखलै

प्रबंध निदेशक एवं सीईओ

यूनियन बैंक ऑफ इंडिया अनेक प्रकार के ग्राहक अनुकूल डिजिटल उत्पादों के माध्यम से ग्राहकों को बेहतर डिजिटल अनुभव प्रदान करने के लिए प्रतिबद्ध है। आज के युग में जहाँ पूरी दुनिया आपस में जुड़ी हुई है, वहीं वित्तीय लेन-देन में सेंधमारी तथा साइबर खतरे में अपार वृद्धि भी देखी जा रही है। ऐसी स्थिति में, साइबर सुरक्षा जागरूकता हमें साइबर हमलों से सुरक्षित रखने में अहम भूमिका निभाती है।

"साइबर सुरक्षा जागरूकता मार्गदर्शिका" के रूप में जारी इस पुस्तक के माध्यम से, जोखिमों को कम करने, सुरक्षा को मजबूत करने एवं अधिक सुरक्षित डिजिटल पारिस्थितिकी तंत्र स्थापित करने में अपना योगदान देने हेतु हम मार्गदर्शिका में प्रदत्त साइबर सुरक्षा जागरूकता तथा शिक्षा को प्राथमिकता के साथ सीख सकते हैं।

संदेश

श्री संजय रूद्र,

कार्यपालक निदेशक

निरंतर परिवर्तनशील समय में साइबर सुरक्षा विकल्प नहीं अपितु आवश्यकता है-यह विश्वास की नींव है। यूनियन बैंक, अपने हितधारकों को त्वरित, सुरक्षित और सुदृढ़ बैंकिंग सेवाएँ प्रदान करने के लिए प्रतिबद्ध है। यह मार्गदर्शिका इसी मुहिम का अभिन्न अंग है। यह अंक साइबर जगत में प्रतिदिन आने वाले नए खतरों से आपको अवगत करवाकर, आपकी और आपके प्रियजनों की सुरक्षा को सुनिश्चित करता है।

मैं आपको न केवल इसके ज्ञानार्जन के लिए प्रोत्साहित करता हूँ बल्कि अपने परिवारजन को भी इस बारे में अवश्य अवगत करवाएँ। आज के डिजिटल युग में सूचित रहते हुए ही हम स्वयं को सुरक्षित रख सकते हैं।

संदेश

श्री आर पी सिंह,

सीआईएसओ

हमारा बैंक देश के सबसे बड़े बैंकों में से एक है,अतः हमें अपने ग्राहकों को साइबर सुरक्षा की सर्वोत्तम प्रथाओं से सम्बद्ध व्यावहारिक ज्ञान से अवगत करने की आवश्यकता है। साइबर सुरक्षा जागरूकता एवं शिक्षा को प्राथमिकता देकर, ग्राहक जोखिमों को कम कर सकते हैं, सुरक्षा में मजबूती प्रदान कर सकते हैं तथा एक सुदृढ़ व सुरक्षित डिजिटल तंत्र के निर्माण में अपना योगदान दे सकते हैं।

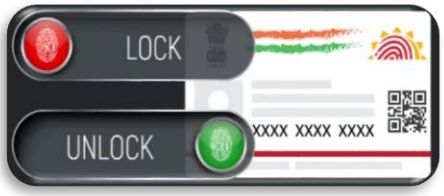
याद रखें, जब साइबर सुरक्षा की बात आती है, तो जागरूकता ही बचाव की पहली कड़ी है। यह पुस्तक हमारे कर्मचारियों एवं ग्राहकों को साइबर धोखाधड़ी के खतरों से बचाने हेतु उन्हें शिक्षित करने के उद्देश्य से प्रकाशित की गई है।

How to Enhance Aadhaar Enabled Payments Security?

Fraudsters collect biometric data from websites/shops/ SIM card outlets & use them to steal money from Aadhaar linked bank accounts.

Methods for locking/unlocking biometric data for Aadhaar payment when not in use?

Using mAadhaar App	Using UIDAI website	Sending SMS to 1947



How to Lock/Unlock Aadhaar Biometric through SMS/OTP:

Step 1: Send SMS to 1947 with the words GETOTP and the last four digits of your Aadhaar card number.
Step 2: Send another text message to 1947 with LOCKUID [SPACE], the last four digits of your Aadhaar card number [SPACE], and the previously obtained OTP. Aadhaar Biometric will be locked.
Step 3: Repeat step 1 first, then send a text message to 1947 with 'UNLOCKUID [space], the last four digits of your Aadhaar card number [SPACE], and the previously obtained OTP. Aadhaar Biometric will be unlocked.
Step 4: A text message confirming the current status of your Aadhaar card number will be delivered to your registered mobile number.

Aadhaar Card Biometric Lock through UIDAI Portal

To lock their Aadhaar biometrics, an applicant should follow the guidelines below.
Step 1: Visit UIDAI's official website.
Step 2: Go to 'My Aadhaar' and select 'Aadhaar Services' from the drop-down menu. Now, click on 'Lock/Unlock Biometrics.'
Step 3: Tick the box, then select 'Lock/Unlock Biometrics.'
Step 4: Enter both your 12-digit Aadhaar number and the captcha code.
Step 5: Enter your OTP, then turn on the locking feature.
Step 6: Aadhaar biometric data will be encrypted.

Aadhaar Biometric Lock through Mobile Application

Step 1: Access your mAadhaar app.
Step 2: Click the hamburger icon (three vertical dots) in the application's upper right corner.
Step 3: Check the Enable Biometric Locking box under Biometric Settings.
Step 4: An OTP will be obtained from your mobile number and automatically entered into the application (there is no option to enter the OTP manually).
Step 5: Your biometric is locked once you authorize it. The lock, however, may take up to 6 hours to activate.

आधार आधारित भुगतानों की सुरक्षा कैसे बढ़ाएं?

जालसाज वेबसाइटों/दुकानों/सिम कार्ड आउटलेट्स से बायोमेट्रिक डेटा एकत्र करते हैं तथा उसका उपयोग आधार से जुड़े बैंक खातों से पैसे चुराने के लिए करते हैं।

उपयोग में न होने पर आधार भुगतान के लिए बायोमेट्रिक डेटा लॉक करने के तरीके:

एमआधार ऐप्प का प्रयोग करें	यूआईडीएआई की वैबसाइट का प्रयोग करें	1947 पर एसएमएस करें

एसएमएस के माध्यम से आधार बायोमेट्रिक को कैसे लॉक/अनलॉक करें:

चरण 1: 1947 पर GETOTP और अपने आधार कार्ड नंबर के अंतिम चार अंक लिखकर संदेश भेजें।
चरण 2: 1947 पर LOCKUID [SPACE], अपने आधार कार्ड नंबर के अंतिम चार अंक [SPACE] और पहले प्राप्त ओटीपी के साथ एक और संदेश भेजें। आपका आधार बायोमेट्रिक अब लॉक हो जाएगा।
चरण 3: पहले चरण की प्रक्रिया को दोहराएँ फिर 1947 पर UNLOCKUID [SPACE], अपने आधार कार्ड के अंतिम 4 अंक [SPACE) और पहले प्राप्त ओटीपी के साथ संदेश भेजें। अब आपका आधार बायोमेट्रिक अनलॉक हो चुका है।

चरण 4 : आपके आधार कार्ड नंबर की वर्तमान स्थिति की पुष्टि करने वाला एक संदेश आपके पंजीकृत मोबाइल नंबर पर भेजा जाएगा।

यूआईडीएआई (UIDAI) पोर्टल के ज़रिए आधार कार्ड बायोमेट्रिक लॉक करें:

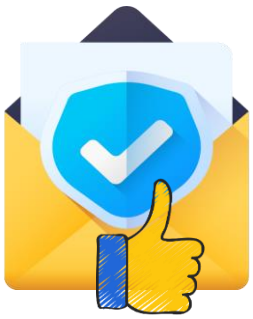
आवेदक अपना आधार बायोमेट्रिक लॉक करने के लिए नीचे दिए गए दिशा-निर्देशों का पालन करें-
चरण 1: यूआईडीएआई की आधिकारिक वेबसाइट पर जाएँ।
चरण 2: 'माई आधार' पर जाएँ और ड्रॉप-डाउन मेनू से 'आधार सेवाएँ' चुनें। अब, 'लॉक/अनलॉक बायोमेट्रिक्स' पर क्लिक करें।
चरण 3: बॉक्स पर टिक करें, फिर 'लॉक/अनलॉक बायोमेट्रिक्स' चुनें।
चरण 4: अपना 12-अंकीय आधार नंबर और कैप्चा कोड दोनों दर्ज करें।
चरण 5: अपना ओटीपी दर्ज करें, फिर लॉकिंग सुविधा चालू करें।
चरण 6: आधार बायोमेट्रिक डेटा एन्क्रिप्ट किया जाएगा।

मोबाइल एप्लीकेशन के माध्यम से आधार बायोमेट्रिक लॉक

चरण 1: अपने एमआधार (mAadhaar) ऐप पर जाएँ।
चरण 2: एप्लीकेशन के ऊपरी दाएँ कोने में हैमबर्गर आइकन (तीन लंबवत बिंदु) पर क्लिक करें।
चरण 3: बायोमेट्रिक सेटिंग के अंतर्गत बायोमेट्रिक लॉकिंग सक्षम करें बॉक्स को चेक करें।
चरण 4: आपके मोबाइल नंबर पर एक ओटीपी प्राप्त होगा और स्वचालित रूप से एप्लीकेशन में दर्ज हो जाएगा (ओटीपी को मैन्युअल रूप से दर्ज करने का कोई विकल्प नहीं है)।
चरण 5: आपके द्वारा इसे अधिकृत करने के बाद आपका बायोमेट्रिक लॉक हो जाता है। हालाँकि, लॉक को सक्रिय होने में 6 घंटे तक का समय लग सकता है।

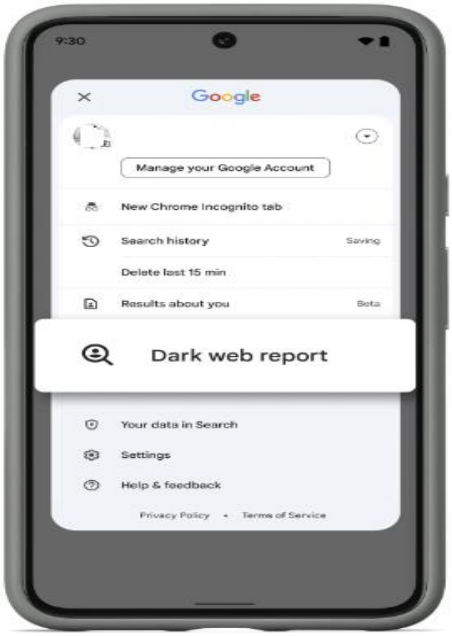
How to Enhance Your Email Security?

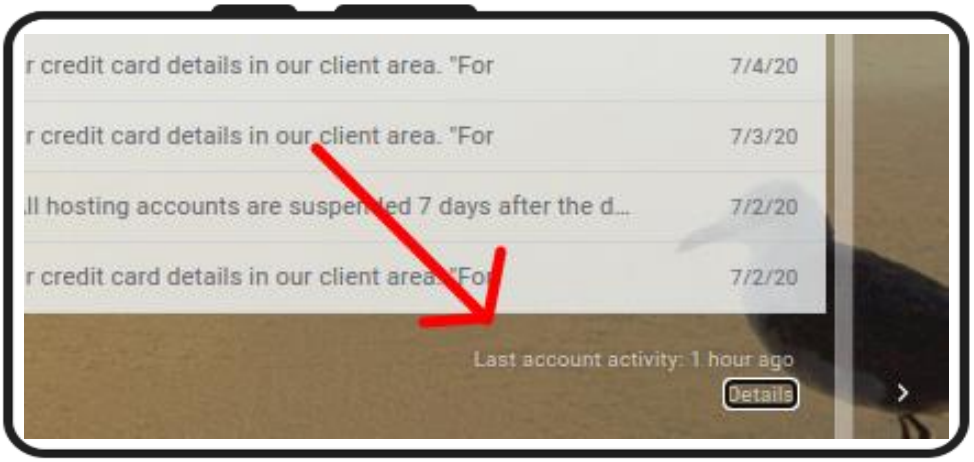
Phishing emails are designed to deceive the user to collect sensitive personal information and it provides the attacker, an initial access to your computer/mobile.

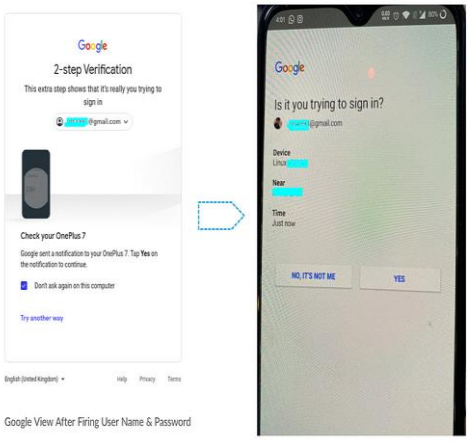


Methods to enhance Email security:

- Always use a Strong Password: Weak, reused, and leaked passwords are the most common cause of email account compromise. Always use Multi-factor authentication (MFA) wherever possible.
- Never click on links in emails received from unknown senders.
- Never download attachments from unsolicited emails.
- Always use antivirus/antimalware software in your computer/devices & update them regularly.
- Regularly check & monitor your email login activity.







Google View After Firing User Name & Password

Configured Device will get a 2Fa Auth Prompt

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

Visit Security Checkup for more details

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	Location (IP address) [?]	Date/Time (Displayed in your time zone)
Browser (Chrome) Show details	* Qatar	11:16 am (0 minutes ago)
Mobile	Qatar (	9:45 am (1.5 hours ago)
Browser (Chrome) Show details	* Qatar	9:36 am (1.5 hours ago)
Browser (Chrome) Show details	* Qatar	9:04 am (2 hours ago)
Browser (Chrome) Show details	* Qatar	Feb 21 (20 hours ago)
Browser (Chrome) Show details	* Qatar	Feb 21 (22 hours ago)
Browser (Chrome) Show details	* Qatar	Feb 21 (23 hours ago)
Unknown	Qatar (	Feb 21 (1 day ago)
Browser (Chrome) Show details	Qatar (	Feb 21 (1 day ago)
Browser (Chrome) Show details	Qatar (	Feb 21 (1 day ago)

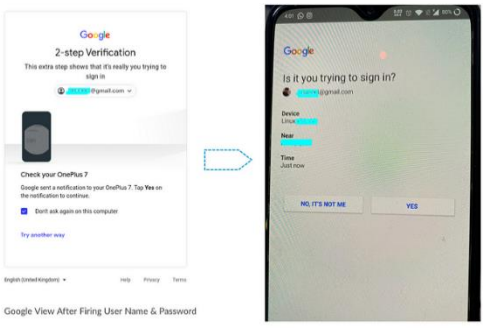
* indicates activity from the current session.

अपनी ईमेल की सुरक्षा को कैसे बढ़ाएँ?

उपयोगकर्ता को धोखा देकर संवेदनशील व्यक्तिगत जानकारी एकत्र करने के लिए फ़िशिंग ईमेल डिज़ाइन किए जाते हैं तथा यह हमलावर को आपके कंप्यूटर/मोबाइल तक प्रारंभिक पहुंच प्राप्त करने में मदद करता है।

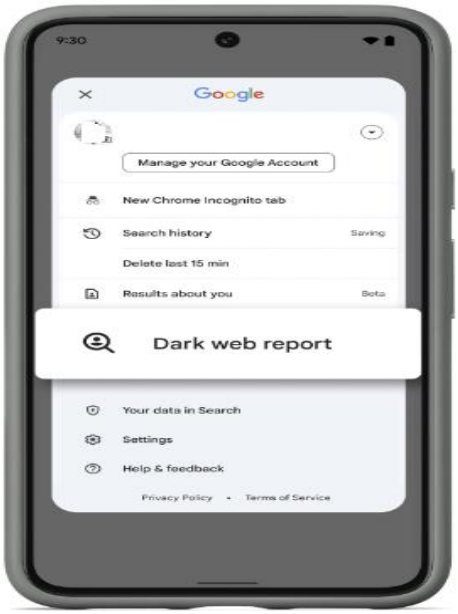
ईमेल सुरक्षा बढ़ाने के तरीके:

- हमेशा मजबूत पासवर्ड का उपयोग करें: कमज़ोर, दोबारा इस्तेमाल किया गया तथा उजागर हो चुका पासवर्ड प्रायः ईमेल खाते हैक होने का सबसे आम कारण होते हैं। यथासंभव मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) का ही उपयोग करें।
- अज्ञात प्रेषकों से प्राप्त ईमेल में दिए गए लिंक पर कभी भी क्लिक न करें।
- कभी भी अवांछित ईमेल से अटैचमेंट डाउनलोड न करें।
- अपने कंप्यूटर/डिवाइस में हमेशा एंटीवायरस/एंटीमैलवेयर सॉफ़्टवेयर का उपयोग करें एवं उसे नियमित रूप से अपडेट करें।
- अपनी ईमेल लॉगिन गतिविधि की नियमित तौर पर जांच एवं निगरानी करें।



Google View After Firing User Name & Password

Configured Device will get a 2Fa Auth Prompt



This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

Visit Security Checkup for more details

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	Location (IP address) [?]	Date/Time (Displayed in your time zone)
Browser (Chrome) Show details	* Qatar	11:16 am (0 minutes ago)
Mobile	Qatar (	9:45 am (1.5 hours ago)
Browser (Chrome) Show details	* Qatar	9:36 am (1.5 hours ago)
Browser (Chrome) Show details	* Qatar	9:04 am (2 hours ago)
Browser (Chrome) Show details	* Qatar	Feb 21 (20 hours ago)
Browser (Chrome) Show details	* Qatar	Feb 21 (22 hours ago)
Browser (Chrome) Show details	* Qatar	Feb 21 (23 hours ago)
Unknown	Qatar (	Feb 21 (1 day ago)
Browser (Chrome) Show details	Qatar (	Feb 21 (1 day ago)
Browser (Chrome) Show details	Qatar (	Feb 21 (1 day ago)

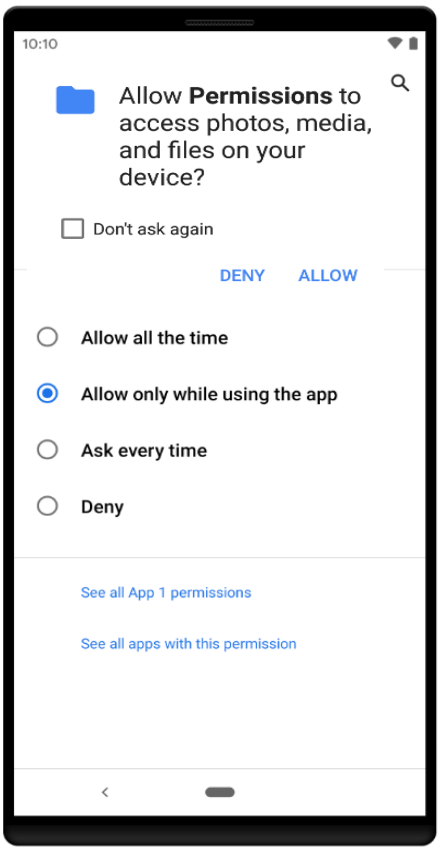
* indicates activity from the current session.

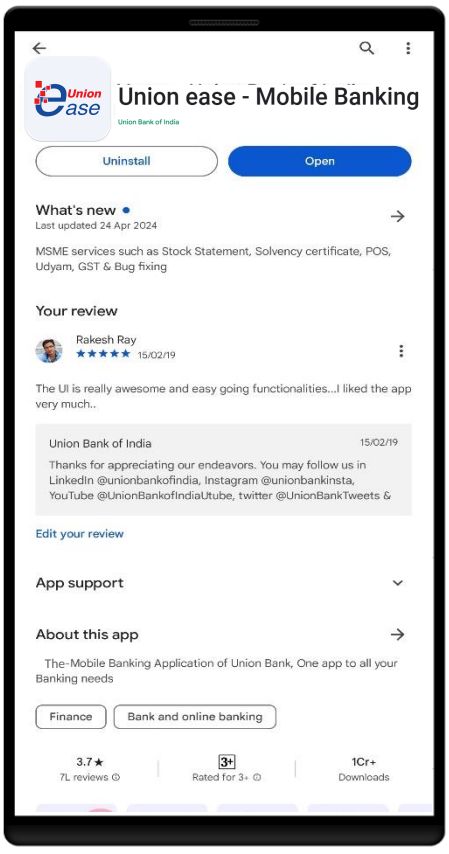
How to Enhance Your Mobile App Security?

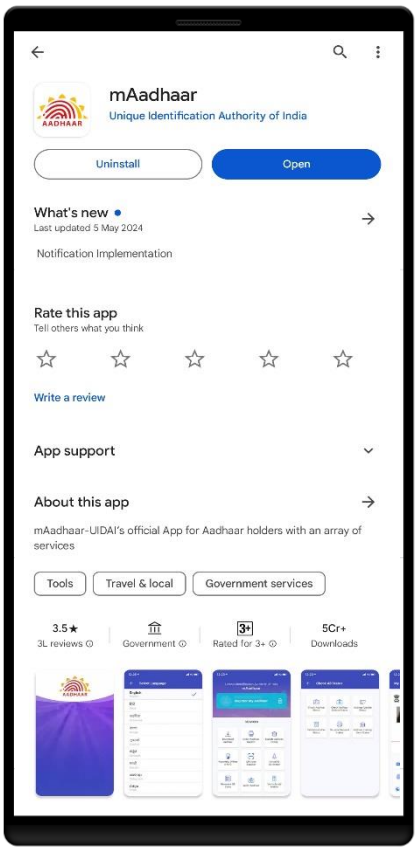
Scammers distribute .apk/.ipa of Fake/Malicious Mobile App through social media, WhatsApp messages, Telegram channels & SMS to commit cybercrime.

Methods to enhance App security:

- Always download apps from official app stores (such as Google Play Store, Apple App Store & Govt. App Store) as they have stringent security checks in place.
- Always check the app details before you download to filter out fake or malicious apps – look at who the developer is, look for User reviews, Number of downloads etc.
- Always review permissions that are requested by the application.
- Always use antivirus/antimalware software in the system/computer & scan it regularly.
- Regularly check the installed applications in your mobile device and delete unknown or idle apps.
- **Avoid downloading apps received through WhatsApp, SMS, emails, social media messages.**





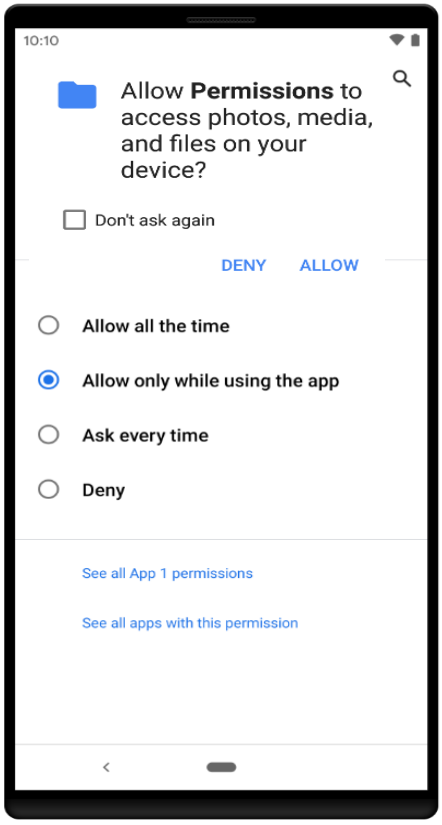


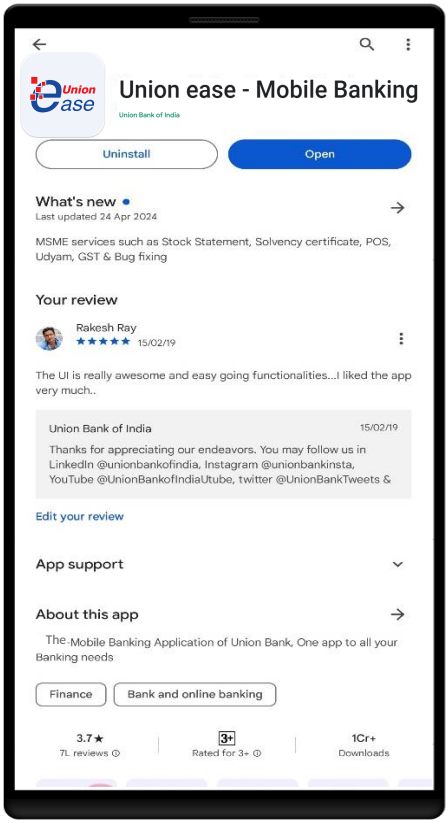
अपने मोबाइल ऐप की सुरक्षा कैसे बढ़ाएं ?

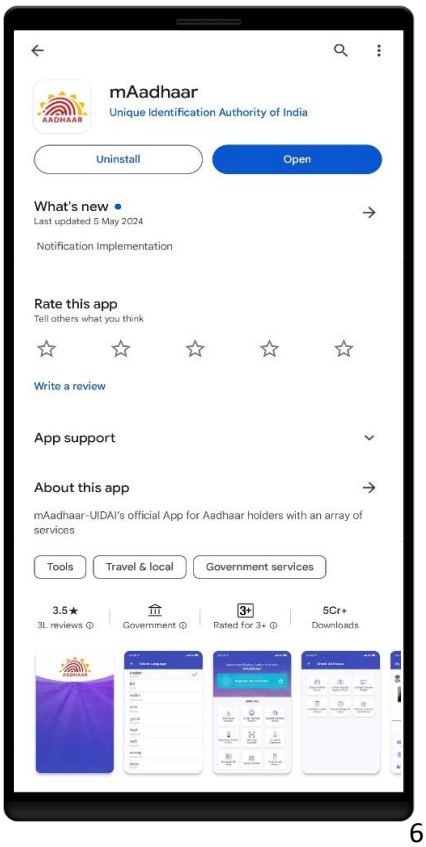
घोटालेबाज साइबर अपराध करने के लिए सोशल मीडिया, व्हाट्सऐप संदेश, टेलीग्राम चैनल एवं एसएमएस के माध्यम से .apk/.ipa फाइलों वाले फर्जी/विद्वेषपूर्ण मोबाइल ऐप प्रसारित करते हैं।

ऐप सुरक्षा बढ़ाने के तरीके:

- हमेशा आधिकारिक ऐप स्टोर (जैसे गुगल प्ले स्टोर, एप्पल ऐप स्टोर एवं सरकारी ऐप स्टोर) से ऐप डाउनलोड करें क्योंकि ये सख्त सुरक्षा मानकों का पालन करते हैं।
- फर्जी अथवा विद्वेषपूर्ण ऐप्स को परखने के लिए डाउनलोड करने से पहले हमेशा ऐप विवरण की जांच करें - देखें कि डेवलपर कौन है, उपयोगकर्ता की समीक्षा, डाउनलोड की संख्या आदि को देखें।
- एप्लिकेशन द्वारा अनुरोधित अनुमतियों की हमेशा समीक्षा करें।
- सिस्टम/कंप्यूटर में हमेशा एंटीवायरस/एंटीमैलवेयर सॉफ़्टवेयर का उपयोग करें तथा इसे नियमित रूप से स्कैन करें।
- अपने मोबाइल डिवाइस में इंस्टॉल किए गए एप्लिकेशन की नियमित रूप से जांच करें तथा अज्ञात अथवा निष्क्रिय ऐप्स को हटा दें।
- व्हाट्सऐप, एसएमएस, ईमेल, सोशल मीडिया संदेशों से ऐप्स डाउनलोड करने से बचें।





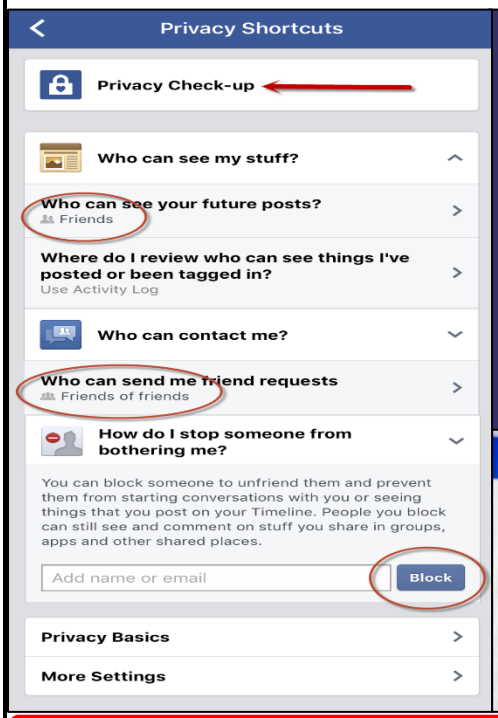


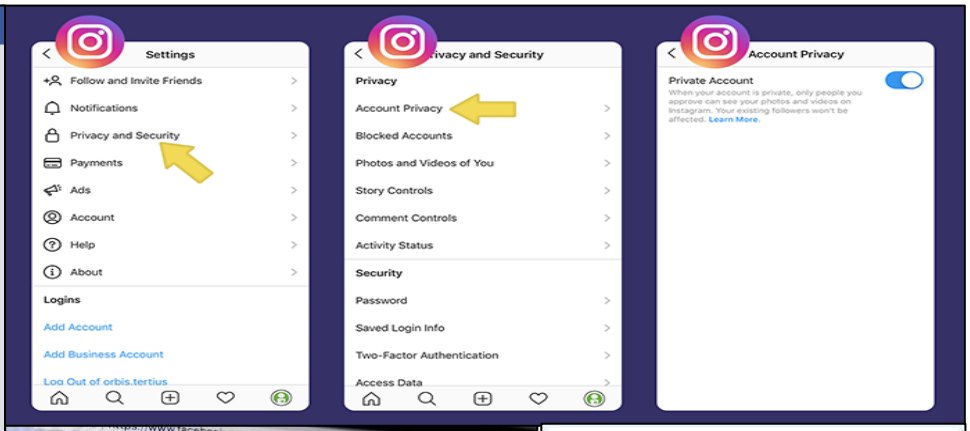
How to Enhance Your Social Media Account Security?

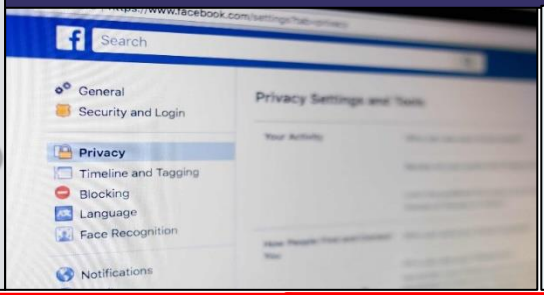
Scammers create fake profiles on social media platforms (sometimes using data available from Original profile) to collect sensitive personal information (PII), with a motive to defraud individuals.

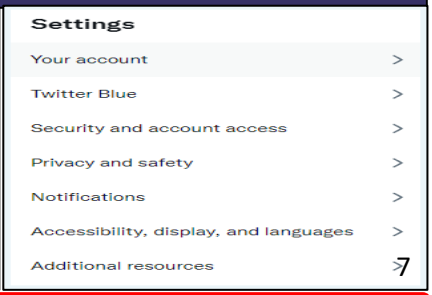
Methods to enhance your Social Media Account security:

- Avoid sharing your personal information like address, mobile number, personal email id and other sensitive identity related information on social media.
- Do not share your personal pictures online publicly on social media accounts.
- Never accept friend requests without appropriate verification and confirmation.
- Never click on suspicious links or download any app received through messages for logging into your social media accounts until you verify the authenticity of the source.
- Use different passwords for different social media accounts & Enable multi-factor authentication.
- Disable profile visibility from public searches.
- Never share social media credentials with anyone & log out after each session.
- Keep the privacy settings of social media profile at 'most restricted level', especially for public viewing.
- Apply maximum caution while sharing photographs, videos, status and comments etc. as cyber criminals may collect enough information about the user from these posts.

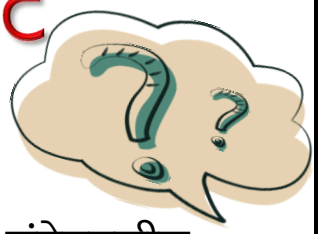








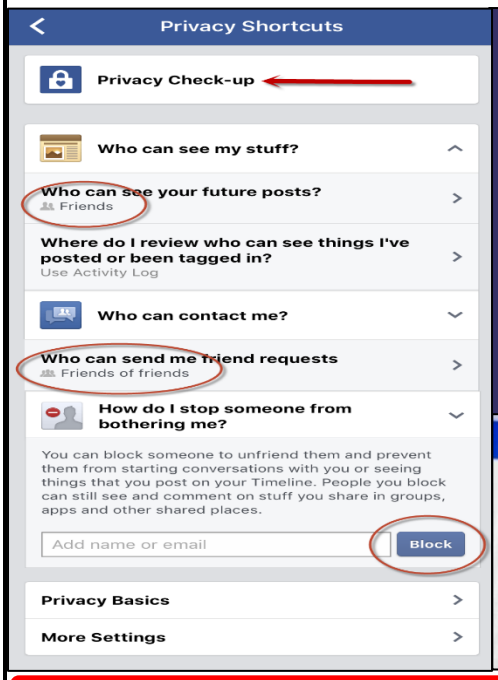
अपने सोशल मीडिया अकाउंट की सुरक्षा कैसे बढ़ाएं?

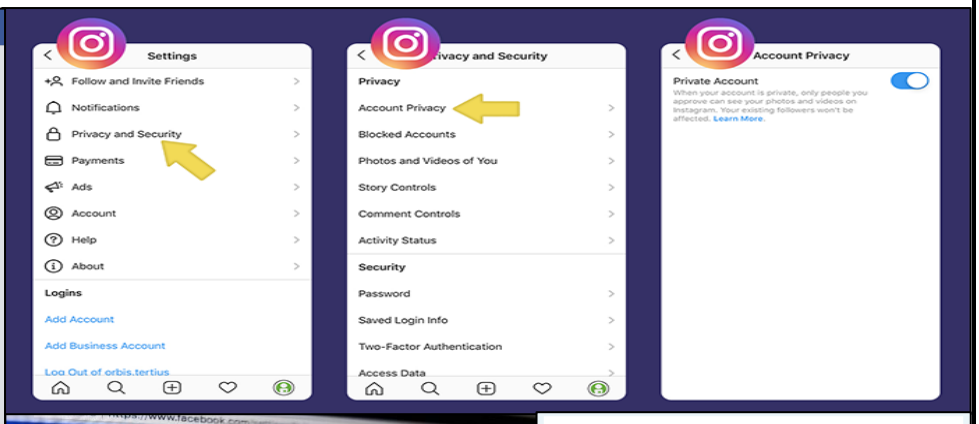


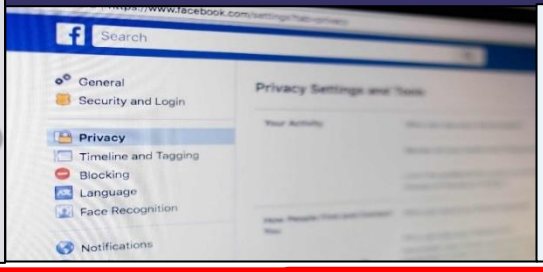
घोटालेबाज आम लोगों को धोखा देने के उद्देश्य से उनकी संवेदनशील व्यक्तिगत जानकारी (पीआईआई) एकत्र करने के लिए सोशल मीडिया प्लेटफॉर्म पर फर्जी प्रोफाइल बनाते हैं (कभी-कभी वास्तविक प्रोफ़ाइल में उपलब्ध डेटा का उपयोग करते हैं)।

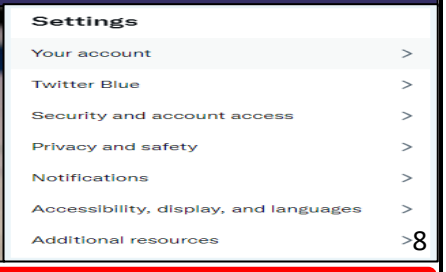
सोशल मीडिया अकाउंट की सुरक्षा बढ़ाने के तरीके:

- अपनी व्यक्तिगत जानकारी जैसे पता, मोबाइल नंबर, व्यक्तिगत ईमेल आईडी तथा पहचान संबंधी अन्य संवेदनशील जानकारी सोशल मीडिया पर साझा करने से बचें।
- अपनी निजी तस्वीरें सोशल मीडिया अकाउंट पर सार्वजनिक रूप से साझा न करें।
- उचित सत्यापन एवं पुष्टि के बिना कभी भी ऑनलाइन मित्रता के अनुरोध को स्वीकार न करें।
- अपने सोशल मीडिया अकाउंट में लॉगइन करने के लिए कभी भी किसी संदिग्ध लिंक पर क्लिक न करें या संदेशों के माध्यम से प्राप्त किसी भी ऐप को डाउनलोड न करें, जब तक कि आप स्रोत की प्रामाणिकता सत्यापित न कर लें।
- विभिन्न सोशल मीडिया अकाउंट के लिए अलग-अलग पासवर्ड का उपयोग करें तथा मल्टी-फैक्टर प्रमाणीकरण को सक्रिय रखें।
- सार्वजनिक सर्च से अपनी प्रोफ़ाइल दृश्यता के विकल्प को निष्क्रिय रखें।
- सोशल मीडिया क्रेडेंशियल्स को कभी भी किसी के साथ साझा न करें तथा प्रत्येक सत्र के बाद लॉग-आउट अवश्य करें।
- सोशल मीडिया प्रोफाइल की गोपनीयता सेटिंग को 'मोस्ट रिस्ट्रिक्टेड लेवल' (अत्यधिक सीमित स्तर) पर रखें, विशेष रूप से सार्वजनिक दृश्यता (विज़िबल टु पब्लिक) के विकल्प को सीमित रखें।
- फोटो, वीडियो, स्टेटस, टिप्पणी आदि साझा करते समय अत्यधिक सावधानी बरतें क्योंकि साइबर अपराधी उपयोगकर्ताओं के पोस्ट एवं प्रोफाइल से उनके बारे में पर्याप्त जानकारी एकत्र कर सकते हैं।







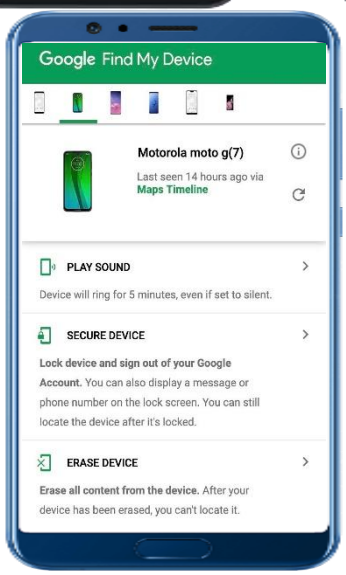


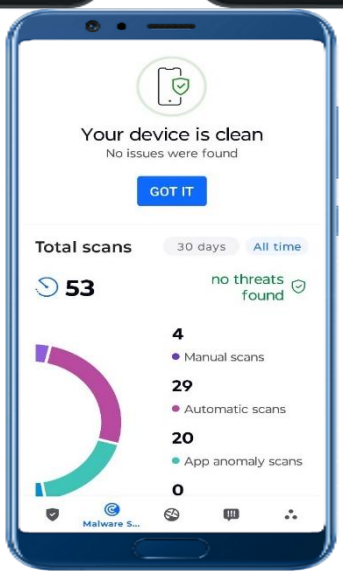
How to Enhance Your Mobile Device Security?

Fraudsters infect user's mobile devices through phishing, hacking, call forwarding, SMS for undertaking malicious activities like stealing sensitive personal information (PII) to siphon off money.

Methods to enhance your Mobile Device security:

- Always use password/PIN/biometric lock for accessing your mobile device.
- Always use an antimalware/antivirus software in your mobile phone and scan it regularly.
- Never download apps from 3rd party app stores. Always download from official app stores only.
- Never download .apk/.ipa files shared through social media messaging apps.
- Don't leave your mobile device unattended or don't give it to unknown people.
- Always take back up of your device data to avoid data loss in case of any cyber incident or losing your mobile unfortunately.
- Use Google's "Find My Device" feature to find your lost mobile & erase data remotely in case of necessity.



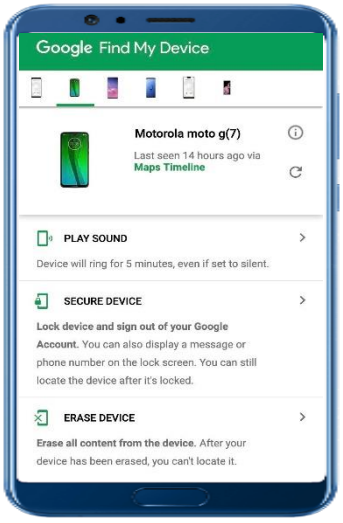


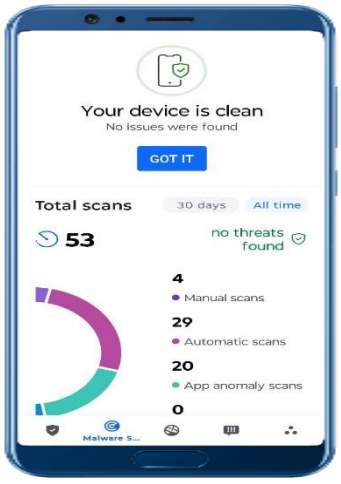
अपने मोबाइल डिवाइस की सुरक्षा कैसे बढ़ाएं?

धोखेबाज़ फ़िशिंग, हैकिंग, कॉल फ़ॉरवर्डिंग, एसएमएस के माध्यम से उपयोगकर्ताओं के मोबाइल डिवाइस को संक्रमित करते हैं तथा पैसे हड़पने के लिए संवेदनशील व्यक्तिगत जानकारी (पीआईआई) चुराने जैसी आपराधिक गतिविधियों को अंजाम देते हैं।

मोबाइल डिवाइस की सुरक्षा बढ़ाने के तरीके:

- अपने मोबाइल डिवाइस को एक्सेस करने के लिए हमेशा पासवर्ड/पिन/बायोमेट्रिक लॉक का उपयोग करें।
- अपने मोबाइल फोन में हमेशा एंटीमैलवेयर/एंटीवायरस सॉफ्टवेयर का उपयोग करें तथा उसे नियमित रूप से स्कैन करें।
- थर्ड पार्टी ऐप स्टोर से ऐप डाउनलोड न करें। हमेशा आधिकारिक ऐप स्टोर से ही ऐप डाउनलोड करें।
- सोशल मीडिया मैसेजिंग ऐप्स के माध्यम से साझा की गई .apk/.ipa फ़ाइलों को कभी भी डाउनलोड न करें।
- अपने मोबाइल डिवाइस को लावारिस न छोड़ें, अथवा उसे किसी अनजान व्यक्ति को न दें।
- किसी भी साइबर घटना या दुर्भाग्यवश अपना मोबाइल खो जाने की स्थिति में डेटा के नुकसान से बचने के लिए हमेशा अपने डिवाइस डेटा का बैकअप रखें।
- अपने खोए हुए मोबाइल को ढूंढने तथा आवश्यकता पड़ने पर डेटा को मिटाने के लिए गुगल की "फाइंड माई डिवाइस" सुविधा का उपयोग करें।



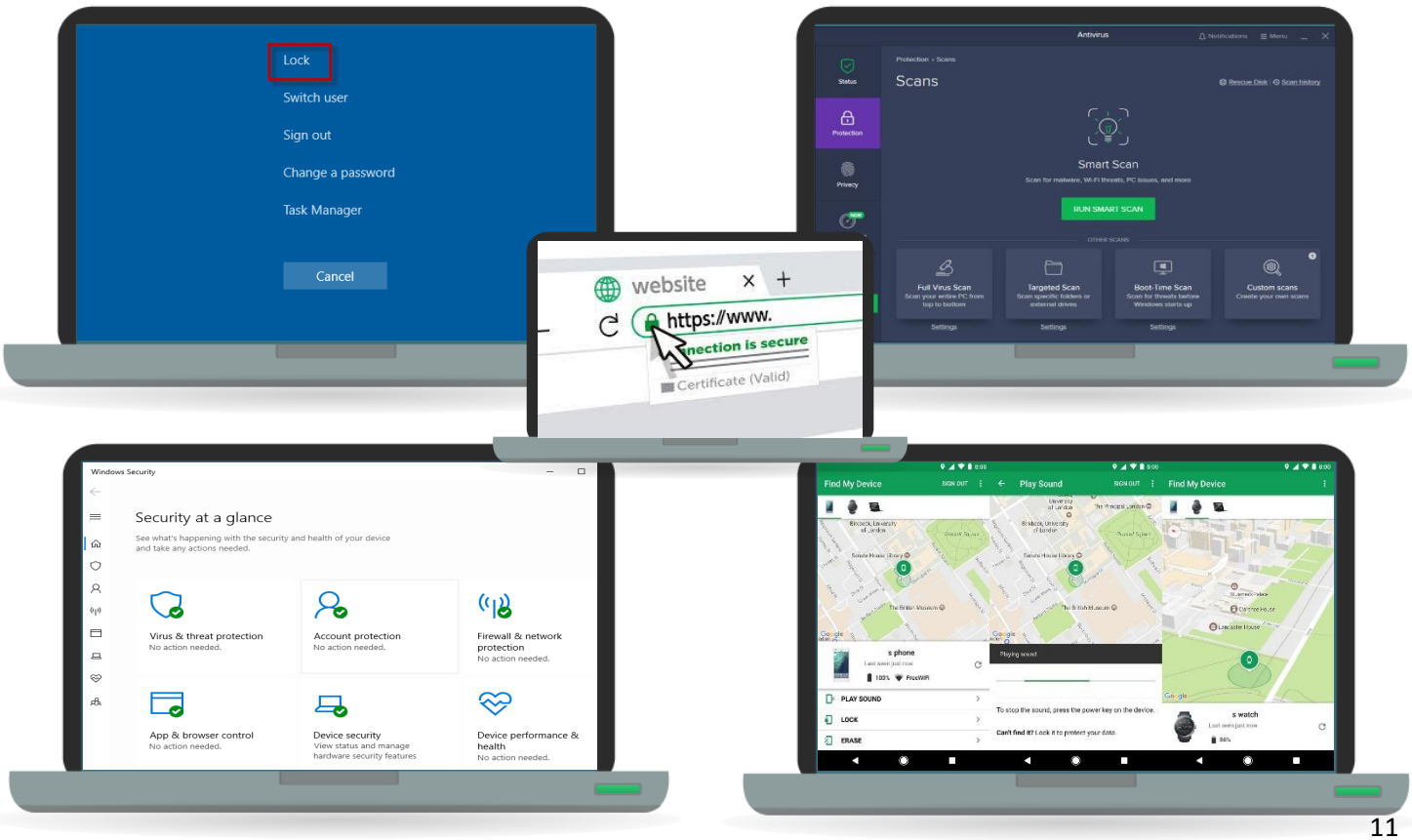


How to Enhance Your Desktop/Laptop Security?

Cyber criminal uses various methods for hacking a victim's computer/device such as infecting them with a virus or malware. Hacking may lead to data corruption/deletion/stealing. Sometimes, it is done by known people and insiders in an organization by taking advantage of the user.

Methods to enhance your Desktop/Computer Device security:

- Never open unknown USB devices directly in your computer without scanning with antivirus.
- Always keep your desktop clean. Important files must be kept in folder & secured with password.
- Always use an antimalware/antivirus software in your device and scan it regularly.
- Never download apps from 3rd party app stores. Always download from official app stores only.
- Never download .apk/.ipa setup files shared through social media messaging apps/unofficial app stores/websites.
- Don't leave your device unattended or don't give it to unknown people.
- Always take back up of your device data to avoid data loss in case of any cyber incident or losing your mobile unfortunately.
- Visit & browse safe websites on internet. Malicious websites can download virus into computer.

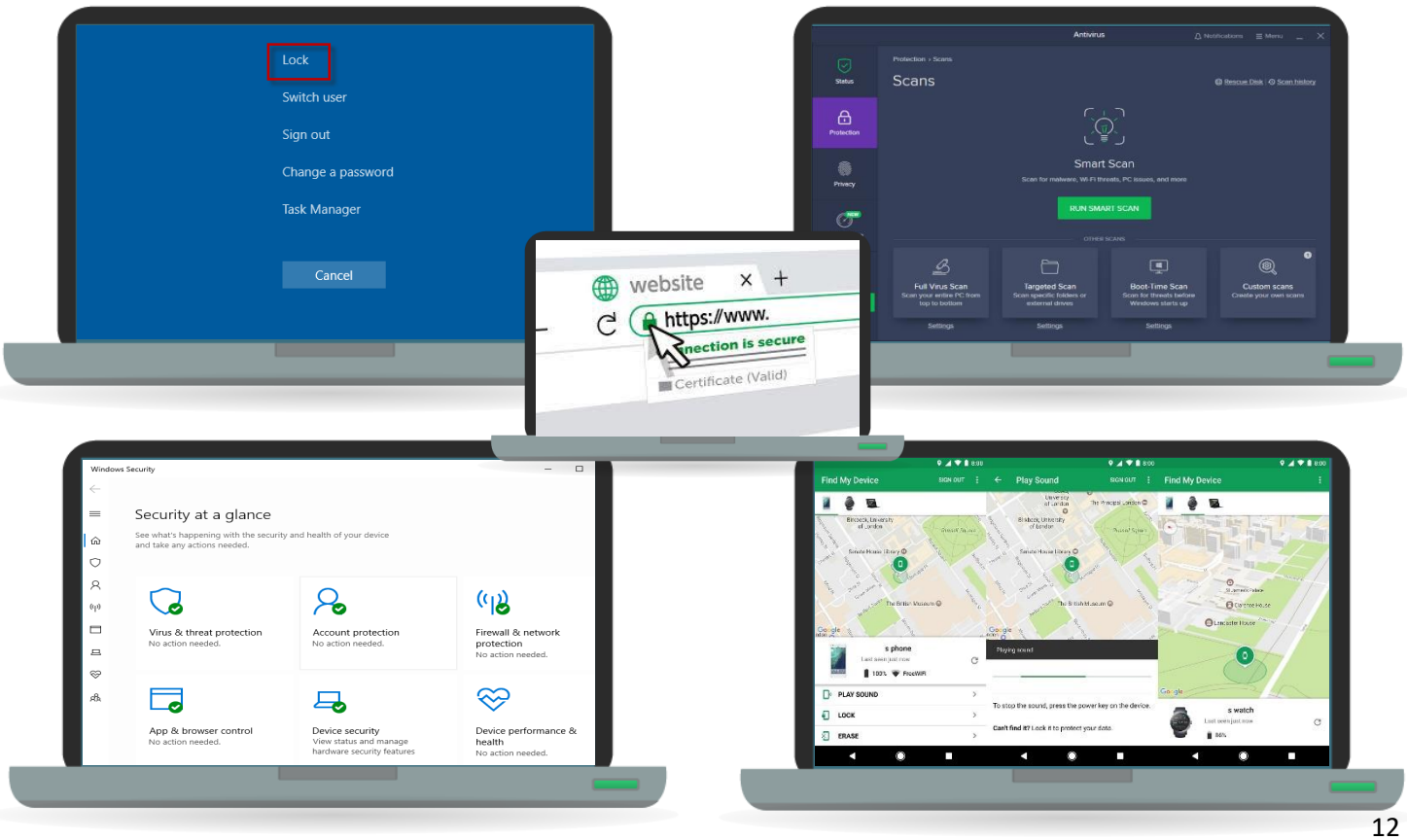


अपने डेस्कटॉप/लैपटॉप की सुरक्षा कैसे बढ़ाएँ?

साइबर अपराधी पीड़ित के कंप्यूटर/डिवाइस को हैक करने के लिए कई तरह के तरीके अपनाते हैं, जैसे कि उन्हें वायरस अथवा मैलवेयर से संक्रमित करना। हैकिंग से डेटा करप्शन/डिलीशन/चोरी हो सकती है। कभी-कभी, यह किसी उपयोगकर्ता का फ़ायदा उठाकर संगठन केअंदरूनी लोगों द्वारा किया जाता है।

डेस्कटॉप/कंप्यूटर डिवाइस की सुरक्षा बढ़ाने के तरीके:

- एंटीवायरस से स्कैन किए बिना कभी भी अपने कंप्यूटर सिस्टम में अज्ञात USB डिवाइस को न खोलें।
- अपने डेस्कटॉप को हमेशा साफ रखें। महत्वपूर्ण फाइलों को फोल्डर में रखें तथा पासवर्ड से सुरक्षित रखें।
- अपने डिवाइस में हमेशा एंटीमैलवेयर/एंटीवायरस सॉफ़्टवेयर का उपयोग करें तथा उसे नियमित रूप से स्कैन करें।
- थर्ड पार्टी ऐप स्टोर से ऐप डाउनलोड न करें। हमेशा आधिकारिक ऐप स्टोर से ही ऐप डाउनलोड करें।
- सोशल मीडिया मैसेजिंग ऐप्स/अनाधिकारिक ऐप स्टोर/वेबसाइटों के माध्यम से साझा की गई .apk/.ipa सेटअप फ़ाइलों को कभी भी डाउनलोड न करें।
- अपने डिवाइस को लावारिस न छोड़ें अथवा अनजान लोगों को न दें।
- किसी भी साइबर घटना या दुर्भाग्यवश अपना मोबाइल खो जाने की स्थिति में डेटा नुकसान से बचने के लिए हमेशा अपने डिवाइस डेटा का बैकअप रखें।
- इंटरनेट पर सुरक्षित वेबसाइट को ही देखें तथा ब्राउज़ करें। विद्वेषपूर्ण वेबसाइटें कंप्यूटर में वायरस डाउनलोड कर सकती हैं।

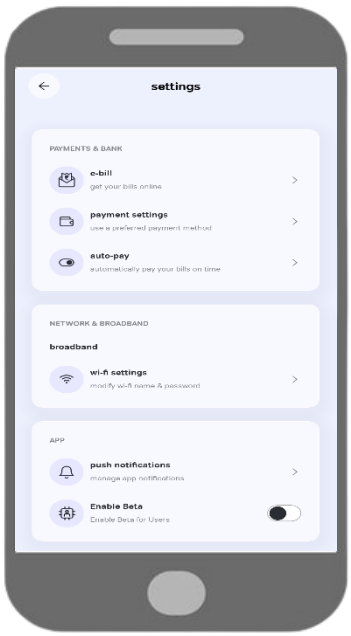


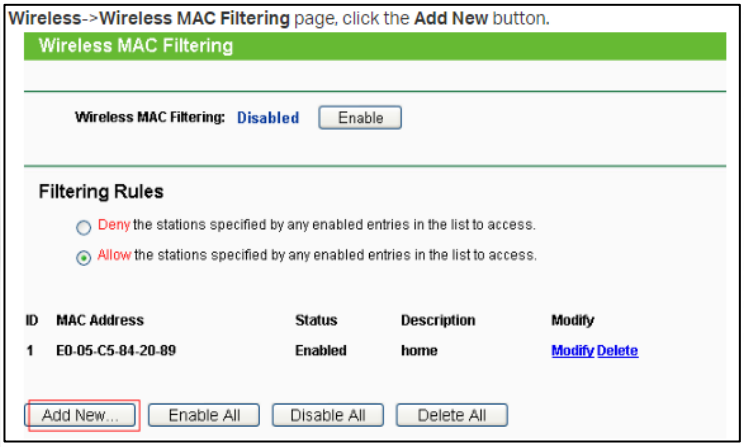
How to Enhance Your WiFi Security?

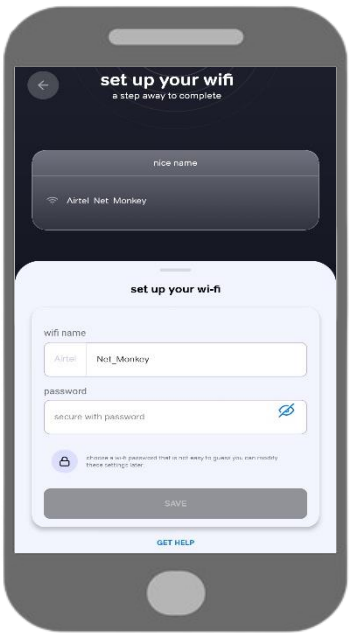
Scammers intercept or hack your computer/devices while they are connected to free/unsecured WiFi in public places such as a hotel room, at a railway station etc. for stealing sensitive personal information (PII) & use it for various cyber crimes.

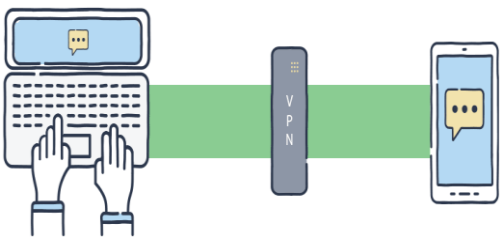
Methods to enhance your WiFi security:

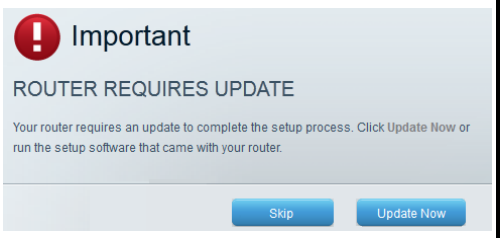
- Always avoid using public Wi-Fi hotspots.
- When you must have to use such Wi-Fi, use VPN to protect the data and the device.
- Don't leave WiFi or Bluetooth of your device turned on when not in use.
- Never do financial transactions, access social media accounts or emails using public Wi-Fi.
- Make your wireless network password unique and strong.
- Always keep your router's software up to date.
- Change the default username and password of your home WiFi router.
- Enable MAC Address Filtering while installing WiFi. It will limit the number of devices that can connect to the home network.









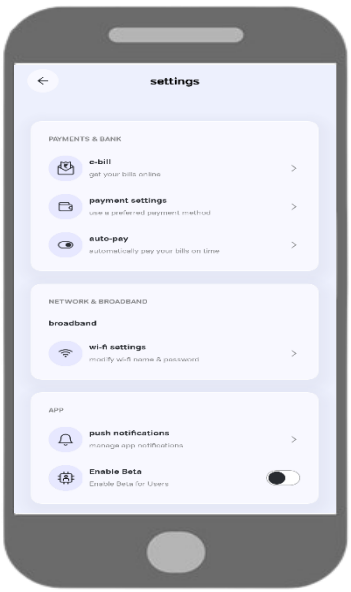


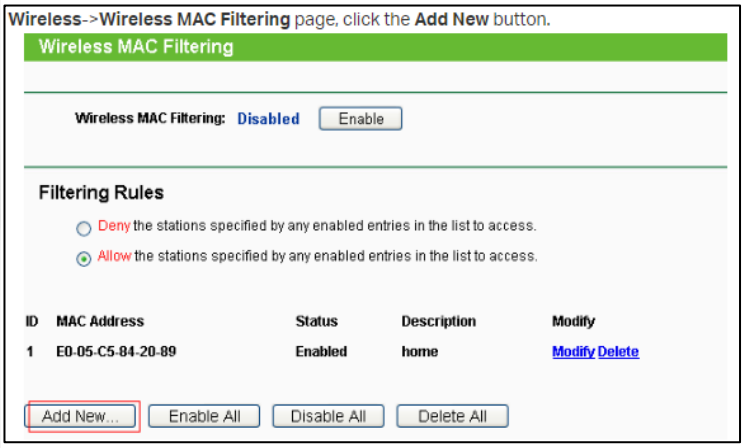
अपनी वाई-फ़ाई की सुरक्षा कैसे बढ़ाएं?

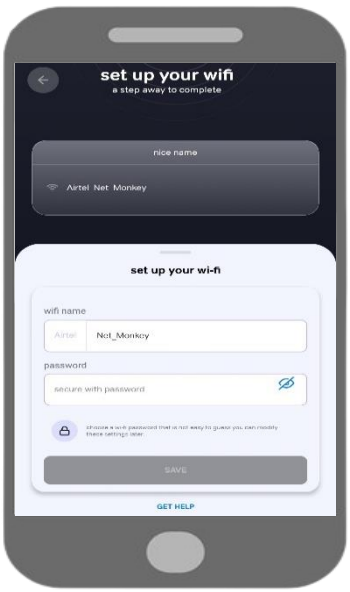
संवेदनशील व्यक्तिगत जानकारी (पीआईआई) चुराने तथा विभिन्न साइबर अपराधों में इसका उपयोग करने के लिए घोटालेबाज सार्वजनिक स्थानों जैसे होटल के कमरे, रेलवे स्टेशन आदि में लगे निःशुल्क/असुरक्षित वाईफाई से जुड़े आपके कंप्यूटर/डिवाइस को बाधित या हैक कर लेते हैं।

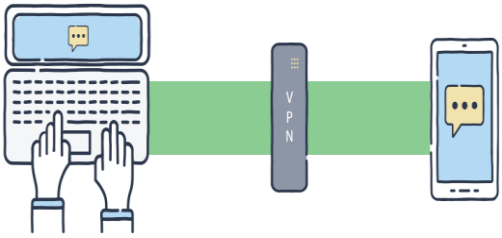
वाईफ़ाई सुरक्षा बढ़ाने के तरीके:

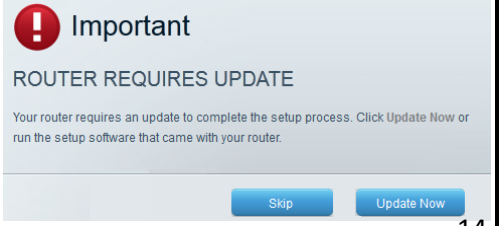
- सार्वजनिक वाई-फाई हॉटस्पॉट का उपयोग करने से हमेशा बचें।
- जब आपको ऐसे वाई- फ़ाई का उपयोग करना अति आवश्यक हो, तो डेटा एवं डिवाइस की सुरक्षा के लिए वीपीएन का उपयोग करें।
- उपयोग में न होने पर अपने डिवाइस का वाई-फ़ाई अथवा ब्लूटूथ बंद रखें।
- सार्वजनिक वाई- फ़ाई का उपयोग करके कभी भी वित्तीय लेनदेन न करें, सोशल मीडिया खातों या ईमेल का इस्तेमाल न करें।
- अपने वायरलेस नेटवर्क पासवर्ड को विशिष्ट एवं मजबूत बनाएं।
- अपने राउटर के सॉफ्टवेयर को हमेशा अपडेट रखें।
- अपने घर में लगे वाईफाई राउटर का डिफ़ॉल्ट उपयोगकर्ता नाम तथा पासवर्ड को बदल लें।
- वाईफाई इंस्टॉल करते समय मैक एड्रेस फ़िल्टरिंग सक्षम करें। यह उन उपकरणों की संख्या को सीमित कर देगा जो होम नेटवर्क से जुड़ सकते हैं।





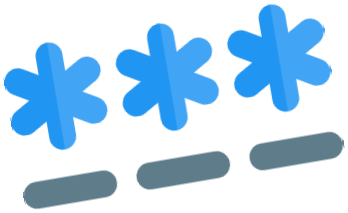






How to Enhance Your Password Security?

Simple and commonly used passwords used in device/accounts (i.e. social media/Email/Banking accounts etc.) enables intruders to easily gain access and control of a computing device/account and perpetrate various cyber crimes.



Methods to enhance your Password security:

- Never use personal information in password.
- Include a combination of letters, numbers, and symbols to make a password stronger.
- Use Strong, Unique Passwords: Avoid using the same password across multiple platforms.
- Change Passwords Regularly. Update your passwords periodically to enhance security.
- Avoid using dictionary words. Hackers use malicious programs to crack it easily.
- Always use multi-factor authentication (MFA).
- Never share your password with anyone.
- Always use virtual key boards on internet sites if available. It saves hijacking of key strokes.
- Make password length of eight characters or more for stronger password.
- Never use one word passwords. Always use long phrases for password.

Strong password	Stronger passwords
Walk2milestoday	WALK2M!LE$2day
Keepitlockeddown	K33p!tL0CK3dD0Wn
learnfromanyone	l3@rNfr0M@ny0n3

How Safe Is Your Password?

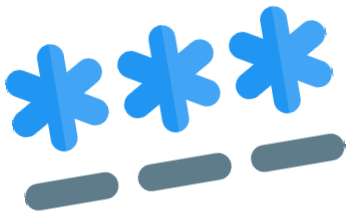
Time it would take a computer to crack a password with the following parameters

Number of Characters	Lowercase Letters Only	At Least One Uppercase Letter	At Lease One Uppercase Letter + Number	At Lease One Uppercase Letter + Number + Symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 minutes	6 minutes
8	Instantly	22 minutes	1 hour	8 hours
9	2 minutes	19 hours	3 days	3 weeks
10	1 hour	1 month	7 months	5 years
11	1 day	5 years	41 years	400 years
12	3 weeks	300 years	2,000 years	34,000 years

Source: Security.org

अपनी पासवर्ड की सुरक्षा को कैसे बढ़ाएं?

डिवाइस/खातों (अर्थात सोशल मीडिया/ईमेल/बैंकिंग खाते आदि) में प्रयुक्त सरल एवं सामान्य पासवर्ड, हैकर्स को कंप्यूटिंग डिवाइस/खाते तक आसानी से पहुँचने तथा उनपर नियंत्रण प्राप्त करने एवं विभिन्न साइबर अपराधों को अंजाम देने में सक्षम बनाते हैं।



पासवर्ड की सुरक्षा बढ़ाने के तरीके:

- पासवर्ड में कभी भी व्यक्तिगत जानकारी का उपयोग न करें।
- पासवर्ड को अधिक मजबूत बनाने के लिए अक्षरों, संख्याओं और प्रतीकों के संयोजन को शामिल करें।
- मजबूत एवं विशिष्ट पासवर्ड का उपयोग करें: एक ही पासवर्ड को कई प्लेटफार्मों पर उपयोग करने से बचें।
- पासवर्ड नियमित रूप से बदलें। सुरक्षा बढ़ाने के लिए समय-समय पर अपने पासवर्ड अपडेट करें।
- शब्दकोश के शब्दों का प्रयोग करने से बचें। हैकर्स विद्वेषपूर्ण प्रोग्राम का उपयोग कर इन्हें आसानी से हासिल कर लेते हैं।
- हमेशा मल्टी-फैक्टर प्रमाणीकरण (MFA) का उपयोग करें।
- अपना पासवर्ड कभी भी किसी के साथ साझा न करें।
- यदि उपलब्ध हो, तो इंटरनेट साइटों पर हमेशा वर्चुअल की-बोर्ड का उपयोग करें। इससे की-स्ट्रोक के हाइजैक से बचा जा सकता है।
- मजबूत पासवर्ड के लिए पासवर्ड आठ अक्षर अथवा उससे अधिक अक्षरों का बनाएँ।
- कभी भी एक शब्द का पासवर्ड न बनाएँ। पासवर्ड के लिए हमेशा एकाधिक शब्दों/अक्षरों/अंकों का उपयोग करें।

Strong password

Walk2milestoday

Keepitlockeddown

learnfromanyone

Stronger passwords

WALK2M!LE$2day

K33p!tL0CK3dD0Wn

l3@rNfr0M@ny0n3

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of Characters	Lowercase Letters Only	At Least One Uppercase Letter	At Lease One Uppercase Letter + Number	At Lease One Uppercase Letter + Number + Symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 minutes	6 minutes
8	Instantly	22 minutes	1 hour	8 hours
9	2 minutes	19 hours	3 days	3 weeks
10	1 hour	1 month	7 months	5 years
11	1 day	5 years	41 years	400 years
12	3 weeks	300 years	2,000 years	34,000 years

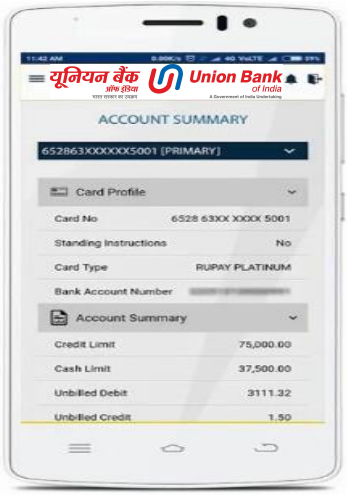
Source: Security.org

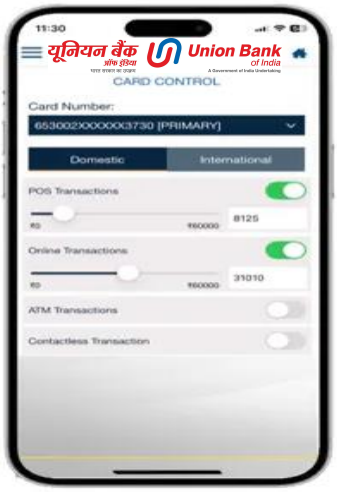
How to Enhance Your Debit/Credit Card Security?

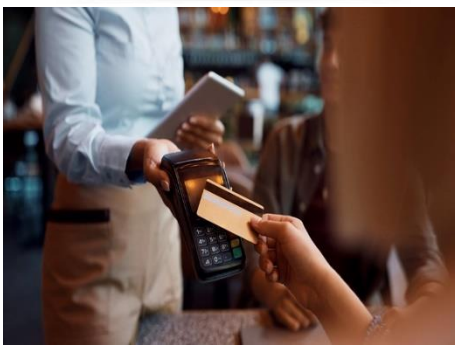
Fraudsters obtain victim's debit/credit card information through various social engineering techniques like skimming at ATM/PoS terminal, physical theft, phishing/vishing/smishing or card swapping at places like restaurants/hotels to siphon off money from the victim.

Methods to enhance your Debit/Credit Card security:

- Enter the PIN yourself in ATM/PoS machines taking due care to hide the PIN.
- Check for hidden cameras/skimmer devices before withdrawing cash.
- Physically check the keypad to ensure it does not have an overlay device.
- Do not allow anyone to stand beside or behind you while carrying out transaction in ATM/PoS.
- Do not keep a PIN which can be guessed easily. Keep changing your card PINs.
- Ensure you get transaction receipt or confirmation through SMS.
- Never hand over your credit/debit card to waiters in Hotels/Restaurants for billing. It can lead to exchange of card and leaking of sensitive credentials like Card details, CVV, Expiry, name & account no. etc.
- Check your card statements regularly to make sure all transactions are genuine.
- Always review your card usage limit & other control settings (like daily transaction limit, PoS, Domestic & International Ecommerce, ATM withdrawal, Tap & Pay etc.) as per your requirement and disable them if not required.
- Always keep your international usage disabled & enable on requirement.





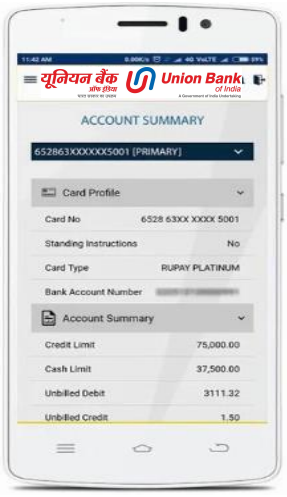


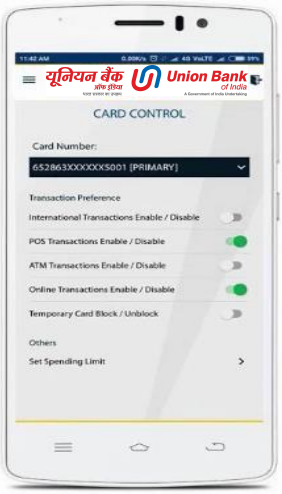
अपने डेबिट/क्रेडिट कार्ड की सुरक्षा कैसे बढ़ाएं?

जालसाज विभिन्न सोशल इंजीनियरिंग तकनीकों, जैसे एटीएम/पीओएस टर्मिनल पर स्कीमिंग, प्रत्यक्ष चोरी, फिशिंग/विशिंग/स्मिशिंग अथवा रेस्तरां/होटल जैसे स्थानों पर कार्ड स्वैपिंग के माध्यम से पीड़ित के डेबिट/क्रेडिट कार्ड की जानकारी प्राप्त करते हैं और पीड़ित से पैसे हड़पने का प्रयास करते हैं।

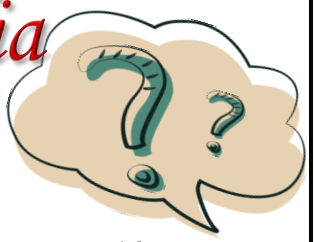
डेबिट/क्रेडिट कार्ड की सुरक्षा बढ़ाने के तरीके:

- एटीएम/पीओएस मशीनों में पिन स्वयं दर्ज करें, तथा पिन छिपाने का पूरा ध्यान रखें।
- नकदी निकालने से पूर्व छिपे हुए कैमरे/स्किमर डिवाइस की जांच अवश्य करें।
- कीपैड की भौतिक जांच करें, सुनिश्चित करें कि उसमें कोई ओवरले डिवाइस तो नहीं है।
- एटीएम/पीओएस में लेनदेन करते समय किसी को भी अपने आस-पास अथवा पीछे खड़ा न होने दें।
- ऐसा पिन न रखें जिसका आसानी से अनुमान लगाया जा सके। अपने कार्ड का पिन निरंतर बदलते रहें।
- सुनिश्चित करें कि आपको एसएमएस के माध्यम से लेनदेन की रसीद अथवा पुष्टि प्राप्त हो गई है।
- होटल/रेस्तरां में बिलिंग के लिए वेटर को अपना क्रेडिट/डेबिट कार्ड कभी न दें। इससे कार्ड के बदलने का जोखिम हो सकता है तथा कार्ड विवरण, सीवीवी, समाप्ति तिथि, नाम एवं खाता संख्या आदि जैसे संवेदनशील क्रेडेंशियल उजागर हो सकते हैं।
- यह सुनिश्चित करने के लिए कि सभी लेनदेन वास्तविक हैं, अपने कार्ड विवरणी की नियमित जांच करें।
- हमेशा अपनी आवश्यकता के अनुसार अपने कार्ड की उपयोग सीमा एवं अन्य नियंत्रण सेटिंग्स (जैसे दैनिक लेनदेन सीमा, पीओएस, अंतर्देशीय व अंतर्राष्ट्रीय ई-कॉमर्स, एटीएम से आहरण, टैप व भुगतान करें आदि) की समीक्षा करें तथा यदि आवश्यक न हो, तो किसी भी साइबर हमले से सुरक्षा के लिए उन्हें अक्षम कर दें।
- अंतर्राष्ट्रीय प्रयोग के विकल्प को हमेशा बंद रखें, आवश्यकता पड़ने पर ही विकल्प सक्षम करें।



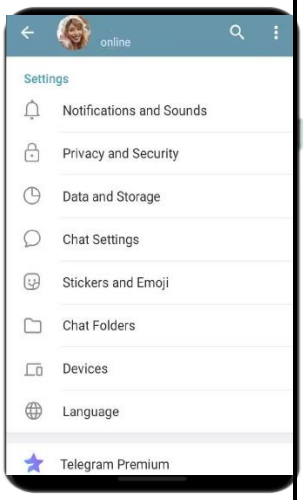


How to Enhance Social Media App Security?



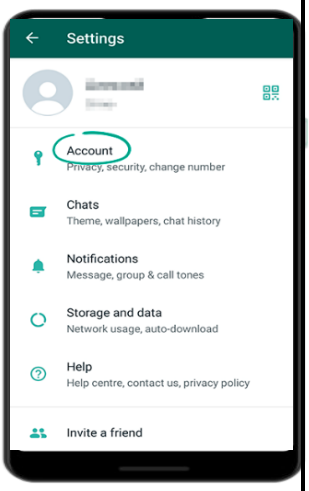
Fraudsters use social media apps like Telegram, WhatsApp, Messenger & other messaging apps to steal money by gathering personal credentials through phishing links, malicious .apk files.

Telegram App Security:



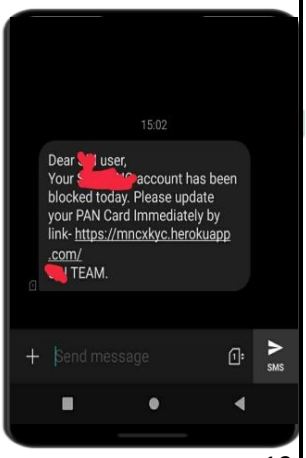
- ✓ Always enable 2 factor authentication in Telegram app (Settings > Privacy and Security > 2-Step Verification).
- ✓ Always use strong password (set up PIN/Password/Pattern lock) for your app.
- ✓ Use private chat option settings to chat in groups without making your phone number visible to others (Settings > Privacy and Security > Phone Number).
- ✓ Never click or download any link, .apk/.ipa file or any suspicious documents received from unsolicited contacts.
- ✓ Never accept group invitations received from unknown senders if you are not sure about it.
- ✓ Always keep your app updated to ensure you have the latest security patches & features.
- ✓ Avoid sharing personal information with unknown contacts as it could lead to attempt of phishing.

WhatsApp Security:



- ✓ Always enable 2 factor authentication for WhatsApp (Settings > Privacy and Security > 2-Step Verification).
- ✓ Never click or download any link, .apk/.ipa file or pdf documents received from unsolicited contacts.
- ✓ Never accept group invitations received from unknown senders if you are not sure about it.
- ✓ Always keep your app updated to ensure you have the latest security patches & features.
- ✓ Avoid sharing personal information with unknown contacts as they could lead to attempt of phishing.
- ✓ Regularly update WhatsApp to the latest version to benefit from security patches and new features.
- ✓ Manage Your Privacy Settings: Go to Settings > Account > Privacy and adjust settings for last seen, profile photo, about and status to limit who can see your information.
- ✓ Always check your Group Privacy settings: Go to Settings > Account > Privacy > Groups to control who can add you to groups.
- ✓ Periodically review your devices linked to your WhatsApp account and remove any that you do not recognize.

Messaging App/SMS Security:



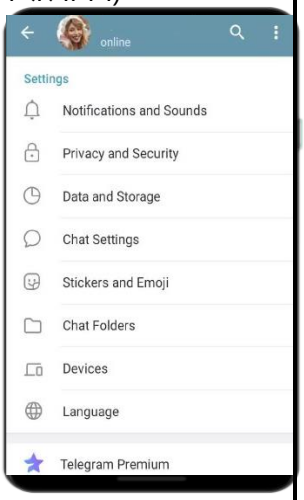
- ✓ Never click or download any link, .apk file or pdf documents received from unsolicited contacts.
- ✓ Always use strong password (set up PIN/Password/Pattern lock).
- ✓ Avoid sharing sensitive personal information through messaging apps unless absolutely necessary.
- ✓ Set a screen lock on your phone to prevent unauthorized access to your messaging app if your device is lost or stolen.
- ✓ Always review access of SMS app requested by other applications. Never give permission if not required.

अपने सोशल मीडिया ऐप्प की सुरक्षा कैसे बढ़ाएं?

जालसाज विभिन्न सोशल मीडिया ऐप्पस्, जैसे टेलीग्राम/व्हाट्सऐप्प, मेसेंजर और अन्य संदेश प्रेषित करने वाले ऐप्पस् और फिशिंग लिंक्स, विद्वेषपूर्ण .apk फाइलों का प्रयोग करके आपकी निजी जानकारी हासिल करके अनाधिकृत तरीके से पैसे चोरी करते हैं।

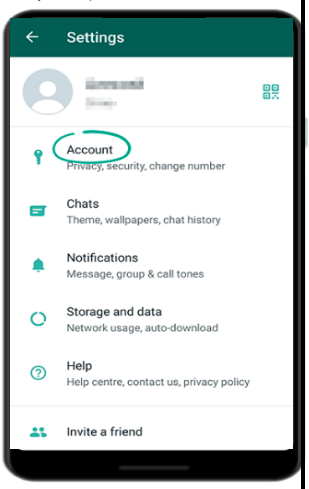
टेलीग्राम ऐप्प सुरक्षा:

- ✓ टेलीग्राम ऐप्प में हमेशा 2 फ़ैक्टर प्रमाणीकरण को सक्षम करें। (सेटिंग्स > प्राइवेसी व सुरक्षा > 2-स्टेप सत्यापन)
- ✓ अपने ऐप्प के लिए कठिन पासवर्ड (पिन/पासवर्ड/ पैटर्न लॉक) का ही प्रयोग करें।
- ✓ दूसरों को अपना नंबर दिखाये बिना समूह में चैट करते वक़्त सेटिंग्स में प्राइवेट चैट विकल्प का प्रयोग करें (सेटिंग्स > प्राइवसी व सुरक्षा > फोन नंबर)।
- ✓ अनचाहे, अनाधिकृत संपर्क सूत्रों से प्राप्त संदिग्ध दस्तावेजों और .apk/.ipa फाइलों पर न क्लिक करें और न ही उन्हें कभी डाउनलोड करें।
- ✓ यदि आप पहले से नहीं जानते हैं तो अज्ञात प्रेषकों के समूह-निमंत्रण को स्वीकार न करें।
- ✓ सुरक्षा पैच और नयी सुविधाओं का लाभ उठाने के लिए व्हाट्सऐप्प को नियमित रूप से नवीनतम संस्करण में अपडेट करें।
- ✓ अज्ञात संपर्क सूत्रों से कभी भी अपनी निजी जानकारी साझा न करें, यह फिशिंग की कोशिश हो सकती है।



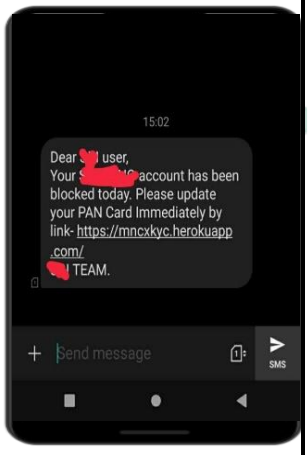
व्हाट्सऐप्प सुरक्षा:

- ✓ व्हाट्सऐप्प के लिए 2 फ़ैक्टर प्रमाणीकरण का प्रयोग करें (सेटिंग्स > प्राइवसी व सुरक्षा > 2-स्टेप सत्यापन)।
- ✓ अज्ञात संपर्क से प्राप्त किसी भी लिंक, .apk/.ipa फ़ाइल या पीडीएफ़ फ़ाइल पर कभी न क्लिक करें, न ही कभी डाउनलोड करें।
- ✓ यदि आप पहले से नहीं जानते हैं तो अज्ञात प्रेषकों के समूह निमंत्रण को कभी स्वीकार न करें।
- ✓ सुरक्षा पैच और नयी सुविधाओं का लाभ उठाने के लिए ऐप्पस् को नियमित रूप से नवीनतम संस्करण में अपडेट करें।
- ✓ अज्ञात संपर्क सूत्रों से कभी भी अपनी निजी जानकारी साझा न करें, यह फिशिंग की कोशिश हो सकती है।
- ✓ अपनी प्राइवसी सेटिंग्स को प्रबंधित करें: सेटिंग्स पर जाएँ > अकाउंट > प्राइवसी > लास्ट सीन के लिए सेटिंग्स में अपेक्षित परिवर्तन करें, प्रोफ़ाइल चित्र, अपने बारे में और स्टेटस (अबाउट और स्टेटस) पर जाकर नियंत्रित करें की आपकी प्रोफ़ाइल की जानकारी कौन-कौन देख सकता है।
- ✓ हमेशा अपनी समूह प्राइवसी सेटिंग की जांच करें: सेटिंग्स पर जाएँ > अकाउंट > प्राइवसी > समूह में जाकर नियंत्रित करें की कौन-कौन आपको समूह में जोड़ सकता है।
- ✓ समय-समय पर अपने व्हाट्सऐप्प अकाउंट से सम्बद्ध डिवाईसेज़ की जांच करें और जिन्हें आप नहीं पहचानते हैं उन्हें हटा दें।



मेसेजिंग ऐप्प/एसएमएस सुरक्षा :

- ✓ अज्ञात संपर्क से प्राप्त किसी भी लिंक, .apk/.ipa फ़ाइल या पीडीएफ़ फ़ाइल पर न क्लिक करें, न ही डाउनलोड करें।
- ✓ अपने ऐप्प के लिए कठिन पासवर्ड (पिन/पासवर्ड/ पैटर्न लॉक) का ही प्रयोग करें।
- ✓ जबतक की अत्यंत आवश्यक न हो तब तक किसी प्रकार की संवेदनशील जानकारी मेसेजिंग ऐप्प के माध्यम से साझा न करें।
- ✓ डिवाइस चोरी होने और खो जाने की स्थिति में अथवा सामान्य स्थितियों में भी अपने मेसेजिंग ऐप्प तक अनाधिकृत पहुँच रोकने के लिए अपने फोन पर स्क्रीन लॉक लगाएँ।
- ✓ हमेशा अन्य एप्लिकेशन द्वारा अनुरोधित एसएमएस ऐप्प की पहुँच की समीक्षा करें। यदि आवश्यक न हो तो कभी भी अनुमति न दें।



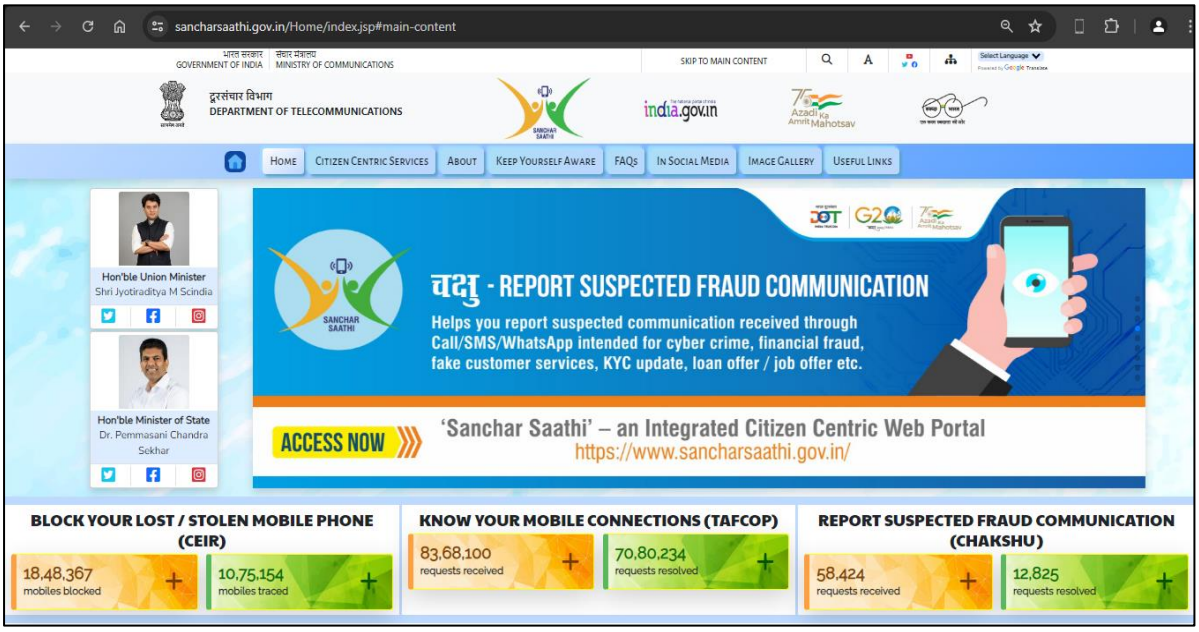
Steps to Report suspected Cyber Fraud communications received through Call, WhatsApp, SMS in CHAKSHU Portal:

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.

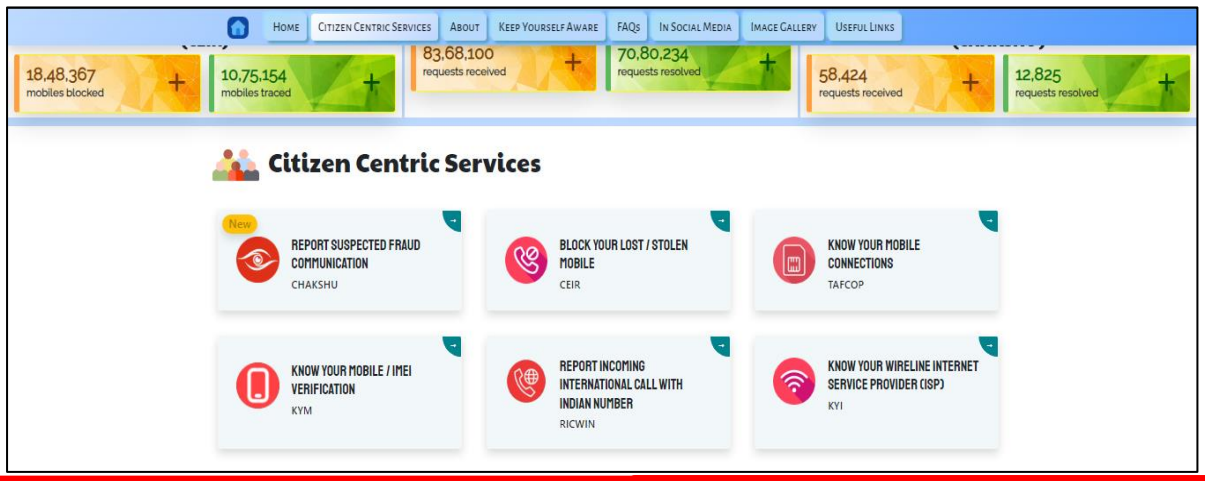
Few examples of suspected fraud communications are communication related to Bank Account / Payment Wallet / SIM / Gas connection / Electricity connection / KYC update / expiry / deactivation, impersonation as Government official / relative, sextortion related etc.

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.

Step 1: Login to the CHAKSHU Portal https://sancharsaathi.gov.in/sfc and select the CHAKSHU option under "Citizen Centric Services".



Step 2: Select the "CHAKSHU" option under "Citizen Centric Services".

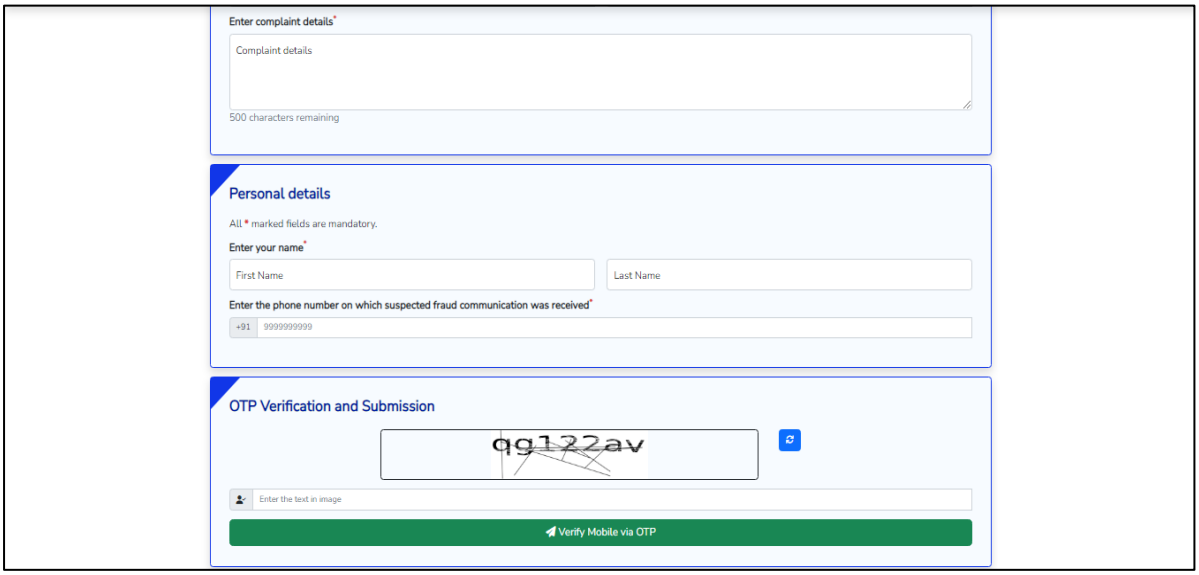


Steps to Report suspected Cyber Fraud in CHAKSHU Portal Cont.

Step 3: Review the uses of CHAKSHU, then click "continue for reporting".

Step 4: Fill out the form with details such as medium, category, timing of the suspected fraud communication received & upload the screenshot of the same.

Step 5: After filling out the form completely, enter the complainants personal details, verify the mobile no. with OTP & then submit.



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.

Indian Cyber Crime Coordination Centre

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

लेटेस्ट अपडेट के लिए फॉलो करें
CYBERDOST

@cyberdost
@CyberDosti4c
@cyberdost.i4c
@cyberdosti4c
@cyberdost
@cyberdosti4c
@cyberdosti4c
@cyberdosti4c
@cyberdost

ऑनलाइन वित्तीय धोखाधड़ी के मामले में
डायल करें 1930

किसी भी साइबर अपराध की शिकायत के लिए रिपोर्ट करें
WWW.CYBERCRIME.GOV.IN

SCAN QR TO VISIT

FOLLOW US !

@unionbankofindia @UnionBankTweets unionbankinsta @UnionBankofIndiaUtube @unionbankofIndia @unionbankinsta