NEIGRIHMS
पूर्वोत्तर इंन्दिरा गांधी क्षेत्रीय स्वास्थ एवं आयुर्विज्ञान संस्थान शिलांग
NORTH EASTERN INDIRA GANDHI REGIONAL INSTITUTE OF HEALTH & MEDICAL SCIENCES, SHILLONG
(भारत सरकार स्वास्थ एवं परिवार कल्याण मंत्रालय स्वायत संस्थान)
(An Autonomous Institute, Ministry of Health and Family Welfare, Government of India)
निदेशक ब्लॉक मावडीयांगडीयांग, शिलांग - 793018 मेघालय
Director's Block, Mawdiangdiang, Shillong – 793018 Meghalaya
www.neigrihms.gov.in
EPABX : (0364) 2538025

No. : **ITCELL-CYBS/1/2026-ITCell**

CIRCULAR

Subject: National Cyber Security Awareness Month – October

As per D.O. No. 46/92/2020-NSCS(CS) dated 19.09.2025, October is observed annually as National Cyber Security Awareness Month (NCSAM) to promote cyber hygiene and cyber security best practices.

In this regard, the Cyber Security Cell, Ministry of Health & Family Welfare (MoHFW), has issued the following advisories to strengthen cyber security awareness and promote best practices among all employees of the Institute:

1. General Cyber Security Guidelines
2. Cyber Fraud – Do's and Don'ts
3. Cyber Security Awareness Posters issued by CERT-In

All Departments/Sections are requested to circulate the enclosed advisories among their employees for information and necessary compliance. The advisories will also be made available on the Institute's website and e-Office Notice Board for wider dissemination.

These advisories are aimed to strengthen cyber awareness and promote best practices among all employees of the Institute. Therefore, all employees are advised to adhere to the prescribed guidelines to enhance cyber security and safeguard the Institute's digital infrastructure.

Digitally signed by
David Teirylang Umdor
Date: 17-11-2026
15:15:38

D. T. Umdor
Deputy Director (Admn.)

Memo No. ITCELL-CYBS/1/2026-ITCell

Copy to:-

1. All HoDs/Section Heads/In-charge for information and necessary circulation in their respective Department.
2. The P.A. to Director for kind information of Director.
3. The P.A. to the Medical Superintendent, Shillong for kind information of Medical Superintendent and wide circulation in the Department/Section/Unit under direct control of MS.
4. The P.A to the Dean, for kind information of Dean and wide circulation in Academic Department.

General Cyber Security Guidelines

Cybersecurity Do's



1 Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers, and special characters. Change your passwords at least once in 45 days. Use multi-factor authentication, wherever available.

2 Maintain an offline backup of your critical data.

3 Keep your Operating System and BIOS firmware updated with the latest updates/patches.



4 Install enterprise antivirus client offered by the government on your official desktops/laptops. Ensure that the antivirus client is updated with the latest virus definitions, signatures, and patches.

5 Use authorized and licensed software only.

6 When you leave your desk temporarily, always lock/log-off from your computer session.

7 When you leave office, ensure that your computer and printers are properly shutdown.



8 Keep your printer's software updated with the latest updates/patches.

9 Setup unique passcodes for shared printers.

10 Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centers.

11 Keep the GPS, Bluetooth, NFC, and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.



12 Download Apps from official app stores of google (for android) and apple (for iOS).

13 Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.

14 Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/ malware webpage, which could compromise your device.

15 Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in

16 Adhere to the security advisories published by NIC-CERT (https://nic-cert.nic.in/advisories.jsp) and CERT-In (https://www.cert-in.org.in).

Cybersecurity Don'ts



1 Don't use the same password in multiple services/websites/apps.

2 Don't save your passwords in the browser or in any unprotected documents.

3 Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material.

4 Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.



5 Don’t install or use any pirated software.
6 Don’t open any links or attachments contained in the emails sent by any unknown sender.
7 Don’t disclose any sensitive details on social media or 3rd party messaging apps.
8 Don’t share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.



9 Don’t plug-in any unauthorized external devices, including USB drives shared by any unknown person.

Source: *Ministry of Electronics and Information technology Cybersecurity Guidelines*

Cyber Fraud Do’s and Don’ts

Below is a list of the Do’s and Don’ts of Cyber Fraud:

- Beware of Cyber Fraud.
  - Cyber Fraudsters can generate authentic-looking phishing emails, text messages, or websites that trick users to reveal sensitive information, such as login credentials, financial details or personal data.
  - It can create deceptive messages to trick users to click on malicious links/attachments leading to malware infections.
  - It can imitate human conversation with users to share sensitive information or to perform harmful actions.
  - It can help hackers create fraudulent documents, invoices, or payment requests for financial scams.
- Don’t click on links/attachments from unknown sources.
- Always verify the authenticity of calls, emails or messages, especially those asking for sensitive information or financial transactions.
- Contact the organization directly through their official channels to validate such requests.
- Regularly update security software, install patches, and use genuine antivirus programs to protect against potential threats.
- Online Portal for filing complaint online at **cybercrime.gov.in**. Cyber fraud can be reported directly at helpline number **1930**.
- Never attend the calls looking similar to toll-free number of any bank or unauthorized company.
- Always visit the official website of the bank or any authorized company and verify the number from which the call/ SMS has been received.
- Never share OTP, PIN, CVV, Debit/Credit card details with anyone.
- Do not share any OTP/UPI PIN for receiving with money.
- Do not respond to any calls asking to confirm or share bank account, credit/debit card details or sensitive information.

सत्यमेव जयते

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE

Cyber Security Awareness



Protect yourself from UPI fraud

Keep your UPI-PIN/OTP confidential

Safety Tips

Fraudsters employ techniques such as sending harmful QR codes, malicious apps, user impersonation etc.

- Always check the UPI ID/number of the payee before making the payment.
- Never share UPI Pin/OTP with anyone.
- Enter UPI pin/OTP on UPI app page only.
- Scanning QR code or entering UPI pin is only for making Payments and not for receiving money.
- Pay attention and carefully check all messages received through all communication channels from your bank.
- Know the difference between sending and receiving money using UPI apps.
- Use UPI help option in the application for transaction related concerns.

Security is our first priority



Beware of FraudGPT Scam

FraudGPT, an AI-powered Chatbot is used by Cyber criminals to craft fraudulent content for cyber frauds and crimes.

Modus Operandi

- FraudGPT can generate authentic-looking phishing emails, text messages, or websites that trick users to reveal sensitive information, such as login credentials, financial details, or personal data.
- It can create deceptive messages to trick users to click on malicious links/attachments leading to malware infections.
- It can imitate human conversation with users to share sensitive information or to perform harmful actions.
- It can help hackers create fraudulent documents, invoices, or payment requests for financial scams.

Safety Tips

- Avoid clicking on links/ attachments from unknown sources.
- Always verify the authenticity of calls, emails or messages, especially those asking for sensitive information or financial transactions.
- Contact the organization directly through their official channels to validate such requests.
- Regularly update security software, install patches, and use genuine antivirus programs to protect against potential threats.

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

सत्यमेव जयते

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE

Cyber Security Awareness



» BEWARE OF OTP FRAUDS

Safety Tips

- Never Attend the calls looking similar to toll-free number of any bank or authorized company.
- Do not share any personal information like credit/ debit card details, CVV, OTP, account number, date of birth, expiry date of debit/credit cards etc. to unknown caller.
- Always visit the official website of the bank or any authorized company and verify the number from which the call/ SMS has been received.
- Do not get tricked and give your OTP's on phone calls, emails, and SMS for the sake of cashbacks or to claim for reward points or any such offers etc.
- Banks never ask for CVV, OTP, PIN or any personal information over phone, email and SMS.



Beware of Morphing

Morphing is altering or changing the pictures of the person using morphing tools available online. Young girls and women usually fall prey at the hands of the online criminals, who use their photographs posted online and misuse these images by morphing the pictures.

The morphed pictures are then used by perpetrators for blackmailing the victims, creating fake online profile, sexting, sex chats, pornographic content, nude pictures etc.,

Morphing can damage the victim's online reputation and cause emotional trauma, can also be prone to threats from perpetrators and may fall prey to their attempts at blackmailing them.

Safety Tips

- Enable your security and privacy features on social media accounts
- Never share your personal pictures online publicly on social media accounts
- Use watermark while sharing pictures
- Enable multi-factor authentication with strong passwords for your social media accounts.
- Save the evidence and the screen shots for referring to the incident later.
- Don't suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.
- If you observe your fake profile or any such objectionable posts in social media, report to the respective social media help centre .

eHealth Section

Report Cyber fraud Incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

सत्यमेव जयते

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE

Cyber Security Awareness



» BEWARE OF OTP FRAUDS

Safety Tips

- Never Attend the calls looking similar to toll-free number of any bank or authorized company.
- Do not share any personal information like credit/ debit card details, CVV, OTP, account number, date of birth, expiry date of debit/credit cards etc. to unknown caller.
- Always visit the official website of the bank or any authorized company and verify the number from which the call/ SMS has been received.
- Do not get tricked and give your OTP's on phone calls, emails, and SMS for the sake of cashbacks or to claim for reward points or any such offers etc.
- Banks never ask for CVV, OTP, PIN or any personal information over phone, email and SMS.



Beware of Morphing

Morphing is altering or changing the pictures of the person using morphing tools available online. Young girls and women usually fall prey at the hands of the online criminals, who use their photographs posted online and misuse these images by morphing the pictures.

The morphed pictures are then used by perpetrators for blackmailing the victims, creating fake online profile, sexting, sex chats, pornographic content, nude pictures etc.,

Morphing can damage the victim's online reputation and cause emotional trauma, can also be prone to threats from perpetrators and may fall prey to their attempts at blackmailing them.

Safety Tips

- Enable your security and privacy features on social media accounts
- Never share your personal pictures online publicly on social media accounts
- Use watermark while sharing pictures
- Enable multi-factor authentication with strong passwords for your social media accounts.
- Save the evidence and the screen shots for referring to the incident later.
- Don't suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.
- If you observe your fake profile or any such objectionable posts in social media, report to the respective social media help centre .

eHealth Section

Report Cyber fraud Incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

सत्यमेव जयते

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE

Cyber Security Awareness



Safety Tip

- An essential step in preventing and identifying infections is installing antivirus and anti malware software solutions from trustworthy vendors.
- Malicious applications and files can be detected by antivirus and anti-malware solutions, which defends your devices from getting infected.
- Never click on any links in third party websites, emails, chats for downloading antivirus and anti-malware solutions.
- Directly visit the vendor's website and install the antivirus and anti-malware solutions.
- Keep your antivirus and anti-malware solutions updated since attackers are always producing new types of malicious code.
- Keep your operating system updated.



Beware of Malicious Android apps

- Malicious android apps can access messages, steal user data and credentials.
- Such apps may autosubscribe to different apps and download unnecessary apps.

Safety Tips

- Before downloading a mobile application check for play protect feature on Play Store.
- Always download applications only from trusted sources like legitimate websites or authorized app store.
- Avoid downloading apps from SMS, APIs, emails, social media messages.
- Allow only necessary permissions during the installation of apps.
- Properly verify the app details in the developer's website before downloading.
- Pay attention to reviews and comments of the users, before installing any mobile application.

eHealth Section

Report Cyber fraud Incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE

Cyber Security Awareness

Always Install and Update antivirus software In Your System



Safety Tip

- An essential step in preventing and identifying infections is installing antivirus and anti malware software solutions from trustworthy vendors.
- Malicious applications and files can be detected by antivirus and anti-malware solutions, which defends your devices from getting infected.
- Never click on any links in third party websites, emails, chats for downloading antivirus and anti-malware solutions.
- Directly visit the vendor's website and install the antivirus and anti-malware solutions.
- Keep your antivirus and anti-malware solutions updated since attackers are always producing new types of malicious code.
- Keep your operating system updated.



Beware of Malicious Android apps

- **Malicious android apps can access messages, steal user data and credentials.**
- **Such apps may autosubscribe to different apps and download unnecessary apps.**

Safety Tips

- **Before downloading a mobile application check for play protect feature on Play Store.**
- **Always download applications only from trusted sources like legitimate websites or authorized app store.**
- **Avoid downloading apps from SMS, APIs, emails, social media messages.**
- **Allow only necessary permissions during the installation of apps.**
- **Properly verify the app details in the developer's website before downloading.**
- **Pay attention to reviews and comments of the users, before installing any mobile application.**

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE

Cyber Security Awareness



! Vishing Alert !
Beware of fraudulent calls

- Fraudsters contact the victim pretending to be calling from trusted sources like bank/ income tax/ Gas agency etc.
- They ask victim's for bank account details & collect financial information about debit/credit cards, expiry date etc.
- The fraudster tells the victim to share OTP sent on mobile for depositing the amount.
- Once the victim shares the OTP, money is deducted from their account.

Safety Tips

- Never share OTP, PIN, CVV, Debit/Credit card details with anyone.
- Do not share any OTP/UPI PIN for receiving money.
- Do not respond to any calls asking to confirm or share bank account, credit/debit card details or sensitive information.
- Do not provide personal information in order to recieve prize/ lottery/ gifts/ updating KYC etc.,
- Do not call the numbers of service providers randomly found in search engines as they can be fake numbers.
- Use the customer care service numbers available on authorized websites of the institute/ organisations/ banks etc.
- Incase of any incident user should change password of account immediately or block the card/ freeze the account to prevent financial loss and also inform your bank.
- Users should routinely review bank & credit card statement & report any irregularities.
- Beware of calls ashing to share personal information or ashing to install any remote access apps on the pretext of helping.



BEWARE OF ONLINE EXTORTION

Sextortion is an emerging form of online abuse.
It occurs when a cybercriminal reaches out to a victim online through a dating app, social media channel, etc.
In many cases, Cyber criminals initiate intimate video chats and lures the victim to pose nude in front of camera and record the same to blackmail the victim.
Sextortion attempts to harass, embarrass and blackmail the victims for financial gains.

Modus Operandi

- **Sextortion can be done through social media apps** : Cyber criminals open fake accounts on social media apps. Victims, thinking the account is genuine, start chatting/ video calling and pose nude in front of the Cyber criminal, who records and take pictures. Later, Cyber criminals black mail them by revealing their intimate pictures/ videos.
- **Through porn sites**: Users of porn sites are sent blackmailing e-mail messages by cyber criminals. Victims are threatened to make their activity on porn sites public and asked to pay money (usually in cryptocurrency).

Safety Tips

- Never share intimate pictures over online video calls/ social media platforms with anybody. It can be used for blackmailing and seeking money from you.
- Avoid clicking intimate/ nude/ semi-nude photos/videos on your phone, which if leaked could cause embarrassment.
- Malicious mobile apps with access permission to gallery/ storage can access your photos and can be used to blackmail you.
- Report sextortion to the nearby police station or on www.cybercrime.gov.in immediately.
- Don't hesitate to file a complaint or to contact the police.
- Use the "Report User" option over social media platforms to report any such accounts.
- Don't click on any links/download any apps received through chats, social media posts.
- Provide only necessary access permissions to apps in your mobile.

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE

Cyber Security Awareness



BEWARE OF OTP FRAUDS

Safety Tips

- Never Attend the calls looking similar to toll-free number of any bank or authorized company.
- Do not share any personal information like credit/ debit card details, CVV, OTP, account number, date of birth, expiry date of debit/credit cards etc. to unknown caller.
- Always visit the official website of the bank or any authorized company and verify the number from which the call/ SMS has been received.
- Do not get tricked and give your OTP's on phone calls, emails, and SMS for the sake of cashbacks or to claim for reward points or any such offers etc.
- Banks never ask for CVV, OTP, PIN or any personal information over phone, email and SMS.



Beware of Morphing

Morphing is altering or changing the pictures of the person using morphing tools available online. Young girls and women usually fall prey at the hands of the online criminals, who use their photographs posted online and misuse these images by morphing the pictures.

The morphed pictures are then used by perpetrators for blackmailing the victims, creating fake online profile, sexting, sex chats, pornographic content, nude pictures etc.,

Morphing can damage the victim's online reputation and cause emotional trauma, can also be prone to threats from perpetrators and may fall prey to their attempts at blackmailing them.

Safety Tips

- Enable your security and privacy features on social media accounts
- Never share your personal pictures online publicly on social media accounts
- Use watermark while sharing pictures
- Enable multi-factor authentication with strong passwords for your social media accounts.
- Save the evidence and the screen shots for referring to the incident later.
- Don't suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.
- If you observe your fake profile or any such objectionable posts in social media, report to the respective social media help centre .

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE

Cyber Security Awareness



Protect yourself from UPI fraud

Keep your UPI-PIN/OTP confidential

Safety Tips

Fraudsters employ techniques such as sending harmful QR codes, malicious apps, user impersonation etc.

- Always check the UPI ID/number of the payee before making the payment.
- Never share UPI Pin/OTP with anyone.
- Enter UPI pin/OTP on UPI app page only.
- Scanning QR code or entering UPI pin is only for making Payments and not for receiving money.
- Pay attention and carefully check all messages received through all communication channels from your bank.
- Know the difference between sending and receiving money using UPI apps.
- Use UPI help option in the application for transaction related concerns.



Beware of FraudGPT Scam

FraudGPT, an AI-powered Chatbot is used by Cyber criminals to craft fraudulent content for cyber frauds and crimes.

Modus Operandi

- FraudGPT can generate authentic-looking phishing emails, text messages, or websites that trick users to reveal sensitive information, such as login credentials, financial details, or personal data.
- It can create deceptive messages to trick users to click on malicious links/attachments leading to malware infections.
- It can imitate human conversation with users to share sensitive information or to perform harmful actions.
- It can help hackers create fraudulent documents, invoices, or payment requests for financial scams.

Safety Tips

- Avoid clicking on links/ attachments from unknown sources.
- Always verify the authenticity of calls, emails or messages, especially those asking for sensitive information or financial transactions.
- Contact the organization directly through their official channels to validate such requests.
- Regularly update security software, install patches, and use genuine antivirus programs to protect against potential threats.

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE



Debit/Credit Card Fraud

Debit and Credit Card Fraud occurs when your card details are used without your consent for unauthorised transactions. Criminals may steal your physical card, skim your details, or trick you into sharing sensitive information through phishing scams.

✓ Dos:

- **Deactivate Unused Features:** Turn off online, international, or NFC transactions when not needed.
- **Check Before You Pay:** Verify the amount on the screen before entering your PIN and check pos machine for skimming device.
- **Keep Your Card in Sight:** Always watch your card during transactions.
- **Shield Your PIN:** Cover the keypad when entering your PIN at ATMs or POS machines.

✗ Don'ts:

- **Don't Share Details:** Never share card information or PIN with anyone.
- **Don't Store PIN:** Avoid writing down or saving your PIN in easy-to-access places.
- **Avoid Public Wi-Fi:** Don't use your card on unsecured networks.
- **Don't Ignore Alerts:** Report suspicious transactions to your bank immediately.



Online Job Scam

Online Job Scams trick people looking for work. Scammers post fake jobs on websites, social media, or send emails, offering high pay and easy work. Their goal is to steal the victim's money or personal information.

✓ Dos:

- **Use Trusted Sources:** Refer to newspapers, job portals, or government portals for authentic private and government job listings.
- **Check Credentials:** For international job offers, verify the company's credentials and ensure you have the correct work visa.
- **Ask Questions:** During online interviews, ask detailed questions about the company and the interviewer.
- **Verify Emails:** Look out for email addresses that mimic genuine companies. For e.g., info@company.net in place of info@company.com.

✗ Don'ts:

- **Avoid Upfront Fees:** Do not pay any consulting fees without verifying the company's legitimacy.
- **Be Skeptical:** Do not trust sponsored search results or unsolicited job emails blindly.
- **Verify Advertisements:** Never apply for jobs without verifying the authenticity of advertisements, especially on social media platforms or groups.

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE



SMS, Email & Call Scams

SMS, Email, and Call Scams are used by fraudsters to deceive victims with fake offers. They impersonate trusted NDFCs by using their logos and fake IDs, gaining credibility. Scammers may send counterfeit sanction letters or cheques, asking for upfront payments. Once the payment is made, the fraudsters disappear with the money.

✓ Dos:

- **Verify Authenticity:** Always cross-check sender details and contact official sources directly.
- **Report Suspicious Messages:** Forward any fake messages to official reporting channels and warn others.

× Don'ts:

- **Don't Trust Unsolicited Offers:** Never trust loan offers via phone, email, or text without verification.
- **Don't Share Sensitive Info:** Avoid giving personal or financial details without confirming the legitimacy of the offer.
- **Don't Click Links or Open Suspicious Emails:** Don't click on links or open emails from unknown sources with attachments or links.
- **Don't Pay Upfront Fees:** Genuine lenders don't require upfront payments for loan processing.



Quishing

Quishing Scams are on the rise. The scammer lure victims with promises of deals or convenience by asking to scan QR codes but ultimately initiate unauthorised financial transactions. Malicious codes can redirect users to phishing sites, steal login credentials, or transfer money directly to the scammer's account.

✓ Dos:

- **Scan Trusted Sources:** Only scan QR codes from official websites or verified businesses.
- **Verify Before Acting:** Scammers often create urgency—take your time to verify.
- **Report Suspicious Codes:** If you suspect a scam, report the code to the legitimate source and relevant authorities.

× Don'ts:

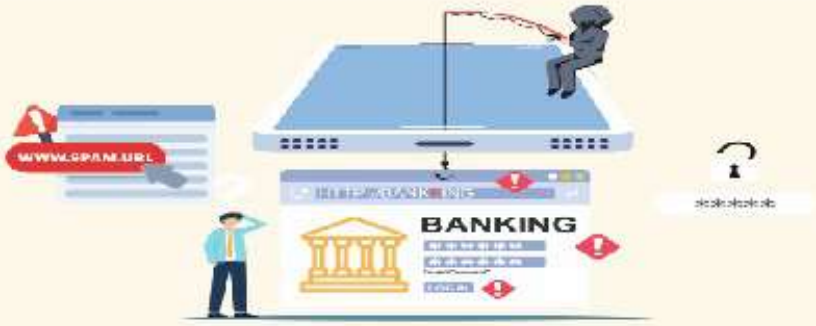
- **Be Cautious with Payments:** Avoid scanning QR codes with payment apps, as they may contain embedded account details for fraudulent transfers.
- **Don't Scan to Receive Money:** Never scan QR codes to receive funds. Legitimate transactions don't require scanning codes or entering banking details like m-PIN or passwords.
- **Avoid Unknown Sources:** Don't scan codes from emails, texts, or unfamiliar sources.

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE



Secure Browsing

Secure Browsing involves using practices and tools to protect yourself from online threats like phishing, malware, and identity theft while surfing the internet. It ensures safer interactions with websites and reduces cyber risks.

✓ Dos:

- **Use Secure Browsers:** Always browse with updated, secure browsers and ensure sites use HTTPS.
- **Install Antivirus:** Protect your device with trusted antivirus software.
- **Verify URLs:** Check website links before entering sensitive information.
- **Enable Firewalls:** Use firewalls for an added layer of security.

✗ Don'ts:

- **Avoid Clicking Unknown Links:** Stay away from unverified or suspicious links.
- **Be Cautious on Public Wi-Fi:** Don't use unsecured public Wi-Fi without protection.
- **Don't Save Passwords on Public Devices:** Avoid storing login credentials on shared or public computers.
- **Skip Unsafe Sites:** Don't ignore browser warnings and avoid visiting flagged or unsecured websites.



Digital Arrest

Digital Arrest is when someone is detained or restricted through digital means (like video calls) instead of traditional physical arrest methods. This often involves scammers impersonating government officials to extort money.

✓ Dos:

- **Know the Facts:** Police or government officials never conduct interrogations via video calls.
- **Don't Share Personal Info:** No government official will ask for money or personal details via video calls.
- **Stay Calm:** If you receive such calls, report them immediately on the "Report Suspect Tab" of cybercrime.gov.in.
- **Understand the Law:** There is no such thing as a "digital arrest" process in India.

✗ Don'ts:

- **Don't Panic:** Stay calm and avoid falling for scams.
- **Don't Give In to Scammers:** Don't send money if someone pressures you through a video call.
- **Don't Engage for Long:** Avoid getting trapped in long video calls that seem suspicious.
- **Don't Trust Unverified Calls:** Ignore any video calls claiming to be from government authorities asking for money.

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE



Phishing

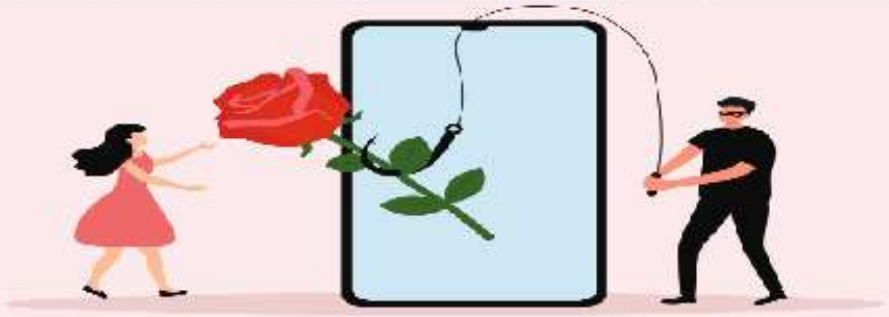
Phishing is a common cybercrime tactic that deceives victims into clicking on fake links. These links appear as emails or websites from trusted sources but redirect users to fraudulent sites designed to steal sensitive data, such as login credentials, personal information, or financial details. Phishing can also install malware, giving cybercriminals unauthorised access to your device.

✓ Dos:

- **Be Suspicious:** Treat unexpected messages from known sources with caution.
- **Check URLs:** Hover over links to reveal the genuine destination and spot discrepancies.
- **Verify Senders:** Contact the sender through a trusted method if you're unsure about a message's authenticity.
- **Update Regularly:** Keep your software and systems up-to-date to close security gaps.
- **Phishing Report:** Alert the relevant authorities or platforms if you encounter phishing attempts.

× Don'ts:

- **Avoid Clicking Links:** Don't click on suspicious links; delete messages from unknown senders immediately.
- **Unsubscribe & Block:** Unsubscribe from emails with suspicious links and block the sender's email.
- **Visit Official Websites:** Always go directly to the official website for financial transactions and verify website security (HTTPS with a padlock).



Social Media Impersonation

Social Media Impersonation happens when someone sets up a fake account mimicking a real person or organisation. These fraudulent accounts are used to deceive others, often leading to identity theft, financial scams, reputational damage, and the spread of false information.

✓ Dos:

- **Verify Accounts:** Look for blue checkmarks, consistent usernames, and familiar profile pictures to confirm authenticity.
- **Be Cautious:** Avoid unsolicited messages and never share personal details or click suspicious links.
- **Report Impersonation:** Inform the platform and the real person or organisation being impersonated.

× Don'ts:

- **Confirm Fund Requests:** Verify requests for money from friends or relatives through a phone call or in-person meeting.
- **Don't Make Payments:** Avoid paying unknown individuals online and untrusted / unverified charities.
- **Keep Info Private:** Never share personal or confidential details on social media.

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in

सत्यमेव जयते

स्वास्थ्य एंव परिवार कल्याण मंत्रालय
MINISTRY OF HEALTH AND FAMILY WELFARE



Phishing

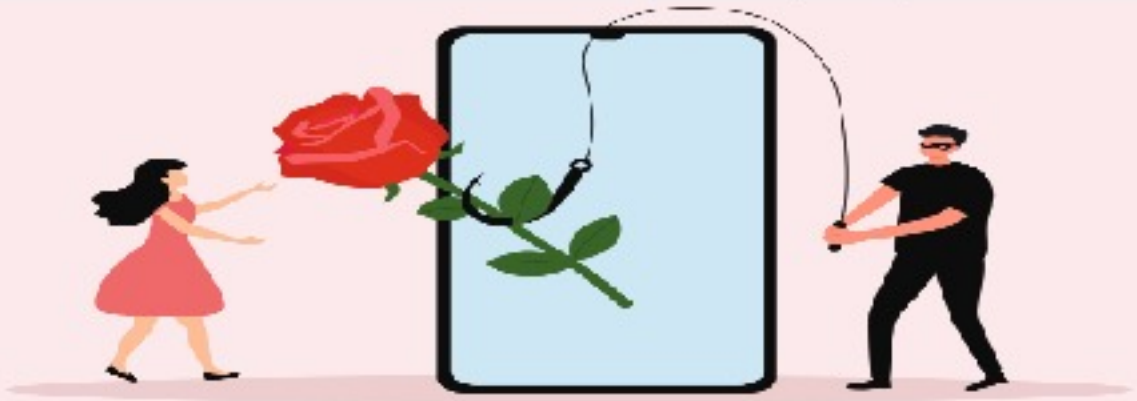
Phishing is a common cybercrime tactic that deceives victims into clicking on fake links. These links appear as emails or websites from trusted sources but redirect users to fraudulent sites designed to steal sensitive data, such as login credentials, personal information, or financial details. Phishing can also install malware, giving cybercriminals unauthorised access to your device.

✓ Dos:

- **Be Suspicious:** Treat unexpected messages from known sources with caution.
- **Check URLs:** Hover over links to reveal the genuine destination and spot discrepancies.
- **Verify Senders:** Contact the sender through a trusted method if you're unsure about a message's authenticity.
- **Update Regularly:** Keep your software and systems up-to-date to close security gaps.
- **Phishing Report:** Alert the relevant authorities or platforms if you encounter phishing attempts.

✗ Don'ts:

- **Avoid Clicking Links:** Don't click on suspicious links; delete messages from unknown senders immediately.
- **Unsubscribe & Block:** Unsubscribe from emails with suspicious links and block the sender's email.
- **Visit Official Websites:** Always go directly to the official website for financial transactions and verify website security (HTTPS with a padlock).



Social Media Impersonation

Social Media Impersonation happens when someone sets up a fake account mimicking a real person or organisation. These fraudulent accounts are used to deceive others, often leading to identity theft, financial scams, reputational damage, and the spread of false information.

✓ Dos:

- **Verify Accounts:** Look for blue checkmarks, consistent usernames, and familiar profile pictures to confirm authenticity.
- **Be Cautious:** Avoid unsolicited messages and never share personal details or click suspicious links.
- **Report Impersonation:** Inform the platform and the real person or organisation being impersonated.

✗ Don'ts:

- **Confirm Fund Requests:** Verify requests for money from friends or relatives through a phone call or in-person meeting.
- **Don't Make Payments:** Avoid paying unknown individuals online and Untrusted / unverified charities.
- **Keep Info Private:** Never share personal or confidential details on social media.

eHealth Section

Report Cyber fraud incident to https://www.cybercrime.gov.in or call 1930

For more safety tips visit: https://www.cert-in.org.in and https://www.csk.gov.in