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 व्लॉक मावडीयांगडीयांग, शिलांग - 793018 मेघालय
Director's Block, Mawdiangdiang, Shillong – 793018 Meghalaya
www.neigrihms.gov.in
EPABX : (0364) 2538025

No. :ITCELL-CYBS/1/2024-ITCell **Dated __ May, 2025**

CIRCULAR

Subject: Cyber Security Advisories - precautionary measures that must be undertaken in view of the prevailing situation.

In view of the prevailing situation, and as a precautionary measure, the Cyber Security Cell, Ministry of Health & Family Welfare (MoHFW), has issued the following advisories for awareness and necessary compliance by all departments. These advisories aim to strengthen cyber awareness and promote best practices among all employees of the Institute.

The following Advisories have been received and are to be disseminated:

1. Cybersecurity Do's
2. Cybersecurity Don'ts
3. Cyber Fraud Do's and Don'ts
4. Eight (8) Cyber Security Awareness Posters issued by CERT-In

In this regard, all departments/sections are requested to **circulate the above advisories (enclosed herewith)** for necessary information and compliance.

All employees are advised to adhere to the guidelines to enhance cyber security awareness and safeguard digital infrastructure.

This issues with the approval of the competent authority.

Signed by Pawan Deep
Date: 15-05-2025 18:03:32
Lt.Cdt.Pawan Deep
Deputy Director (Admn.)

Memo No. ITCELL-CYBS/1/2024-ITCell **Dated __ May, 2025**

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.
5. The Assistant Registrar, Estt-III & GAD to arrange for printing of the posters and display them on all Notice Boards in the Institute.

Lt.Cdt.Pawan Deep
Deputy Director (Admn.)

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.

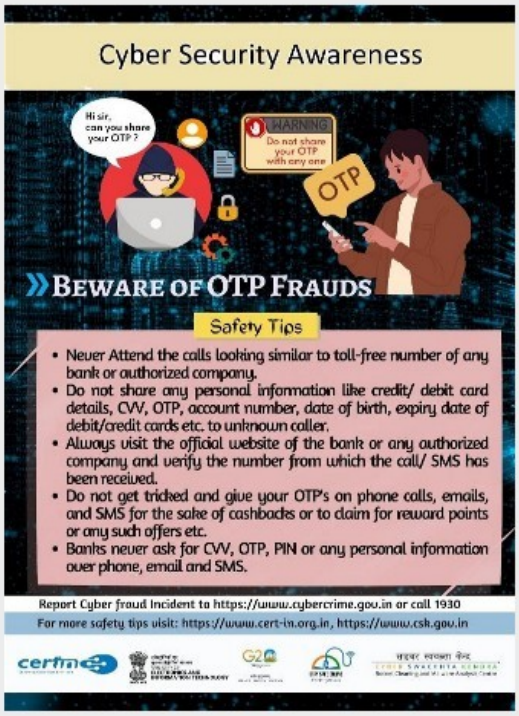
Source: *Ministry of Electronics and Information technology Cybersecurity Guidelines*

Cyber Fraud Do's and Don'ts

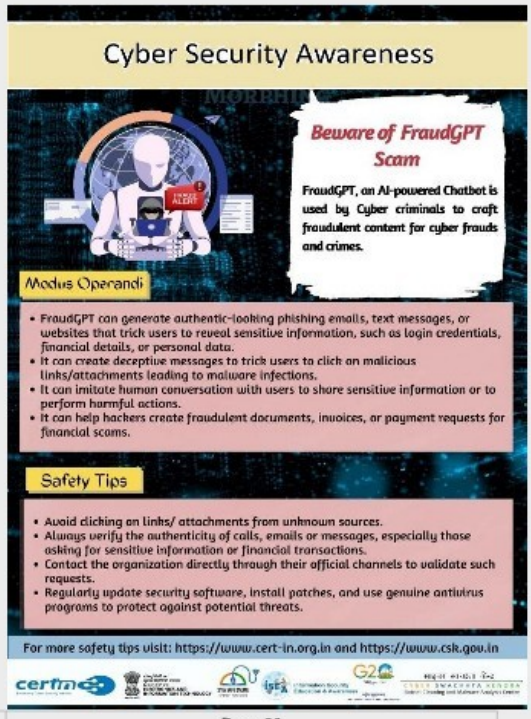
Below is a list of the Do's and Don'ts of Cyber Fraud:

- 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.


Cyber Security Awareness
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 .
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


Cyber Security Awareness
Hi sir, can you share your OTP ?
WARNING
Do not share your OTP with any one
OTP
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.
Report Cyber fraud Incident to https://www.cybercrime.gov.in or call 1930
For more safety tips visit: https://www.cert-in.org.in, https://www.csk.gov.in


Cyber Security Awareness
UPI
ACCEPT
Request sent to user
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.
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


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

Cyber Security Awareness

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.

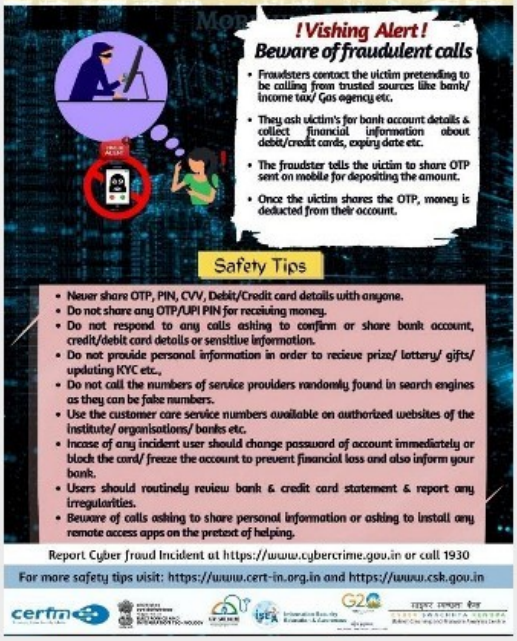
Safety Tips

- 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.

Report Cyber Fraud Incident at 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

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 asking to share personal information or asking to install any remote access apps on the pretext of helping.

Report Cyber Fraud Incident at 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

Cyber Security Awareness

BE WARE OF ONLINE SEXTORTION

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.

Report Cyber Crime Incident at 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

Cyber Security Awareness

BEWARE OF QUICK RESPONSE CODE (QR CODE) SCAM

QR code fraud is a form of cybercrime where criminals attempt to steal user's data by making them to scan a malicious Quick Response (QR) code.

QR code scams have become more and more popular amongst cyber-criminals. Just by making the victim to scan a malicious QR code, they gain access to victim's sensitive data and do financial frauds.

Safety Tips

- Never scan a QR code box that doen't appear to be linked to anything else and has no accompanying.
- Be wary about scanning a QR code in public places, like transportation depots, bus stops or city centers.
- If you decide to scan, check whether the code is pasted on sticker. If its a sticker, don't scan.
- Use a scanner app that actually checks the website the QR code is pointing to, before taking you there.
- If you scan a code and find yourself on a web page that asks for confidential information like passwords, even if it looks genuine, don't key the information in.

Report Cyber Crime Incident at 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