Cyber-hygiene & Security

- Sanjit Sahu

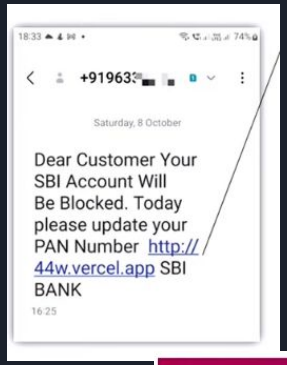
Why is Cyber Security a Concern ?

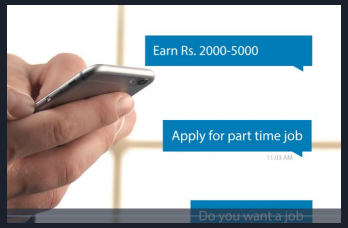
- Today internet, computers, smart phones and other technology devices have become an integral part of our life.
- The world is becoming increasingly connected.
- Size and impact of data breaches is on the rise.

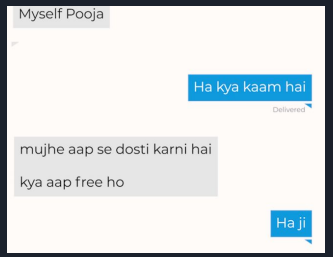
Do you know that cyber-attacks are becoming more complex and sophisticated and are increasingly targeted on stealing the personal information such as phone number, address, photographs, bank details etc.? The personal information can be used by cyber criminals against you in different ways like creating you fake profile, cyber bullying, etc.

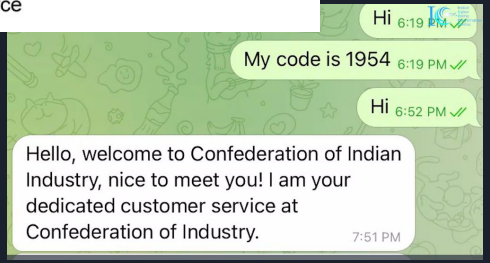
Recent trends in cyber frauds

- Part time job fraud
- Ransomware attack
- Catfishing fraud
- Cyber Stalking / Bullying
- Sextortion
- Identity fraud
- Dating fraud
- YouTube Like & Subscribe scam
- SMS phishing
- Advertisement fraud









Contd..

- Olx Fraud
- Remote Access fraud
- KYC fraud
- QR code
- Instant Loan App scam

Cyber Hygiene

Cyber hygiene is a set of practices that help keep devices, networks, data, and users secure. It's similar to personal hygiene, which helps maintain health, and cyber hygiene helps maintain the health of an organization's network and assets.

Cyber Hygiene Practices

1.. Use Strong, Unique Passwords

- **Avoid common passwords** like "password123" or "123456."
- **Create unique passwords** for each account, especially for sensitive sites like banking or email.
- Use a **password manager** to generate and store complex passwords securely.

2. Enable Two-Factor Authentication (2FA)

- Activate 2FA wherever possible to add an extra layer of security.
- Use authentication apps like **Google Authenticator** or **Authy** instead of SMS-based 2FA when possible, as it's generally more secure.

3. Be Cautious with Links and Attachments

- Avoid clicking on links or downloading attachments in unsolicited or suspicious emails, as these could be phishing attempts.
- Always double-check URLs and sender addresses before interacting with emails, especially those that ask for sensitive information.

4. Keep Software and Devices Updated

- Regularly update your operating system, apps, and antivirus software to protect against vulnerabilities.
- Enable **automatic updates** if possible to ensure you don’t miss important patches.

Contd..

5. Use Antivirus and Anti-Malware Tools

- Install reputable antivirus software to help detect and remove malware.
- Run regular scans to check for threats and keep the software updated.

6. Be Mindful of Public Wi-Fi

- Avoid accessing sensitive accounts (like banking) over public Wi-Fi without a VPN.
- Use a **Virtual Private Network (VPN)** to encrypt your internet connection on unsecured networks.

7. Back Up Your Data Regularly

- Schedule regular backups of important files and documents to an external drive or a secure cloud service.
- In case of a cyberattack, having backups will make data recovery easier.

8. Secure Your Mobile Devices

- Use strong passcodes or biometrics (fingerprint, face ID) to lock your devices.
- Enable "Find My Device" options in case of loss or theft.

Contd..

9. Limit Personal Information Shared Online

- Be careful about what personal information you post on social media, as it can be used for identity theft.
- Check privacy settings on social platforms to control who sees your information.

10. Log Out of Accounts When Not in Use

- Log out from websites and apps, especially on shared or public devices.
- Use secure, trusted browsers that clear cache and cookies on exit if you need extra privacy.

11. Educate Yourself on Phishing and Scams

- Learn to recognize phishing signs, such as urgent messages, grammatical errors, and unexpected attachments.
- Report and delete phishing emails to prevent potential attacks.

12. Use Encryption for Sensitive Files

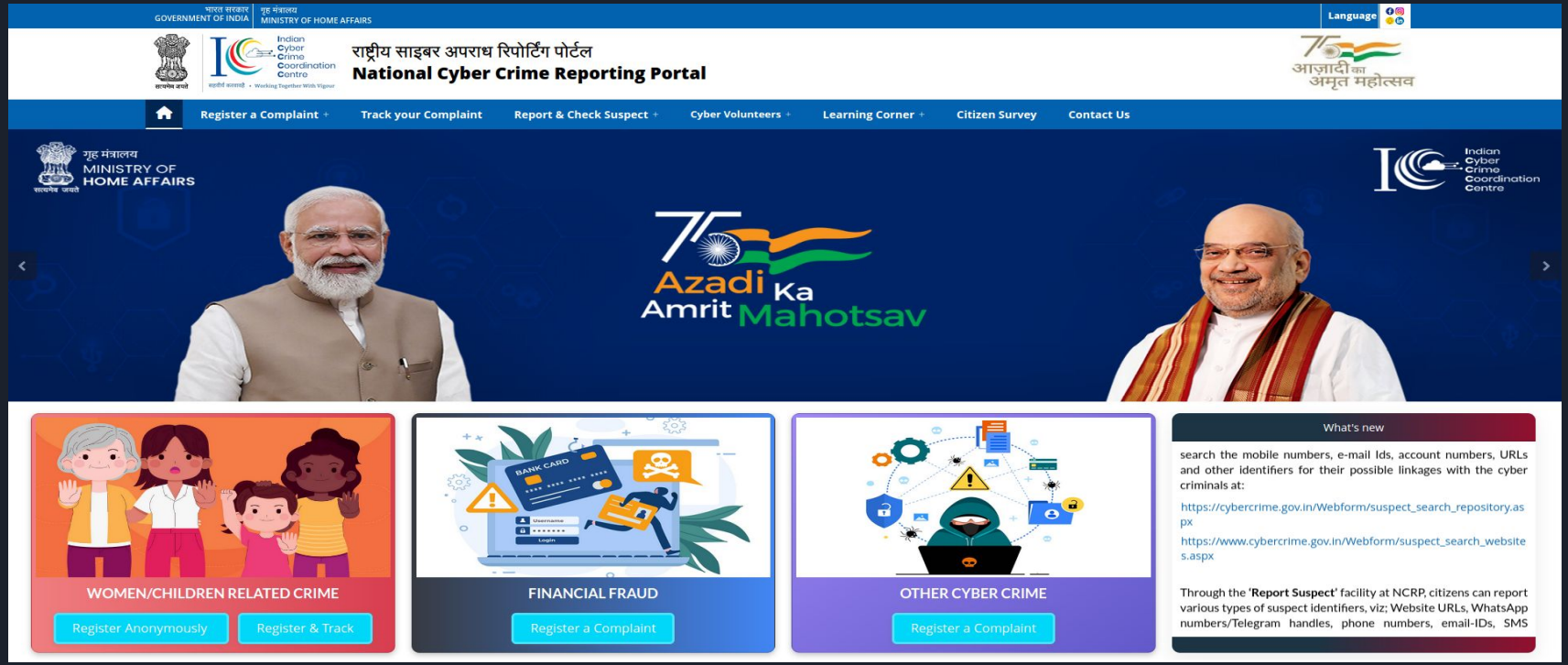
- Encrypt sensitive files or folders to prevent unauthorized access if your device is compromised.
- Use tools like **BitLocker** (for Windows) or **FileVault** (for macOS) for device-level encryption.

13. Monitor Account Activity Regularly

- Review account activity for unusual logins or transactions, especially on financial accounts.
- Enable alerts for suspicious activity where available.

Register your complain:-

https://cybercrime.gov.in or 1930



Questions..

Is ransomware a type of malware?

- Yes
- No

What is cyber bullying?

- Unauthorized access to sensitive information
- Manipulating online search results
- Using technology to harass, intimidate, or humiliate others
- Spreading false information to deceive individuals

What is the primary objective of a firewall in a computer network?

- ◯ To protect the network from unauthorized access and cyber threats
- ◯ To store backup data
- ◯ To speed up internet connection
- ◯ To enhance the graphics of web pages

Which of the following is an example of a cloud-based email service?

- ◯ Gmail
- ◯ Apple Mail
- ◯ Thunderbird
- ◯ Microsoft Outlook

What is the primary function of the 'BCC' field in an email?

- ○ To send a copy of the email to the recipients without showing their addresses to other recipients
- ○ To send a copy of the email to the recipients and show their addresses to all recipients
- ○ To categorize the email
- ○ To add attachments to the email

4) Which one is considered to be a type of antivirus program?

a) Kaspersky

b) Mcafee

c) Quick heal

d) All of the above

What is the role of a VPN (Virtual Private Network) in cybersecurity?

- To monitor network traffic
- To increase internet speed
- To protect data by creating a secure connection over a public network
- To delete cookies from web browsers

What is the significance of encryption in digital communications?

- It reduces the cost of internet service
- It protects data from unauthorized access by convertin g it into a secure format
- It compresses data files for easier storage
- It speeds up data transmission

किस तरह का सुरक्षा उल्लंघन (सिक्यूरिटी ब्रीच) यूज़र को एक्सप्लॉइट या मैनिपुलेट करता है, उन्हें सेटिंग में बदलाव करने या ऐड-ऑन इंस्टॉल करने में मदद करता है, जिससे डेटा चोरी हो सकता है?

- ब्राउज़र
- पासवर्ड
- सोशल इंजीनियरिंग

What is the Cybercrime helpline number ?

- 1190
- 1974
- 1930
- 1440

Thank You