इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND INFORMATION TECHNOLOGY

सत्यमेव जयते

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

G20 भारत 2023 INDIA
वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

आज़ादी का अमृत महोत्सव

Cyber Security Awareness Booklet

for Digital Nagriks and Digital Enterprises

by

Indian Computer Emergency Response Team

certin
Enhancing Cyber Security in India

On the occassion of

National Cyber Security Awareness Month (1st-31st October)

NCSAM, 2023

"Secure Our World"

Index

1) Preface 3

2) Phishing 4

3) Vishing 5

4) Malicious mobile applications 6

5) Malware 7

6) Social media frauds 8

7) Attacks targeting:

- Senior citizens 9
- Children 10
- Women 11
- Person with Disability 12
- Organization 13

8) Safety tips for Passwords 14

9) Basic cyber hygiene- Best practices 15

10) CERT-In Alert/ Advisories & Security tools 16

11) Reporting Cyber Security Incidents to CERT-In 17

12) Report Cyber Crime or Cyber fraud to I4C 17

Preface

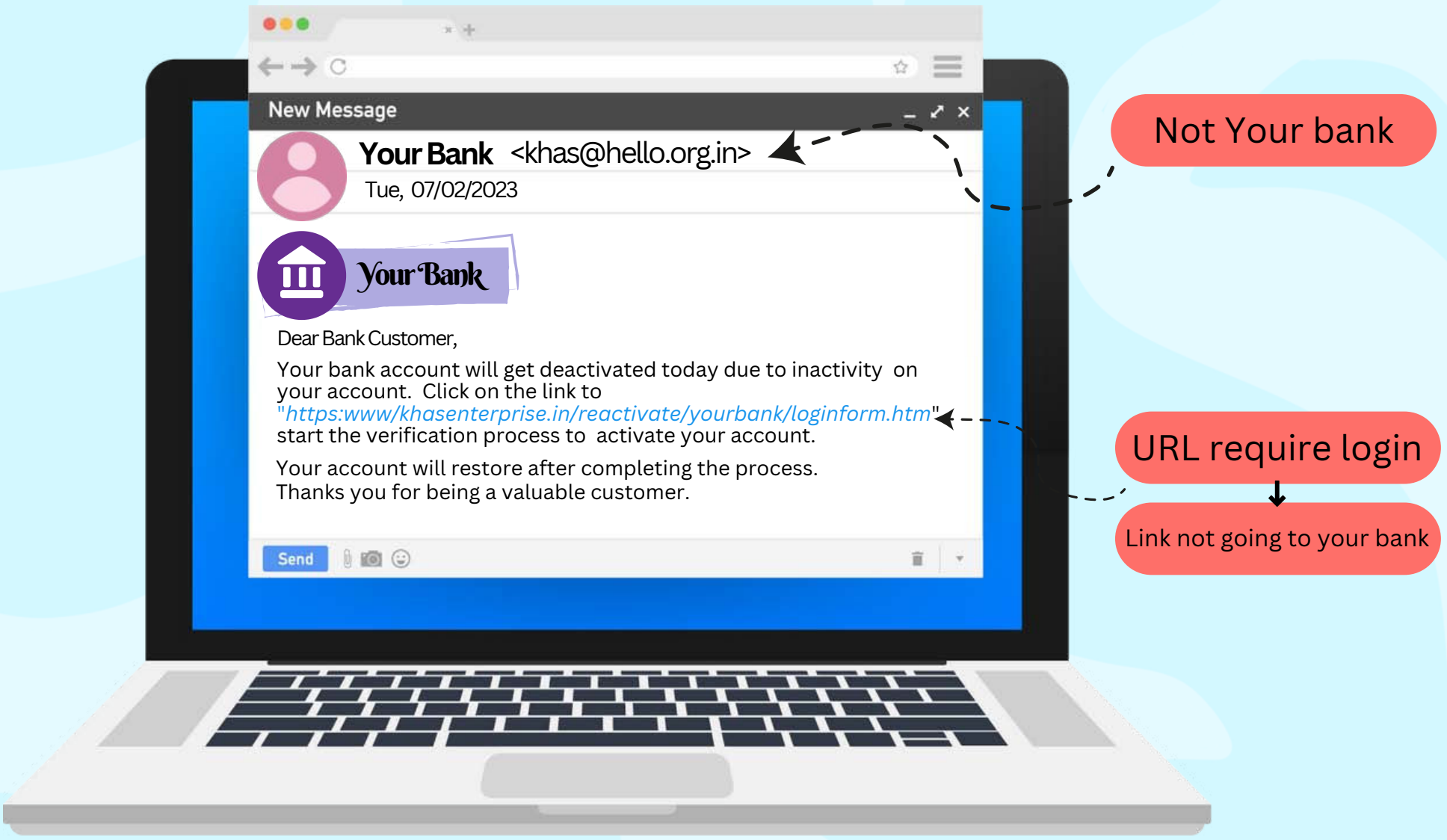
The Indian Computer Emergency Response Team (CERT-In) is a Government Organization under Ministry of Electronics and Information Technology (MeitY), Government of India established with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

CERT-In has been designated to serve as national agency for incident response under Section 70B of the Information Technology Act, 2000 (Amendment 2008). As part of services of CERT-In, for creation of awareness in the area of cyber security as well as training/ upgrading the technical knowhow of various stakeholders, CERT-In is observing the National Cyber Security Awareness Month (NCSAM) during October 2023 by organizing various events and activities for citizens as well as the technical cyber community in India with the theme of "Secure Our World".

This Awareness Booklet for Digital Nagriks and Digital Enterprises is released as a part of CERT-In's awareness initiatives to educate the users on the best practices that needs to be followed to protect them from different cyber security attacks and cyber crime frauds.

Phishing

Phishing is a common method that cybercriminals use to do the fraudulent activity by creating authentic-looking emails or websites to trick victims into sharing personal information or financial data.



Safety Tips

- Carefully check the URL before clicking on it.
- Never react to the messages which shows urgency.
- Do not trust promotional offers which look “too good to be true”.
- Do not hesitate to report to Law Enforcement Agencies, if you become a victim of phishing.
- Verify the email ids in emails addressed to generic recipients.
- Look for typing errors (eg., Acc0unt, ema1l, dep0sit, passw0rd)
- “Do yu kare about yurself?” Look for poor grammar and unprofessional Language.

Vishing

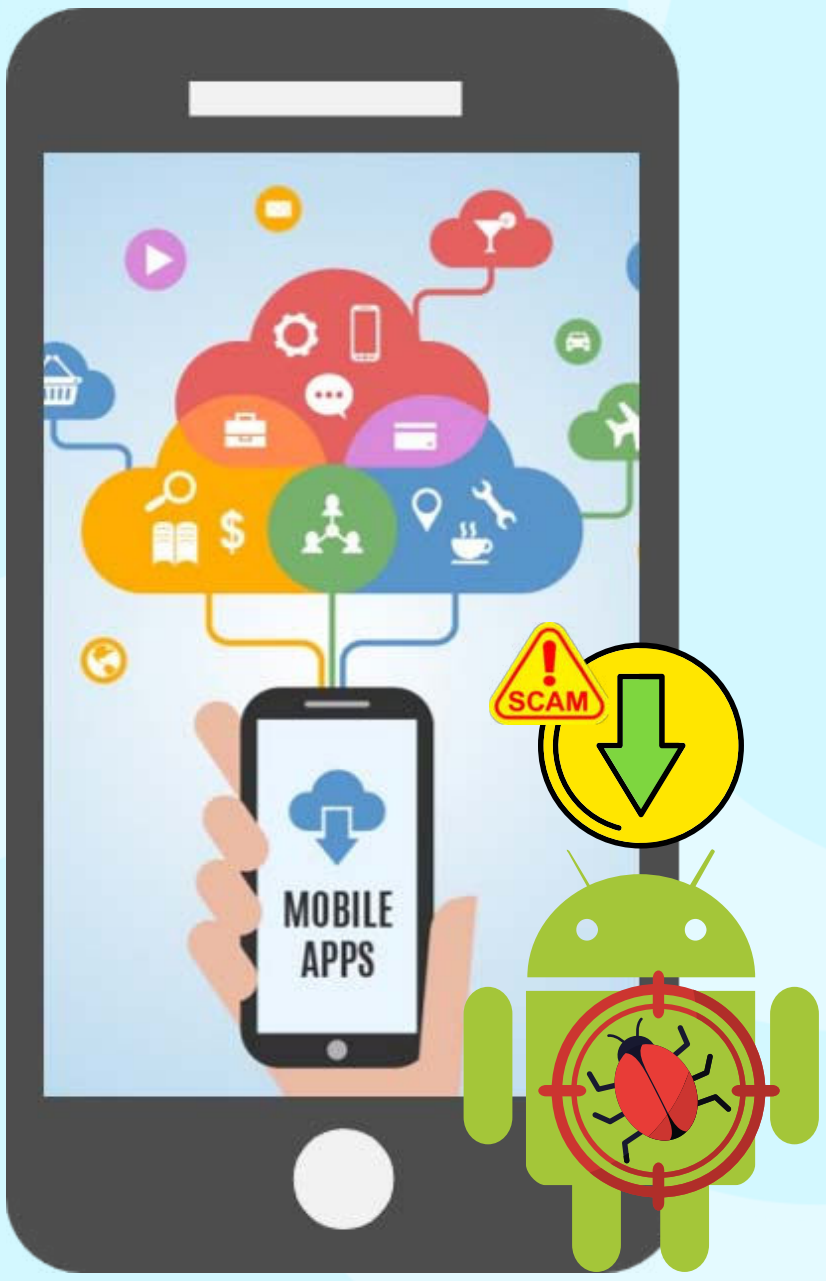
- Fraudsters contact the victim pretending to be calling from trusted sources like bank/ income tax/ Gas agency etc.
- They ask victim's for bank account details & collect financial information about debit/credit cards, expiry date etc.
- The fraudster tells the victim to share OTP sent on mobile for 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.
- In case of any incident, user should call 1930 and change the password of their account immediately or block the card/ freeze the account to prevent financial loss.
- Users should regularly 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.

Malicious Mobile Applications

Infected mobile applications may contain malware that can steal your data, login credentials and autosubscribe to premium services.

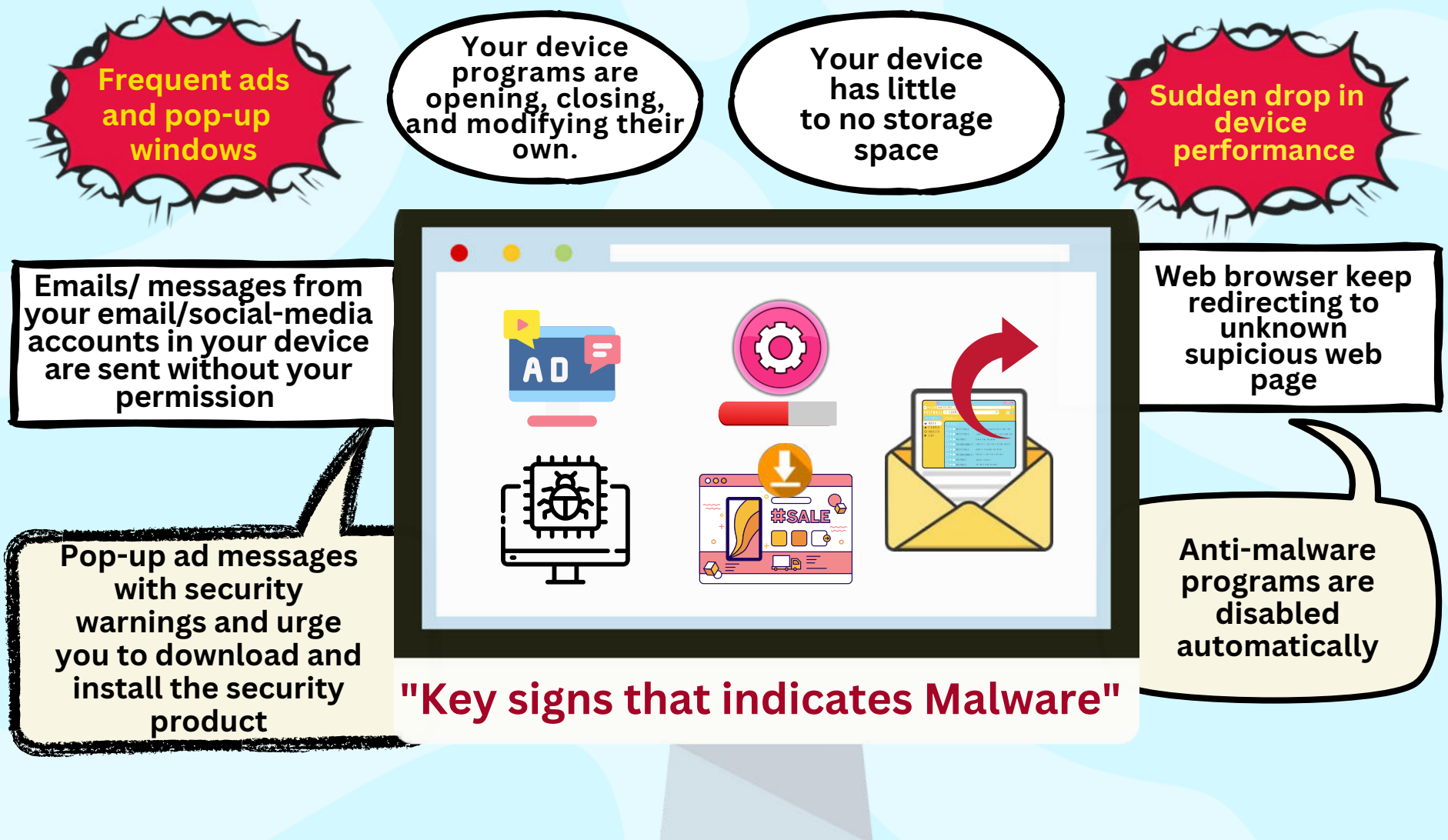


Safety Tips

- Before downloading any 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, emails, social media messages.
- Be cautious about allowing any new permissions during the installation of the application.
- Pay attention to reviews and comments of the users, before installing any mobile application.

Malware

Malware is a piece of malicious code inserted in an application, program or system by threat actors. They can infect your systems and perform malicious operations.



"Key signs that indicates Malware"

Safety Tips

- Avoid clicking on suspicious emails, links, and sites from unknown source.
- As soon as you click on any malicious link, your mobile can be hacked or your data can be stolen.
- Browse only secure and authorised websites.
- Always keep your computer software/browser up to date .
- Maintain backup of your data regularly.
- Install software like pop-up/ ad-blocker to block the malicious advertisements appearing on websites.
- Install antivirus and antimalware solutions in your devices and keep them updated.
- Hover over the images/links to find the actual link.
- Do not install any apps through links received on chats or social media posts.

Social Media Frauds

- Scammers use "bots" to trick unsuspecting users into making online payments to accounts under their control, such as through internet banking or UPI transfers.
- Fraudsters use Fake Profile of the victim :
    1. To spread false or fake information.
    2. Sends friend requests to other friends of victim to gain financial benefits.
    3. To damage the reputation of the victim.

Safety Tips

- Avoid sharing your personal information like address, mobile number, personal mail 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 recieved through messages until you verify the authenticity of the source.
- Use different passwords for different social media accounts and emails.
- Enable multi-factor authentication for social media accounts.
- Disable profile visibility from public searches.
- Log out after each session.
- Never share social media credentials with any one.
- Keep the privacy settings of social media profile at most restricted level, especially for public viewing.
- Apply maximum caution while sharing photographs, videos, status, comments etc.
- Criminals may collect enough information about users from the posts and profile of the users.

Attacks Targeting Senior Citizens

Fraudsters target Senior citizens as they are more vulnerable to online financial scams and frauds.

Senior Citizens must exercise caution when they are online.

Financial frauds targeting Senior Citizens

- Fraudsters target senior citizens as they are more vulnerable to online financial scams and frauds.
- Senior citizens must exercise caution when they are online.
- Fraudsters trick victims to provide personal sensitive information like Date of Birth, credit or debit card numbers, passwords, OTPs, etc to steal their money.
- Fraudsters target senior citizens through fake insurance schemes, low-cost medications, card renewal, KYC verification, free gifts and offers.
- Fraudsters exploit the loneliness of elderly people and deceive them with fake relationships.
- Fraudsters also create fake social media accounts to target senior citizens and convince them to pay money or share banking credentials/OTP/PIN.

Safety Tips

- Be aware of fraudsters disguising themselves to be from banks or other institutions asking for personal sensitive information.
- Never share OTP, username, passwords, credit/debit card details, PIN over phone or internet.
- Never click or download any link/attachments from unknown sources.
- Avoid shopping online if you are not familiar with it.
- Always have a lock, PIN, password, or fingerprint to access your mobile/laptop/computer.
- Enable multi-factor authentication to your emails, banking and social media accounts.
- Never share sensitive personal information with strangers and in social media.
- Avoid making charity contributions over phone.
- Always remember that banks or other financial institutions never ask for your username/passwrord, OTP, PIN, credit/debit card details.

Attacks Targeting Children

Cyberbullying is a form of harassment that includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.

Safety Tips

- Review your social media privacy settings and restrict to family and known friends.
- Educate children about password safety.
- Check their social media accounts and keep track of it.
- Ensure they don't share easily identifiable information like trackable location.
- Stop regular engagement on social media.
- Do not accept “Friend Requests” from strangers on social media.
- When bullied log off the site, save the chat/ messages/ e-mail, and inform your parents/ teachers/ elders whom you trust.
- Don't respond. Block the e-mail /messages.
- Think well before sharing online.
- Make use of privacy setting and control the posts you do online.
- Never share your password. Even your friends may misuse your password.
- Being kind to others online will help to keep you safe.
- Talk to an adult you trust, about any messages/posts you get online. They can help you to get rid of the bullying.

Attacks Targeting Women

- 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.

Attacks Targeting Person with Disability

Fraudulent individuals often pose as authorized representatives to scam people with disability. These scammers will call or email the victim and ask for their personal information. Fraudsters often offer them promising opportunities such as chance to work from home and make extra income.

Safety Tips

- Before engaging with any unknown person or business online or over the phone make sure no confidential information is shared without confirming who is on the receiving end of any communication.
- Be aware about the different types of threats and learn to spot a scam.
- Call 1930 if you become a victim
- Don't click on any suspicious links and attachments.
- Don't download any application received through chats, e-mail and social media platforms.

Attacks Targeting Organisation

Cybercriminals are persistently looking for new ways to expose security risks. They perform cyberattacks to steal, expose, alter, disable, or destroy organisation's assets through unauthorized access to computer systems. Cyber-attack could cause financial loss and disruption of business.

Safety Tips

- Do not click on direct link recieved through emails, text messages etc. asking you to enter your personal/ sensitive information.
- Avoid using public networks.
- Avoid reuse of passwords between any website or services.
- Report any suspicious emails to at your workplace, instead of deleting the mail.
- Invest in password management tool, as it is hard to remember multiple passwords.
- Always change the passwords when employees leave the organisations.
- Implement multi-factor authentication.
- Keep your software up-to-date.
- Use a secure file-sharing solution to encrypt data.
- Use updated antivirus and anti-malware solutions.
- Use a VPN to encrypt your connection and protect your private information.
- Back up important data.

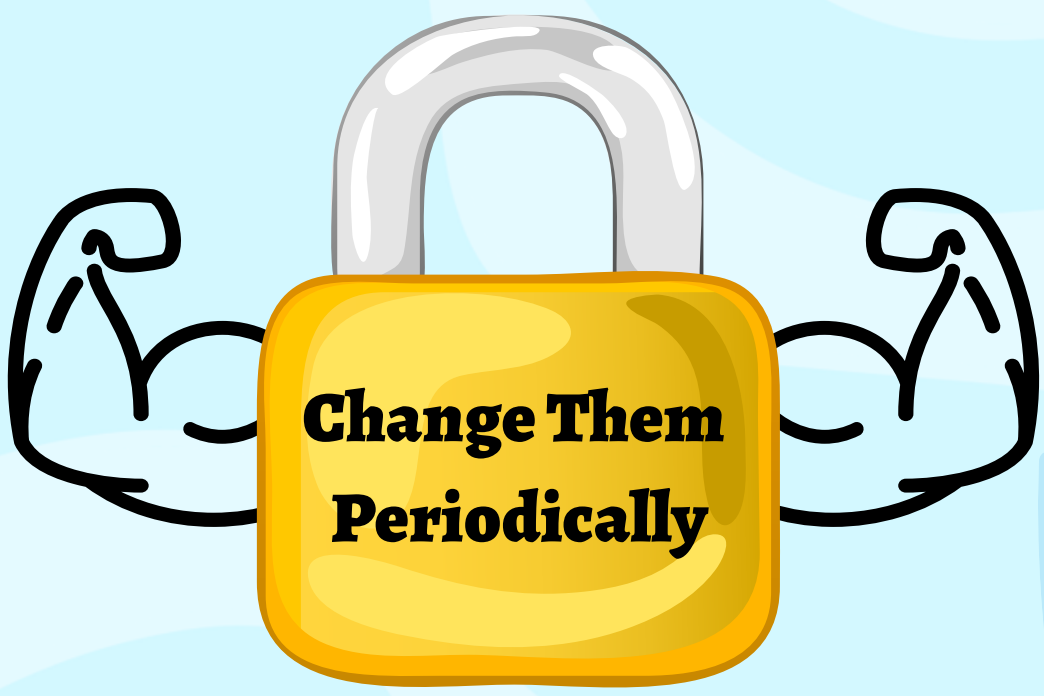
Always use strong and complex passwords

********** Weak

********** Moderate

********** Strong

"Stronger the password, Stronger the security"



Safety Tips

- Never use your name, age, birthday, phone number, address, place, or any other sensitive personal information as part of your password.
- Use unique password for each account.
- Make long passwords by mixing upper case, lower case, numbers and symbols.
- Don't share your password with anyone.
- Enable multi-factor authentication.
- Regularly change passwords.

Basic Cyber Hygiene

Best Practices

- Use genuine software
- Keep your software up-to-date
- Avoid opening suspicious emails
- Think before you click on suspicious links/ attachments
- Use updated anti-virus and anti-malware
- Use updated browsers
- Use strong passwords and regularly change them
- Don't share your passwords with anyone
- Enable Multi-Factor Authentication
- Avoid using public Wi-Fi networks for secured transactions
- Regularly take backup of your data

Alerts/ Advisories

Alerts:

Visit: ***https://www.csk.gov.in/alerts/Monti_ransomware.html***

https://www.csk.gov.in/alerts/Nitrogen_malware.html

https://www.csk.gov.in/alerts/Daam_android_botnet.html

Advisories:

Visit : ***https://www.cert-in.org.in***

CERT-In Advisory CIAD-2021-0004 : Preventing Data Breaches/ Data Leaks

CERT-In Advisory CIAD-2022-0026 : Password Management and Security

CERT-In Advisory CIAD-2022-0003 : Securing Twitter Accounts

CYBER SWACHHTA KENDRA

Security Tools

Free Bot Removal Tool- For Microsoft Windows

- **eScan Antivirus**
- **K7 Security**
- **Quick Heal**

Free Bot Removal Tool - For Android

- **eScan Antivirus**

Free Mobile Security Application - For Android

- **M-Kavach 2**

Other Relevant tools:

- **USB Pratirodh**
- **AppSamvid**
- **Browser JSGuard**

Scan Me

Report Cyber Security Incident to CERT-In

For reporting Cyber Security Incidents to CERT-In:

Visit website: ***https://www.cert-in.org.in***

Email: ***incident@cert-in.org.in***

Toll Free Phone: ***+91-1800-11-4949***

Toll Free Fax: ***+91-1800-11-6969***

Information Desk

Phone: ***+91-11-24368551***

Fax: ***+91-11-24368546***

For Reporting Cyber Fraud & Crime to I4C:

Visit website: ***https://www.cybercrime.gov.in***

Call : ***1930***

For reporting Vulnerabilities & Collaboration with CERT-In in the area of Cyber Security:

Visit website: ***https://www.cert-in.org.in***

Email: ***vdisclose@cert-in.org.in***

collaboration@cert-in.org.in

Phone: ***+11-22902600*** *Ext:* ***1012, +91-11-24368572***

For Trainings/ Awareness programmes:

Email: ***training@cert-in.org.in***

Official social media handles of @IndianCERT

https://www.facebook.com/IndianCERT/

https://twitter.com/IndianCERT

https://www.kooapp.com/profile/IndianCERT

https://www.pixstory.com/user/indiancert/9280

Scan Me

www.cert-in.org.in

Scan Me

www.csk.gov.in