इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

सत्यमेव जयते

certin
Enhancing Cyber Security in India

ISEA Information Security Education & Awareness

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

CYBER SECURITY HANDBOOK

FOR

"Mahila Suraksha"

certin
Enhancing Cyber Security in India

INTERNATIONAL WOMEN'S DAY

8th March 2025

TABLE OF CONTENTS

TABLE OF CONTENTS

ABOUT CERT-In

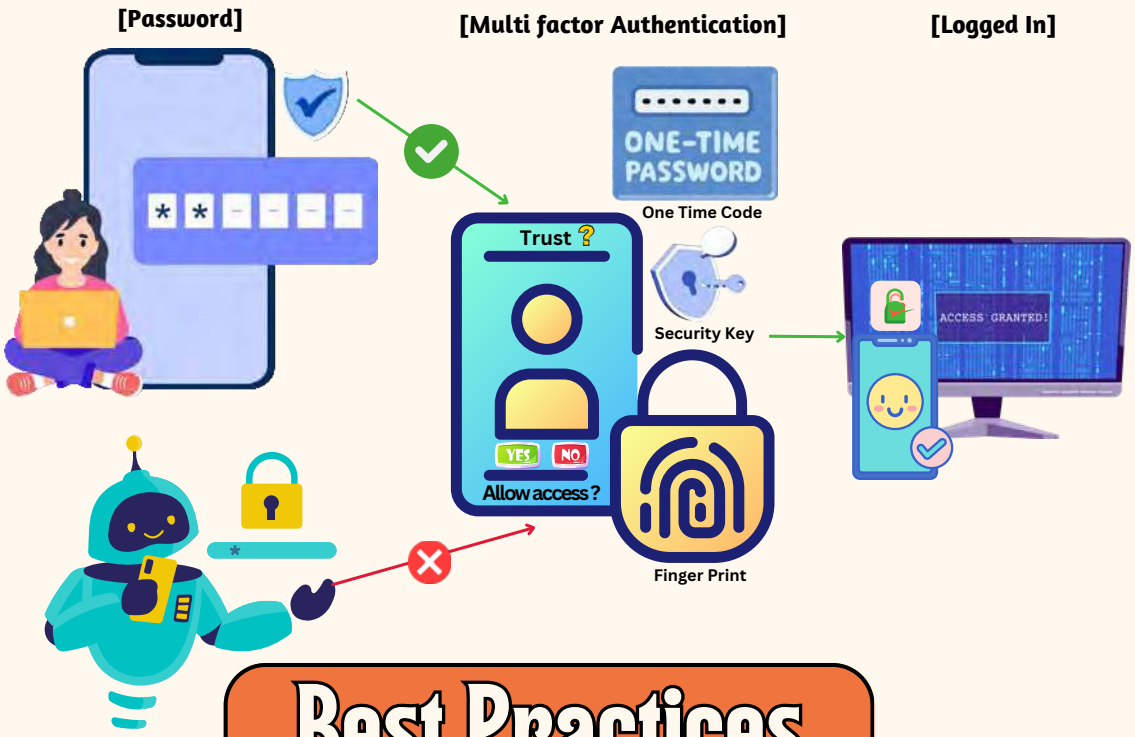
The Indian Computer Emergency Response Team (CERT-In)

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 International women's Day on 8th March 2025.

This Cyber Security Handbook for women is released as a part of CERT-In's awareness initiatives to educate women and other online users on the best practices that needs to be followed to protect them from different cyber security attacks and cyber frauds.

ONLINE ACCOUNT SECURITY



Best Practices

- Enable Multi-Factor Authentication, it adds an extra layer of security by requiring a second form of verification in addition to your password.
- Regularly update your passwords.
- Do not reuse passwords.
- Do not share your passwords with anyone.
- Use unique, complex, and long passwords.
- Regularly check your account activity and look for any suspicious login attempts.

DESKTOP SECURITY

Best Practices

- Use genuine Operating System and Software.
- Keep your Operating System updated.
- Install anti-virus and anti-malware solutions and keep them updated.
- Use strong login password and change them periodically.
- Regularly take backups of your important files and data.
- Incase of incidents such as hardware failure, or cyberattacks, having backups can help you restore important information.
- Maintain multiple copies of critical data in different locations to prevent loss in case of disasters.
- Periodically test and verify your backups to ensure that they can be used for restoration when needed.

MOBILE SECURITY

#Secure your mobile by restricting permissions to apps

Best Practices

- Download apps from official app stores to avoid downloading potentially harmful apps.
- Do not download any apps from ads or third party websites.
- Ensure your OS and applications are up to date.
- Always read the reviews about the app and developer before downloading and installing an app.
- Carefully review the permission requests and ensure that it is related to the purpose of the app.
- Remove/ Uninstall apps with excessive permissions.
- Always read the app's privacy policy on how your data will be shared.
- To avoid unnecessary data collection, uninstall apps you no longer use.
- Restrict permissions to social media and banking accounts.
- Report immediately to concerned authorities if any unauthorized activity is detected.

SOCIAL MEDIA BEST PRACTICES FOR WOMEN

» **To protect yourself from harassment on social media, it's not enough to simply remove your accounts or cut off network contact.**

Best Practices

- If an individual is causing trouble to you or others, it is recommended to block and report them to the social media platform and other concerned agencies.
- Set the privacy settings on your social media accounts to prevent unauthorized individuals from viewing, chatting, or tagging your content.
- Exercise caution while accepting friend requests or responding to strangers in social media.
- Restrict visibility to your posts and profile information.
- Avoid sharing personal and sensitive details online through posts or chats.
- Disable automatic addition to unknown groups without your permission.
- Keep a record of all online or virtual workplace discomforts and document every aspect of your work environment.
- Exercise caution while sharing photos online.
- If you are becoming a victim of any cyber frauds or cyber harassments report to the nearest police station or report at https://www.cybercrime.gov.in or call 1930.

STAYING SAFE AGAINST SCAMS

1. Never merge/ respond to calls or video calls from unknown people.
2. Always verify callers identity.
3. Never share sensitive information or PIN, OTP etc. over phone call or Online.
4. Never share intimate pictures over online video calls/ social media platforms with anybody.
5. Malicious mobile apps with access permission to gallery/ storage can access your photos and can be used to blackmail you.
6. Enable multi-factor authentication with strong passwords for all online accounts.

BEWARE OF MORPHING

Adult Website

Fake ID Card

Social Media Post

Best Practices

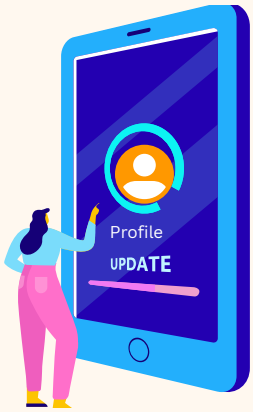
Morphing is altering or changing the pictures of the persons in photos or videos.

- Enable your security and privacy features on social media accounts
- Never share your personal pictures online publicly on social media accounts
- 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 .

BEWARE OF CYBER STALKING

Do not accept “Friend Requests” from strangers on Social media

Review your social media privacy settings and restrict to family and known friends



Do not post your home address, phone number, or any personal information, which can be used to stalk you

Turn off location services on Social media platforms

Enable Multi-Factor Authentication (MFA) for your social media accounts

REMEMBER

- Take screenshot of online messages, comments, conversation etc. as a proof.
- Note down the mobile number and available details of the criminals.
- Report cyber crime incident to https://www.cybercrime.gov.in or call 1930.

BEWARE OF MALICIOUS APK SCAM

Fraudsters may use messaging through social media to send malicious APK files. Clicking on such links or installing such files received in chats may result in financial losses and theft of sensitive information.

Best Practices

- Avoid clicking on suspicious links.
- Do not respond to messages that request personal information or requests to click on links to download APK files from third party websites.
- Malicious APKs target banking apps and steal financial data.
- Do not share login credentials, passwords, credit card numbers, or any other sensitive information to strangers.
- Only install apps from trusted sources instead of links sent via messages.
- Immediately report cyber frauds through the National Cyber Crime Reporting Helpline at 1930 or file a complaint at the official portal (https://cybercrime.gov.in).

BE SMART- STAY SAFE WHILE USING FREE PUBLIC WI-FI

Beware it could be a trap

Best Practices

Be cautious when connecting to any public network at airport, hotel, train/bus station, cafe, and other public places.

- Always confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.
- Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network.
- Use a VPN service.
- Use public Wi-Fi only when required.
- Switch off Wi-Fi service when not in use.

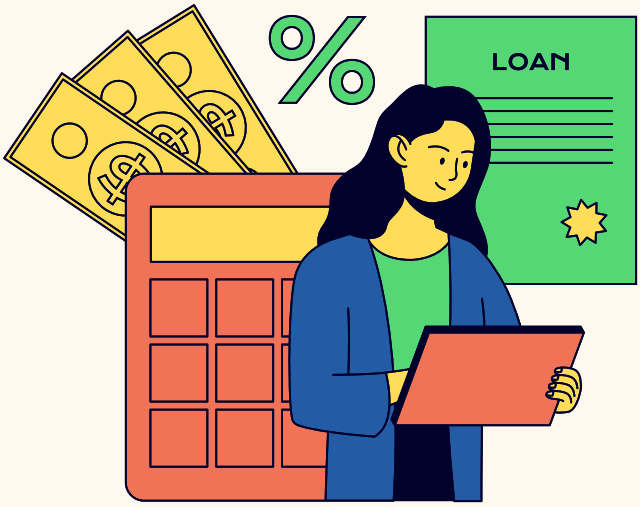
BEWARE OF DIGITAL ARREST SCAM

Best Practices

Cybercriminals threaten individuals as Investigation officers and create a sense of fear through fake calls.

- Never accept to join any online video calls for any investigation or arrest through calls received from strangers.
- Avoid answering video calls from unknown contacts, even if they claim to know you.
- Avoid sharing sensitive personal information online with strangers.
- Never make any payments to strangers claiming to be investigation officer in online calls.
- Keep the privacy settings of your social media profile at the most restricted levels.
- If you receive any calls about arrest or investigation, visit the nearest police station.

BEWARE OF INSTANT LOAN APPS SCAM



Best Practices

- Always download apps from official websites and app playstores.
- Always avail loans from RBI regulated entities.
- Always check whether the lender is approved by RBI and/or is associated with a financial institution.
- Do not enter your PIN or password anywhere to receive money.
- Visit only the official website of your bank or service provider.
- Do not download any applications from any unknown sources.
- Always check the terms and conditions of lending, genuineness of their website, physical office locations, Company Identification Number (CIN), and details of the Certificate of Registration (CoR).
- Always check URLs and domain names received in emails for spelling errors.
- Apply for loans only through applications related to Non Banking Financial Corporation (NBFC) or authorized bank.

PASSWORD MANAGEMENT BEST PRACTICES

1

Use Strong and long passwords

Always prefer to create lengthy passwords.
Short length passwords are easy to crack.

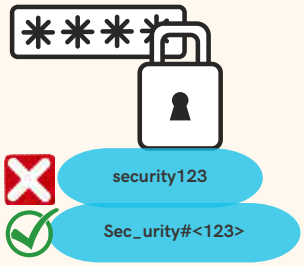
2

Don't use dictionary words as passwords

Such passwords are too easy to crack.

Dictionary words are vulnerable to brute-force attack by hackers.

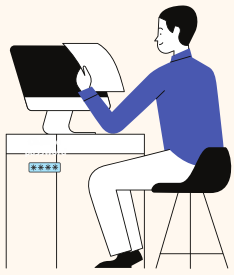
3



Create passwords using special characters

Passwords mixed with uppercase, lowercase, numerals and special characters are difficult to crack

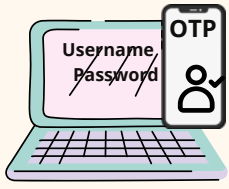
4



Change passwords periodically

Avoid using guessable patterns of password.

5



Enable Multi Factor Authentication

MFA adds another layer of security to your accounts.

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

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

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

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

For Trainings/ Awareness programmes:

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

Scan Me

www.cert-in.org.in

Official social media handles of @IndianCERT

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

https://twitter.com/IndianCERT

https://www.instagram.com/cert_india/

https://www.linkedin.com/company/indiancert-cert-in/

https://youtube.com/@indiancert

Scan Me

www.csk.gov.in

Download Botnet removal tools