इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

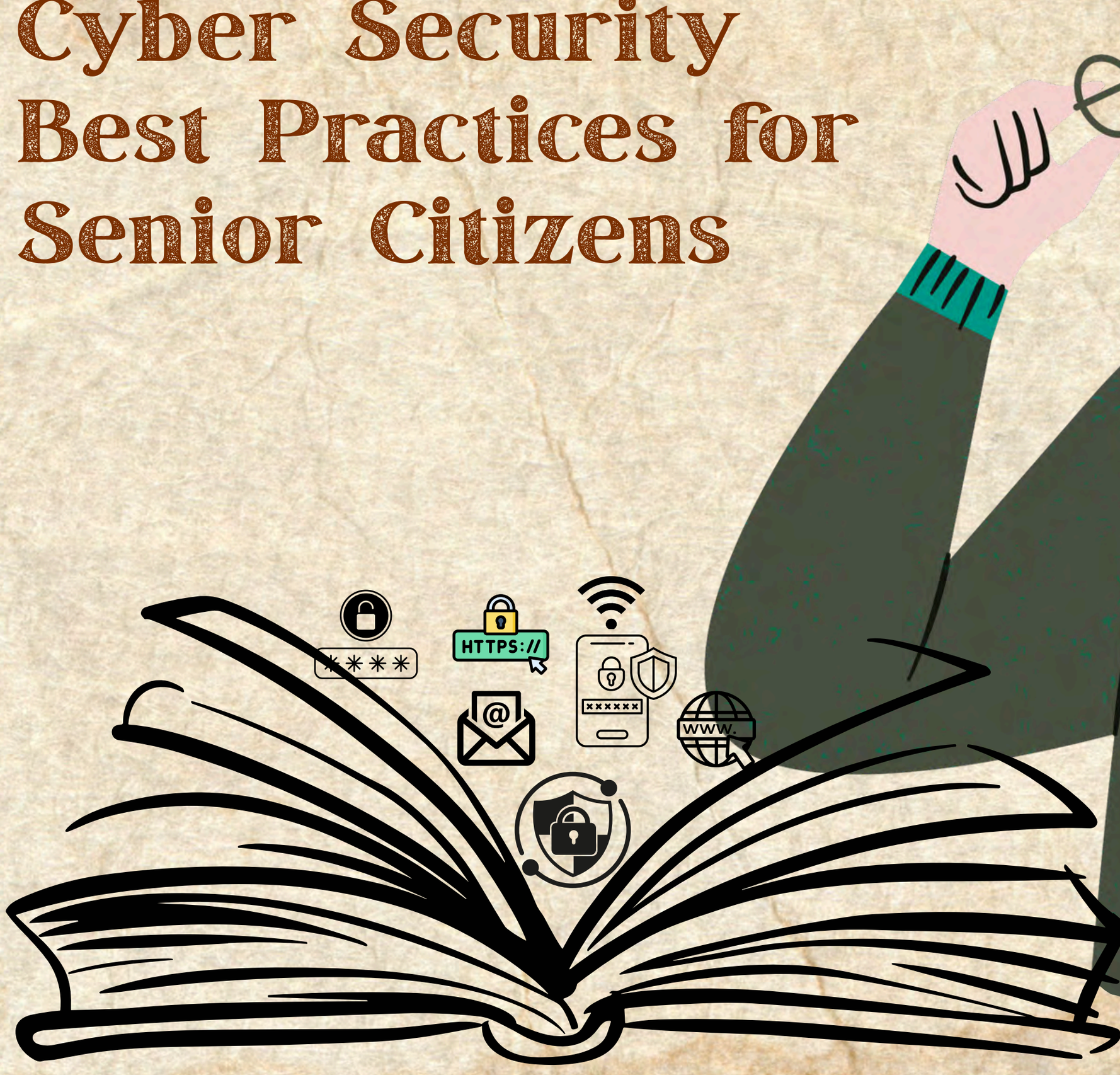
certin
Enhancing Cyber Security in India

ISEA
Information Security Education & Awareness

10 Years of Digital India

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

Cyber Security Best Practices for Senior Citizens



by

Indian Computer Emergency Response Team (CERT-In)

On the occasion of

NATIONAL CYBER SECURITY AWARENESS MONTH

(October 2025)

#CyberJagritBharat

Table of Contents

PREFACE

The **Indian Computer Emergency Response Team (CERT-In)** under the Ministry of Electronics and Information Technology (MeitY), Government of India is 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 the national agency for incident response under Section 70B of the Information Technology Act, 2000 (Amendment 2008). As part of services of CERT-In, for the creation of awareness in the area of cybersecurity as well as training/upgrading the technical know-how of various stakeholders, CERT-In is observing the National Cyber Security Awareness Month 2025.

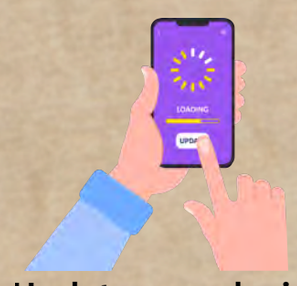
This Cyber Security Best Practices Booklet for Senior Citizens is released as a part of CERT-In's awareness initiatives to educate the Senior Citizens on the best practices that needs to be followed for using the internet in a safe and secure manner.

Mobile Safety

Possible Threats

- Phishing Messages
- Courier Fraud
- Financial Frauds
- Emotional Manipulation

Stay Safe



Update your device

Strong Password

Fake Email

Fake sms

Impersonation

Phishing URL

Fake calls

Fake banking apps

Install Antivirus

MFA

Privacy is power

Best Practices

- Use a strong screen lock (PIN, password, fingerprint, or face ID).
- Never share OTPs, PINs, or passwords with strangers.
- Keep your device software updated.
- Download apps only from official app stores.
- Always verify sources before clicking links.
- Review app permissions.
- Avoid public Wi-Fi or use a VPN when needed.
- Turn off Bluetooth and location when not in use.
- Be cautious of fake update alerts or pop-ups.
- Install antivirus or mobile security apps.

Email Safety

Possible Threats

- Phishing Emails
- Malicious Attachments
- Financial Frauds
- Emotional Manipulation

Stay Safe

Visit secured websites

Strong Password

Spam emails

Impersonation

Install Antivirus

Phishing emails

MFA

Urgent Scams

Privacy is power

Malicious Attachments

Best Practices

Update your device

- Check the sender's email address and look for spelling errors or odd domains
- Don't trust urgent or emotional messages without verifying.
- Avoid clicking on unknown links or attachments.
- Avoid sharing personal info like PAN, Aadhaar, or banking details via email or phone.
- Don't reply to suspicious messages.
- Enable multi-factor authentication (MFA) for your email account.
- Keep your email app, system software and antivirus updated.
- Log out from shared devices after checking email.

Safe Online Banking

Possible Threats

- Phishing Websites
- Fake Banking Apps
- Vishing
- Smishing (SMS Phishing)

Fake banking sites that steal login credentials.

Malicious Attachments

Fraudulent apps that mimic real banking apps.

Scammers call pretending to be bank officials.

Fraudulent SMS asking for banking info or offering fake rewards.

Visit secured websites

Strong Password

Install Antivirus

MFA

Privacy is power

Update your device

Best Practices

- Use only verified and trusted browsers.
- Use HTTPs secured websites for payments.
- Don't share your online banking PIN/ OTPs with anyone.
- Enable Multi-Factor Authentication (MFA).
- Logout after each online Banking session.
- Change your password regularly.
- Keep your online payment apps updated to latest version.
- Avoid banking over public Wi-Fi; use a secure connection or VPN.
- In case of suspicious activity contact your bank immediately using the official customer care number.
- Keep a regular check on all messages received from your bank.

Vishing

Possible Threats

- **Phishing Websites**
- **Fake Banking Apps**
- **Vishing**
- **Smishing (SMS Phishing)**

Stay Safe

Fake Bank Calls

KYC Update Scams

Lottery or Prize Scams

Lottery or Prize Scams

Strong Password

MFA

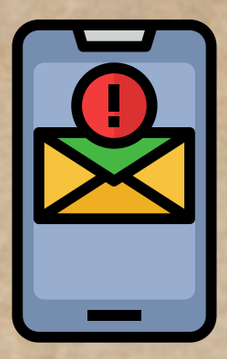
Privacy is power

Best Practices

- **Never share OTP, PIN, CVV, Debit/Credit card details with anyone.**
- **Do not respond to any calls asking to share bank account, credit/debit card details or sensitive information.**
- **Do not provide personal information in order to receive prize/ lottery/ gifts/ updating KYC etc.**
- **Use the customer care service numbers available on authorized websites of the institute/ organizations/ banks etc.**
- **Hang up immediately if the caller pressures you or creates panic.**
- **Report suspicious calls to your bank and concerned authorities.**

Smishing

Possible Threats



Fake Bank Alerts

Lottery/Prize Messages

KYC Update Request

Government Impersonation

Malicious Links/ attachments

Stay Safe

Visit secured websites

Strong Password

Install Antivirus

MFA

Privacy is power

Update your device

Best Practices

- Avoid clicking unfamiliar links received through messages. It may steal your personal data from your mobile.
- Always verify the authenticity of the message.
- Never share personal information (OTP, PIN, passwords) via SMS.
- Verify sender identity because banks and government bodies don’t ask for sensitive info via SMS.
- Be alert for spelling mistakes or poor grammar, these are signs of fraudulent messages.
- Avoid replying to unknown numbers or engaging with prize/lottery claims.
- Use official apps or websites to check account or service updates.

Quishing

Possible Threats

Fake Payment QR Codes

Phishing via QR Codes

Malware Downloads

Public Poster Scams

Stay Safe

Strong Password

Install Antivirus

MFA

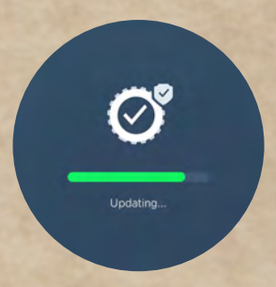
Update your device

Privacy is power

Best Practices

- Examine the URLs before opening them through QR code scanners.
  - Always check for spelling mistakes and verify the domain names in URLs.
  - Do not click on shortened URLs without validating the original URL.
- Do not scan QR codes received from strangers through chats/ emails.
- Before scanning, ensure the QR code is legitimate and not altered, and verify whether it is covered with any fraudulent sticker.
- Avoid entering personal or banking details on websites opened via QR codes.
- Avoid scanning QR codes on public posters or flyers unless verified.

Safe Browsing



Best Practices

- Be cautious with downloads, only use trusted sources.
- Don’t share personal info (like your address or bank details) online.
- Use antivirus protection on all devices.
- Back up your data regularly.
- Log out of accounts when using shared or public devices.
- Limit what you post on social media like current location and personal details.
- Use strong, unique passwords for each account.
- Keep software and apps updated.
- Avoid clicking on suspicious links in emails, messages, or pop-ups.
- Check website URLs carefully and look for HTTPS and spelling errors.
- Report suspicious activity to trusted authorities.
- If you become a victim, immediately call 1930 and report cyber frauds/crimes at https://www.cybercrime.gov.in.

Report Cyber Security Incidents 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 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***

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

csk@cert-in.org.in

साइबर स्वच्छता केन्द्र

CYBER SWACHHTA KENDRA

Botnet Cleaning and Malware Analysis Centre

Announcements

https://www.csk.gov.in/announcements/index.html

Security Tools

https://www.csk.gov.in/security-tools.html