



इलेक्ट्रॉनिकी एवं  
सूचना प्रौद्योगिकी मंत्रालय  
MINISTRY OF  
**ELECTRONICS AND  
INFORMATION TECHNOLOGY**



75  
आज़ादी का  
अमृत महोत्सव



# Internet Safety Awareness Booklet

for Digital Nagriks and  
Digital Enterprises

by

**Indian Computer  
Emergency Response Team**



**On the occassion of  
Safer Internet Day  
(6th February 2024)**



**"Security is our first priority"**

# Index

|                                                   |    |
|---------------------------------------------------|----|
| 1) Preface                                        | 3  |
| 2) Online shopping best practices                 | 4  |
| 3) Email best practices                           | 5  |
| 4) Browser best practices                         | 6  |
| 5) Social media best practices                    | 7  |
| 6) Mobile phone best practices                    | 8  |
| 7) Aadhaar best practices                         | 9  |
| 8) Desktop best practices                         | 10 |
| 9) CERT-In Awareness materials & Security tools   | 11 |
| 10) Reporting Cyber security incidents to CERT-In | 12 |
| 11) Report Cybercrime or Cyber fraud to I4C       | 12 |

# 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 Safer Internet Day on 6th February 2024 .

This Internet Safety 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 for using the internet in a safe and secure manner .

# Online Shopping Best Practices



## Best Practices



- Always visit trusted websites to do your online shopping.
- Keep your device secured with antivirus, anti-malware solutions.
- Keep track of your digital payments.
- Check the security aspects of the website, such as whether the site is secured with https://: or a padlock on the browser address bar.
- Never respond to emails that ask about your personal information and account details.
- Change your passwords frequently.
- Always use a secured internet connection.
- Avoid using public Wi-Fi for doing financial transactions.
- Don't click on suspicious links offering discounts or prizes that seems too good to be true.



# E-mail Best Practices

## Tips for E-mail Safety



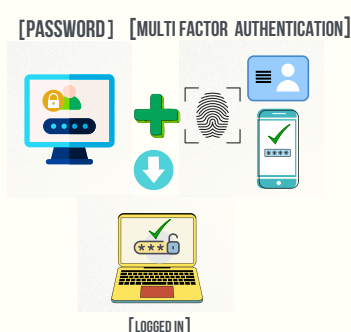
**Always use e-mail filtering software to avoid spam so that only messages from authorized users are received.**



**Avoid opening links/attachments from unknown sources as they may be malicious .**



**Regularly scan your system with updated antivirus and anti-malware software.**



**Enable Multi-Factor Authentication**



**Avoid filling of forms that comes via unsolicited email or clicking on links in emails received from untrusted sources.**

**Emails or messages that create a sense of urgency is a warning!**

# Browser Best Practices



## Best Practices

- Always update your web browser with the latest patches.
- Disable pop-up windows in your browser.
- Delete browser cookies and cache regularly.
- Enable private browsing or incognito mode.
- Be careful with the websites/links you visit.
- Expand shortened URLs and verify them before clicking.
- Use privacy or security settings that are inbuilt into the browser.
- Disable the login and password remember option.
- Enable warn the user option when websites try to install extensions or themes.
- Enable "Safe Search" ON in Search Engines.

# Social Media Best Practices



## Best Practices



- 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 received 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.



# Mobile Phone Best Practices



## Best Practices

- Use updated antivirus and anti-malware software.
- Use updated Operating system.
- Always download apps from playstore or appstore.
- Do not download apps from third party websites or links received through messages or chats.
- Enable only necessary permissions for apps.
- Do not click on any suspicious link received from strangers.
- Do not share your OTP received for any application with anyone.
- Enable Multi-Factor Authentication whenever possible.
- Always keep your phone locked if not in use.
- Avoid USB charging in public places.

# Aadhaar Best Practices



## Best Practices

- Lock your biometrics through the m-Aadhaar app/ UIDAI portal to prevent unauthorized access to your account details.
- Use Virtual ID (VID) or Masked Aadhaar to avoid disclosure of Aadhaar number.
- Link your aadhaar data to your mobile number to get alert of any activity.
- Keep your digital aadhaar copies secure.
- Do not share your aadhaar details, OTP to strangers.
- Avoid saving your digital aadhaar in Public computers.
- Delete aadhar information/copies from public computers, once your work is completed.



# Desktop Best Practices



## Best Practices

- Use genuine operating systems and software.
- Keep your operating system updated.
- Install anti-virus and anti-malware solutions.
- Keep your antivirus and anti-malware solutions updated.
- Use strong login password and change them periodically.
- Regularly take backups of your important files and data.
- In-case 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 they can be used for restoration when needed.

# Awareness Materials

## Guidelines:

***Guidelines on Information Security Practices for Government Entities***

Visit: <https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf>

***Guidelines for Secure Application Design, Development, Implementation & Operations***

Visit: [https://www.cert-in.org.in/PDF/Application\\_Security\\_Guidelines.pdf](https://www.cert-in.org.in/PDF/Application_Security_Guidelines.pdf)

## Advisories:

Visit : <https://www.cert-in.org.in>

***CERT-In Advisory CIAD-2024-0006 : Securing Social Media Accounts***

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

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

## Awareness Booklet:

Visit: [https://www.cert-in.org.in/PDF/CSA\\_Booklet.pdf](https://www.cert-in.org.in/PDF/CSA_Booklet.pdf)

# 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](mailto:incident@cert-in.org.in) Information Desk

Toll Free Phone: [+91-1800-11-4949](tel:+91-1800-11-4949) Phone: [+91-11-24368551](tel:+91-11-24368551)

Toll Free Fax: [+91-1800-11-6969](tel:+91-1800-11-6969) Fax: [+91-11-24368546](tel:+91-11-24368546)

**For Reporting Cyber Fraud & Crime to I4C:**

Visit website: <https://www.cybercrime.gov.in>

Call : [1930](tel: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](mailto:vdisclose@cert-in.org.in) (Vulnerability disclosure)  
[collaboration@cert-in.org.in](mailto:collaboration@cert-in.org.in) (Collaboration)

Phone: [+11-22902600](tel:+11-22902600) Ext: [1012, +91-11-24368572](tel:+91-11-24368572)

**For Trainings/ Awareness programmes:**

Email: [training@cert-in.org.in](mailto: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>



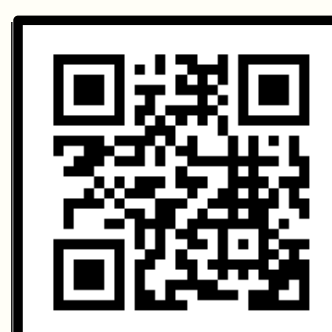
[https://www.instagram.com/cert\\_india/](https://www.instagram.com/cert_india/)

Scan Me



[www.cert-in.org.in](http://www.cert-in.org.in)

Scan Me



[www.csk.gov.in](http://www.csk.gov.in)