Ministry of Electronics and Information Technology
Government of India

certin
Enhancing Cyber Security in India

ISEA Information Security Education & Awareness

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

DIGITAL SAFETY COMPASS HANDBOOK

For Digital Nagriks & Digital Enterprises

By

Indian Computer Emergency Response Team

[CERT-In]

On the occasion of

Safer Internet Day

11th Feb 2025

Security is our first priority

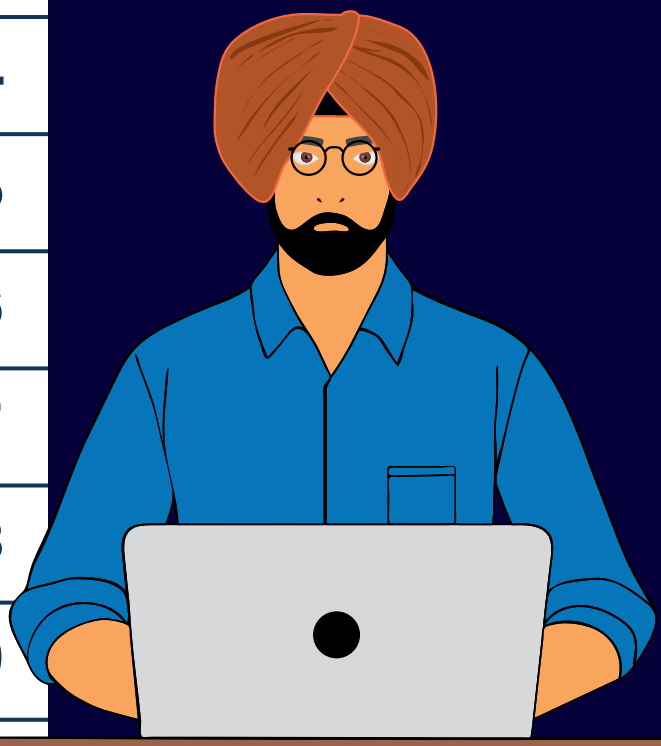
Table of Contents

Preface	03
Phishing Website Scams	04
Digital Arrest	05
Package Fraud	06
Cash-on-Delivery (CoD) Scams	07
Banking App Frauds	08
Phone Scams	09
Fake Job Proposals	10
Emotional Manipulation	11
Lottery and Prize Frauds	12
Fake Technical Assistance	13
Online Payment Scams	14
Fake Charity Appeal	15
Fraudulent Loan App Scam	16
Fake Trading Apps	17
Awareness Materials	18
Contact Us	19

certin
Enhancing Cyber Security in India

CERT-In's

Digital Safety Compass Handbook



PREFACE

The **Indian Computer Emergency Response Team (CERT-In)** is a Government Organization under the 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 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 Safer Internet Day on 11th February, 2025.

This Digital Safety Compass Handbook 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 need to be followed for using the internet in a safe and secure manner.

Enhancing
Cyber Security
in India

PHISHING WEBSITE SCAMS

Scammers create fake websites and steal personal information such as banking details, card details, personal information.

How Attacks Work

Scammer sends fake email.

Email arrives in inbox with a link .

Victim click on the link.

Fake website asks sensitive information.

Victim's enters the information.

Unauthorized access and data misuse.

Safety Practices

- Be cautious while clicking on links & attachments in emails received from strangers.
- Never share sensitive details like passwords or PINs via email or text.
- Watch for poor grammar or spelling mistakes, which can be signs of phishing.
- Use unique, complex passwords for each account.
- Expand and verify shortened URLs before clicking on them.

certin
Enhancing Cyber Security in India

DIGITAL ARREST

Victims get messages/calls claiming that they're under investigation for doing illegal activities.

Initial Contact

Scammers impersonate authorities by sending urgent messages about legal actions via texts, calls, and social media apps.

The Accusation

Targets are falsely accused of carrying out illegal activity, and they are threatened using legal jargon and fake case numbers.

Scare Tactics and Urgency

Scammers pressure victims to act fast by threatening arrest or fines. If questioned, they behave aggressive and make harsher threats to scare the victim into complying.

SAFEGUARDS

Beware of fake official calls. Stay calm, don't panic.

Legitimate law enforcement never asks for payment details.

Government agencies do not use WhatsApp and Skype for official communication.

Package Fraud

Scammers claim your package was seized for illegal items like drugs or prohibited items. Ignore such calls, emails, or messages.

Scammers pretend to be delivery workers/ Customer care executives to trick people.

They tell victims that their package has illegal items and make them scared.

The call is passed to fake Law enforcement officers to create a fake threat.

Victims are threatened to pay money to avoid arrest and reputational damage.

Safety Practices

- Beware of unsolicited calls or messages.
- Verify claims with official sources.
- Do not transfer money under pressure
- Never share sensitive personal information.
- Resist threats and urgency tactics.

CASH-ON-DELIVERY (COD) SCAMS

Scammers send fake or low-quality products after collecting cash.

They may send random packages, expecting you to pay without questioning.

Restrictions on checking parcels beforehand help scammers deceive buyers.

Stay alert, stay safe!

- Research sellers and their reviews before buying. Use trusted websites to avoid fake sellers.
- Stay aware of what you've ordered. If a package arrives unexpectedly, don't accept it.
- If you didn't order it, say no! Don't feel pressurized to pay.
- check for secure online payment options with buyer protection .

BANKING APP FRAUDS

Scammers trick users into installing fake banking apps to steal credentials and empty their accounts.

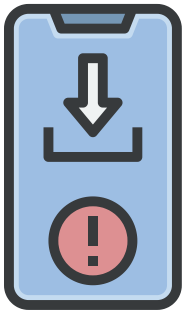
Victims receive an SMS or WhatsApp message about a security issue.

The app mimics a bank login to steal credentials and OTPs.

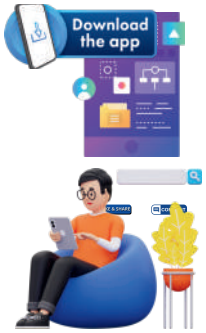
A fake banking app (.apk file) is sent for installation.

Attackers intercept OTPs to access and drain bank accounts.

Protect Yourself



Avoid downloading apps from unknown sources and third party platforms.



Banks never ask to download any apk file/app through social media platforms.

Never share otp, banking credentials with anyone.

PHONE SCAMS

Victims receive calls claiming to be from telecom regulators/banks/service providers stating there's an issue with their service and scammers ask to install app or click links for remote access.

- Tries to steal your personal or financial details by asking directly.
- Tricks you into downloading harmful software or giving remote access to your device.
- Falsely claims your bank or online accounts are hacked to make you panic.

PAUSE AND THINK
the caller is likely to be a scam

Stay Alert, Stay Secure

Never share personal, financial, or login details over the phone.

If in doubt, contact the organization directly using official channels.

Block scam numbers immediately to prevent repeat calls and stay safe.

FAKE JOB PROPOSALS

Scammers promise fake high-paying jobs with little effort, aiming to steal your money and identity.

Red Flags in Job Offers

- Unexpected contact from a recruiter via text or encrypted platforms.
- Promises of high income with minimal effort from home.
- Rapid hiring with no interviews or qualifications discussed.
- Asked to pay a fee or top up an account to start tasks.
- Tasks involve money transfers, purchases, or package handling.

Safety Practices

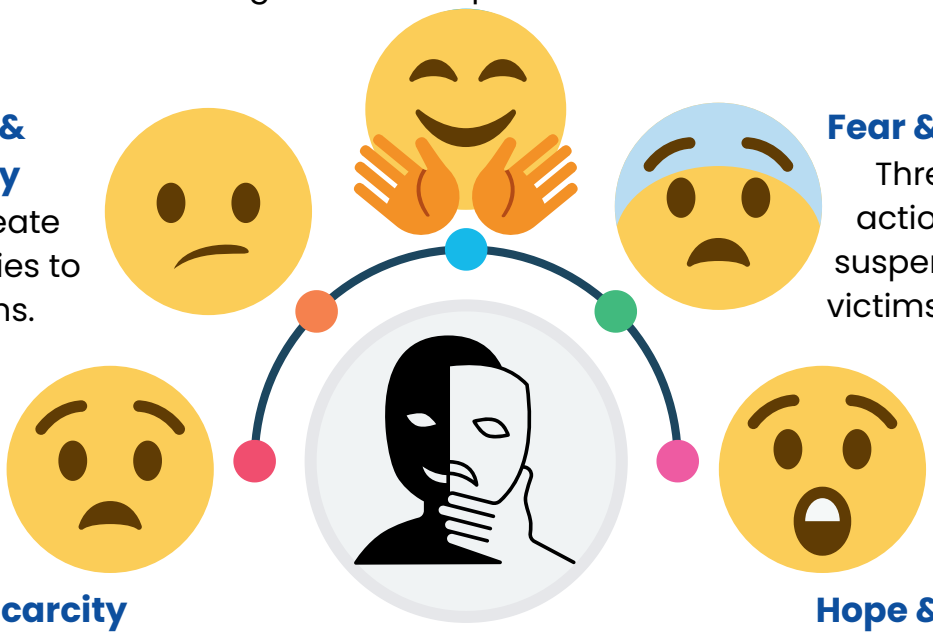
- Verify job offers carefully, even on trusted platforms.
- Genuine employers don't ask for upfront payments or fees.
- Avoid sharing personal or banking details with unverified recruiters.
- Be cautious of pressure tactics and rushed offers.

EMOTIONAL MANIPULATION

Emotional manipulation scams use fake profiles to exploit victims for money.

Authority & Trust
Attackers impersonate trusted figures to manipulate victims.

Confusion & Complexity
Scammers create fake emergencies to rush decisions.



Fear & Intimidation
Threats of legal action or account suspension pressure victims to act quickly.

Urgency & Scarcity
Attackers use urgent offers or emergencies to pressure quick decisions.

Hope & Excitement
Scammers lure victims with fake rewards, job offers, or emotional bonds.

BE CAUTIOUS

- Avoid sharing personal details with unfamiliar individuals.
- Remain cautious regarding unsolicited messages.
- Conduct thorough research prior to committing to any financial decisions.
- Always inquire for clarification when uncertain.

LOTTERY AND PRIZE FRAUDS

- Some scammers might try to trick you by claiming you've won a contest in order to steal your money or personal information.
- They often request advance payments for things like fees or taxes to supposedly release your prize.
- Victims, hoping to receive something special, may send money or share their information, only to find that no prize ever arrives, exposing the scam for what it is.

Be Alert

Avoid clicking on shortened **links**.

Stick to websites starting with **https://**.

Always verify **authenticity** before responding.

Never pay an **advance** fee to claim competition prizes.

FAKE TECHNICAL ASSISTANCE

Beware of calls, emails, or pop-ups claiming your computer has issues. Scammers often pose as trusted companies to create fear.

Scammer's Tactics

Request remote access.

Enrolls in Fake Programs.

Install malware for password access.

Demand credit card info for scams.

Try to sell worthless service/software.

Direct to fake websites for sensitive info.

Useful Techniques

- Hang up if someone claims your computer has a problem; scammers often use fake caller IDs.
- Avoid calling numbers or clicking links in pop-ups warning of system issues.
- Contact your security software provider directly using official contact details.
- Seek help only from verified cybersecurity professionals.
- Never share passwords or grant remote access to unverified contacts.

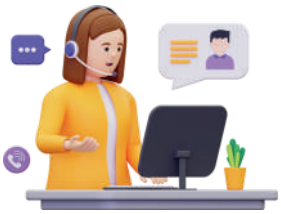
ONLINE PAYMENT SCAMS

Has a stranger 'accidentally' sent you money on a payment app?
Beware — it might be an online payment app scam.

Ways used by Scammers

Impersonation

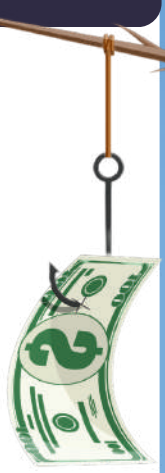
E-Commerce



Customer support

Lottery or jackpot

Lucrative investments



Safety Practices

- Verify urgent payment requests through direct communication or unique personal questions.
- You don't need a UPI PIN or OTP to receive money.
- Be cautious of offers that seem too good to be true.
- Monitor financial statements regularly for unauthorized activity.

FAKE CHARITY APPEAL

Charity scammers pretend to be from real charities and contact people by phone, email, social media, or in person. They create fake websites and materials to look trustworthy.

Do's

- Ask questions about the charity's mission and spending.
- Donate securely through official platforms.
- Most legitimate charity organisation websites use .org rather than .com.
- Be cautious of urgent or emotional appeals.

Dont's

- Don't send cash or gift cards.
- Don't trust links from random emails or messages.
- Don't share personal or financial details with strangers.
- Don't rush into donating without proper verification.

FRAUDULENT LOAN APP SCAM

Fake loan app scams target individuals in financial need and distress. Scammers pose as legitimate lenders, offering quick loans with little or no paperwork.

Scammers target vulnerable people via fake websites, ads, or emails.

Once victims show interest, fraudsters ask for advance fees, or bank access and makes the victim to install malicious apps.

Victims are lured into high-interest loans, making repayment nearly impossible.

Scammers extort money by manipulating photos and threatening victims.

Safety Practices

- Legitimate lenders don't request upfront fees. Avoid those demanding payment before loan disbursement.
- Be cautious of unsolicited loan offers promising guaranteed approval without credit checks.
- Carefully scrutinize interest rates and terms; if they seem too good to be true, they likely are.
- Make sure the app has a Reserve Bank of India's (RBI's) mobile-only Non-Banking Financial Company (NBFC) license to give loans.

FAKE TRADING APPS

The fraudulent trading app scam involves creating deceptive apps to trick investors, promising high returns with low risk to lure you into investing.

Scammers try to contact victims through social media and establish trust.

After gaining trust, scammers offer a fake trading app as a profitable investment.

The app falsely shows rising investments, misleading victims into investing more.

Scammers impose hidden fees when victims withdraw funds, hindering their recovery efforts.

Safety Tactics

- Ensure your broker is SEBI-registered. Verify on SEBI's official website.
- Use the official app or website of a registered broker for fund transfers.
- Some influencers may promote fake investments. Research before trusting their advice.
- Avoid transferring money to personal accounts; always use the official app or website of a registered broker.

AWARENESS MATERIALS

Guidelines on Information Security Practices for Government Entities:
https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf

Guidelines for Secure Application Design, Development, Implementation & Operations:
https://www.cert-in.org.in/PDF/Application_Security_Guidelines.pdf

Technical Guidelines on SOFTWARE BILL OF MATERIALS (SBOM):
https://www.cert-in.org.in/PDF/SBOM_Guidelines.pdf

Awareness Booklets:
https://www.cert-in.org.in/AwarenessBooklets.jsp

Check CERT-In's latest advisories at:
https://www.cert-in.org.in/s2cMainServlet?pageid=PUBADVLIST

Check CERT-In's latest vulnerabilities notes at:
https://www.cert-in.org.in/s2cMainServlet?pageid=VLNLIST

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

csk@cert-in.org.in

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

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

certin
Enhancing Cyber Security in India

CONTACT US

FOR REPORTING CYBER SECURITY INCIDENTS TO 24/7 INCIDENT RESPONSE HELP DESK

incident@cert-in.org.in

FOR QUERIES RELATED TO BOTNET CLEANING INITIATIVE

csk@cert-in.org.in

CERT-IN INFORMATION DESK

info@cert-in.org.in

subscribe@cert-in.org.in

advisory@cert-in.org.in

FOR INDUSTRY & ACADEMIA COLLABORATION

collaboration@cert-in.org.in

FOR TRAININGS/ AWARENESS PROGRAMMES

training@cert-in.org.in

FOR REPORTING CYBER SECURITY VULNERABILITIES

vdisclose@cert-in.org.in

Indian Computer Emergency Response Team
Government of India, Ministry of Electronics and Information Technology,
Electronics Niketan, 6, CGO Complex, Lodhi Road,
New Delhi-110003

FOLLOW US ON

@IndianCERT

@cert_india

24X7 Incident Response Help Desk
+91-11-24368572

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

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

Training/Awareness

Tel: +91-11-22902600 **Ext:** 1012

Information Desk

Phone: +91-11-24368551

Fax: +91-11-24368546

For Reporting Cyber Fraud & Crime to I4C:

- https://www.cybercrime.gov.in/ or call 1930

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

SCAN ME!

https://www.csk.gov.in