

AI AWARENESS GUIDE

CYBER SMART INDIA

SECURE TODAY, RESILIENT TOMORROW



NATIONAL CYBER SECURITY AWARENESS MONTH (OCTOBER 2026)

ORGANISED BY
**INDIAN COMPUTER EMERGENCY
RESPONSE TEAM**

Follow us :



@IndianCERT



@cert_india

Table of Contents

- Preface 3
- AI-enhanced phishing & social engineering 4
- Voice & video deepfakes (vishing) 5
- AI-assisted malware & automated attacks 6
- Fake Websites & Identity Theft 7
- Red flags checklist 8
- Online safety 9
- Device safety 10
- Use AI responsibly 11
- Choose Trusted Apps 12
- Report cyber security incidents to CERT-In 13

Follow us :



@IndianCERT



@cert_india

Preface

Artificial Intelligence (AI) is transforming the way we live, work, and communicate. It enables innovation, improves productivity, and helps solve complex problems across different sectors. However, the same technology is also being misused by threat actors to create more advanced and convincing cyber threats.

AI is making digital threats more difficult to identify because attackers can now create highly realistic emails, messages, audio, videos, and websites. Traditional warning signs, such as poor grammar, unusual formatting, or obvious mistakes, may no longer be reliable indicators. Verification and responsible digital practices have become more important than ever.

AI tools and smart devices we use every day can introduce new privacy and security risks if they are not used carefully. Sharing personal or confidential information with untrusted AI applications, granting unnecessary permissions, or relying on AI generated information without verification may expose individuals and organizations to security risks.

This booklet by Indian Computer Emergency Response Team (CERT-In) on “AI Cyber Awareness” is designed for everyday citizens, employees, and digital users, not only cybersecurity professionals. It explains how AI is changing the digital threat landscape and provides simple, practical steps that everyone can follow to protect personal information, devices, and online identity.

Follow us :



@IndianCERT



@cert_india

AI-ENHANCED PHISHING & SOCIAL ENGINEERING



How It Works ?

Threat actors now send emails and texts that look real and error free. They use details about you, such as your job, services you use, or recent activities, to make messages feel personal. Since these messages are well written, they can be much harder to spot.

How to Identify ?

- The message feels highly specific to you but arrives unexpectedly.
- It uses an urgent or threatening tone and demands immediate action.
- It asks you to click a link, verify an account, reset a password, or make a payment.
- The sender's address looks almost right, but not quite.

How to Stay Safe ?

- Do not click links in unsolicited messages. Go directly to the official website or app instead.
- Verify requests through a separate, trusted contact channel, such as an official phone number or app.
- Never enter credentials or OTPs on a page reached through a message link.
- Report and delete suspicious messages, then block the sender.

Follow us :



@IndianCERT



@cert_india

VOICE & VIDEO DEEPFAKES (VISHING)



How It Works ?

Threat actors can clone voices or create fake videos that look and sound real. They may pose as family, colleagues, or officials to pressure you into sharing sensitive information, sending money, or acting quickly.

How to Identify ?

- Unusual urgency, panic, or requests for secrecy, such as don't tell anyone.
- A slightly off tone, pacing, background noise, or audio quality.
- Requests to bypass normal verification or approval processes.
- Requests for payment via gift cards, cryptocurrency, or wire transfer.

How to Stay Safe ?

- Hang up and call the person back using their known, saved number.
- Set a family or workplace safe word to verify identity in emergencies.
- Never authorize payments based on a call or video alone. Confirm in writing through a separate channel.
- Pause before reacting. Threat actors rely on panic to cloud your judgment.

Follow us :



@IndianCERT



@cert_india

AI-ASSISTED MALWARE & AUTOMATED ATTACKS



How It Works ?

Threat actors use AI tools to create or hide malicious code, test stolen passwords across multiple sites, and identify systems that need updates. This makes attacks faster and more widespread.

How to Identify ?

- Unexpected login alerts, password reset emails, or MFA prompts you didn't request
- Unfamiliar devices or sessions listed in your account activity
- Antivirus warnings, pop-ups, or unusually slow device performance
- Files, settings, or browser extensions you don't recognize

How to Stay Safe ?

- Use a unique, strong password for every account.
- Enable multi factor authentication (MFA) on all important accounts.
- Keep antivirus software, systems, and apps up to date.
- Act immediately on unexpected login or MFA alerts.

Follow us :



@IndianCERT



@cert_india

Fake Websites & Identity Theft



How It Works ?

Threat actors can create look alike websites and chatbots that appear genuine, such as banking or shopping portals, to steal your login credentials, OTPs, or payment details. They may also use fake photos or documents to create false identities.

How to Identify ?

- Slightly altered website URLs, such as extra letters, hyphens, or a different domain ending.
- Chatbots or agents asking for OTPs, PINs, or full card numbers.
- Missing HTTPS or unusual design inconsistencies on a familiar site.

How to Stay Safe ?

- Always type official URLs directly or use verified bookmarks, rather than clicking links
- Never share OTPs, PINs, or full card details with any chatbot or "support agent"
- Check for HTTPS and look closely at the domain name before logging in anywhere
- Monitor your bank statements and credit report regularly for unfamiliar activity.

Follow us :



@IndianCERT



@cert_india

RED FLAGS CHECKLIST



Watch for these signs of an AI-enabled attack:



- ☒ Urgent, pressured request for money, credentials, or approval
- ☒ Slight audio/video inconsistencies in a call or video from a "known" person
- ☒ Request to bypass normal verification/ approval procedures
- ☒ Unfamiliar sender domain or slightly altered URL
- ☒ Unexpected MFA prompts or OTPs you didn't request
- ☒ Requests to disable security software or "verify" via unofficial links
- ☒ Job/investment offers requiring upfront payment or personal financial details

When in doubt — pause, verify independently, and don't act under pressure.

Follow us :



@IndianCERT



@cert_india

Online Safety



Protect Your Accounts

- Use strong and unique passwords for every account; use a password manager to store them securely.
- Enable Multi-Factor Authentication (MFA) wherever available.
- Never share OTPs, PINs, passwords, or security codes with anyone.
- Use biometric authentication (fingerprint/face recognition) as an additional security layer.

Stay Safe While Using Email & the Internet

- Check sender details carefully for suspicious or look-alike email addresses.
- Verify links before clicking and avoid opening unexpected attachments.
- Confirm website authenticity before entering login or financial details.
- When in doubt, stop and verify before you act.

Prepare Before Something Goes Wrong

- Maintain regular backups of important files, stored offline or in a secure cloud service
- Keep account recovery information (email/phone) updated and secure

Follow us :



@IndianCERT



@cert_india

Device Safety

ESSENTIAL DEVICE SAFETY & CYBERSECURITY TIPS FOR ALL USERS

1. KEEP UPDATED



2.

TRUSTED SOFTWARE



3. SECURE DEVICES



4.

PROTECT NETWORK



Keep devices updated

- Regularly update operating systems, applications, browsers, and security software to fix known vulnerabilities.
- Enable automatic updates wherever possible.

Install trusted software only

- Use genuine software and install applications only from official app stores or trusted sources.
- Use reliable antivirus or security solutions and keep them updated.

Secure your devices and accounts

- Use strong passwords or screen locks on all devices.
- Enable device encryption and security features whenever available.
- Review and remove unnecessary applications and permissions.

Protect your network connection

- Secure your Wi-Fi with a strong password and change default router credentials.
- Use updated router firmware and secure network settings.
- Avoid accessing sensitive accounts or sharing confidential information over unsecured networks.

Follow us :

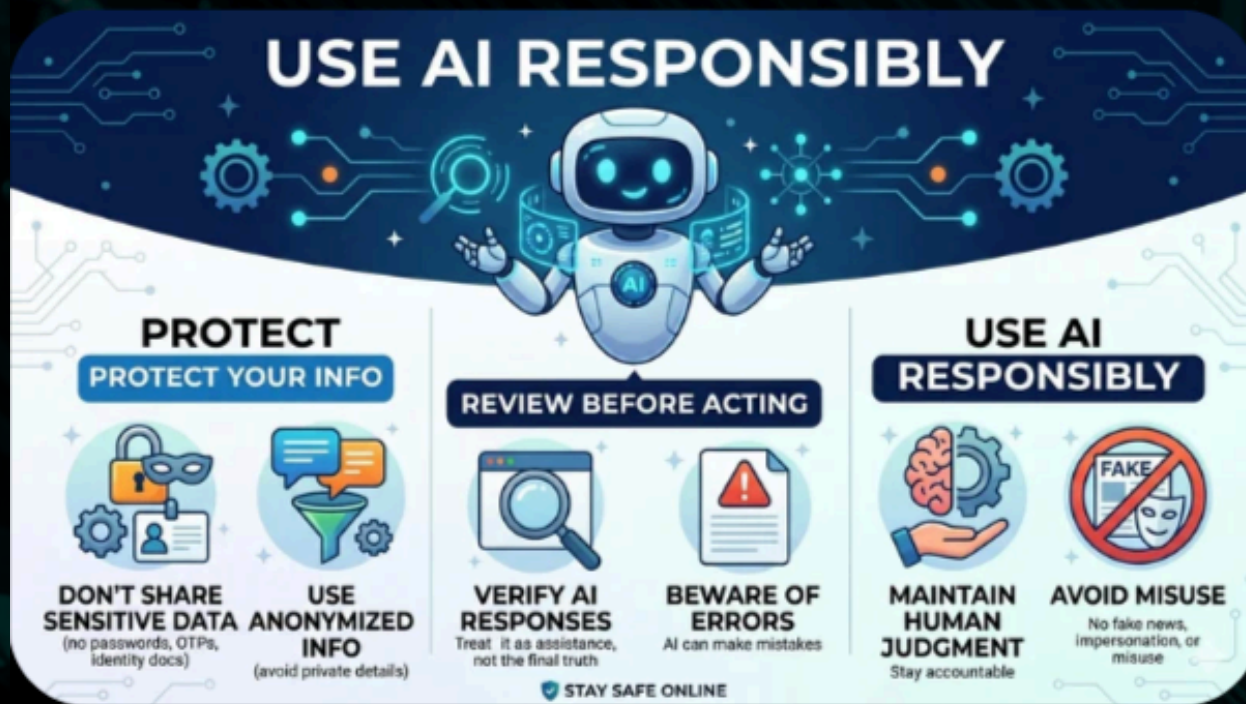


@IndianCERT



@cert_india

Use AI Responsibly



»» *Protect Your Personal Information*

- Do not enter personal, financial, health, official, or confidential information into public AI tools or unknown online services.
- Avoid sharing sensitive details such as passwords, OTPs, account numbers, identity documents, customer data, or private conversations.
- Use anonymized or general information when asking AI tools for assistance.

»» *Review Before You Share or Act*

- Treat AI-generated responses as assistance, not as a final source of truth.
- Verify important information before using it for financial, legal, professional, or personal decisions.
- Be aware that AI tools may produce incorrect, incomplete, or misleading information.

»» *Use AI Tools Responsibly*

- Use AI to support your work and learning, but maintain human judgment and accountability.
- Do not use AI to create or spread false information, impersonate others, or misuse someone's personal data.

Follow us :

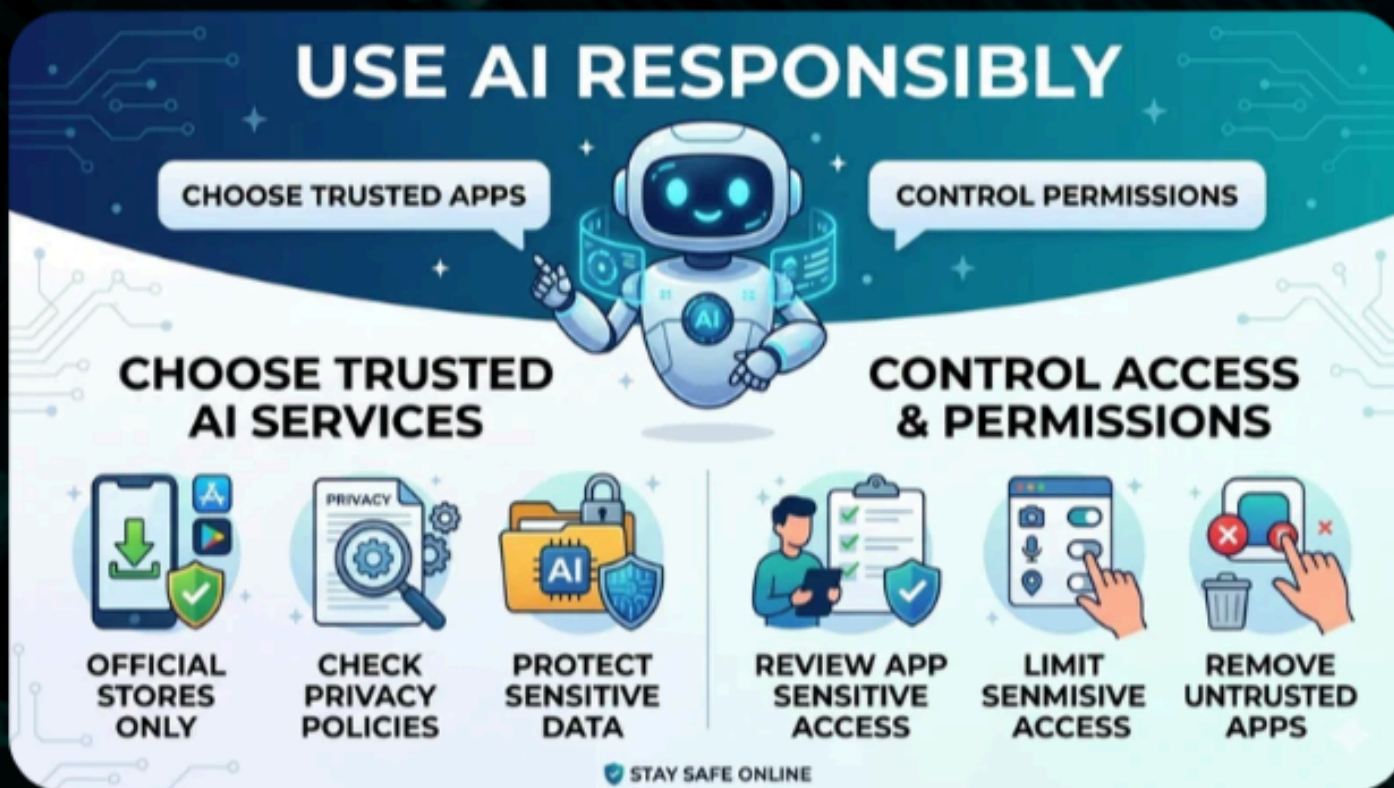


@IndianCERT



@cert_india

Choose Trusted Apps



» *Control App Access & Permissions*

- Review permissions granted to AI applications and digital assistants.
- Allow access only when necessary to features such as the camera, microphone, contacts, or location.
- Remove unnecessary permissions and uninstall apps from untrusted sources.

» *Choose Trusted AI Services*

- Use AI applications from reputable providers and download them only from official app stores.
- Review privacy settings, terms of use, and data handling practices before using AI services.
- Avoid connecting AI tools to sensitive accounts or files unless the security controls are verified.

Follow us :



@IndianCERT



@cert_india

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: **+91-11-22902657**

Follow us :



@IndianCERT



@cert_india



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

साइबर स्वच्छता केन्द्र

CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre



Awareness Booklet

<https://cert-in.org.in/AwarenessBooklets.jsp>



Security Tools

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