Cyber Society of India

CONNECT | COLLABORATE | SECURE

Regn. No.: 254/2004
www.cysi.in

CYBERCRIME AWARENESS MONTH

STAY ALERT

STAY SAFE

BE A RESPONSIBLE NETIZEN

Stronger Community | Safer Cyberspace | Digital India

The digital world brings great opportunities, but also risks. Cybercriminals exploit trust, fear and lack of awareness. Let's stay informed, be vigilant and protect ourselves and our loved ones.

Think - Verify - Protect

Common Cyber Threats

- **UPI and Payment Fraud**
  - Fake payment screenshots, fraudulent collect requests, QR-code scams, or requests to enter UPI PIN to receive money.
- **Digital Arrest Scams**
  - Fraudsters impersonating Police, CBI, customs or government officials and threatening arrest to extort money.
- **Investment & Cryptocurrency Scams**
  - Promises of guaranteed returns, fake trading apps, manipulated profits and pressure to invest more.
- **Phishing & Impersonation**
  - Fake emails, SMS, social media profiles and websites designed to steal credentials or financial information.
- **Job & Task Scams**
  - Fake work-from-home offers demanding registration fees, deposits or advance payments.
- **Social Media & Romance Scams**
  - Fake identities, emotional manipulation, blackmail and requests for money or intimate content.
- **Malicious Apps & Links**
  - Fake APK files, screen-sharing requests and apps that steal credentials or enable unauthorized access.
- **Identity Theft & Account Takeover**
  - Misuse of personal data, OTPs, passwords and compromised accounts.

Follow These Cyber Safety Practices

1. **Never share OTPs, PINs, passwords, CVV numbers** or banking credentials with anyone.
2. **Never transfer money under pressure.** Government agencies do not demand payment through video calls or personal bank transfers.
3. **Verify before you trust.** Independently confirm the identity of callers, payment requests, job offers and investment platforms.
4. **Use strong, unique passwords** and enable multifactor authentication wherever available.
5. **Keep devices and applications updated** and install apps only from trusted official sources.
6. **Do not click suspicious links** or install APKs received through WhatsApp, SMS, email or social media.
7. **Secure your social media accounts.** Review privacy settings and restrict public exposure of personal information.

8. **Verify UPI requests carefully.** A UPI PIN is used to authorize a payment, not to receive money.
9. **Back up important data and use trusted security software** on your devices.
10. **Educate children and senior citizens** about online grooming, cyberbullying, fake offers, impersonation and financial fraud.

The Golden Rules - S T V P R

S — STOP	: Do not act in panic or under pressure.
T — THINK	: Recognize urgency, fear, greed and unrealistic promises as warning signs.
V — VERIFY	: Confirm identities and requests through independently obtained official channels.
P — PROTECT	: Secure your devices, money, identity and personal information.
R — REPORT	: Speak up promptly. Do not let embarrassment delay action.

If You Become a Cybercrime Victim

- **Act immediately — every minute matters.**
- **1930:** Call India's cybercrime helpline (especially for financial fraud resulted monetary loss
- **cybercrime.gov.in:** Report online at the National Cyber Crime Reporting Portal.
- **Contact your bank or payment service provider immediately** to report the transaction and request protection.
- **Preserve evidence:** Save transaction IDs, statements, messages, URLs, screenshots and other details.
- **Secure your accounts:** Change passwords, revoke suspicious sessions and enable multifactor authentication.
- **Report impersonation** or malicious content to relevant platforms and law-enforcement authorities.
- *Reporting does not guarantee recovery, but prompt action can improve the chances of limiting financial loss and supporting investigation.*

Our Collective Responsibility:
Cybersecurity is not just a technical issue — it's a shared social responsibility. Discuss cyber threats with your family, colleagues, students and community. Share verified information, report suspicious activity and help potential victims seek assistance without blame or stigma.

Stay informed. Stay vigilant. Stay cyber-safe.

With warm regards,
Vijayakumar KM,
Secretary,
Cyber Society of India

Together for a Safer Digital Tomorrow