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

Digital India
Power To Empower

एनआईसी National Informatics Centre

CYBER SECURITY AWARENESS

NEVER TRUST. ALWAYS VERIFY.

Building a Safer Digital Environment

Cyber security protects sensitive data., ICT equipment, endpoints, servers, networks, applications and mission-critical assets through technology, processes and practices.

For government officers and organisations, one compromised account, device, email or application can become an entry point for a larger cyber attack.

UNDERSTANDING THE CYBER THREAT

Cyber attacks often begin with information gathered from a person's or organisation's digital footprint. Attackers use this intelligence to send malicious links or messages and exploit human action. This can lead to account takeover, information theft or financial loss.

Pause. Verify. Think before you click.

COMMON CYBER THREATS

- Phishing & Multilayer Phishing
- Credential Theft
- OTP Fraud
- QR Code Scams
- Fake Website Scams
- Malicious APKS & Side-Loading Apps
- Shadow IT Systems
- Payment Receiving Traps
- Freebie / Reward Scams
- Account Takeover
- Information Gathering through Digital Footprints

THE HUMAN FACTOR

Cybersecurity is not just about technology; it's about people. Attackers exploit urgency, fear, curiosity and trust when verification fails.

URGENT | FEAR | CURIOSITY | TRUST | LACK OF VERIFICATION

Suspicious links, unexpected attachments, unknown applications, fake websites and urgent requests can begin a cyber incident.

REAL-WORLD SCENARIOS

FAKE WEBSITES
Fake websites look real and are designed to steal your credentials or financial information.

OTP FRAUD
Fraudsters trick you into sharing OTP and gain access to your accounts.

QR-CODE SCAMS
Malicious QR Codes can lead to fake websites or trigger unwanted transactions.

MALICIOUS APPLICATIONS
Fake or harmful apps can also be installed on your device.

ACCOUNT TAKEOVER
Attackers use stolen credentials or tricks to take over your accounts and misuse them.

ZERO TRUST & EVERYDAY CYBER HYGIENE

THE ZERO TRUST APPROACH

1 **NEVER TRUST, ALWAYS VERIFY**
Verification before access or action.

2 **LEAST PRIVILEGE**
- Minimum privilege
- Temporary privilege
- Just-enough access
- Just-in-time access

3 **ASSUME BREACH**
- Reduce the blast radius
- Improve visibility and detection
- Respond effectively
- Enable recovery

SEVEN LAYERS OF CYBER SECURITY

1 HUMAN LAYER → 2 PERIMETER SECURITY → 3 NETWORK SECURITY → 4 ENDPOINT SECURITY → 5 APPLICATION SECURITY → 6 DATA SECURITY → 7 MISSION-CRITICAL ASSETS

TAKEAWAY: Cyber attacks may involve multiple stages, but prevention can often begin with one simple action—**verify before you trust.**

PRACTICAL SECURITY MEASURES

EMAIL SECURITY

- Do not open unknown links or attachments.
- Verify the sender's email address.
- Watch for urgency, fear or unusual requests.
- Be cautious of generic greetings and requests for personal information.
- Check suspicious links using appropriate security tools.
- Contact the sender directly when necessary.
- Delete suspicious emails and scan the device.
- Report incidents to the organisational CISO / Dy. CISO as appropriate.

PASSWORD SECURITY

- Use strong, long passwords with mixed characters.
- Change passwords regularly.
- Never reuse passwords.
- Enable MFA wherever available.
- Never share passwords, OTPs, or PINs, even with genuine-looking callers or messages.

WHATSAPP & COMMUNICATION SECURITY

- Be cautious of unexpected messages, links, files, or requests.
- Don't click unknown links or download unknown files.
- Verify the sender through a trusted channel.
- Don't share personal, financial, or confidential information.
- Report and block suspicious accounts.

MALICIOUS APK PROTECTION

- Disconnect from the Internet/Intranet.
- Log out and uninstall sensitive apps.
- Restart in Safe Mode and remove the malicious app.
- Run a security scan.
- Change sensitive passwords.
- Clear cache and downloads.
- Reset/format the phone if required.
- Report the incident on https://cybercrime.gov.in or call to 1930.

VERIFY BEFORE YOU ACT

Use trusted security tools such as VirusTotal and URLScan to check links, files and websites for phishing and malicious content before you click or download.

VIRUS TOTAL | URL SCAN

"The best firewall against cyber criminals is your brain."

BUILDING CYBER RESILIENCE THROUGH POLICY REALIGNMENT

Streamlining Data Security, Governance & Responsible Data Management

Cyber resilience is built on strong policies, responsible data governance, clear data classification, and continuous compliance with evolving requirements.

Under the DPDP Act, 2023, DPDP Rules, 2025 and NDSAP, 2012, organisations are responsible not only for protecting data, but also for ensuring that data sharing is lawful, authorised, secure and accountable."

Key Focus Areas

Policy & Regulatory Alignment

Align with DPD Act, 2023 DPP Rules, 2025 & NDSAP, 2012

- Build compliance into systems
- Operationalising policy through governance frameworks

Data Processing & Maturity

- Strengthen data quality and maturity
- Ensure secure processing at every stage
- Enable trustworthy insights for decision-making

Data Confidentiality

- Classify data based on sensitivity
- Apply least privileged access
- Protect data across its lifecycle
- Prevent unauthorised use, disclosure and leakage

DATA PROCESSING LIFECYCLE

Raw Data

Examples:
- Security
- Safety
- Confidentiality
- Satellite imagery
- Machine readings

Processed Data

Examples: Cleaner and structured and solidified datasets

Enriched Data

Examples: Analytics, visualization, GIS, system and statistical techniques, AI processed etc.

RESILIENT ECOSYSTEM

- Policy
- Data Classification
- Secure Processing
- Controlled Access
- Responsible Sharing
- Continuous Compliance

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Protecting Personal Data, Building Trust in India's Digital Economy.

WHY THIS ACT MATTERS

- Establishes a strong legal framework for protection of personal data.
- Promotes trust in digital services and strengthens the digital economy.
- Defines clear rights for individuals and duties for organisations.
- Supports innovation with responsible and ethical data practices.

KEY PRINCIPLES

- Purpose Limitation — Personal data should be used only for a specified purpose.
- Data Minimisation — Collect only the personal data that is necessary.
- Storage Limitation — Retain data when only as it is needed, and erase it when the purpose is fulfilled.
- Consent & Transparency- Consent may be free, specific, unifiable, or required, supported by appropriate notice.
- Should ensure that personal data is complete, accurate and consistent.
- Appropriate technical and ethical training should be implemented to protect personal data and address breaches.

INDIVIDUAL RIGHTS

- Right to access personal data held by organisations.
- Right to correction and updating of inaccurate data.
- Right to ensure of personal data when no longer necessary.
- Right to object to processing of personal data.
- Right to data portability in an usable format.
- Right to be informed and notified of data breaches.

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते
Digital India Power To Empower
एनआईसी National Informatics Centre