

Securing Your Devices: A Comprehensive Guide

HIMANSHU SHEKHAR

PROJECT ENGINEER

C-DAC PATNA

Agenda

- 1) Why Security Matters.
- 2) The Foundation: Passwords & MFA.
- 3) Securing Your Computers.
- 4) Securing Your Mobile Devices.
- 5) Network & Wi-Fi Safety.
- 6) Identifying and Avoiding Scams (Phishing, Malware).

Why Security Matters

- 1) Data Loss/Theft.
 - **Phishing** was the top attack vector (18% of incidents), and **Business Email Compromise (BEC)** was the costliest root cause, averaging **₹215 Million** (2024). (Source: IBM Cost of a Data Breach Report (2024)).
- 2) Financial Fraud.
 - 36.4 lakh financial fraud cases were reported in 2024 via the NCRP and CFCFRMS, up from 24.4 lakh in 2023. (Source: National Cyber Crime Reporting Portal (NCRP) & Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)).
- 1) Impersonation/Identity Theft.
 - 'Digital Arrest' scams (a form of impersonation) resulted in an estimated loss of ₹2,000 Crore (approx. \$240 Million) in 2024. (Source: BioCatch Report (2025))
- 2) Loss of Trust.
 - 77% of Indian companies reported that fraud had influenced customer satisfaction, and 78% noted its impact on customer conversion rates. (Source: LexisNexis True Cost of Fraud Study (2024))

"Cybersecurity is not an option, it's a necessity."

Strong Passwords: Your First Line of Defense

- 1) **Complexity:** Use a mix of upper/lower case, numbers, and symbols.
- 2) **Length:** At least 12-14 characters.
- 3) **Uniqueness:** Never reuse passwords.
- 4) **Tool:** Use a reputable Password Manager (e.g., LastPass, 1Password).

“DO NOT USE SAME PASSWORD ON DIFFERENT PLATFORMS”

Multi-Factor Authentication (MFA)

- 1) What is MFA?** An extra layer of security (Something you Know + Something you Have).
- 2) Types:** Authenticator App (Best), SMS/Email (Good), Biometrics.
- 3) Action:** Enable MFA on all critical accounts (Email, Banking, Social Media).

Computer Security: The Golden Rule

- 1) Regular Updates (Patching):** OS, Browser, and Applications. Updates fix security holes.
- 2) Antivirus/Anti-Malware:** Use a reputable solution and keep it active/updated.
- 3) Firewall:** Keep the built-in firewall enabled for network protection.

Computer Security: Best Practices

- 1) **Encryption:** Enable full-disk encryption (BitLocker/FileVault).
- 2) **Backups:** Regularly backup data to an external drive or cloud.
- 3) **Access Control:** Lock your screen when away. Use a complex PIN/Biometric login.

Mobile Device Security: The Basics

- 1) Screen Lock:** Mandatory use of PIN/Pattern/Biometrics.
- 2) App Permissions:** Review and limit permissions (Location, Contacts, Camera).
- 3) Official Stores Only:** Download apps only from official App Stores (Google Play/App Store).

Mobile Device Security: Pro Tips

- 1) **Remote Wipe:** Know how to remotely erase your device if stolen.
- 2) **Disable unused:** Turn off Wi-Fi, Bluetooth, and Location when not in use.
- 3) **Physical Security:** Do not leave your device unattended in public.

Network Safety: Home Wi-Fi

- 1) **Router Default:** Change the default router password immediately.
- 2) **Strong Encryption:** Use WPA2 or WPA3 security protocol.
- 3) **Guest Network:** Use a separate Guest Network for visitors/smart devices.

Network Safety: Public Wi-Fi

- 1) Avoid Sensitive Data:** Do not check banking or confidential emails on public Wi-Fi.
- 2) VPN:** Use a Virtual Private Network (VPN) for a secure, encrypted connection.
- 3) Use Mobile Data:** Prefer your mobile data/hotspot over unknown public networks.

Recognizing Phishing (The Bait)

- 1) What is Phishing?** Scammers tricking you into giving personal data via email/SMS/Call.
- 2) Red Flags:** Sense of urgency, generic greeting, spelling/grammar errors, suspicious sender address, requests for login/financial data.
- 3) The Link Test:** Hover your mouse over a link to see the actual URL before clicking.

Malware and Ransomware

- 1) What is Malware?** Malicious software (Virus, Spyware, Ransomware) designed to harm.
- 2) Ransomware Threat:** Locks your files and demands money for release.
- 3) Protection:** Keep Antivirus updated, be cautious of attachments/downloads, and maintain good backups.

Software Piracy and Cracks

- 1) The Risk:** Cracked or pirated software is a major source of malware infection.
- 2) Trust:** Only download software from official, trusted sources (vendor website) and perform Hash check before installing.
- 3) Unofficial App Stores:** Avoid third-party app stores that offer "free" paid apps.

Physical Device Security

- 1) **Public Spaces:** Use privacy screens on laptops/devices in public. Be aware of shoulder-surfing.
- 2) **Secure Storage:** Lock up laptops/devices when leaving your office/home.
- 3) **USB Danger:** Never plug in an unknown USB drive you find.

Securing Your Digital Footprint

- 1) Privacy Settings:** Review and restrict privacy settings on social media and apps.
- 2) Over-sharing:** Limit the amount of personal information you share online (birthdays, pets' names, etc. – often used for security questions).
- 3) Delete/Deactivate:** Delete old, unused accounts and apps.

Your Digital Toolbox

Quick list of essential tools:

1. Password Manager.
2. Antivirus/Security Suite.
3. VPN.
4. Encrypted Messaging
5. Secure Backup Solution.

Action Plan: Start Today

- 1) Enable MFA on Email & Banking.
- 2) Change default router password.
- 3) Review app permissions and delete unused apps.
- 4) Start using a Password Manager.

Key Takeaways

- 1) **Be Proactive:** Don't wait for a breach.
- 2) **Update Always:** Patching is your best defense.
- 3) **Think Before You Click:** Phishing is the biggest threat.
- 4) **Secure Your Passwords:** MFA is non-negotiable.

Q&A Session