

अपने उपकरणों को सुरक्षित करें: एक व्यापक गाइड

Securing Your Devices: A Comprehensive Guide

HIMANSHU SHEKHAR/ हिमांशु शेखर

PROJECT ENGINEER/ परियोजना अभियंता

C-DAC PATNA/ सी – डैक पटना

Agenda/कार्यावली

- 1) Why Security Matters. / सुरक्षा क्यों ज़रूरी है
- 2) The Foundation: Passwords & MFA. / नींव: पासवर्ड और MFA
- 3) Securing Your Computers. / कंप्यूटर को सुरक्षित करना
- 4) Securing Your Mobile Devices. / मोबाइल डिवाइस को सुरक्षित करना
- 5) Network & Wi-Fi Safety. / नेटवर्क और Wi-Fi सुरक्षा
- 6) Identifying and Avoiding Scams (Phishing, Malware). / स्कैम से बचना (फ़िशिंग, मलवेयर)

Why Security Matters/ सुरक्षा क्यों ज़रूरी है

1) Data Loss/Theft/ डेटा चोरी/नुकसान

- **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 / वित्तीय धोखाधड़ी

- 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 / पहचान की चोरी

- '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 / विश्वास का नुकसान

- 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."

"साइबर सुरक्षा कोई विकल्प नहीं, एक ज़रूरत है।"

First Line of Defense/रक्षा का पहला कदम

- 1) **Complexity/ जटिलता** : Use a mix of upper/lower case, numbers, and symbols/ बड़े/छोटे अक्षर, संख्याएं, और प्रतीकों का मिश्रण करें।
- 2) **Length/ लंबाई** : At least 12-14 characters/ कम से कम 12-14 वर्ण।
- 3) **Uniqueness/ विशिष्टता** : Never reuse passwords / पासवर्ड को कभी न दोहराएं।
- 4) **Tool/ टूल**: Use a reputable Password Manager / एक भरोसेमंद पासवर्ड मैनेजर का उपयोग करें।

"विभिन्न प्लेटफार्मों पर एक ही पासवर्ड का उपयोग न करें"

Multi-Factor Authentication (MFA)

- 1) **What is MFA?** An extra layer of security/सुरक्षा की एक अतिरिक्त परत

Something you Know
जो आपको पता है



Something you Have
जो आपके पास है

- 2) **Types/प्रकार:** Authenticator App (Best), SMS/Email (Good), Biometrics/
ऑथेंटिकेटर ऐप (सबसे अच्छा), SMS/ईमेल (अच्छा), बायोमेट्रिक्स
- 3) **Action/कार्रवाई:** Enable MFA on all critical accounts (Email, Banking, Social Media)/ सभी महत्वपूर्ण खातों पर MFA सक्षम करें।

Computer Security: The Golden Rule/कंप्यूटर सुरक्षा: स्वर्णिम नियम

- 1) **Regular Updates / नियमित अपडेट**: OS, Browser, and Applications. Updates fix security holes/ OS, ब्राउज़र और ऐप्स को अपडेट रखें। अपडेट सुरक्षा कमियों को ठीक करते हैं।
- 2) **Antivirus/Anti-Malware/ एंटीवायरस /एंटी-मैलवेयर**: Use a reputable solution and keep it active/updated/ एक भरोसेमंद समाधान का उपयोग करें और उसे सक्रिय रखें।
- 3) **Firewall/फ़ायरवॉल**: Keep the built-in firewall enabled for network protection/ नेटवर्क सुरक्षा के लिए फ़ायरवॉल को चालू रखें।

Computer Security: Best Practices/कंप्यूटर सुरक्षा: सर्वोत्तम अभ्यास

- 1) **Encryption/एन्क्रिप्शन** : Enable full-disk encryption / फुल-डिस्क एन्क्रिप्शन चालू करें।
- 2) **Backups/ बैकअप** : Regularly backup data to an external drive or cloud/ डेटा का नियमित रूप से बैकअप लें।
- 3) **Access Control/एक्सेस कंट्रोल** : Lock your screen when away. Use a complex PIN/Biometric login/ दूर जाने पर स्क्रीन लॉक करें। जटिल PIN/बायोमेट्रिक लॉगिन का उपयोग करें

Mobile Device Security: The Basics/मोबाइल डिवाइस सुरक्षा: कुछ मूल बातें

- 1) **Screen Lock/ स्क्रीन लॉक**: Mandatory use of PIN/Pattern/Biometrics/
PIN/पैटर्न/बायोमेट्रिक्स का अनिवार्य उपयोग।
- 2) **App Permissions/ ऐप की अनुमतियाँ**: Review and limit permissions
(Location, Contacts, Camera)/ अनुमतियों की समीक्षा करें और सीमित रखें।
- 3) **Official Stores Only/ केवल आधिकारिक स्टोर**: Download apps only from
official App Stores (Google Play/App Store)/ ऐप्स केवल आधिकारिक स्टोर से
डाउनलोड करें।

Mobile Device Security: Pro Tips/मोबाइल डिवाइस सुरक्षा: कुछ जरूरी सुझाव

- 1) **Remote Wipe/ रिमोट वाइप**: Know how to remotely erase your device if stolen/ चोरी होने पर डिवाइस के डाटा को दूर से मिटाने का तरीका समझें।
- 2) **Disable unused Features/ उपयोग न होने पर बंद करें**: Turn off Wi-Fi, Bluetooth, and Location when not in use/ Wi-Fi, ब्लूटूथ, और लोकेशन को बंद रखें।
- 3) **Physical Security/ भौतिक सुरक्षा**: Do not leave your device unattended in public/ सार्वजनिक स्थानों पर डिवाइस को अकेला न छोड़ें।

Network Safety: Home Wi-Fi/नेटवर्क सुरक्षा: घर में इस्तेमाल होने वाले वाईफाई

- 1) **Router Default/ राउटर डिफॉल्ट** : Change the default router password immediately/ डिफॉल्ट राउटर पासवर्ड तुरंत बदलें।
- 2) **Strong Encryption/ मजबूत एन्क्रिप्शन** : Use WPA2 or WPA3 security protocol/ WPA2 या WPA3 सुरक्षा प्रोटोकॉल का उपयोग करें।
- 3) **Guest Network/ गेस्ट नेटवर्क** : Use a separate Guest Network for visitors/smart devices/ आगंतुकों के लिए एक अलग गेस्ट नेटवर्क का उपयोग करें।

Network Safety: Public Wi-Fi/नेटवर्क सुरक्षा: सार्वजनिक वाई-फ़ाई

- 1) Avoid Using Sensitive Data/ संवेदनशील डेटा इस्तेमाल करने से बचें:** Do not check banking or confidential emails on public Wi-Fi/ सार्वजनिक Wi-Fi पर बैंकिंग या गोपनीय ईमेल चेक न करें, इससे आपका डाटा चोरी होने कि संभावना बढ़ जाती है
- 2) VPN:** Use a Virtual Private Network (VPN) for a secure, encrypted connection/ सुरक्षित, एन्क्रिप्टेड कनेक्शन के लिए VPN का उपयोग करें।
- 3) Use Mobile Data/ मोबाइल डेटा का उपयोग करें:** Prefer your mobile data/hotspot over unknown public networks/ अज्ञात नेटवर्क के बजाय अपने मोबाइल डेटा/हॉटस्पॉट को प्राथमिकता दें।

Recognizing Phishing/फ़िशिंग को कैसे पहचाने

- 1) **What is Phishing?/ फ़िशिंग क्या है?** Scammers tricking you into giving personal data via email/SMS/Call/ ईमेल/SMS/कॉल के माध्यम से व्यक्तिगत डेटा देने के लिए घोटाला करने वाले आपको धोखा देते हैं।
- 2) **Red Flags/ भयसूचक चिह्न** : Sense of urgency, generic greeting, spelling/grammar errors, suspicious sender address, requests for login/financial data/ जल्दबाजी की भावना, सामान्य अभिवादन, वर्तनी की त्रुटियां, संदिग्ध प्रेषक का पता, लॉगिन/वित्तीय डेटा के लिए अनुरोध।
- 3) **The Link Test:** Hover your mouse over a link to see the actual URL before clicking/ क्लिक करने से पहले वास्तविक URL देखने के लिए लिंक पर माउस घुमाएँ।

Malware and Ransomware/मैलवेयर और रैंसमवेयर

- 1) What is Malware?** Malicious software (Virus, Spyware, Ransomware) designed to harm. / **मैलवेयर क्या है?** नुकसान पहुँचाने के लिए डिज़ाइन किया गया दुर्भावनापूर्ण सॉफ़्टवेयर (वायरस, स्पाइवेयर, रैंसमवेयर)।
- 2) Ransomware Threat:** Locks your files and demands money for release. / **रैंसमवेयर खतरा:** आपकी फ़ाइलों को लॉक कर देता है और रिलीज़ के लिए पैसे मांगता है।
- 3) Protection:** Keep Antivirus updated, be cautious of attachments/downloads, and maintain good backups. / **सुरक्षा:** एंटीवायरस अपडेट रखें, अटैचमेंट से सावधान रहें, और अच्छा बैकअप रखें।

Software Piracy / सॉफ्टवेयर चोरी

- 1) The Risk:** Cracked or pirated software is a major source of malware infection./
जोखिम : क्रैक या पायरेटेड सॉफ्टवेयर मैलवेयर संक्रमण का एक प्रमुख स्रोत है।
- 2) Trust:** Only download software from official, trusted sources (vendor website) and perform Hash check before installing./ **विश्वास :** केवल आधिकारिक, भरोसेमंद स्रोतों से सॉफ्टवेयर डाउनलोड करें।
- 3) Unofficial App Stores:** Avoid third-party app stores that offer "free" paid apps./
अनौपचारिक ऐप स्टोर : थर्ड-पार्टी ऐप स्टोर से बचें।

Physical Device Security/ भौतिक उपकरण सुरक्षा

- 1) Public Spaces:** Use privacy screens on laptops/devices in public. Be aware of shoulder-surfing./ **सार्वजनिक स्थान:** सार्वजनिक स्थानों पर गोपनीयता स्क्रीन (Privacy Screens) का उपयोग करें।
- 2) Secure Storage:** Lock up laptops/devices when leaving your office/home./ **सुरक्षित भंडारण:** लैपटॉप/डिवाइस को लॉक करके रखें।
- 3) USB Danger:** Never plug in an unknown USB drive you find./ **USB खतरा:** पाए गए किसी भी अज्ञात USB ड्राइव को कभी भी प्लग न करें।

Securing Your Digital Footprint/अपने डिजिटल पदचिह्न को सुरक्षित करना

- 1) Privacy Settings:** Review and restrict privacy settings on social media and apps./ गोपनीयता सेटिंग्स: सोशल मीडिया और ऐप्स पर सेटिंग्स की समीक्षा करें।
- 2) Over-sharing:** Limit the amount of personal information you share online (birthdays, pets' names, etc. – often used for security questions)./ अधिक साझा करना: ऑनलाइन साझा की जाने वाली व्यक्तिगत जानकारी की मात्रा सीमित करें।
- 3) Delete/Deactivate:** Delete old, unused accounts and apps./ हटाएँ/निष्क्रिय करें: पुराने, अप्रयुक्त खातों और ऐप्स को हटाएँ।

Your Digital Toolbox/आपका डिजिटल टूलबॉक्स

Quick list of essential tools:

1. Password Manager/ पासवर्ड मैनेजर
2. Antivirus/Security Suite/ एंटीवायरस/सुरक्षा सूट
3. VPN.
4. Encrypted Messaging/ एन्क्रिप्टेड मैसेजिंग
5. Secure Backup Solution/ सुरक्षित बैकअप समाधान।

Action Plan: Start Today

- 1) Enable MFA on Email & Banking./ ईमेल और बैंकिंग पर MFA सक्षम करें।
- 2) Change default router password/ डिफ़ॉल्ट राउटर पासवर्ड बदलें।
- 3) Review app permissions and delete unused apps/ ऐप अनुमतियों की समीक्षा करें और अप्रयुक्त ऐप्स हटाएँ।
- 4) Start using a Password Manager/ पासवर्ड मैनेजर का उपयोग शुरू करें।

मुख्य निष्कर्ष

4 महत्वपूर्ण सिद्धांत

- 1. MFA (बहु-कारक प्रमाणीकरण) सक्षम/सत्यापित करें:** सुनिश्चित करें कि आपके प्राथमिक खातों, विशेष रूप से आपके वित्तीय और अन्य संवेदनशील खातों पर बहु-कारक प्रमाणीकरण (MFA) सक्रिय है। यह खाता अधिग्रहण (account takeover) के विरुद्ध आपको सबसे अच्छा बचाव हो सकता है।
- 2. अपने एंड पॉइंट डिवाइस अपडेट करें:** अपने कार्य कंप्यूटर और मोबाइल डिवाइस पर किसी भी लंबित ऑपरेटिंग सिस्टम या एप्लिकेशन अपडेट की जांच करें और उन्हें तुरंत इंस्टॉल करें।
- 3. पासवर्ड प्रबंधन:** 10 मिनट का समय लें और अपने द्वारा बनाए जा रहे प्रत्येक खाते के लिए **मज़बूत और अद्वितीय** पासवर्ड सेट करने हेतु अपने सभी पासवर्ड की समीक्षा करें और उन्हें रीसेट करें।
- 4. फ़िशिंग हमलों पर सतर्क रहें** और घोटालों को पहचानने की अपनी क्षमता का परीक्षण करें और उनकी सही रिपोर्टिंग करें!

Q&A Session

प्रश्न एवं उत्तर सत्र