

**शीर्षक:** डिवाइस और नेटवर्क सुरक्षा  
**उप-शीर्षक:** मोबाइल और ऐप सुरक्षा  
**प्रस्तुतकर्ता:** शुभम त्रिपाठी

## मोबाइल सुरक्षा का महत्व

सुरक्षा एक आवश्यकता क्यों है?

- **कॉर्पोरेट /व्यक्तिगत संगम (Convergence):** डिवाइस पर व्यक्तिगत और व्यावसायिक डेटा (Email, CRM, Cloud Access) का मिश्रण.
- **सेंसर डेटा का जोखिम:** माइक्रोफोन, कैमरा और लोकेशन सेंसर तक अनधिकृत पहुँच.
- **वित्तीय और पहचान धोखाधड़ी:** सिम स्वैप (SIM Swap) और ज़ीरो-क्लिक (Zero-Click) हमलों के माध्यम से सीधा वित्तीय नुकसान.
- **जीरो-ट्रस्ट मॉडल:** यह मानना कि कोई भी नेटवर्क या डिवाइस डिफॉल्ट रूप से सुरक्षित नहीं है.

## गहन खतरे और हमले (Deep Threats and Attacks)

सबसे बड़े और जटिल जोखिम:

1. **ज़ीरो-क्लिक हमले (Zero-Click Exploits):** उपयोगकर्ता के किसी एक्शन के बिना हमला (जैसे iMessage/WhatsApp के ज़रिए).
2. **रैनसमवेयर (Ransomware):** डिवाइस को लॉक करके डेटा वापस करने के लिए फिरौती (Ransom) मांगना.
3. **सप्लाई चेन हमले (Supply Chain Attacks):** विश्वसनीय, लेकिन दुर्भावनापूर्ण कोड वाली थर्ड-पार्टी लाइब्रेरी के माध्यम से ऐप को निशाना बनाना.
4. **सिम स्वैप (SIM Swap):** फ़ोन नंबर का नियंत्रण चुराकर 2FA को बायपास करना.

## व्यावहारिक सुरक्षा: स्क्रीन लॉक और बायोमेट्रिक्स

तुरंत लागू किए जाने वाले उपाय:

- **मज़बूत पिन/पासवर्ड**: कम से कम 6 अंक या उससे अधिक के PIN का उपयोग करें; पैटर्न लॉक से बचें.
- **बायोमेट्रिक सेटअप**: फिंगरप्रिंट या फेस आईडी को **मज़बूत पासवर्ड के बैकअप** के रूप में उपयोग करें.
- **SIM कार्ड पिन लॉक (SIM PIN Lock)**: सिम कार्ड पर PIN सेट करें ताकि SIM चोरी होने पर उसका दुरुपयोग न हो सके.
- **लॉकडाउन मोड (iOS) / एन्हांसड लॉक (Android)**: आपातकालीन स्थिति के लिए तुरंत बायोमेट्रिक्स को अक्षम (disable) करने की क्षमता.

## उन्नत प्रमाणन (Advanced Authentication)

पासवर्ड से परे:

- **टू-फैक्टर ऑथेंटिकेशन (2FA) अपग्रेड:** OTP SMS के बजाय **ऑथेंटिकेटर ऐप्स** (जैसे Google Authenticator, Authy) का उपयोग करें (SMS ज़्यादा असुरक्षित है).
- **फ़िज़िकल सुरक्षा कुंजी (Hardware Security Keys):** FIDO/U2F मानक वाली USB या ब्लूटूथ कुंजियाँ (Keys) (जैसे YubiKey) का उपयोग करें - यह सुरक्षा का **सबसे मजबूत** रूप है.
- **पासवर्ड मैनेजर का उपयोग:** जटिल और अद्वितीय पासवर्ड बनाने और स्टोर करने के लिए मैनेजर (जैसे LastPass, Bitwarden) को अनिवार्य बनाएं.

## ऐप अनुमतियों का ऑडिट (App Permissions Audit)

न्यूनतम विशेषाधिकार सिद्धांत (Principle of Least Privilege):

- **इंस्टॉल के बाद प्रबंधन:** ऐप इंस्टॉल करने के बाद उसकी अनुमतियों को नियमित रूप से जांचें और रद्द करें (Revoke).
- **'उपयोग के दौरान ही' (While In Use):** लोकेशन, कैमरा और माइक्रोफोन जैसी संवेदनशील अनुमतियों को केवल ऐप के उपयोग के दौरान ही दें.
- **बैकग्राउंड गतिविधि :** जाँच करें कि कौन से ऐप्स बैकग्राउंड में डेटा या बैटरी का उपयोग कर रहे हैं और अनावश्यक ऐप्स को सीमित करें.
- **थर्ड-पार्टी एक्सेस:** अपने Google या सोशल मीडिया अकाउंट से जुड़े ऐप्स की सूची की नियमित समीक्षा करें और अनावश्यक एक्सेस हटाएं.

## सुरक्षित ऐप स्रोत और साइडलोडिंग के खतरे (Safe App Sources and Sideloaded Risks)

स्रोत की विश्वसनीयता :

- **केवल आधिकारिक स्टोर:** Google Play Store या Apple App Store के अलावा किसी भी स्रोत से ऐप डाउनलोड करना साइडलोडिंग कहलाता है.
- **साइडलोडिंग के खतरे:** साइडलोडेड ऐप्स में अक्सर अज्ञात मैलवेयर, ट्रैकिंग कोड या बैंकिंग ट्रोजन (Banking Trojans) हो सकते हैं.
- **ऐप सत्यापन:** ऐप डाउनलोड करने से पहले डेवलपर का नाम, अपडेट की तारीख और सुरक्षा प्रमाणपत्र (Security Certificate) की जाँच करें.

## ऑपरेटिंग सिस्टम का जीवनकाल (OS End-of-Life and Updates)

निरंतर पैचिंग (Continuous Patching):

- **तुरंत अपडेट:** OS और ऐप अपडेट्स को तुरंत इंस्टॉल करें, क्योंकि उनमें **क्रिटिकल ज़ीरो-डे (Zero-Day)** कमजोरियों के लिए पैच होते हैं.
- **एंड-ऑफ-लाइफ (EOL) जोखिम:** जब निर्माता डिवाइस को सॉफ्टवेयर अपडेट देना बंद कर देता है, तो डिवाइस **असुरक्षित (Vulnerable)** हो जाता है. EOL डिवाइस का उपयोग बंद करें.
- **फर्मवेयर (Firmware) अपडेट:** डिवाइस के मॉडम, ब्लूटूथ और NFC फर्मवेयर को भी अपडेट रखें (आमतौर पर OS अपडेट के साथ होता है).

## मोबाइल थ्रेट डिफेंस (MTD) और एंडपॉइंट प्रोटेक्शन (Endpoint Protection)

### सुरक्षा का सक्रिय निरीक्षण:

- **MTD क्या है?** यह पारंपरिक एंटी-वायरस से अधिक है, यह वास्तविक समय में जोखिमों की पहचान करता है.
- **कार्य:** इसमें मैलवेयर स्कैनिंग, नेटवर्क हमलों (जैसे Man-in-the-Middle) से सुरक्षा, और डिवाइस के कॉन्फिगरेशन की सुरक्षा ऑडिट शामिल है.
- **व्यवहारिक उपयोग:** बैंकिंग या संवेदनशील काम करने से पहले MTD ऐप द्वारा डिवाइस के 'सुरक्षा स्कोर' की जाँच करें.

## डेटा एन्क्रिप्शन का विस्तार (Deepening Data Encryption)

डेटा की अखंडता और गोपनीयता :

- **पूर्ण डिस्क एन्क्रिप्शन (FDE):** सुनिश्चित करें कि आपका पूरा फ़ोन स्टोरेज एन्क्रिप्टेड है (आधुनिक फ़ोन में डिफ़ॉल्ट).
- **एंड-टू-एंड एन्क्रिप्शन (E2EE):** संवेदनशील संचार के लिए केवल E2EE-सक्षम मैसेजिंग ऐप्स (जैसे Signal, WhatsApp) का उपयोग करें.
- **क्लाउड एन्क्रिप्शन :** क्लाउड सेवाओं में डेटा अपलोड करते समय, संवेदनशील फ़ाइलों को अपलोड से पहले एन्क्रिप्ट करें.

## Wi-Fi/हॉटस्पॉट पर एन्हांस्ड प्राइवेसी (Enhanced Privacy on Wi-Fi/Hotspots)

नेटवर्क ट्रैकिंग से बचाव:

- **प्राइवेट DNS (DNS over HTTPS/TLS):** DNS अनुरोधों को एन्क्रिप्ट करने के लिए सेटिंग्स में प्राइवेट DNS (जैसे Cloudflare या Google) का उपयोग करें. यह आपके ISP/हॉटस्पॉट को आपकी ब्राउज़िंग गतिविधि जानने से रोकता है.
- **VPN को अनिवार्य बनाएं:** किसी भी सार्वजनिक Wi-Fi नेटवर्क (होटल, कैफे) पर काम करते समय **हमेशा** एक भरोसेमंद VPN का उपयोग करें.
- **MAC एड्रेस रैंडमाइजेशन (MAC Address Randomization):** इस सुविधा को सक्रिय करें ताकि नेटवर्क ऑपरेटर आपको ट्रैक न कर सकें.

## **ब्लूटूथ और NFC का कठोर प्रबंधन (Strict Management of Bluetooth and NFC)**

**वायरलेस हमले की रोकथाम:**

- आवश्यकतानुसार सक्रियण:** ब्लूटूथ/NFC को केवल उपयोग के समय ही सक्रिय करें.
- असुरक्षित पेयरिंग से बचें:** अज्ञात डिवाइस के साथ पेयरिंग अनुरोधों को सख्ती से अस्वीकार करें.
- ब्लूटूथ की अनुमतियाँ:** ऐप्स को ब्लूटूथ एक्सेस देने में सावधानी बरतें, क्योंकि इसका उपयोग भी स्थान (Location) को ट्रैक करने के लिए किया जा सकता है.

## रिमोट मैनेजमेंट और डेटा वाइप (Remote Management and Data Wipe)

### आपदा प्रबंधन:

- **रिमोट वाइप (Remote Wipe):** 'Find My Device' (Android) या 'Find My iPhone' (iOS) में रिमोट डेटा मिटाने की सुविधा सक्रिय रखें.
- **डेटा बैकअप की रणनीति:** क्लाउड बैकअप के अलावा, नियमित रूप से **डिवाइस का ऑफलाइन बैकअप** (हार्ड ड्राइव पर) लें ताकि रैनसमवेयर या रिमोट वाइप की स्थिति में डेटा उपलब्ध रहे.
- **Trusted Contacts:** आपातकालीन स्थिति में अपने डिवाइस को एक्सेस करने के लिए एक विश्वसनीय संपर्क सेट करें (यदि उपलब्ध हो).

## गोपनीयता सेटिंग्स और डिजिटल ऑडिट (Privacy Settings and Digital Audit)

गोपनीयता पर नियंत्रण:

- **गोपनीयता ऑडिट:** अपने सोशल मीडिया, Google, और क्लाउड खातों की सुरक्षा सेटिंग्स की **हर तीन महीने में** ऑडिट करें.
- **एप्लिकेशन ट्रैकिंग ट्रांसपेरेंसी (ATT):** ऐप्स को अन्य ऐप्स और वेबसाइटों पर आपकी गतिविधि को ट्रैक करने की अनुमति को प्रबंधित करें.
- **विज्ञापन पहचानकर्ता (Advertising ID) रीसेट:** समय-समय पर अपने डिवाइस का विज्ञापन पहचानकर्ता रीसेट करें ताकि विज्ञापनदाता आपके प्रोफ़ाइल को फिर से बनाना शुरू करें.

## सुरक्षित ब्राउज़िंग और फ़िशिंग पहचान (Secure Browsing and Phishing Detection)

### वेब पर सुरक्षा:

- **HTTPS की जाँच:** किसी भी वेबसाइट पर संवेदनशील जानकारी दर्ज करने से पहले URL में 'HTTPS' और एक **पैडलॉक आइकन** की जाँच करें.
- **फ़िशिंग पहचान:** किसी भी ईमेल या मैसेज में दिए गए लिंक को खोलने से पहले, URL पर थोड़ी देर तक दबाकर (long press) उसके वास्तविक गंतव्य (actual destination) की जाँच करें.
- **ब्राउज़र सुरक्षा:** Chrome/Safari में **फ़िशिंग और मेलवेयर सुरक्षा** सुविधाओं को सक्रिय रखें.

## मालिशियस ऐप का विश्लेषण (Analyzing Malicious App Behavior)

असामान्य व्यवहार की निगरानी:

- **अत्यधिक बैटरी / डेटा उपयोग:** बिना उपयोग के भी यदि कोई ऐप बहुत ज़्यादा बैटरी या डेटा खपत कर रहा है, तो वह संदिग्ध है.
- **अनचाही पॉप-अप:** बार-बार विज्ञापन या अजीब सिस्टम संदेश (System Messages) दिखाने वाले ऐप्स.
- **रूटिंग / जेलब्रेकिंग से बचें:** अपने फ़ोन को 'रूट' (Root) या 'जेलब्रेक' (Jailbreak) न करें, क्योंकि इससे OS की सुरक्षा परतें हट जाती हैं.

## बच्चों और परिवार के लिए सुरक्षा (Security for Children and Family)

### सुरक्षित डिजिटल आदतें:

- पैरेंटल कंट्रोल:** बच्चों के उपकरणों पर मजबूत पैरेंटल कंट्रोल (Parental Controls) और स्क्रीन टाइम लिमिट सेट करें.
- ऐप समीक्षा:** बच्चों को कोई भी नया ऐप डाउनलोड करने से पहले हमेशा आपसे पूछने का नियम बनाएं.
- सुरक्षित खोज (Safe Search):** सर्च इंजनों में Safe Search मोड को सक्रिय करें.

## मुख्य उन्नत सुरक्षा सुझाव (Key Advanced Security Tips)

याद रखने योग्य उन्नत कदम:

1. **मज़बूत प्रमाणन**: SMS 2FA से ऑथेंटिकेटर ऐप या हार्डवेयर कुंजी पर स्विच करें.
2. **ऑडिट**: ऐप अनुमतियों और सोशल मीडिया सेटिंग्स की नियमित रूप से ऑडिट करें.
3. **नेटवर्क**: सार्वजनिक Wi-Fi पर VPN और प्राइवेट DNS का उपयोग करें.
4. **EOL**: पुराने, EOL हो चुके डिवाइस का उपयोग करना तुरंत बंद करें.
5. **बैकअप**: क्लाउड के अलावा ऑफलाइन (Offline) डेटा बैकअप भी रखें.
6. **जागरूकता**: जीरो-क्लिक और सिम स्वैप जैसे नए हमलों के बारे में जागरूक रहें.