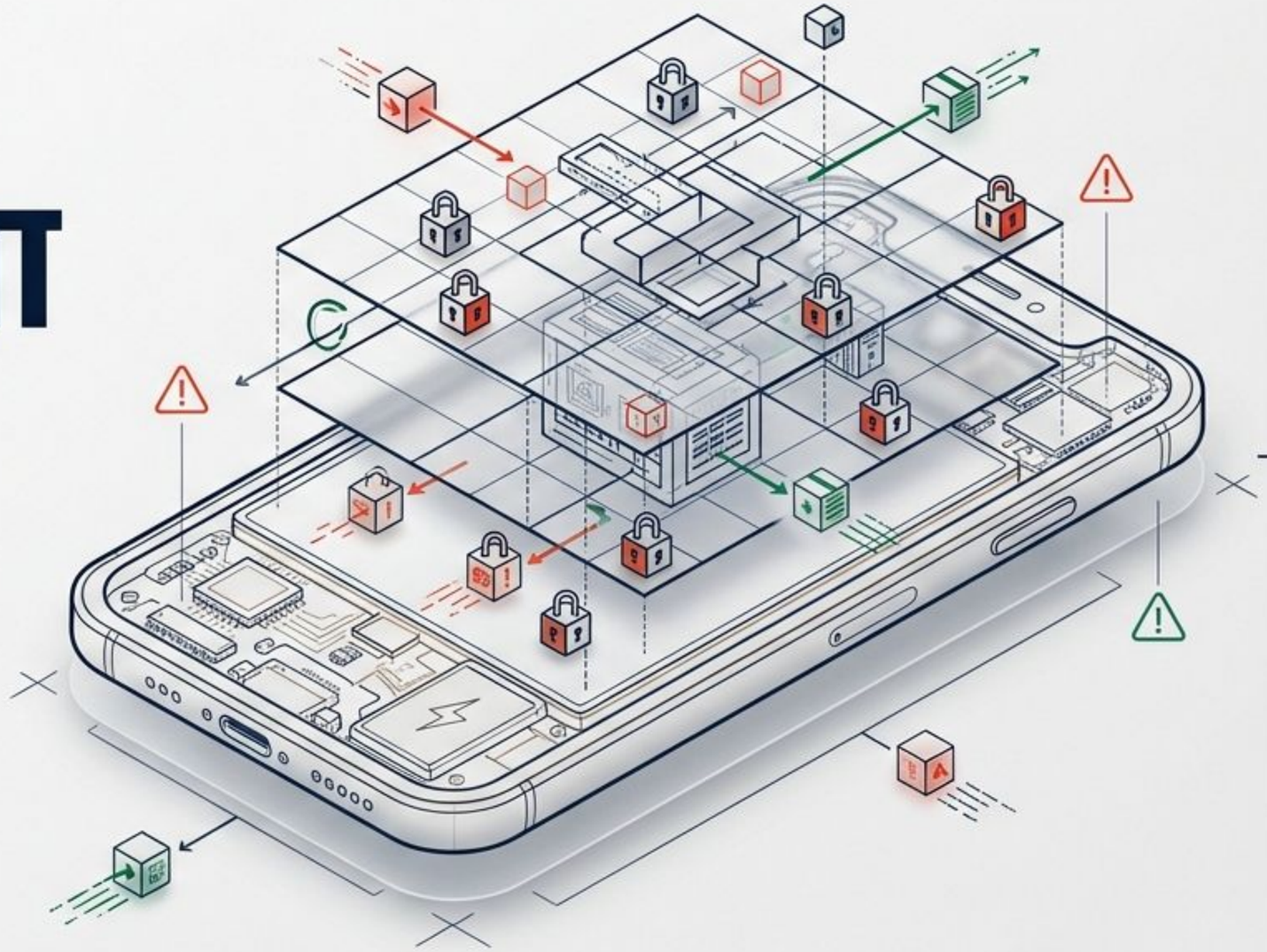
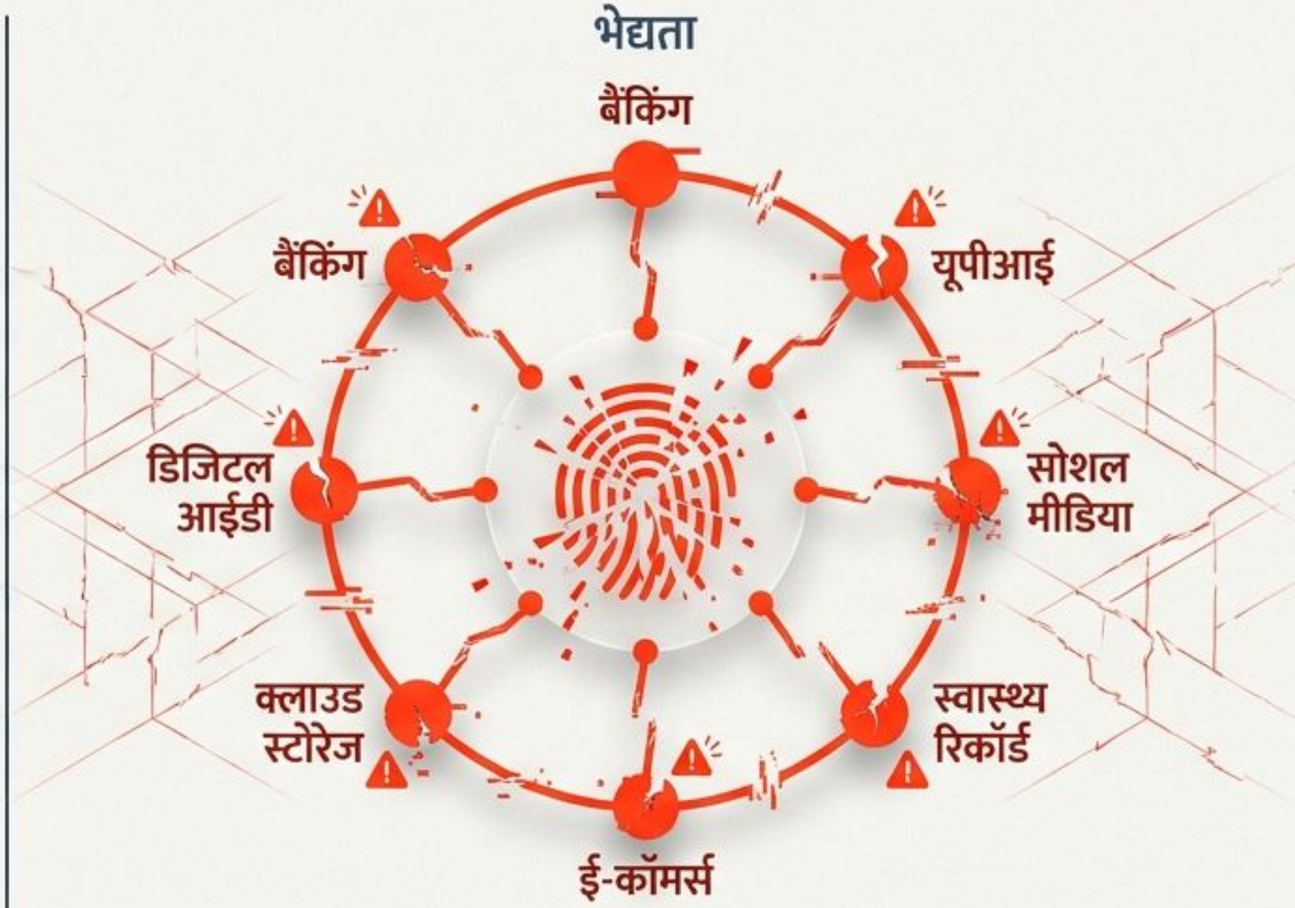
साइबर सुरक्षा कमांड सेंटर

डिजिटल ठगी के नए तरीके और बचाव की अचूक रणनीतियां



हमारा डिजिटल जीवन: सुविधावानक लेकिन असुरक्षित

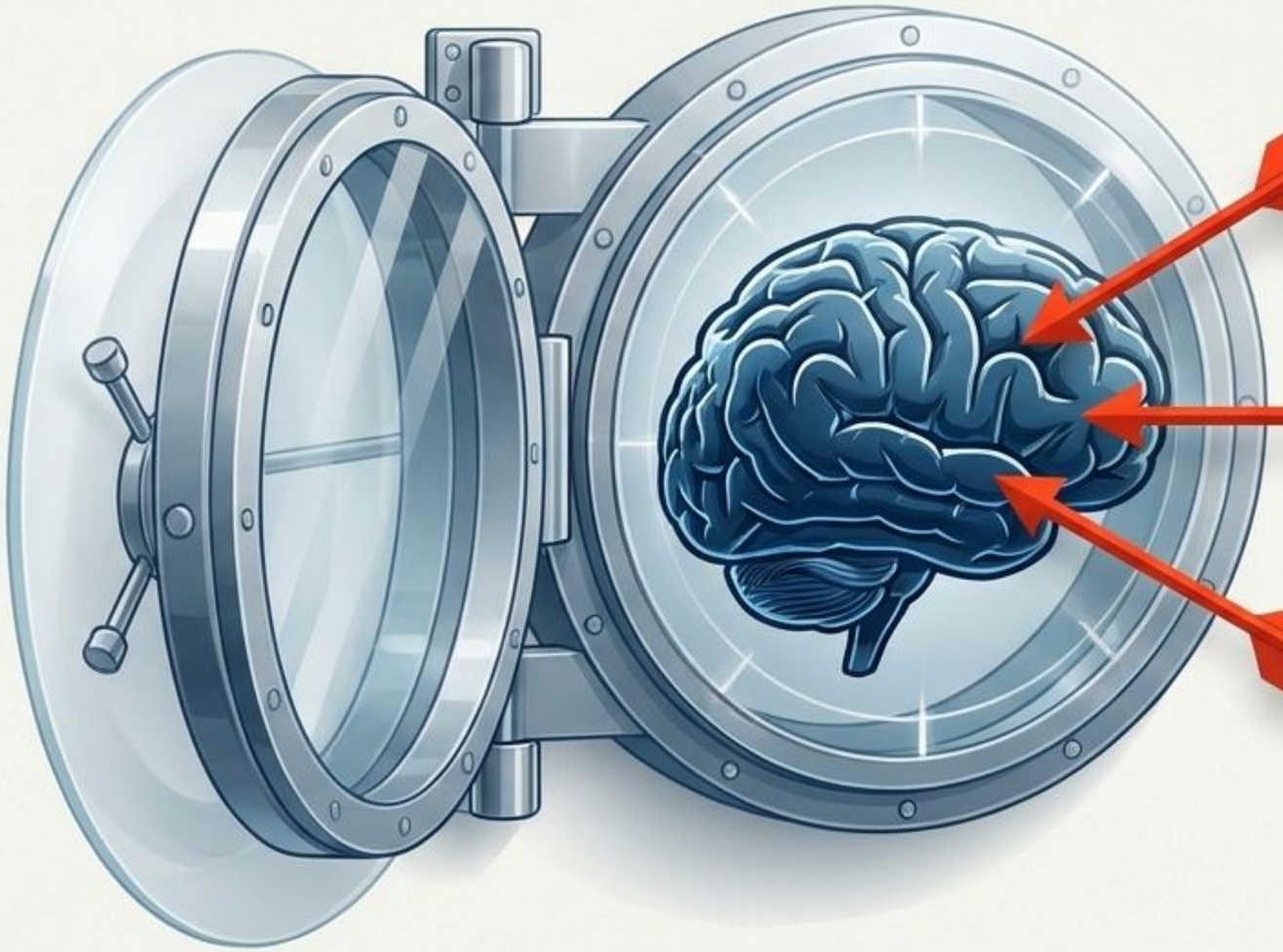
हमारी पूरी जिंदगी—हमारे बैंक खाते, हमारी पहचान और हमारे संपर्क—अब एक सिंगल स्क्रीन के पीछे कैद हैं।



सुविधाओं ने हमें गति दी है, लेकिन इसी गति ने हमारी सुरक्षा में अनदेखी सेंध भी लगा दी है।

सिस्टम को हैक नहीं किया जाता, आपके दिमाग को हैक किया जाता है

आधुनिक साइबर अपराधी अब आपके डिवाइस की सुरक्षा तोड़ने में समय बर्बाद नहीं करते।
वे सीधे आपकी भावनाओं को निशाना बनाते हैं:



1. **खौफ (Fear):** पुलिस, केस या अकाउंट बंद होने का डर।

2. **लालच (Greed):** रिवॉर्ड, सब्सिडी या लॉटरी का प्रलोभन।

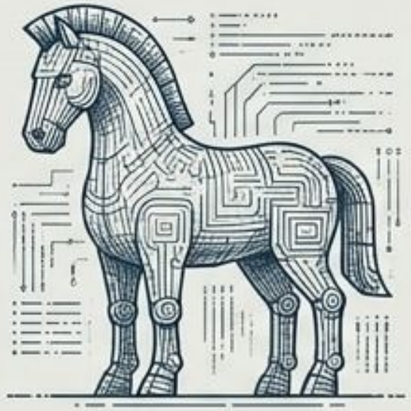
3. **जल्दबाजी (Urgency):** 'अभी तुरंत करें, वरना...' का दबाव।

ठगों के तीन मुख्य हथियार

डिजिटल पहचान चुराने के लिए हैकर्स मुख्य रूप से इन तीन तरीकों का इस्तेमाल करते हैं:

‘डिजिटल अरेस्ट’

अनजान वीडियो कॉल के जरिए मनोवैज्ञानिक दबाव और फर्जी गिरफ्तारी का खौफ।



रिमोट एक्सेस ऐप्स

KYC या सपोर्ट के बहाने आपके डिवाइस का पूरा कंट्रोल लेना।

अदृश्य जाल (Phishing Links)

लुभावने या डराने वाले अनजान लिंक्स के जरिए मैलवेयर इंस्टॉल करना।

‘डिजिटल अरेस्ट’ का मनोवैज्ञानिक जाल

यह कोई कानूनी प्रक्रिया नहीं है; यह एक मानसिक अपहरण है।

अनजान वीडियो कॉल

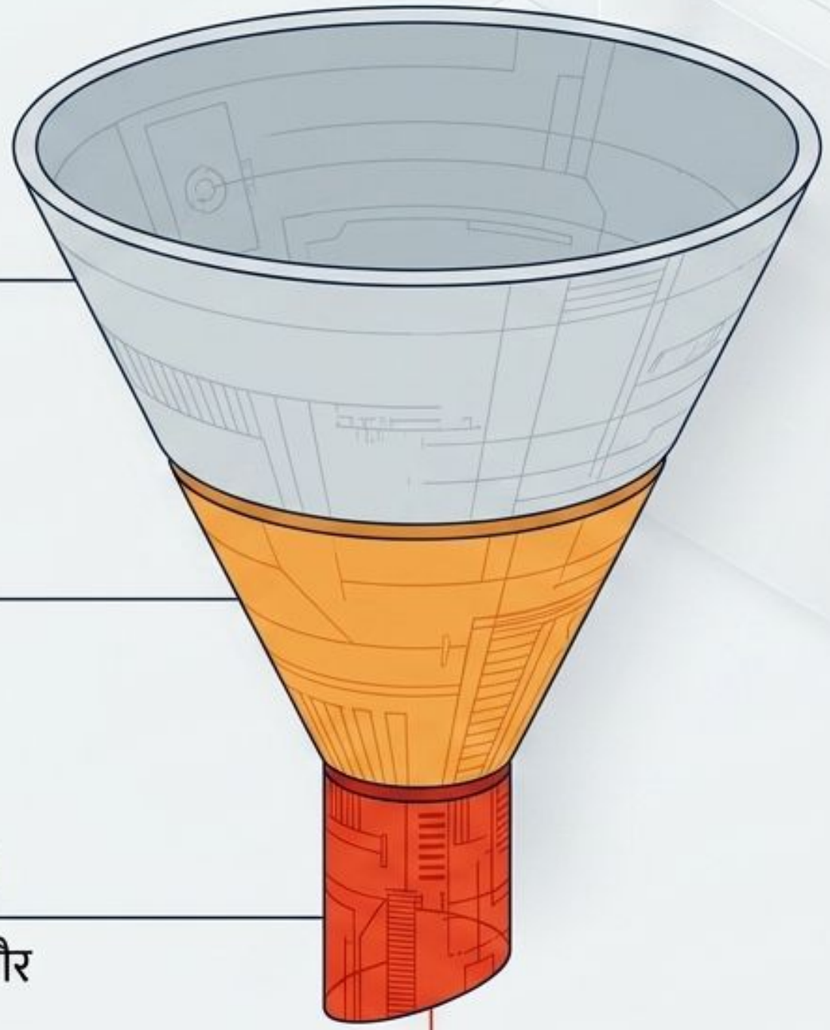
अचानक कॉल आना। स्क्रीन पर फर्जी पुलिस वर्दी या नकली सरकारी कार्यालय का सेटअप।

खौफ और दबाव का निर्माण

‘आपके खिलाफ पार्सल/मनी लॉन्ड्रिंग का केस दर्ज है।’ तुरंत गिरफ्तारी की धमकी देना।

सोचने की क्षमता खत्म (Cognitive Bypass)

घबराहट में पीड़ित तार्किक रूप से सोचना बंद कर देता है और ठगों की हर बात (पैसे ट्रांसफर करना) मानने लगता है।



अंतिम परिणाम: आप 'डिजिटल अरेस्ट' में हैं।

रिमोट ऐप्स: एक डिजिटल 'ट्रोजन हॉर्स'

बहाना (The Bait)

ठग आपको KYC अपडेट, बैंक वेरिफिकेशन, रिवॉर्ड, सब्सिडी या लोन के बहाने कॉल करते हैं।

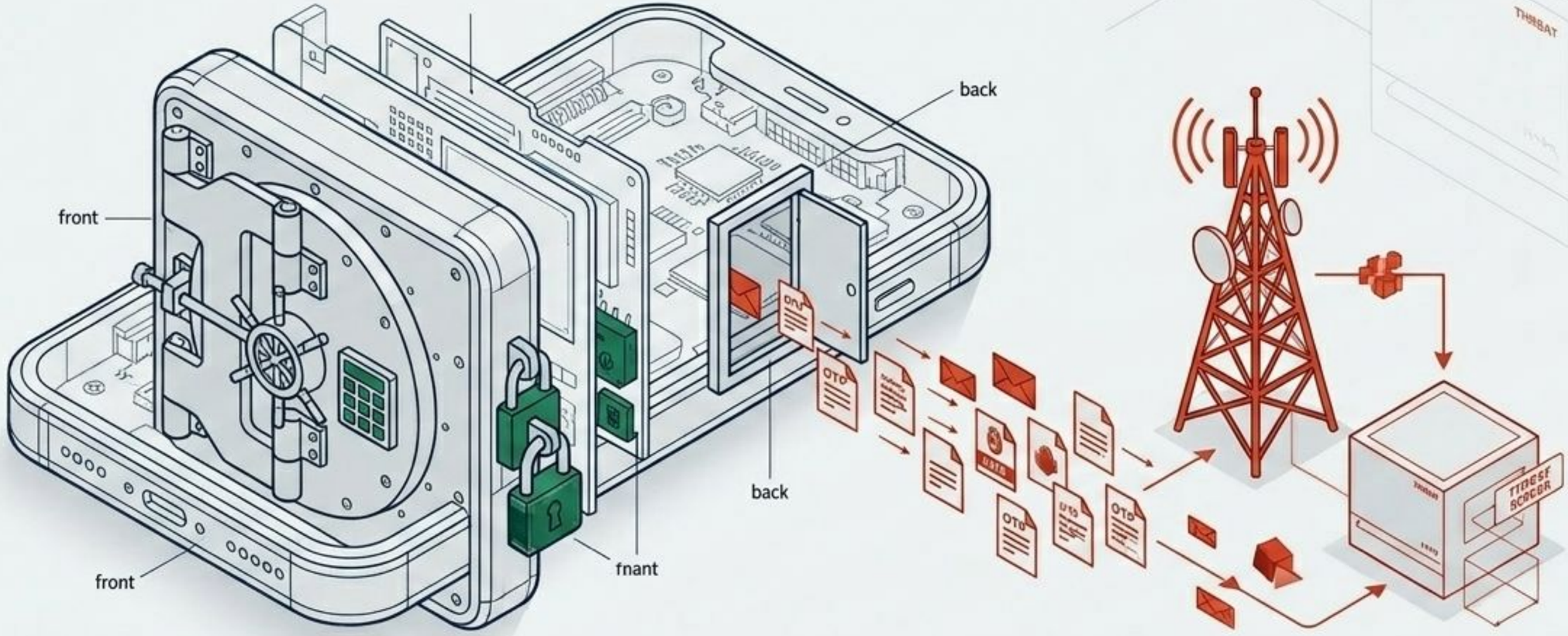
घुसपैठ (The Infiltration)

वे आपको AnyDesk, TeamViewer, QuickSupport या Screen Sharing ऐप इंस्टॉल करने को कहते हैं।

चोरी (The Extraction)

ऐप इंस्टॉल होते ही स्क्रीन शेयरिंग शुरू। ठगों के पास आपके डिवाइस का पूरा कंट्रोल आ जाता है।

रिमोट ऐप्स कैसे काम करते हैं: खुला हुआ 'बैकडोर'



जब आप किसी के कहने पर रिमोट एक्सेस ऐप डालते हैं, तो आपके बैंक की सुरक्षा (पासवर्ड/बायोमेट्रिक) मजबूत होने के बावजूद कोई फायदा नहीं होता।

आप अनजाने में अपने फोन का 'पिछला दरवाजा' (Backdoor) खोल देते हैं, जहां से ठग आपकी स्क्रीन पर आने वाला हर OTP और पासवर्ड लाइव देख रहे होते हैं।

अनजान लिंक्स का अदृश्य जाल

1. संदेहास्पद लिंक पर क्लिक:
SMS या WhatsApp पर आए 'अकाउंट ब्लॉक' या 'फ्री गिफ्ट' वाले लिंक पर क्लिक करना।

2. मैलवेयर इंस्टॉलेशन:
बैकग्राउंड में छुपकर एक जासूस सॉफ्टवेयर (Malware) डाउनलोड हो जाना।

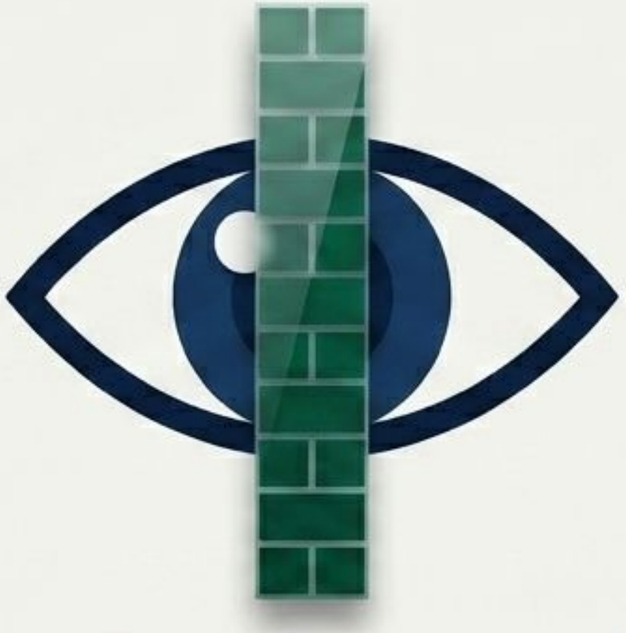
3. कीस्ट्रोक ट्रैकिंग:
आप फोन पर जो भी टाइप करते हैं (पासवर्ड, PIN), वह सीधे ठगों तक पहुंचना।

4. अकाउंट हैक:
आपकी जानकारी के बिना आपके खातों तक पहुंच स्थापित होना।

जब सुरक्षा चक्र टूटता है: नुकसान का सीधा प्रभाव

ठगों के चंगुल में फंसने का मतलब सिर्फ पैसे खोना नहीं है। एक गलती से:

1. आपका WhatsApp हैक हो सकता है।
2. बैंकिंग ऐप्स और UPI की पूरी जानकारी चोरी हो सकती है।
3. आपके गुप्त OTP, पासवर्ड और व्यक्तिगत डेटा लीक हो सकते हैं।
4. पलक झपकते ही आपके खाते से सारे पैसे निकाले जा सकते हैं।
5. आपके नाम और पहचान का इस्तेमाल करके दूसरों के साथ धोखाधड़ी की जा सकती है।



निचोड़: आपका 'संयम' ही आपका सबसे मजबूत फायरवॉल है

चाहे वह डिजिटल अरेस्ट हो, रिमोट ऐप हो, या कोई फर्जी लिंक... सभी तरीके एक ही बात पर निर्भर करते हैं: आपके द्वारा अपने ही हाथों से सुरक्षा चाबियां सौंपना।

ठग सिस्टम को नहीं, आपकी भावनाओं को बायपास करते हैं।

इसलिए, जब भी कोई ऑनलाइन डराए या लालच दे... बस एक पल रुकें और सोचें।

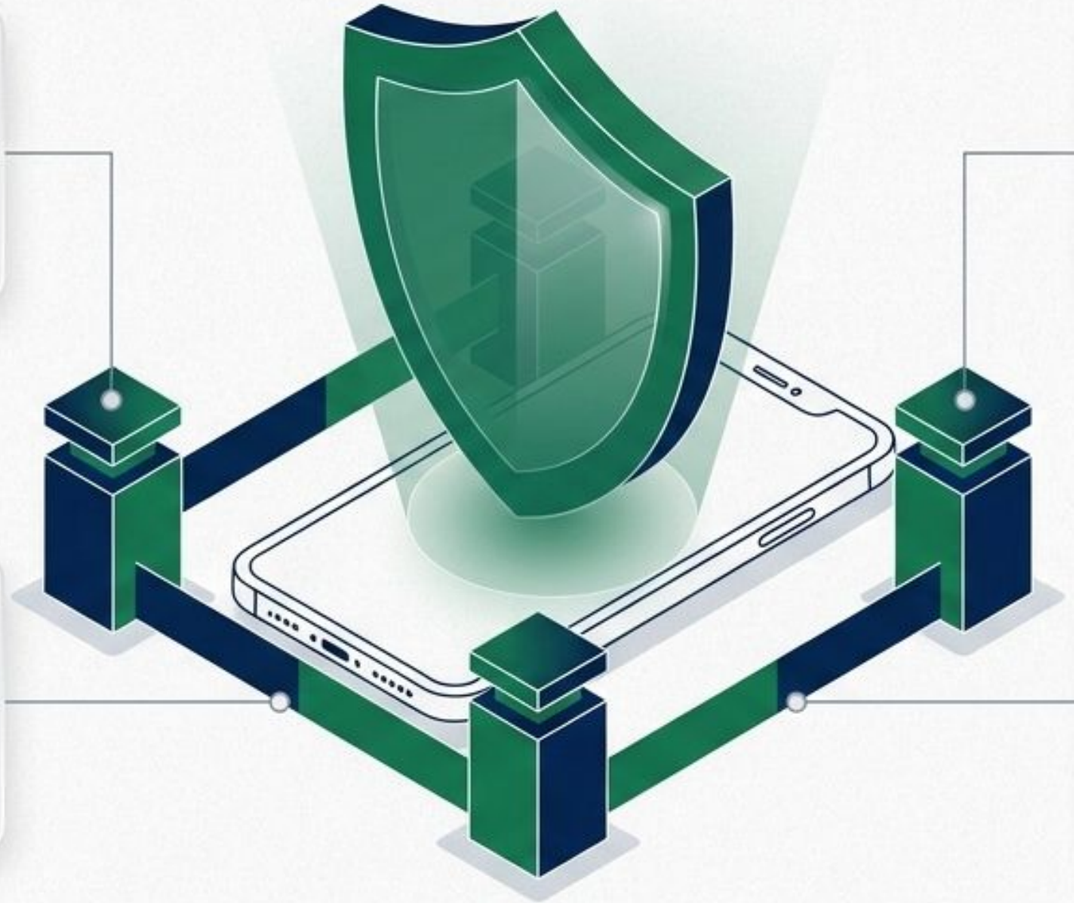
असली बनाम नकली की पहचान

मापदंड	असली संस्था (बैंक/पुलिस)	साइबर ठग
संपर्क का तरीका	आधिकारिक ऐप, पत्र या ब्रांच से कॉल	WhatsApp वीडियो कॉल या अनजान नंबर
बातचीत की भावना	शांत, पेशेवर और सामान्य	अत्यधिक खौफ, दबाव और जल्दबाजी
मुख्य मांग	ब्रांच में आकर संपर्क करने को कहेंगे	ऐप इंस्टॉल करने, लिंक पर क्लिक करने या OTP मांगेंगे
समाधान का तरीका	कानूनी और दस्तावेजी प्रक्रिया	तुरंत ऑनलाइन पैसे ट्रांसफर करने का दबाव

आपका डिजिटल सुरक्षा कवच: बचाव के 4 स्वर्ण नियम

1. कभी कोई ऐप इंस्टॉल न करें:
बैंक कभी भी फोन पर आपसे AnyDesk या QuickSupport जैसे ऐप इंस्टॉल करने के लिए नहीं कहता।

2. गुप्त जानकारी साझा न करें:
किसी को भी अपना OTP, PIN, CVV या पासवर्ड कभी न बताएं।



3. केवल आधिकारिक स्रोत:
ऐप्स हमेशा आधिकारिक ऐप स्टोर (Google Play/App Store) से ही डाउनलोड करें। संदेहास्पद लिंक्स से बचें।

4. वीडियो कॉल को नजरअंदाज करें:
किसी अनजाने नंबर से आए हुए वीडियो कॉल को रिसीव न करें और 'डिजिटल अरेस्ट' के बहकावे में न आएं।

प्रीमियम इंटेलिजेंस डोसियर

आपातकालीन प्रोटोकॉल

यदि सुरक्षा कवच टूट जाए, तो पलटवार कैसे करें?

आपकी एक छोटी सी सावधानी और सही समय पर उठाया गया कदम आपको बड़े आर्थिक और मानसिक नुकसान से बचा सकता है।
अगर आपको लगे कि आपके साथ धोखा हुआ है, तो आपके पास कार्रवाई करने के लिए पहला 'गोल्डन ऑवर' (शुरुआती 1 घंटा) सबसे अहम है।

‘गोल्डन ऑवर’ रिस्पांस टाइमलाइन: धोखा होने पर तुरंत क्या करें?

0 Min — **60 Min**

Minute 0-5: कनेक्शन काटें और ब्लॉक करें

सबसे पहले इंटरनेट/वाई-फाई बंद करें। स्क्रीन शेयरिंग ऐप तुरंत डिलीट करें। बैंक को कॉल करके अपने डेबिट/क्रेडिट कार्ड और अकाउंट को तुरंत ब्लॉक/फ्रीज करवाएं।

Minute 5-15: 1930 पर कॉल करें

तुरंत राष्ट्रीय साइबर क्राइम हेल्पलाइन नंबर 1930 डायल करें। पैसे के लेन-देन को रोकने (Lien mark) के लिए यह सबसे तेज़ तरीका है।

Minute 15-60: आधिकारिक शिकायत दर्ज करें

National Cyber Crime Reporting Portal (www.cybercrime.gov.in) पर जाकर घटना की पूरी विस्तृत शिकायत दर्ज करें और प्रमाण (स्क्रीनशॉट/नंबर) अपलोड करें।

सतर्क रहें, सुरक्षित रहें

साइबर ठगी से बचने का सबसे बड़ा हथियार तकनीक नहीं, बल्कि आपकी 'जागरूकता' है।
अपने परिवार, विशेषकर बुजुर्गों को इन नए डिजिटल खतरों के बारे में शिक्षित करें।
जागरूक बनें, दूसरों को भी जागरूक करें।

Teachers of Bihar

The Change Makers

धन्यवाद

Publication: Teachers of Bihar

email: teachersofbihar@gmail.com

Developed By: P. K. Pankaj, Head Teacher,
P S Adalpur, Motipur, Muzaffarpur

Tob whatsapp Channel

https://whatsapp.com/channel/0029Va9AFpl65yD3brB8Sl17

Scan करें और जुड़ें