

केंद्रीय रिज़र्व पुलिस बल

अगस्त, 2026

साइबर बाइट

फर्जी टैक्स
नोटिस घोटाले
क्लिक करने से
पहले सोचें



डिजिटल अरेस्ट घोटालों से निपटने के लिए सुप्रीम कोर्ट ने जारी किए 13 सूत्रीय निर्देश

आईजी (कॉमन एंड आईटी) डीटीई. सीआरपीएफ

1. LATEST CYBER THREAT

1. फर्जी टैक्स नोटिस घोटाले

साइबर क्रिमिनल तेज़ी से इनकम टैक्स डिपार्टमेंट (ITD) जैसी सरकारी एजेंसियों की नकल करके लोगों को गलत फ़ाइलें डाउनलोड करने के लिए फंसा रहे हैं। एक आम स्कैम में WhatsApp या SMS मैसेज होते हैं, जिनमें दावा किया जाता है कि पाने वाले ने टैक्स में गड़बड़ी की है और पेनल्टी या कानूनी कार्रवाई से बचने के लिए उसे 72 घंटे के अंदर जवाब देना होगा। इन मैसेज में अक्सर ITD.zip जैसे अटैचमेंट या संदिग्ध लिंक होते हैं, जो पीड़ित के डिवाइस पर मैलवेयर इंस्टॉल कर देते हैं।



घोटाला कैसे काम करता है

ZIP फ़ाइल एक बार खुलने के बाद, मॉलिसियस सॉफ़्टवेयर इंस्टॉल हो जाता है, जिससे अटैकर बैंकिंग क्रेडेंशियल, पासवर्ड, पर्सनल जानकारी और वन-टाइम पासवर्ड (OTP) चुरा सकते हैं। पीड़ित अपने डिवाइस पर कंट्रोल भी खो सकते हैं, जिससे फाइनेंशियल फ्रॉड और आइडेंटिटी थेफ़्ट हो सकता है।

सुरक्षित कैसे रहें

टैक्स से जुड़ी बातचीत को हमेशा ऑफिशियल इनकम टैक्स पोर्टल या ईमेल से वेरिफाई करें। कभी भी बिना मांगे WhatsApp या SMS मैसेज से मिले अटैचमेंट डाउनलोड न करें या लिंक पर क्लिक न करें। अगर कोई मैसेज अर्जेंट हो या लीगल एक्शन की धमकी दे, तो उसे संदिग्ध समझें और तुरंत रिपोर्ट करें।

मूल संदेश: "क्लिक करने से पहले सोचें—सरकारी नोटिस कभी भी संदिग्ध WhatsApp अटैचमेंट के ज़रिए नहीं भेजे जाते हैं।"

2. एजेंटिक और मशीन-स्पीड एक्सप्लॉइट्स

साइबर अटैक एक नए दौर में आ रहे हैं, जहाँ आर्टिफिशियल इंटेलिजेंस (AI) बहुत कम या बिना किसी इंसानी दखल के काम कर सकता है। थ्रेट एक्टर्स कमज़ोरियों को पहचानने, एक्सप्लॉइट कोड बनाने और मशीन की स्पीड से अटैक करने के लिए ऑटोनॉमस AI एजेंट्स का तेज़ी से इस्तेमाल कर रहे हैं। यह ऑटोमेशन अटैकर्स को घंटों या दिनों के बजाय मिनटों में सिस्टम को कॉम्प्रोमाइज़ करने में मदद करता है, जिससे साइबर क्राइम का स्केल और एफिशिएंसी बहुत ज़्यादा बढ़ जाती है।



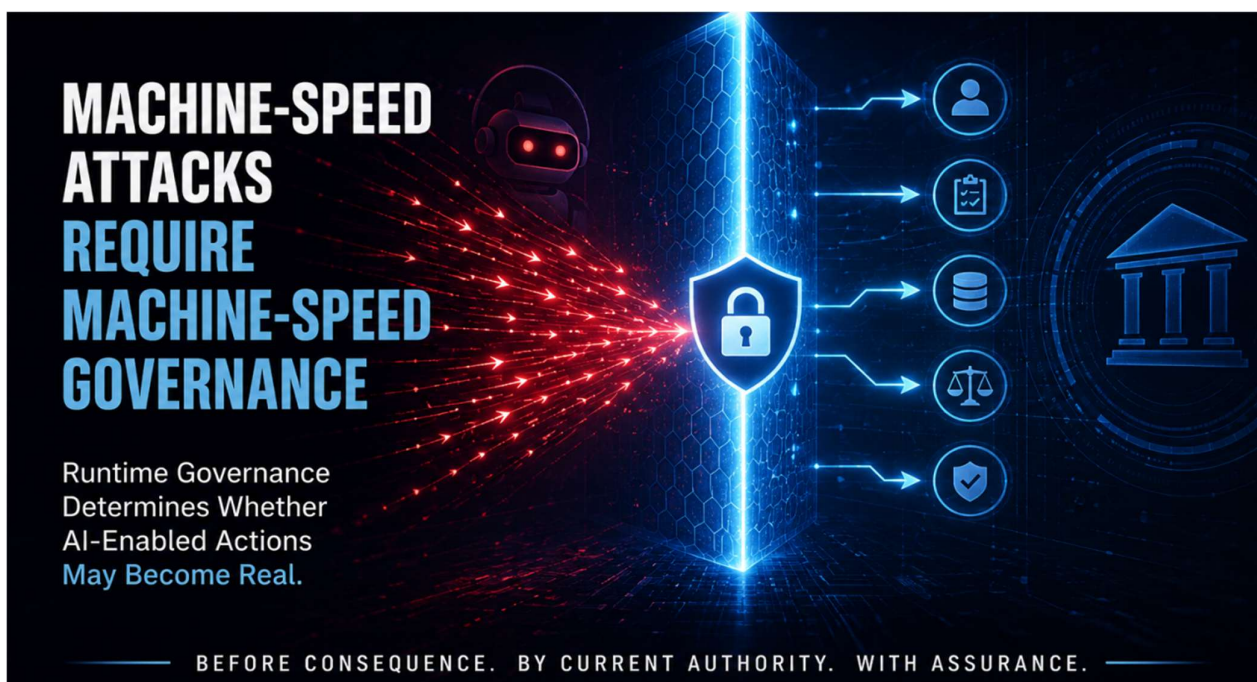
थ्रेट कैसे काम करता है

AI से चलने वाले एजेंट लगातार पब्लिक-फेसिंग एप्लिकेशन, क्लाउड एनवायरनमेंट और एंटरप्राइज़ नेटवर्क को सिक्योरिटी की कमियों के लिए स्कैन करते रहते हैं। एक बार vulnerability मिलने पर, AI अटैक कोड बना सकता है, vulnerability का फ़ायदा उठा सकता है, कनेक्टेड सिस्टम में इधर-उधर जा सकता है और पर्सिस्टेंस बना सकता है—यह सब कम से कम इंसानी दखल के साथ कर सकता है। हाल की साइबर सिक्योरिटी रिपोर्ट के मुताबिक, एवरेज ब्रेकआउट टाइम—अटैकर को शुरुआती ब्रीच से दूसरे सिस्टम में जाने में लगने वाला समय—कम होकर सिर्फ़ 29 मिनट रह गया है, जिससे ऑर्गनाइज़ेशन के पास जवाब देने के लिए बहुत कम समय बचता है।

यह क्यों मायने रखती है

मशीन-स्पीड एक्सप्लॉइट से तेज़ी से डेटा चोरी हो सकता है, रैंसमवेयर फैल सकता है और सिक्योरिटी टीम के रिएक्ट करने से पहले ही बड़े पैमाने पर नुकसान हो सकता है। इन बढ़ते खतरों से बचने के लिए, कंपनियों को AI-पावर्ड थ्रेट डिटेक्शन अपनाना होगा, अपने नेटवर्क पर लगातार नज़र रखनी होगी, कमज़ोरियों को जल्दी से ठीक करना होगा और ज़ीरो ट्रस्ट सिक्योरिटी मॉडल लागू करना होगा।

मूल संदेश: "ऑटोनॉमस AI के ज़माने में, हर मिनट मायने रखता है—क्योंकि साइबर अटैक अब इंसानों की नहीं, बल्कि मशीनों की स्पीड से होते हैं।"



2. नॉलेज बैंक

1. ट्रेलिक्स एंडपॉइंट सिक्योरिटी: मॉडर्न साइबर खतरों से डिवाइस को सुरक्षित रखता है।

एक बेहतर तरीका एंडपॉइंट सुरक्षा का

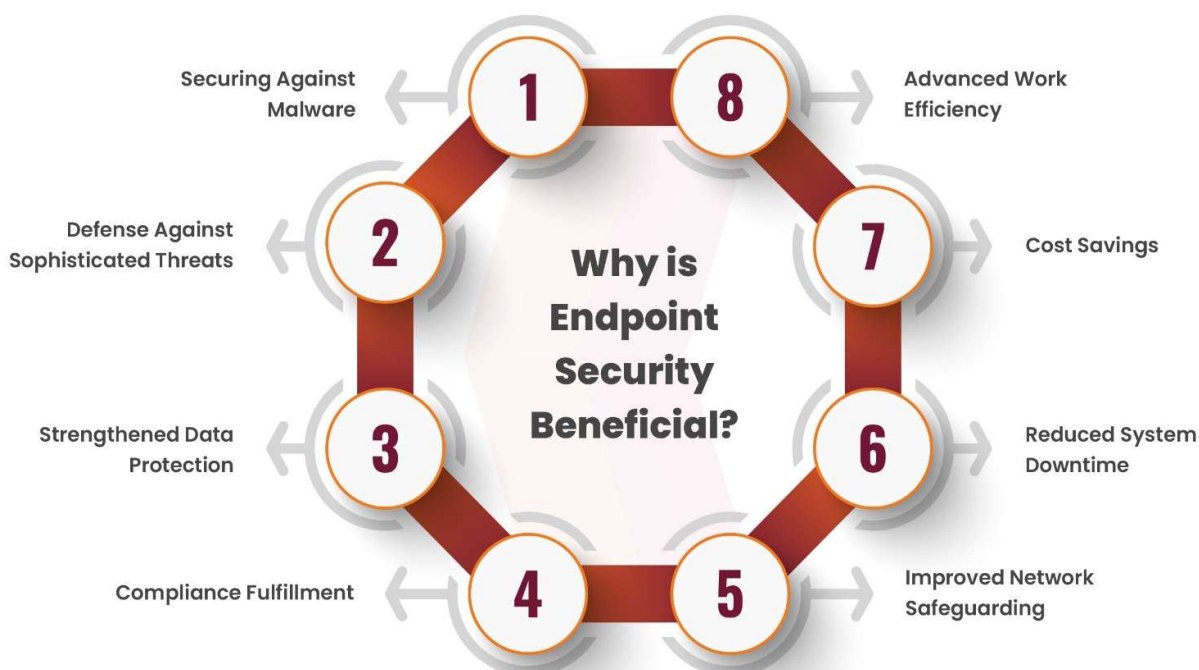
ऑफिस, घरों और दूर-दराज की जगहों पर काम करने वाले कर्मचारियों की वजह से, लैपटॉप, डेस्कटॉप और सर्वर साइबर क्रिमिनल्स के लिए खास टारगेट बन गए हैं। ट्रेलिक्स एंडपॉइंट सिक्योरिटी (ENS) एक एडवांस्ड एंडपॉइंट प्रोटेक्शन प्लेटफॉर्म है, जिसे इन डिवाइस को मैलवेयर, रैंसमवेयर, फाइललेस अटैक और दूसरे मुश्किल साइबर खतरों से बचाने के लिए डिज़ाइन किया गया है। कई सिक्योरिटी टेक्नोलॉजी को एक ही सॉल्यूशन में मिलाकर, यह कंपनियों को बिज़नेस ऑपरेशन पर असर डालने से पहले अटैक का पता लगाने, रोकने और उन पर जवाब देने में मदद करता है।



ट्रेलिक्स एंडपॉइंट सिक्योरिटी रियल-टाइम थ्रेट डिटेक्शन, बिहेवियर-बेस्ड एनालिसिस और मशीन लर्निंग का इस्तेमाल करके जाने-पहचाने और अनजाने खतरों की पहचान करती है। इसके इंटीग्रेटेड मॉड्यूल—जिसमें थ्रेट प्रिवेंशन, फ़ायरवॉल, वेब कंट्रोल, अडैप्टिव थ्रेट प्रोटेक्शन और एंडपॉइंट डिटेक्शन एंड रिस्पॉन्स (EDR) शामिल हैं—साइबर हमलों से बचाव की कई लेयर देते हैं। यह प्लेटफ़ॉर्म सेंटरलाइज़्ड सिक्योरिटी मैनेजमेंट भी देता है, जिससे IT टीमों एंडपॉइंट्स को मॉनिटर कर सकती हैं, सिक्योरिटी पॉलिसी लागू कर सकती हैं और एक ही कंसोल से घटनाओं की जांच कर सकती हैं।

यह क्यों मायने रखती है

जैसे-जैसे रैंसमवेयर, फ़िशिंग और AI से होने वाले हमले बढ़ रहे हैं, एंडपॉइंट सिक्योरिटी हर ऑर्गनाइज़ेशन की साइबर सिक्योरिटी स्ट्रैटेजी का एक ज़रूरी हिस्सा बन गई है। ट्रेलिक्स एंडपॉइंट सिक्योरिटी जैसे सॉल्यूशन अटैक की जगहों को कम करने, खतरे की विज़िबिलिटी को बेहतर बनाने और किसी ऑर्गनाइज़ेशन की पूरी साइबर रेजिलिएंस को मज़बूत करने में मदद करते हैं। एंडपॉइंट एक्टिविटी पर लगातार नज़र रखकर और संदिग्ध व्यवहार पर तुरंत जवाब देकर, ऑर्गनाइज़ेशन सेंसिटिव डेटा को बेहतर ढंग से सुरक्षित रख सकते हैं, बिज़नेस कंटीन्यूटी बनाए रख सकते हैं और आज के तेज़ी से बदलते खतरे के माहौल से बचाव कर सकते हैं।



2. सुप्रीम कोर्ट ने डिजिटल अरेस्ट स्कैम से निपटने के लिए 13-पॉइंट निर्देश जारी किए

भारत के सुप्रीम कोर्ट ने "डिजिटल अरेस्ट" स्कैम के बढ़ते खतरे से निपटने के लिए देश की कार्रवाई को मज़बूत करने के लिए 13 अंतरिम निर्देश जारी किए हैं। इन स्कैम में धोखेबाज़ पुलिस अधिकारी, CBI अधिकारी या दूसरे सरकारी अधिकारी बनकर पीड़ितों को पैसे ट्रांसफर करने या सेंसिटिव जानकारी देने के लिए धमकाते हैं। अपने निर्देशों के तहत, कोर्ट ने रिज़र्व बैंक ऑफ़ इंडिया (RBI) को चार हफ्ते के अंदर एक स्टैंडर्ड ऑपरेटिंग प्रोसीजर (SOP) बनाने का निर्देश दिया है, ताकि पूरे देश में शिकायत दूर करने और फंड वापस पाने के तरीके लागू किए जा सकें। कोर्ट ने धोखाधड़ी वाले फंड की रिकवरी को बेहतर बनाने के लिए बैंकों, कानून लागू करने वाली एजेंसियों, टेलीकॉम ऑपरेटरों और डिजिटल प्लेटफॉर्म के बीच तेज़ी से तालमेल की ज़रूरत पर ज़ोर दिया।

DIGITAL ARREST SCAMS: SUPREME COURT ORDERS STRONGER SAFEGUARDS, SEEKS COMPENSATION PLAN FOR VICTIMS

KEY DIRECTIONS

- RBI TO ISSUE SOP FOR BANKS**
RBI to adopt and circulate SOP within 4 weeks for debit holds, grievance redressal and money restoration
- STATES TO STRENGTHEN CYBER RESPONSE**
Operationalise State Cyber Crime Centres, adopt e-Zero FIR and ensure speedy disposal of account freezing matters
- COMPENSATION FRAMEWORK**
Inter-departmental committee to examine shared liability and compensation plan for scam victims
- CBI THRESHOLD & TELECOM CURBS**
Committee to review CBI monetary threshold and telecom curbs on audio/video calls
- AWARENESS & COORDINATION**
Wide public awareness campaigns on prevention, grievance redressal and fund recovery

FOCUS ON VICTIM PROTECTION AND JUSTICE

68 Mechanism requires wide adoption, faster disposal and continued follow-up. **69** Matter to be next taken up in September

कोर्ट ने साइबर फ्रॉड की शिकायतों की जल्दी रिपोर्टिंग और जवाब देने के लिए 1930 साइबर हेल्पलाइन और नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल (NCRP) जैसे मौजूदा साइबर फ्रॉड रिपोर्टिंग सिस्टम को ज़्यादा अपनाने की भी बात कही। इन निर्देशों का मकसद लोगों में जागरूकता बढ़ाकर, जांच प्रोसेस में तेज़ी लाकर और फाइनेंशियल संस्थानों तथा सरकारी एजेंसियों के बीच सहयोग बढ़ाकर भारत के साइबर फ्रॉड इकोसिस्टम को मज़बूत करना है। इस कदम से नागरिकों को तेज़ी से बढ़ते ऑनलाइन फाइनेंशियल फ्रॉड और नकली पहचान वाले स्कैम से बेहतर सुरक्षा मिलने की उम्मीद है, जिससे समय पर रिपोर्टिंग और डिजिटल सतर्कता की अहमियत और बढ़ेगी।

3. IT इंफ्रास्ट्रक्चर को कैसे सुरक्षित रखें

1. घटना (Incident) की प्रतिक्रिया योजना तैयार करें

कोई भी ऑर्गनाइज़ेशन साइबर अटैक से पूरी तरह सुरक्षित नहीं है, इसलिए इंसिडेंट रिस्पॉन्स प्लान (IRP) साइबर सिक्योरिटी का एक ज़रूरी हिस्सा है। इंसिडेंट रिस्पॉन्स प्लान एक डॉक्यूमेंटेड प्रोसेस है, जो किसी ऑर्गनाइज़ेशन को रैसमवेयर अटैक, डेटा ब्रीच या मैलवेयर इन्फेक्शन जैसे साइबर इंसिडेंट का पता लगाने, रिपोर्ट करने, उन्हें रोकने, जांच करने और उनसे रिकवर करने के तरीके बताता है। एक अच्छी तरह से तैयार किया गया प्लान डाउनटाइम कम करने, फाइनेंशियल नुकसान को कम करने और सेंसिटिव जानकारी को सुरक्षित रखने में मदद करता है।



प्लान में कर्मचारियों, IT टीमों, मैनेजमेंट और बाहरी पार्टनर्स की भूमिका और ज़िम्मेदारियाँ साफ़ तौर पर बताई जानी चाहिए। कंपनियों को रेगुलर तौर पर साइबर अटैक सिमुलेशन और टेबलटॉप एक्सरसाइज़ करनी चाहिए, ताकि यह पक्का हो सके कि किसी घटना के दौरान हर कोई अपनी ज़िम्मेदारियों को समझे। इमरजेंसी कॉन्टैक्ट लिस्ट को अपडेट रखना, सुरक्षित बैकअप बनाए रखना और रिकवरी प्रोसेस को डॉक्यूमेंट करना, रिस्पॉन्स टाइम को काफी बेहतर बना सकता है। एक तेज़ और अच्छी तरह से कोऑर्डिनेटेड रिस्पॉन्स न सिर्फ़ अटैक के असर को कम करता है, बल्कि बिज़नेस ऑपरेशन और कस्टमर का भरोसा भी तेज़ी से वापस लाने में मदद करता है।

2. यूज़र एक्सेस को सीमित करें

किसी ऑर्गनाइज़ेशन के IT इंफ्रास्ट्रक्चर को साइबर खतरों से बचाने के लिए यूज़र एक्सेस को सीमित करना सबसे असरदार तरीकों में से एक है। कर्मचारियों को सिर्फ़ उन्हीं डेटा, एप्लिकेशन और सिस्टम का एक्सेस दिया जाना चाहिए, जो उनके खास काम की ज़िम्मेदारियों को पूरा करने के लिए ज़रूरी हैं। यह सिक््योरिटी प्रैक्टिस, जिसे प्रिंसिपल ऑफ़ लीस्ट प्रिविलेज (PoLP) के नाम से जाना जाता है, बिना इजाज़त एक्सेस, डेटा लीक और अंदरूनी खतरों के जोखिम को कम करने में मदद करती है। अगर किसी यूज़र का अकाउंट फ़िशिंग या मैलवेयर से हैक हो जाता है, तो लिमिटेड एक्सेस अटैकर्स को नेटवर्क पर आसानी से घूमने और ज़रूरी बिज़नेस सिस्टम तक पहुँचने से रोकता है।



ऑर्गनाइज़ेशन को रेगुलर यूज़र परमिशन को भी रिव्यू करना चाहिए, ताकि यह पक्का हो सके कि रोल बदलने या कंपनी छोड़ने के बाद भी एम्प्लॉई के पास गैर-ज़रूरी एक्सेस न रहे। इनएक्टिव अकाउंट को तुरंत डिसेबल कर देना चाहिए और एडमिनिस्ट्रेटर के अधिकार सिर्फ़ ऑथराइज़्ड लोगों को ही मिलने चाहिए। सेंसिटिव जानकारी तक एक्सेस को रेगुलर ऑडिट के ज़रिए मॉनिटर किया जाना चाहिए और ज़रूरी सिस्टम को एक्स्ट्रा अप्रूवल सिस्टम से सुरक्षित किया जाना चाहिए। सही एक्सेस कंट्रोल लागू करके और यूज़र परमिशन को लगातार रिव्यू करके, ऑर्गनाइज़ेशन साइबर अटैक के असर को काफ़ी कम कर सकते हैं, कॉन्फिडेंशियल जानकारी को सुरक्षित रख सकते हैं और एक सुरक्षित और मज़बूत IT माहौल बनाए रख सकते हैं।

4. साइबर गपशप

1) केंद्र ने अलग साइबरबुलिंग कानून को खारिज किया, AI कंटेंट सुरक्षा उपायों को मज़बूत किया :

केंद्र सरकार ने साफ़ किया है कि वह साइबरबुलिंग के लिए अलग कानून बनाने की योजना नहीं बना रही है। सरकार ने कहा है कि इन्फॉर्मेशन टेक्नोलॉजी एक्ट के तहत मौजूदा नियम और मज़बूत IT नियम ऑनलाइन गलत भाषा के इस्तेमाल, डीपफेक और AI से होने वाले नुकसानदायक कंटेंट से निपटने के लिए काफी हैं। सरकार ने संसद को बताया कि उसका वर्तमान फ़ोकस मौजूदा कानूनों को ज़्यादा असरदार तरीके से लागू करने और डिजिटल प्लेटफ़ॉर्म के लिए सुरक्षा उपायों को मज़बूत करने पर है। जैसे-जैसे AI से होने वाला कंटेंट और बेहतर होता जाएगा, वैसे-वैसे तेज़ी से पता लगाने, प्लेटफ़ॉर्म की बेहतर जवाबदेही और ऑनलाइन परेशानी तथा गलत जानकारी से इंटरनेट यूज़र्स की बेहतर सुरक्षा पर ज़ोर रहेगा।

2) झारखंड में पुलिस ने साइबर म्यूल नेटवर्क को पकड़ा, 40 Vulnerable युवाओं को बचाया

ऑर्गनाइज़्ड साइबर क्राइम के खिलाफ़ एक बड़ी कार्रवाई में, झारखंड में पुलिस ने एक ऐसे नेटवर्क को खत्म किया है, जो कथित तौर पर बेरोज़गार युवाओं को "मनी म्यूल" के तौर पर भर्ती करता था, ताकि वे गैर-कानूनी तरीके से कमाए गए पैसे को अपने बैंक अकाउंट के ज़रिए ट्रांसफर कर सकें। खुफिया जानकारी मिलने पर, अधिकारियों ने आदित्यपुर इंडस्ट्रियल एरिया के कई होटलों और लॉज में रेड मारी और झारखंड, बिहार और पश्चिम बंगाल के करीब 40 युवाओं को बचाया। यह घटना दिखाती है कि कैसे साइबर क्रिमिनल कमज़ोर (Vulnerable) लोगों का शोषण करते हैं, उनके बैंक अकाउंट का एक्सेस देने के बदले में आसान पैसे का लालच देकर। लोगों को सलाह दी जाती है कि वे कभी भी अपने बैंक अकाउंट, डेबिट कार्ड या डिजिटल पेमेंट क्रेडेंशियल शेयर या किराए पर न दें, क्योंकि वे अनजाने में साइबर क्राइम ऑपरेशन का हिस्सा बन सकते हैं।

3) 1.6 करोड़ रुपये के डिजिटल अरेस्ट घोटाले में बैंक अधिकारी, फर्म मालिक के खिलाफ चार्जशीट दाखिल की

सेंट्रल ब्यूरो ऑफ़ इन्वेस्टिगेशन (CBI) ने कश्मीर की एक फर्म के मालिक और एक्सिस बैंक के एक डिप्टी मैनेजर के खिलाफ डिजिटल अरेस्ट स्कैम के सिलसिले में चार्जशीट फाइल की है। इस स्कैम में दिल्ली के एक सीनियर सिटिज़न से 1.6 करोड़ रुपये की ठगी की गई थी। बुधवार को एक ऑफिशियल बयान में यह जानकारी दी गई। चार्जशीट में जिन आरोपियों के नाम हैं, वे हैं मेसर्स हिमालयन एंटरप्राइजेज, पुलवामा के मालिक उमर इकबाल और एक्सिस बैंक में डिप्टी मैनेजर उमर अहमद डार।

5. साइबर हाइजीन

- अपने बैंक अकाउंट और ऑनलाइन अकाउंट को रेगुलर तौर पर चेक करें कि कहीं कोई संदिग्ध एक्टिविटी तो नहीं हो रही है।
- कोई भी एक्शन लेने से पहले इन्वेस्टमेंट ऑफर, जॉब के मौके और सरकारी नोटिस वेरिफाई कर लें।
- अपने ऑपरेटिंग सिस्टम, एप्लिकेशन और एंटीवायरस सॉफ्टवेयर को लेटेस्ट सिक्योरिटी पैच के साथ अपडेट रखें।
- लिंक पर क्लिक करने या अटैचमेंट डाउनलोड करने से पहले ईमेल, मैसेज और QR कोड वेरिफाई करें।
- ऐप्स और सॉफ्टवेयर सिर्फ़ भरोसेमंद या ऑफिशियल सोर्स से ही डाउनलोड करें।
- अपने डिवाइस को PIN, पासवर्ड या बायोमेट्रिक ऑथेंटिकेशन से लॉक करें।
- बैंकिंग के लिए या भरोसेमंद VPN के बिना सेंसिटिव जानकारी एक्सेस करने के लिए पब्लिक Wi-Fi का इस्तेमाल करने से बचें।
- ऐप परमिशन चेक करें और सीमित करें, खासकर अपने कैमरा, माइक्रोफ़ोन, कॉन्टैक्ट्स और लोकेशन का एक्सेस।
- शेयर्ड या पब्लिक कंप्यूटर इस्तेमाल करने के बाद अकाउंट से लॉग आउट करें।
- भरोसेमंद सरकारी और साइबर सिक्योरिटी सलाह के ज़रिए लेटेस्ट साइबर खतरों के बारे में जानकारी रखें।

6. IT विंग में नया डेवलपमेंट

अतिथि प्रबंधन प्रणाली – “सत्कार पोर्टल”:

“सत्कार पोर्टल” का विकास कार्यक्रमों के कुशल प्रबंधन एवं समन्वय के लिए किया गया है। जब भी कोई कार्यक्रम आयोजित किया जाता है, तो कार्यक्रम में आमंत्रित सभी अतिथियों के साथ एक कार्यक्रम पंजीकरण लिंक साझा किया जाता है, ताकि उनके प्रवास एवं कार्यक्रम के दौरान आवश्यक व्यवस्थाओं का प्रभावी प्रबंधन एवं समन्वय सुनिश्चित किया जा सके।



सीआरपीएफ के महानिदेशक **श्री जी.पी. सिंह (आईपीएस)** ने नए मुख्यालय भवन के निर्माण की प्रगति की समीक्षा की तथा सभी प्रमुख हितधारकों के साथ संवाद किया।



सीआरपीएफ के महानिदेशक **श्री जी.पी. सिंह (आईपीएस)** ने नॉर्दर्न सेक्टर अस्पताल में अधिकारियों एवं जवानों के साथ बीएमआई 2.0 – 2026 की शुरुआत करते हुए स्वयं इसका आकलन कराया।



सीआरपीएफ के महानिदेशक **श्री जी.पी. सिंह (आईपीएस)** ने हैदराबाद स्थित सरदार वल्लभभाई पटेल राष्ट्रीय पुलिस अकादमी में 77वें नियमित भर्ती (RR) बैच के आईपीएस अधिकारियों की प्रतिष्ठित पासिंग आउट परेड का निरीक्षण किया।

संचार एवं सूचना प्रौद्योगिकी निदेशालय, केंद्रीय रिजर्व पुलिस बल