±

केंद्रीय रिज़र्व पुलिस बल

फरवरी, 2026

साइबर बाइट

गृह मंत्रालय ने एजेंसियों को ऑनलाइन धोखाधड़ी के मामलों में बैंक खातों को फ्रीज करने से पहले शिकायतों का सत्यापन करने को कहा है।

हगिंग फेस इंफ्रास्ट्रक्चर का दुरुपयोग करके एक बड़े पैमाने पर मैलवेयर अभियान में एंड्रॉइड आरएटी को फैलाया गया।

महानिरीक्षक, संचार एवं सूचना प्रौद्योगिकी निदेशालय, सीआरपीएफ

1. साइबर की दुनिया की खबरें

(ए) सी-मित्र पहल से साइबर अपराध पीड़ितों को मिली नई उम्मीद, 10 दिनों में 100 FIR दर्ज:-

हैदराबाद पुलिस के द्वारा तेलंगाना के हैदराबाद में **सी-मित्र (C-Mitra)** पहल की शुरुआत की गई। साइबर अपराध के शिकार लोगों के लिए एक महत्वपूर्ण प्रोत्साहन के रूप में, सी-मित्र की पहल ने महज 10 दिनों में 100 प्रथम सूचना रिपोर्ट (FIR) दर्ज करने में कामयाबी हासिल की है। यह साइबर धोखाधड़ी के मामलों में न्याय तक पहुँच और समय पर पुलिस कार्रवाई को बेहतर बनाने की दिशा में एक बड़ा कदम है। साइबर अपराध से प्रभावित नागरिकों की सहायता के उद्देश्य से शुरू की गई सी-मित्र की पहल, पीड़ितों और कानून प्रवर्तन एजेंसियों के बीच एक सेतु (पुल) के रूप में कार्य करती है। यह पहल व्यक्तियों को साइबर अपराध की शिकायत दर्ज करने की अक्सर जटिल और डराने वाली प्रक्रिया को समझने में मदद करती है, जिससे यह सुनिश्चित होता है कि मामलों को बिना किसी अनावश्यक देरी के औपचारिक रूप से दर्ज किया जाए और उन पर कार्रवाई की जाए।

इस पहल से जुड़े अधिकारियों ने बताया कि जागरूकता की कमी, तकनीकी जटिलताओं या प्रक्रियात्मक बाधाओं के कारण कई साइबर अपराध पीड़ितों को प्रथम सूचना रिपोर्ट (FIR) दर्ज कराने में संघर्ष करना पड़ता है। सी-मित्र मार्गदर्शन, दस्तावेज़ीकरण में सहायता और संबंधित पुलिस स्टेशनों के साथ समन्वय स्थापित करके इन चुनौतियों का समाधान करती है, जिसके परिणामस्वरूप मामलों का पंजीकरण तेजी से और अधिक कुशलता से हो पाता है।

इस पहल के लाभार्थियों ने राहत व्यक्त की और प्रशंसा करते हुए कहा है कि धोखाधड़ी वाले लेनदेन को रोकने, जांच शुरू करने और रिकवरी की संभावनाओं को बेहतर बनाने के लिए समय पर प्रथम सूचना रिपोर्ट(FIR) दर्ज करना अत्यंत महत्वपूर्ण है। कई पीड़ितों ने बताया कि सी-मित्र से संपर्क करने से पहले उन्हें अपनी शिकायतें स्वीकार करवाने में कठिनाइयों का सामना करना पड़ा था। कानून प्रवर्तन अधिकारियों ने भी इस पहल का स्वागत किया है, और कहा है कि उचित रूप से प्रलेखित शिकायतें जांच को तेज करने और साइबर अपराध सेल तथा स्थानीय पुलिस स्टेशनों के बीच समन्वय में सुधार करने में मदद करती हैं।

- यदि आप साइबर धोखाधड़ी के शिकार हैं, तो तुरंत इसकी सूचना दें। समय पर रिपोर्ट करने से धोखाधड़ी वाले लेनदेन को फ्रीज करने(रोकने) की संभावना बढ़ जाती है।

- **ऑनलाइन शिकायत दर्ज करें:-** साइबर अपराध हेल्पलाइन **1930** या आधिकारिक साइबर अपराध पोर्टल (**cybercrime.gov.in**) के माध्यम से शिकायत दर्ज करें। जांच और कानूनी कार्रवाई के लिए प्रथम सूचना रिपोर्ट (FIR) अत्यंत महत्वपूर्ण है। सी-मित्र(C-Mitra) जैसी पहल यह सुनिश्चित करने में मदद करती है कि प्रथम सूचना रिपोर्ट (FIR) सुचारू रूप से दर्ज हो।

- धोखाधड़ी से संबंधित संदेशों के स्क्रीनशॉट, लेनदेन का विवरण (Transaction details), कॉल लॉग, यूआरएल (URL) और ई;-मेल सुरक्षित रखें।
- बैंक और पुलिस कभी भी कॉल या संदेश पर गोपनीय विवरण नहीं मांगते हैं।

(बी) गृह मंत्रालय ने एजेंसियों से ऑनलाइन धोखाधड़ी के मामलों में बैंक खातों को फ्रीज करने से पहले शिकायतों को सत्यापित करने के लिए कहा :-

गृह मंत्रालय ने कानून प्रवर्तन एजेंसियों और साइबर अपराध इकाइयों को बैंक खातों को फ्रीज करने से पहले शिकायतों की ठीक से जांच करने और ऑनलाइन धोखाधड़ी के साथ स्पष्ट संबंध की पुष्टि करने का निर्देश दिया है। यह निर्णय उन चिंताओं के बाद लिया गया है जिनमें गलत पहचान, विवादित लेन-देन या खराब सत्यापन के कारण निर्दोष लोगों और व्यवसायियों के खाते फ्रीज कर दिए गए थे, जिससे वेतन रुकने, व्यावसायिक गतिविधियां ठप होने और दैनिक खर्चों को पूरा करने में कठिनाई होने जैसी गंभीर वित्तीय समस्याएं पैदा हो रही थीं।

नए तरीके के तहत, एजेंसियों को फ्रीज करने का आदेश देने से पहले शिकायतों या प्रथम सूचना रिपोर्ट(FIR) को सत्यापित करना होगा और अपडेट किए गए साइबर धोखाधड़ी नियमों के तहत स्पष्ट और बेहतर प्रलेखित प्रक्रियाओं का पालन करना होगा। गृह मंत्रालय राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (NCRP) के तहत प्रक्रियाओं में भी सुधार कर रहा है ताकि लोगों को बेवजह की वित्तीय कठिनाइयों से बचाते हुए बेहतर जांच सुनिश्चित की जा सके।

👉 **प्रक्रिया पहले कैसे काम करती थी (समस्या)**

पहले, कई साइबर-धोखाधड़ी के मामलों में:

- नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल (NCRP) पर केवल एक शिकायत
- या संदेह के आधार पर दर्ज की गई प्रथम सूचना रिपोर्ट(FIR)

(अक्सर पुलिस के लिए निम्नलिखित कार्यों हेतु पर्याप्त थी):

- बैंकों को पूरे खाते को फ्रीज करने के लिए कहना, जो कभी-कभी कुछ ही घंटों के भीतर कर दिया जाता था।
- भले ही खाताधारक केवल एक माध्यम (pass-through) रहा हो या उसे गलत तरीके से टैग किया गया हो।

👉 गृह मंत्रालय के नए निर्देशों के तहत क्या बदलाव आए हैं :

i. फ्रीज करने से पहले सत्यापन

- शिकायत को केवल ऊपरी तौर पर स्वीकार करने के बजाय उसका सत्यापन करें।
- बैंक खाते और धोखाधड़ी के बीच एक स्पष्ट संबंध स्थापित करें।
- लेनदेन के विवरण (transaction trails), समय और लाभार्थी के विवरण की जाँच करें।
- अब केवल इसलिए खाता फ्रीज नहीं किया जाएगा क्योंकि वह लेन-देन की श्रृंखला (chain) में कहीं दिखाई दिया है।

ii. अब पूरा बैंक अकाउंट पूरी तरह से फ्रीज (बंद) नहीं होगा

(पूरे खाते को फ्रीज करने के बजाय, एजेंसियों से अपेक्षा की जाती है कि वे:)

i. केवल संदिग्ध राशि को ही फ्रीज करें।

ii. जो निधियां संबंधित नहीं हैं, उनको ब्लॉक करने से बचें, जैसे :

iii. वेतन

iv. पेंशन

v. व्यवसाय की कार्यशील पूंजी

iii. पुलिस की ओर से पुख्ता कागजी कार्रवाई

(बैंकों द्वारा कार्रवाई करने से पहले, पुलिस के निर्देशों में अब शामिल होना चाहिए:)

- प्रथम सूचना रिपोर्ट(FIR) / शिकायत का संदर्भ (Reference)।
- खाता फ्रीज करने का तर्कसंगत आधार।
- विशिष्ट लेनदेन का विवरण (राशि, तारीख, ट्रेल/विवरण)।
- बैंकों से अब प्रचलित ई-मेल या मौखिक अनुरोधों पर कार्रवाई करने की अपेक्षा नहीं की जाती है।

iv. छोटी रकम की धोखाधड़ी के लिए त्वरित रिफंड

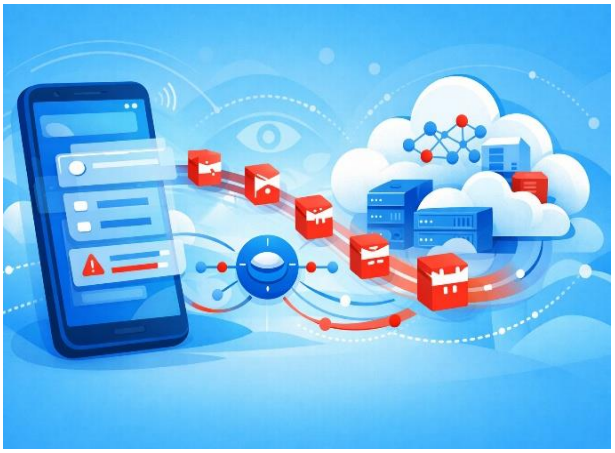
- 50,000 रुपये से कम की धोखाधड़ी वाली राशि को अदालत के आदेश के बिना शीघ्र वापिस (Refund) किया जा सकता है।
- यदि कोई अदालती आदेश या बहाली (restoration) का आदेश मौजूद नहीं है, तो बैंकों को 90 दिनों के भीतर ऐसी राशियों पर लगी रोक हटानी होगी।

यदि आप प्रभावित हैं, तो आपको क्या तैयार रखना चाहिए (अत्यंत महत्वपूर्ण) :

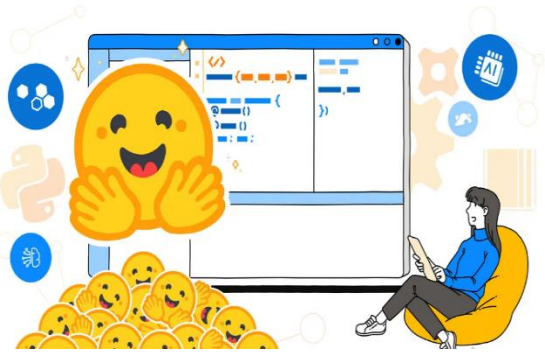
- फंड के वैध स्रोत को दर्शाने वाला बैंक स्टेटमेंट।
- वेतन पर्ची/ बीजक(इनवॉइस)/ जीएसटी रिटर्न (यदि बिजनेस अकाउंट है)।
- इनको लिखित अनुरोध भेजें:
  - जांच अधिकारी
  - बैंक शिकायत सेल(प्रकोष्ठ)
- यदि पुलिस देरी करती है, तो कई मामलों में उच्च न्यायालय की रिट याचिकाएं प्रभावी साबित हुई हैं।

2. साइबर धोखाधड़ी

(ए) बड़े पैमाने पर चलाए गए मैलवेयर अभियान में एंड्रॉइड रैट (RAT) फैलाने के लिए हगिंग फेस (Hugging Face) के इन्फ्रास्ट्रक्चर का दुरुपयोग किया गया :



बिटडिफेंडर (Bitdefender) के साइबर सुरक्षा शोधकर्ताओं ने एक नए एंड्रॉइड मैलवेयर अभियान का पता लगाया है, जो फोन को संक्रमित करने के लिए **'ट्रस्टबास्टियन' (TrustBastion)** नामक एक नकली सुरक्षा ऐप का उपयोग करता है। यह हमला विज्ञापनों या पॉप-अप चेतावनियों से शुरू होता है जो झूठा दावा करते हैं कि उपयोगकर्ता का डिवाइस संक्रमित है और उसे सुरक्षा की आवश्यकता है। जब उपयोगकर्ता **'ट्रस्टबास्टियन' (TrustBastion)** इंस्टॉल करते हैं, तो यह एक असली सुरक्षा ऐप जैसा दिखता है, लेकिन वास्तव में यह एक **'ड्रॉपर' (dropper)** है जिसे गुप्त रूप से और भी अधिक हानिकारक मैलवेयर डाउनलोड करने के लिए डिज़ाइन किया गया है। इंस्टॉल करने के बाद, ऐप एक नकली सिस्टम या गूगल प्ले अपडेट संदेश दिखाता है। यदि उपयोगकर्ता इसे स्वीकार कर लेता है, तो ऐप एक दूसरा दुर्भावनापूर्ण**(malacious)** ऐप डाउनलोड करता है जो हमलावरों को डिवाइस का रिमोट एक्सेस (दूरस्थ नियंत्रण) प्रदान कर देता है।



यह मैलवेयर **'हगिंग फेस' (Hugging Face)** पर होस्ट किया गया है, जो एक लोकप्रिय प्लेटफॉर्म है जिसका उपयोग आमतौर पर डेवलपर्स एआई (AI) मॉडल और डेटा साझा करने के लिए करते हैं। एक भरोसेमंद सेवा का उपयोग करके, हमलावर दुर्भावनापूर्ण **(malacious)** डाउनलोड का पता लगाना कठिन बना देते हैं और इसे सामान्य ट्रैफिक के बीच आसानी से छिपा देते हैं। बिटडिफेंडर ने पाया कि हमलावरों ने एंटीवायरस डिटेक्शन से बचने के लिए मैलवेयर के थोड़े अलग हजारों संस्करण (versions)

अपने आप से बनाए, कभी-कभी तो हर 15 मिनट में एक नया संस्करण। हटाए जाने से पहले, एक दुर्भावनापूर्ण**(malacious)** हगिंग फेस रिपॉजिटरी ने एक महीने से भी कम समय में 6,000 से अधिक अपडेट इकटठा किए थे। इसके बाद भी, यह अभियान थोड़े से बदलावों के साथ तुरंत दूसरी जगह फिर से प्रकट हो गया, जो यह दर्शाता है कि यह अत्यधिक स्वचालित और दीर्घस्थायी (persistent) है। शोधकर्ताओं ने उपयोगकर्ताओं को अप्रत्याशित सुरक्षा अलर्ट और संक्रमण(infection) को "ठीक" करने का दावा करने वाले ऐप्स से सावधान रहने की चेतावनी दी है, क्योंकि इनका उपयोग अक्सर मैलवेयर फैलाने के लिए किया जाता है।

- असली एंड्रॉइड या गूगल प्ले सुरक्षा अलर्ट विज्ञापनों, ब्राउज़र या रैंडम पॉप-अप में दिखाई नहीं देते हैं। यदि कोई संदेश आपको तुरंत ऐप इंस्टॉल करने के लिए दबाव डालता है, तो यह एक खतरे का संकेत है।
- विज्ञापनों, एसएमएस संदेशों या वेबसाइटों के लिंक से ऐप डाउनलोड करने से बचें। गूगल प्ले पर भी, इंस्टॉल करने से पहले डेवलपर का नाम, समीक्षाएं(reviews) और डाउनलोड की संख्या की जांच करें।
- एंड्रॉइड सिस्टम अपडेट डिवाइस की सेटिंग्स के माध्यम से आते हैं, किसी तीसरे पक्ष के ऐप के माध्यम से नहीं। यदि कोई ऐप आपसे "अपडेट" इंस्टॉल करने के लिए कहता है, तो उसे अस्वीकार कर दें।
- यदि कोई सुरक्षा या उपयोगिता(utility) ऐप अत्यधिक अनुमतियाँ मांगता है, विशेष रूप से एक्सेसिबिलिटी एक्सेस (accessibility access), डिवाइस एडमिन अधिकार, या अन्य ऐप इंस्टॉल करने की अनुमति, तो सावधान हो जाएं।
- प्ले प्रोटेक्ट को सक्रिय रखें, यह ऐप्स को स्कैन करता है और आपको ज्ञात दुर्भावनापूर्ण**(malacious)** व्यवहार के बारे में चेतावनी दे सकता है।

- यदि आपका फोन अजीब सा पॉप-अप दिखाने लगता है, अधिक गर्म होने लगता है, या बैटरी असामान्य रूप से जल्दी खत्म होने लगती है, तो हाल ही में शामिल किए गए ऐप्स को अनइंस्टॉल करें और सुरक्षा स्कैन को चलाएं।

Urgency + Fear + "Security App" = Slow Down and Double-Check

(बी) साइबर पुलिस ने क्रिप्टोकरेंसी ट्रेडिंग घोटाले का पर्दाफाश किया; बैंक के दो कर्मचारी भी शामिल:

साइबर पुलिस ने फर्जी यूएसडीटी टीथर(Tether) ट्रेडिंग घोटाले में तीन लोगों को गिरफ्तार किया है। इस मामले में एक पीड़ित को व्हाट्सएप संदेशों के जरिए क्रिप्टोकरेंसी में निवेश के नाम पर झांसा दिया गया था।

पुलिस के अनुसार, गिरफ्तार किए गए आरोपियों में से दो बैंक कर्मचारी थे, जिन्होंने कथित तौर पर फर्जी दस्तावेजों का उपयोग करके बैंक खाते खोलने में अपनी नौकरी का दुरुपयोग किया। इन खातों का इस्तेमाल चोरी के पैसे को इधर-उधर भेजने के लिए किया गया था। 'दिनेश एंटरप्राइजेज' नामक एक शेल कंपनी के तहत खुले ऐसे ही एक खाते से लगभग ₹ 50 लाख भेजे किए गए थे, जिसका उपयोग धोखाधड़ी के नेटवर्क के अंदर बार-बार किया गया। माना जा रहा है कि इन खातों को खुलवाने में मदद करने के बदले आरोपियों को कमीशन मिलता था तथा इस मामले में और भी गिरफ्तारियां होने की संभावना है।

साइबर पुलिस ने स्पष्ट किया कि इस प्रकार के घोटाले आजकल आम हो गए हैं। जालसाज फर्जी ट्रेडिंग वेबसाइट या ऐप बनाते हैं जो दिखने में पेशे से संबंधित और विश्वसनीय लगते हैं। वे व्हाट्सएप, टेलीग्राम, सोशल मीडिया या ईमेल पर लोगों से संपर्क करते हैं और कम समय में बहुत अधिक या गारंटीकृत मुनाफे का वादा करते हैं। विश्वास जीतने के लिए वे मुनाफा होता हुआ दिखाई देने वाले फर्जी स्क्रीनशॉट या डैशबोर्ड दिखाते हैं। एक बार जब पीड़ित बड़ी धनराशि निवेश कर देता है, तो उस राशि को तुरंत दूसरे खातों में भेज दिया जाता है या क्रिप्टोकरेंसी में बदल दिया जाता है, जिससे उसकी रिकवरी करना कठिन हो जाता है। धोखाधड़ी करने वाले अक्सर कंपनी के प्रतिनिधि

होने का नाटक करते हैं या सब कुछ असली दिखाने के लिए फर्जी कार्यालय के विवरण का उपयोग करते हैं।

- यदि कोई निश्चित या असामान्य रूप से उच्च रिटर्न का वादा करता है, तो यह लगभग हमेशा एक घोटाला होता है। क्रिप्टो बाजार अस्थिर होते हैं, कोई भी मुनाफे की गारंटी नहीं दे सकता।
- धोखेबाज अक्सर मैसेजिंग ऐप या सोशल मीडिया के जरिए पीड़ितों से संपर्क करते हैं। वैध वित्तीय संस्थान निवेश के अवसरों के लिए लोगों को अचानक(randomly) संदेश नहीं भेजते हैं।
- भले ही कोई बैंक कर्मचारी होने का दावा करे, बैंक के आधिकारिक कस्टमर केयर नंबर के माध्यम से सीधे इसकी पुष्टि करें। धोखाधड़ी के मामलों में आंतरिक कर्मचारी भी शामिल हो सकते हैं।
- धनराशि ट्रांसफर करने से पहले खाते के नामों की जांच करें। यदि खाते का नाम कंपनी के नाम से मेल नहीं खाता है, तो तुरंत रुक जाएं।

Pressure + Promise of high returns + Urgency to transfer money = Likely Scam

3. इस महीने के सुझाव (TIPS OF THE MONTH)

(ए) वेलेंटाइन वीक धोखाधड़ी:

वेलेंटाइन वीक (7-14 फरवरी) के दौरान, साइबर अपराधी अधिक सक्रिय हो जाते हैं क्योंकि कई लोग ऑनलाइन खरीदारी कर रहे होते हैं, डेटिंग ऐप्स का उपयोग करते हैं और उपहार भेजते हैं। जालसाज पीड़ितों को ठगने के लिए भावनाओं, जल्दबाजी और विशेष प्रस्तावों का फायदा उठाते हैं। यहाँ वेलेंटाइन वीक के सबसे आम घोटाले दिए गए हैं :

1) रोमांस स्कैम ♡

जालसाज डेटिंग ऐप्स या सोशल मीडिया पर फर्जी प्रोफाइल बनाते हैं। वे बहुत जल्दी भावनात्मक विश्वास बना लेते हैं और फिर पैसे, गिफ्ट कार्ड, चिकित्सा सहायता, यात्रा व्यय या क्रिप्टोकरेंसी की मांग करते हैं।

2) उपहार और फूलों की नकली वेबसाइटें 🌹

धोखेबाज फूलों, चॉकलेट और गहनों पर भारी छूट देने वाले नकली ऑनलाइन स्टोर बनाते हैं। भुगतान के बाद, उपहार कभी नहीं पहुँचता।

3) फिशिंग ऑफर और डिस्काउंट लिंक 📩

आपको "वेलेंटाइन स्पेशल ऑफर्स" के साथ एसएमएस, व्हाट्सएप या ई-मेल संदेश प्राप्त हो सकते हैं। लिंक पर क्लिक करने से आपके बैंकिंग विवरण या ओटीपी(OTP) चोरी हो सकते हैं।

4) नकली कार्यक्रम और रात्रिभोज का आरक्षण(डिनर रिजर्वेशन) 🍽

जालसाज रियायती कीमतों पर नकली होटल, रेस्टारेंट या संगीत समारोह (कॉन्सर्ट) की बुकिंग का प्रचार करते हैं और भुगतान मिलने प्राप्त करने के बाद गायब हो जाते हैं।

5) सेक्सटॉर्शन और ब्लैकमेल 💻

धोखेबाज पीड़ितों को निजी फोटो साझा करने या वीडियो चैट में शामिल होने के लिए ललचा सकते हैं, और फिर पैसे न देने पर रिकॉर्डिंग लीक करने की धमकी देते हैं।

4. सूचना प्रौद्योगिकी निदेशालय में नए विकास

1.) कागज रहित प्रक्रिया प्रबंधन प्रणाली (पीपीएमएस

- **व्यक्तिगत उपलब्धि / कौशल प्रविष्टि आदेश**
- **वेतन निर्धारण आदेश**
- **डीसीपीएस वसूली आदेश**

माननीय गृह एवं सहकारिता मंत्री श्री अमित शाह के साथ गुवाहाटी में सीआरपीएफ के 87वें दिवस परेड में सीआरपीएफ के महानिदेशक श्री जी.पी. सिंह (आईपीएस)।

सीआरपीएफ के महानिदेशक श्री जी.पी. सिंह (आईपीएस) 87वें सीआरपीएफ दिवस परेड के दौरान गुवाहाटी में प्रशिक्षुओं के साथ बातचीत करते हुए।

सीआरपीएफ के महानिदेशक श्री जी.पी. सिंह (आईपीएस) 87वें सीआरपीएफ दिवस के दौरान गुवाहाटी के बड़खाना में जवानों के साथ बातचीत करते हुए।