केंद्रीय रिज़र्व पुलिस बल

जून, 2025

साइबर बाइट

दूरसंचार विभाग ने साइबर धोखाधड़ी और जोखिम संकेतक का अनावरण किया

एनसीएससी ने खुदरा विक्रेताओं पर अधिक रैनसमवेयर हमलों के खिलाफ चेतावनी जारी की

केदारनाथ यात्रा साइबर घोटाला पकड़ा गया: फर्जी साइटें, धोखाधड़ी वाले विज्ञापन, 100 से अधिक खाते ब्लॉक किए गए

संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ

1. साइबर गीक्स समाचार

ए. दूरसंचार विभाग ने साइबर धोखाधड़ी और जोखिम संकेतक का अनावरण किया:

साइबर धोखाधड़ी के बढ़ते खतरे से निपटने के लिए, दूरसंचार विभाग (DoT) ने वित्तीय धोखाधड़ी जोखिम संकेतक (FRI) लॉन्च किया है- जो डिजिटल इंटेलिजेंस प्लेटफ़ॉर्म (DIP) की एक मुख्य विशेषता है। यह उपकरण बैंकों, UPI सेवा प्रदाताओं और अन्य वित्तीय संस्थानों के साथ वास्तविक समय की खुफिया जानकारी साझा करने में सक्षम बनाकर डिजिटल भुगतान सुरक्षा को बढ़ाता है।

एफआरआई (FRI) एक बहुआयामी उपकरण है जो वित्तीय धोखाधड़ी में उनकी संभावित संलिप्तता के आधार पर मोबाइल नंबरों को वर्गीकृत करता है। यह राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (एनसीआरपी), दूरसंचार विभाग के चक्षु प्लेटफॉर्म और वित्तीय संस्थानों से प्राप्त इनपुट के आधार पर जोखिम स्तर - निर्धारित करता है, जैसे मध्यम, उच्च या बहुत उच्च स्तर।

प्रारंभिक चेतावनी प्रणाली के रूप में कार्य करते हुए,धोखाधड़ी संकेतक सबसे पहले वित्तीय लेनदेन को अधिकृत करने से पहले हितधारकों के चिंहित सक्रिय मोबाइल नंबरों को सत्यापित करने का अधिकार देता है। जब किसी चिंहित नंबर पर डिजिटल भुगतान शुरू किया जाता है, तो संभावित धोखाधड़ी को रोकने के लिए अतिरिक्त सत्यापन जांच शुरू की जा सकती है।

इस पहल का उद्देश्य एक लचीला, प्रौद्योगिकी-संचालित सुरक्षा ढांचा तैयार करना है जो उभरती हुई धोखाधड़ी तकनीकों के साथ विकसित होता है। डिजिटल भुगतान धोखाधड़ी की पहचान करने और उससे बचने के लिए उपयोगकर्ताओं को जानकारी प्रदान करने के लिए जन जागरूकता अभियान चलाने के समानांतर प्रयास चल रहे हैं।

बी. एनसीएससी ने खुदरा विक्रेताओं पर अधिक रैनसमवेयर हमलों के खिलाफ चेतावनी जारी की:

हाल ही में यूके(ब्रिटेन) के हैरोड्स और मार्क्स एंड स्पेंसर जैसे प्रमुख) रिटेलर्स पर हुए साइबर हमलों के बाद, नेशनल साइबर सिक्योरिटी सेंटर (NCSC) ने बढ़ते रैनसमवेयर खतरों, खासकर रिटेल सेक्टर में, इस बारे में तत्काल चेतावनी जारी की है। जवाब में, इसने व्यवसायों की सुरक्षा को मजबूत करने और वित्तीय जोखिम को कम करने में मदद करने के लिए भी विस्तृत दिशा-निर्देश जारी किए हैं।

एनसीएससी ने व्यवसाइयों से तत्काल और सक्रिय रक्षा उपाय अपनाने के लिए जोरदार आग्रह किया है, तथा इस बात पर बल दिया है कि व्यवसाय की निरंतरता को बनाए रखने और साइबर घटनाओं के प्रभाव को कम करने के लिए तैयारी अत्यंत महत्वपूर्ण है।

रैनसमवेयर हमलों से बचाव के लिए मुख्य दिशानिर्देश:

- पार्श्विक प्रसार को रोकने के लिए खतरे को तुरंत अलग करें और नियंत्रित करें ।
- परिचालन को शीघ्र बहाल करने के लिए सुरक्षित और अद्यतन बैक-अप सिस्टम का उपयोग करें ।
- समन्वित प्रतिक्रिया और सहायता के लिए बिना देरी किए संबंधित प्राधिकारियों को घटना की सूचना दें ।

2. साइबर अपराध

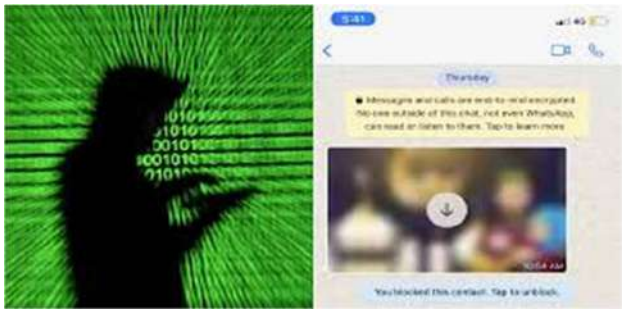
(ए) केदारनाथ यात्रा साइबर घोटाला पकड़ा गया: फर्जी साइटें, धोखाधड़ी वाले विज्ञापन, 100 से अधिक खाते ब्लॉक किए गए: -

चार धाम यात्रा शुरू होते ही साइबर अपराधी फर्जी वेबसाइट और सोशल मीडिया पेज बनाकर केदारनाथ धाम के लिए हेलीकॉप्टर टिकट बुकिंग की धोखाधड़ी की पेशकश कर श्रद्धालुओं को निशाना बना रहे हैं ।

इसके जवाब में, उत्तराखंड पुलिस के विशेष कार्य बल (एसटीएफ) ने बढ़ते साइबर अपराध के खतरे पर आक्रामक कार्रवाई शुरू की है। एसटीएफ चौबीसों घंटे निगरानी कर रहा है और निरंतर दैनिक निगरानी के माध्यम से साइबर आपराधिक ढांचे के खिलाफ निर्णायक कानूनी कार्रवाई कर रहा है। गृह मंत्रालय के भारतीय साइबर अपराध समन्वय केंद्र (I4C) के साथ घनिष्ठ समन्वय का लाभ उठाते हुए, इस अभियान ने धोखेबाजों द्वारा शोषण किए गए सैकड़ों डिजिटल परिसंपत्तियों को सफलतापूर्वक अवरुद्ध कर दिया है। जैसे-जैसे तकनीक

विकसित होती है, वैसे-वैसे कानून प्रवर्तन रणनीतियों को भी विकसित करना चाहिए। इस पहल की सफलता इसके सक्रिय नेतृत्व, अंतर-एजेंसी समन्वय, प्लेटफ़ॉर्म सहयोग और सक्रिय सार्वजनिक भागीदारी में निहित है-एक शक्तिशाली संयोजन जो साइबर अपराध की रोकथाम के लिए एक राष्ट्रीय बेंचमार्क के रूप में काम कर सकता है।

(बी) कोई ओटीपी नहीं, कोई लिंक नहीं-हैकर्स को अब बस एक वॉट्सऐप इमेज की जरूरत:



डिजिटल युग में, जहाँ फ़िशिंग लिंक और ओटीपी धोखाधड़ी आम खतरे हैं, अब एक नया खतरा सामने आया है- जो स्पष्ट रूप से दिखाई नहीं देता है। हैकर्स अब वॉट्सऐप इमेज को ट्रोजन हॉर्स के रूप में इस्तेमाल कर रहे हैं ताकि मैलवेयर को सीधे उपयोगकर्ताओं के डिवाइस पर पहुँचाया जा सके। पारंपरिक/सामान्य घोटालों के विपरीत, यह परिष्कृत तरीका **स्टेगनोग्राफी** का उपयोग करता है - यह एक ऐसी तकनीक है जिसमें दुर्भावनापूर्ण कोड को चुपके से हार्मलेस इमेज फ़ाइलों में अंतर्निहित किया जाता है।

संक्रमित छवि को खोलने के बाद, मैलवेयर चुपचाप पीड़ित के फोन पर खुद को स्थापित कर लेता है। इसके बाद यह बैंकिंग क्रेडेंशियल, ओटीपी जैसी संवेदनशील जानकारी निकाल सकता है और यहां तक कि बिना उपयोगकर्ता की जानकारी के अनधिकृत वित्तीय लेनदेन भी कर सकता है । इसका पता लगाना और उसकी रोकथाम विशेष रूप से चुनौतीपूर्ण है।

इस खतरे की गंभीरता तब सामने आई जब मध्य प्रदेश के जबलपुर निवासी ने एक अनजान व्हाट्सएप नंबर से प्राप्त एक तस्वीर को खोलने के बाद लगभग 2 लाख रुपया गवा दिए। मैलवेयर ने उनके डिवाइस में घुसपैठ की थी, जिससे साइबर अपराधियों को उनके वित्तीय ऐप और व्यक्तिगत डेटा तक पहुँच मिल गई थी।

जवाब में, दूरसंचार विभाग ने तत्काल एक सलाह जारी की, जिसमें उपयोगकर्ताओं को अज्ञात स्रोतों से फ़ोटो/इमेज फ़ाइलें डाउनलोड न करने की चेतावनी दी गई। साइबर सुरक्षा विशेषज्ञों ने तब से इस रणनीति को " पारंपरिक फ़िशिंग से भी ज़्यादा ख़तरनाक " करार दिया है, क्योंकि यह गुप्त रूप से किया जाता है और इसमें स्पष्ट लाल झंडों की कमी होती है।

3. इस माह के टिप

ए) डिजिटल गिरफ्तारी से खुद को कैसे बचाएं:

जानकारी को सत्यापित करें : कभी भी किसी के साथ फोन या ऑनलाइन व्यक्तिगत जानकारी या वित्तीय विवरण साझा न करें, जब तक कि

आप उनकी पहचान और उनके अनुरोध की वैधता के बारे में पूरी तरह आश्वस्त न हों।

अपरिचित नंबरों से सावधान रहें : अज्ञात नंबरों से आने वाली कॉल का उत्तर देने से बचें, विशेषकर उन नंबरों से जिनका क्षेत्र कोड विदेशी हो।

जानकारी की दोबारा जांच करें: यदि आपको कोई संदिग्ध कॉल या संदेश प्राप्त होता है, तो उस जानकारी को किसी विश्वसनीय स्रोत, जैसे कि किसी सरकारी वेबसाइट या किसी ज्ञात कानून प्रवर्तन एजेंसी से सत्यापित करने का प्रयास करें।

शांत रहें : घोटालेबाज अक्सर अपने शिकार को गुमराह करने के लिए डर और धमकी का सहारा लेते हैं। शांत रहें और बिना सोचे-समझे निर्णय लेने से बचें।

घोटाले की रिपोर्ट करें : अगर आपको लगता है कि आप डिजिटल गिरफ्तारी ठगी का शिकार हुए हैं, तो स्थानीय पुलिस या साइबर अपराध अधिकारियों को इसकी रिपोर्ट करें। आप अपने इंटरनेट सेवा प्रदाता या मोबाइल वाहक को भी इसकी रिपोर्ट कर सकते हैं।

बी) लॉटरी ठगी से खुद को कैसे बचाएं:

इस प्रकार के ठगी में, प्रेषक एक बड़ी राशि के हस्तांतरण को सुगम बनाने में सहायता का अनुरोध करता है, आमतौर पर ईमेल के माध्यम से। बदले में, प्रेषक एक कमीशन का वादा करता है, जो आमतौर पर कई मिलियन डॉलर की राशि होती है। फिर स्कैमर प्राप्तकर्ता से हस्तांतरण से जुड़ी लागतों, जैसे प्रसंस्करण शुल्क या करों को कवर करने के लिए पैसे भेजने के लिए कहते हैं। यदि पैसा भेज दिया जाता है, तो स्कैमर या तो तुरंत गायब हो जाते हैं या हस्तांतरण के साथ चल रही समस्याओं का हवाला देते हुए अतिरिक्त धनराशि का अनुरोध करना जारी रखते हैं।

लॉटरी स्कैम से सुरक्षा

➢ कभी भी जवाब न दें, संदेशों की उपेक्षा करें या कॉल को अनदेखा करना जाल में फंसने से बचने के लिए यह एक स्मार्ट कदम है।

➢ इस बारे में शोध करने के लिए समय निकालें और प्रस्ताव लेकर आने वाले किसी भी व्यक्ति से गहन प्रश्न पूछें।

➢ कभी भी संवेदनशील व्यक्तिगत जानकारी साझा न करें क्योंकि स्कैमर्स अक्सर ऐसी जानकारी मांगते हैं। सावधान रहें, क्योंकि प्रतिष्ठित संगठन ऐसे डेटा नहीं मांगते हैं।

➢ किसी भी अप्रत्याशित लाभ को संदेह के साथ लेना आवश्यक है, क्योंकि वास्तविक लॉटरी जीत के लिए आमतौर पर भागीदारी की आवश्यकता होती है।

➢ कथित जीत का दावा करने के लिए किसी भी शुल्क का भुगतान करने से बचें; वैध लॉटरी में अग्रिम धन की मांग नहीं की जाती है।

➢ स्कैमरों द्वारा भुगतान की तत्काल मांग से सावधान रहें; वे प्रायः पीड़ितों पर शीघ्र कार्रवाई करने का दबाव डालते हैं, तथा उनकी तात्कालिकता का फायदा उठाने का प्रयास करते हैं।

सी) फ़िशिंग ईमेल के लिए विंडोज़ सैंडबॉक्स उपयोग संबंधी दिशानिर्देश:

1. विंडोज सैंडबॉक्स चालू करें (यदि पहले से चालू नहीं है)

➢ कंट्रोल पैनल पर जाएं > प्रोग्राम्स > विंडोज़ सुविधाएं चालू या बंद करें।
➢ विंडोज़ सैंडबॉक्स की जाँच करें।
➢ ओके (OK) पर क्लिक करें, फिर अपने पीसी/सिस्टम को पुनः प्रारंभ करें।

⚠ **विंडोज 10/11 प्रो, एंटरप्राइज या जानकारी / शिक्षा की आवश्यकता है.**

2. जांच के लिए फ़िशिंग ईमेल आर्टिफ़ैक्ट्स तैयार करें।

➢ अपने मुख्य सिस्टम पर लिंक या अनुलग्नक न खोलें। संदिग्ध अनुलग्नकों (जैसे, .docx, .exe, .pdf, आदि) को बिना क्लिक किए सहेजें/सेव या URL कॉपी करें।
➢ इन फ़ाइलों को किसी सुरक्षित स्थान पर संग्रहीत करें (जैसे, अपने डेस्कटॉप पर एक समर्पित फ़ोल्डर)।

3. विंडोज सैंडबॉक्स लॉन्च करें

➢ स्टार्ट दबाएं और विंडोज सैंडबॉक्स खोजें।
➢ इसे लॉन्च करें - एक साफ, पृथक विंडोज वातावरण खुल जाएगा।

4. फ़ाइल या लिंक को सैंडबॉक्स में स्थानांतरित करें

➢ अपने होस्ट ऑपरेटिंग सिस्टम से संदिग्ध फ़ाइल/लिंक को कॉपी करें.
➢ इसे सैंडबॉक्स वातावरण के अंदर चिपकाएँ.

5. संदिग्ध सामग्री खोलें और उसका विश्लेषण करें

➢ केवल सैंडबॉक्स के अंदर ही अनुलग्नक खोलें या संदिग्ध लिंक पर क्लिक करें।
➢ व्यवहार का अवलोकन करें:
- क्या यह सॉफ्टवेयर स्थापित करने का प्रयास करता है?
- क्या यह किसी संदिग्ध साइट पर पुनर्निर्देशित करता है?
- क्या प्रमाण-पत्र हेतु कोई अनुरोध है?

◉ व्यक्तिगत जानकारी या वास्तविक क्रेडेंशियल दर्ज न करें ।

6. सैंडबॉक्स सत्र को त्यागें/डिस्कार्ड करें

➢ जब आपका काम पूरा हो जाए तो सैंडबॉक्स विंडो को बंद कर दें ।
➢ सभी सामग्री और परिवर्तन स्थायी रूप से हटा दिए जाएंगे ।

☑ यह किसी भी मैलवेयर या फ़िशिंग प्रयास को सुनिश्चित करता है आपके होस्ट सिस्टम को प्रभावित नहीं कर सकता.

7. फ़िशिंग ईमेल की रिपोर्ट करें और उसे हटाएँ

➢ ई-मेल की रिपोर्ट ISERT निदेशालय या ई-मेल प्रदाता को करें।
➢ अपने इनबॉक्स और ट्रैश से मूल फ़िशिंग ईमेल को हटाएँ।

अतिरिक्त सुझाव

➢ अपने ऑपरेटिंग सिस्टम और एंटीवायरस को अपडेट रखें।
➢ ईमेल फ़िल्टर और स्पैम सुरक्षा का उपयोग करें।
➢ सैंडबॉक्स में भी, अज्ञात प्रेषकों से प्राप्त ईमेल से बातचीत करने से बचें।

खातों की सुरक्षा के लिए बहु-कारक प्रमाणीकरण (MFA) का उपयोग करें।

राजभाषा विभाग स्वर्ण जयंती समारोह

कैरियर परामर्श सत्र

अंतर्राष्ट्रीय योग दिवस 2025

30 वां स्थापना दिवस समारोह कावा

रजत पदक विजेता एल. निरुपमा देवी, सहा0कमा0
(बर्मिंघम में विश्व पुलिस एवं अग्निशमन खेल)

महानिरीक्षक संचार एवं सूचना प्रौधगिकी निदेशालय द्वारा डेटा सेंटर का निरीक्षण