केंद्रीय रिज़र्व पुलिस बल

मई, 2025

साइबर बाइट

महाकुंभ के दौरान 60 लाख से अधिक साइबर अथवा संदिग्ध हमले हुए

पाक स्थित हैकर्स ने आर्मी पब्लिक स्कूलों और अन्य भारतीय साइटों को निशाना बनाया

कर्नाटक में साइबर धोखाधड़ी में दंपत्ति ने 50 लाख रुपये गंवाए, आत्महत्या कर ली

संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ

1.साइबर गीक्स समाचार

ए) महाकुंभ के दौरान 60 लाख से अधिक साइबर अथवा संदिग्ध हमले

साइबर हमलों का उद्देश्य 45 दिनों तक चलने वाले महाकुंभ के सुचारू संचालन के लिए तैनात तकनीकी बुनियादी ढांचे को बाधित करना था। कुंभ के दौरान 100 से अधिक संदिग्ध साइबर हमलों को खाकी वर्दीधारी लोगों की एक समर्पित टीम ने नाकाम कर दिया, जो ऐसे हमलों पर कड़ी नज़र रखते थे, जिनमें से अधिकांश विदेशी आईपी पते से तैयार किए गए थे। पुलिस के अनुसार, ये हमले रैनसमवेयर, डीएनएस पॉइज़निंग, डीडीओएस हमले, हैकिंग, एसक्यूएल इंजेक्शन, स्पूफिंग, ब्रूट फोर्स, वेब ऐप हमले, ट्रोजन जैसे विशिष्ट पोर्ट पर कई कनेक्शन प्रयास, मैलवेयर और दुर्भावनापूर्ण आईपी से भारी ट्रैफ़िक आदि से संबंधित थे।

हालाँकि, केंद्रीय एजेंसियों द्वारा समय पर अलर्ट और विभिन्न सिस्टम इंटीग्रेटर्स के समन्वय में राज्य पुलिस द्वारा त्वरित कार्रवाई के कारण इन सभी हमलों को विफल कर दिया गया।

अपर महानिदेशक (प्रयागराज जोन) के अनुसार " महाकुंभ के दौरान 60 लाख से अधिक संदिग्ध साइबर हमले हुए। कुंभ अवधि और इन आईपी का पता 25 से अधिक देशों में लगाया गया। डिजिटल महाकुंभ के डिजिटल बुनियादी ढांचे की साइबर सुरक्षा सुनिश्चित करके महाकुंभ 2025 को संरक्षित किया गया ।"

बी) पाक स्थित हैकर्स ने आर्मी पब्लिक स्कूलों और अन्य भारतीय साइटों को निशाना बनाया

पाक आधारित लक्ष्यों में आर्मी पब्लिक स्कूल (एपीएस) श्रीनगर, एपीएस रानीखेत , आर्मी वेलफेयर हाउसिंग ऑर्गनाइजेशन (एडब्ल्यूएचओ) डेटाबेस और भारतीय वायु सेना प्लेसमेंट संगठन पोर्टल शामिल थे।

पहलगाम में हुए आतंकी हमले के बाद से पाकिस्तान स्थित साइबर हमलावरों द्वारा भारतीय वेबसाइटों को हैक करने के प्रयास बढ़ गए हैं। इन साइटों में आर्मी पब्लिक स्कूल (APS) श्रीनगर, APS रानीखेत , आर्मी वेलफेयर हाउसिंग ऑर्गनाइजेशन (AWHO) डेटाबेस और भारतीय वायु सेना प्लेसमेंट संगठन पोर्टल शामिल थे। " IOK हैकर" के रूप में काम करने वाले हैकर्स ने इन वेबसाइटों को ख़राब करने का प्रयास किया।

इन हमलों में पृष्ठों को विकृत करने, एपीएस श्रीनगर पर सेवा से वंचित करने के हमले के साथ सेवाओं को बाधित करने और व्यक्तिगत जानकारी तक पहुंच बनाने के प्रयास शामिल थे।

वेबसाइट के पन्नों के ठीक बीच में एक पाकिस्तानी झंडा दिखाई दे रहा था, जिस पर लिखा था "साइट हैक हो गई है", उसके बाद कश्मीर के बारे में एक भड़काऊ संदेश था। बीच में एक व्यक्ति गाइ फॉक्स मास्क (जिसे वी फॉर वेंडेटा मास्क या एनोनिमस मास्क के नाम से भी जाना जाता है) पहने हुए दर्शक की ओर उंगली से इशारा करता हुआ बैठा है।

पिछले कुछ दिनों में पाकिस्तान की ओर से कई बार हैकिंग के प्रयास हुए हैं, जिनमें से अधिकतर सशस्त्र बलों से जुड़े स्वायत्त संस्थानों को निशाना बनाया गया है।

2. साइबर अपराध

ए) कर्नाटक में साइबर धोखाधड़ी में दंपत्ति ने 50 लाख रुपये गंवाए, आत्महत्या की

खानपुर तालुक में एक बुजुर्ग दंपत्ति ने साइबर धोखाधड़ी और कथित उत्पीड़न का शिकार होने के बाद आत्महत्या कर ली, खानपुर के बीड़ी गांव के निवासी , पीड़ित ने दो पन्नों का हस्तलिखित मृत्यु नोट छोड़ा।

पीड़िता ने दो व्यक्तियों का नाम लिया- सुमित बिर्रा और अनिल यादव। उन्होंने लिखा कि बिर्रा ने खुद को नई दिल्ली का दूरसंचार विभाग का अधिकारी बताते हुए उन्हें बताया कि उनके नाम पर धोखाधड़ी से एक सिम कार्ड खरीदा गया है और उसका इस्तेमाल उत्पीड़न और अवैध विज्ञापनों के लिए किया जा रहा है। बाद में बिर्रा ने कॉल को यादव को ट्रांसफर कर दिया, जिन्होंने दावा किया कि वह क्राइम ब्रांच से हैं । यादव ने पीड़ित की संपत्ति

और वित्त का विवरण मांगा, कथित सिम कार्ड के दुरुपयोग पर कानूनी परिणाम भुगतने की धमकी दी।

घोटाले का शिकार होकर, पीड़ित ने उन्हें 50 लाख रुपये से अधिक हस्तांतरित कर दिए, लेकिन वे और अधिक मांग करते रहे, पीड़ित ने आगे कहा कि उसने दोस्तों से पैसे उधार लिए थे और अनुरोध किया कि वह अपनी पत्नी की सोने की चूड़ियाँ
और बालियाँ बेचकर ऋण चुकाए।

बी) ओडिशा के विधायक और पूर्व सूचना प्रौद्योगिकी मंत्री को साइबर धोखाधड़ी में 1.4 करोड़ रुपये का नुकसान हुआ है

ओडिशा के एक विधायक और पूर्व सूचना प्रौद्योगिकी मंत्री ने करीब डेढ़ महीने में साइबर धोखाधड़ी में 1.4 करोड़ रुपये गंवा दिए हैं। एक वरिष्ठ पुलिस अधिकारी ने सोमवार को यह जानकारी दी।

पुलिस ने इस मामले के सिलसिले में सात लोगों को गिरफ्तार किया है - जिनमें से चार कर्नाटक से और तीन तमिलनाडु से हैं। पूर्व मंत्री ने हालांकि इस संबंध में जनवरी में पुलिस में शिकायत दर्ज कराई थी, लेकिन दावा किया कि उनका एक मित्र उनके ट्रेडिंग खाते का इस्तेमाल कर रहा था और उसने पैसे गंवा दिए।

पूर्व मंत्री ने बताया कि आरोपी और उनके सहयोगी खुद को व्यापार विश्लेषक बताते थे और लोगों को उच्च रिटर्न का वादा करके आरंभिक सार्वजनिक निर्गम (आईपीओ), शेयर और अन्य प्रकार के व्यापार में पैसा लगाने के लिए राजी करते थे। जांच के दौरान, अपराध शाखा की साइबर अपराध इकाई ने पाया कि आरोपियों ने धोखाधड़ी करके शिकायतकर्ता से 1.40 करोड़ रुपये प्राप्त किए।

3. इस माह के टिप

ए) निवेश घोटाला

निवेश घोटाला धोखाधड़ी वाली योजनाओं से जुड़ा होता है जो उच्च रिटर्न का वादा करती हैं, जो अक्सर सच होने से
बहुत ज़्यादा अच्छा होता है। ये घोटाले वैध आर्थिक गतिविधि के माध्यम से लाभ कमाने के बजाय नए निवेशकों के पैसे से पहले के निवेशकों को भुगतान करते हैं। इसे पोंजी स्कीम के नाम से भी जाना जाता है।

करें

- पंजीकृत संस्थाओं के साथ निवेश करें: निवेश के लिए केवल सेबी -पंजीकृत मध्यस्थों के साथ ही लेन-देन करें।
- निवेश उत्पादों को सत्यापित करें: हमेशा विनियमित वित्तीय संस्थाओं के माध्यम से निवेश करें।
- सचेत रहें: विनियमित संस्थाओं और वित्तीय उत्पादों के विश्वसनीय सूचना स्रोतों का अनुसरण करें।
- संदिग्ध गतिविधि की रिपोर्ट करें: 1930 पर कॉल करें या cybercrime.gov.in पर कॉल करें

ना करें

- घबराएं नहीं: शांत रहें और ऑफर की पुष्टि करें।
- अविश्वसनीय रिटर्न पर भरोसा न करें: बिना जोखिम के उच्च रिटर्न का वादा करने वाली योजनाओं से बचें।
- संदिग्ध समूहों में शामिल न हों: संदिग्ध ट्रेडिंग ऐप्स को बढ़ावा देने वाले सोशल मीडिया समूहों से दूर रहें।
- लाल झंडों को नज़रअंदाज़ न करें: अगर रिटर्न समय के साथ बहुत ज़्यादा या बहुत ज़्यादा लग रहा है, तो सावधान रहें।

बी) ऑनलाइन गेमिंग

ऑनलाइन गेमिंग साइबर अपराधियों के लिए एक आकर्षण का केंद्र बन गया है, जिसमें वर्चुअल चोरी और अकाउंट सेंधमारी से लेकर वास्तविक दुनिया में वित्तीय धोखाधड़ी और पहचान की चोरी तक के खतरे हैं। हमलावर प्लेटफ़ॉर्म की कमियों का फ़ायदा उठाते हैं और फ़िशिंग स्कैम, मैलवेयर और सोशल इंजीनियरिंग के ज़रिए खिलाड़ियों को निशाना बनाते हैं।

करें

- एक्सेस की निगरानी करें: यदि आप अभिभावक हैं, तो पर्यवेक्षण के तहत ऑनलाइन गेम तक पहुँच प्रदान करें।
- असली पैसे वाले ऐप्स से सावधान रहें: कई असली पैसे वाले गेमिंग ऐप्स धोखाधड़ी वाले हो सकते हैं। सावधान रहें और संदिग्ध लगने वाले ऐप्स से बचें।
- विवेकपूर्ण ऐप अनुमतियाँ: ऐप को संपर्क, संग्रहण और स्थान जैसी अनुमतियाँ देने से पहले सावधान रहें।
- व्यक्तिगत जानकारी सुरक्षित रखें: अपनी संवेदनशील व्यक्तिगत जानकारी, जैसे आपका पूरा नाम, पता, या बैंक खाता विवरण आदि सुरक्षित रखें।

ना करें

- संदिग्ध स्रोतों से बचें: अविश्वसनीय स्रोतों से गेमिंग ऐप्स डाउनलोड न करें।
- सुनिश्चित रिटर्न से सावधान रहें: ऐसे गेमिंग ऐप्स इंस्टॉल न करें जो सोशल मीडिया पर या विज्ञापनों के माध्यम से सुनिश्चित रिटर्न का वादा करते हैं।
- जानकारी निजी रखें: अज्ञात साथी खिलाड़ियों के साथ गोपनीय जानकारी साझा न करें।
- सोशल मीडिया पर शेयरिंग सीमित करें: उत्पीड़न या साइबर हमलों का लक्ष्य बनने से बचने के लिए अपनी गेमिंग उपलब्धियों को सोशल मीडिया पर अधिक शेयर करने से बचें

सी) सर्च इंजन धोखाधड़ी

सर्च इंजन धोखाधड़ी तब होती है जब धोखेबाज खोज परिणामों में हेरफेर करके नकली संपर्क जानकारी प्रदर्शित करते हैं, जो वैध संस्थाओं के रूप में प्रस्तुत की जाती है। अनजाने में इन नंबरों पर कॉल करने वाले पीड़ित पासवर्ड और खाते के विवरण जैसी संवेदनशील जानकारी प्रकट कर सकते हैं, जिससे वित्तीय नुकसान, पहचान की चोरी और अन्य गंभीर परिणाम हो सकते हैं।

करें

- आधिकारिक वेबसाइट पर जाएं: खोज परिणामों पर निर्भर रहने के बजाय, संपर्क विवरण के लिए हमेशा आधिकारिक वेबसाइट देखें।
- संपर्कों को सत्यापित करें: व्यक्तिगत जानकारी साझा करने से पहले कॉलर आईडी या विश्वसनीय निर्देशिकाओं का उपयोग करके फ़ोन नंबर और वेबसाइट की दोबारा जांच करें।
- लाल झंडों पर नज़र रखें: जल्दबाजी, डराने वाली रणनीति या संदिग्ध ऑफ़र से सावधान रहें। वैध कंपनियाँ तुरंत कार्रवाई करने पर ज़ोर नहीं देतीं।

ना करें

- खोज परिणामों पर भरोसा न करें: खोज इंजन परिणामों में सूचीबद्ध नंबरों पर कभी कॉल न करें; धोखेबाज अक्सर खुद को अवैध इकाई के रूप में छिपाते हैं।
- बिना किसी संकेत के जानकारी साझा न करें: फ़ोन पर व्यक्तिगत विवरण केवल तभी साझा करें जब संपर्क आपने शुरू किया हो

श्री आकाश गर्ग और उनके माता-पिता को महानिदेशक सीआरपीएफ द्वारा सम्मानित किया गया

आईजी संचार विदाई समारोह

भूतपूर्व द्वितीय कमान अधिकारी श्री मुंशी राम को महानिदेशक सीआरपीएफ द्वारा सम्मानित किया गया

भौतिकी वल्लाह फाउंडेशन और सीआरपीएफ परिवार कल्याण संघ एमओयू हस्ताक्षर समारोह

,