केंद्रीय रिज़र्व पुलिस बल

अप्रैल, 2025

साइबर बाइट

गृह मंत्रालय की I4सी ने तीर्थयात्रियों और पर्यटकों को निशाना बनाकर की जाने वाली ऑनलाइन बुकिंग धोखाधड़ी पर अलर्ट जारी किया

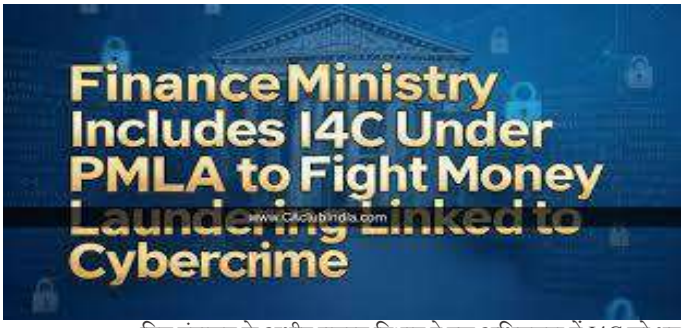
कश्मीरी इंजीनियरिंग छात्र से ₹ 4.30 लाख की ऑनलाइन ठगी

हैदराबाद साइबर अपराध पुलिस ने साइबर धोखाधड़ी के लिए वैवाहिक साइट Shaadi.com बुक किया

1. साइबर गीक्स समाचार

ए. सरकार पीएमएलए के तहत साइबर अपराध केंद्र I4C को ला रही है: -

सरकार ने भारतीय साइबर अपराध समन्वय केंद्र (I4C) को धन शोधन निरोधक कानून के तहत प्रवर्तन निदेशालय से सूचना प्राप्त करने और साझा करने के लिए अधिकृत किया है। इस कदम का उद्देश्य धन के लेन-देन का पता लगाना और साइबर धोखाधड़ी से निपटना है।



वित्त मंत्रालय के अधीन राजस्व विभाग ने एक अधिसूचना में I4C को धन शोधन निवारण अधिनियम की धारा 66 के अंतर्गत शामिल किया है। इससे **I4C को प्रवर्तन निदेशालय और अन्य कानून प्रवर्तन एजेंसियों से सूचना साझा करने और प्राप्त करने में मदद मिलेगी।**

आम आदमी को निशाना बनाकर की जाने वाली साइबर धोखाधड़ी की बढ़ती घटनाओं के बीच, इस सूचना के आदान-प्रदान से ऐसी धोखाधड़ी के पीछे के मास्टरमाइंडों की पहचान करने में मदद मिलेगी, जो ज्यादातर अंतरराष्ट्रीय हैं।

बी. गृह मंत्रालय की I4C ने तीर्थयात्रियों और पर्यटकों को निशाना बनाकर की जाने वाली ऑनलाइन बुकिंग धोखाधड़ी पर अलर्ट जारी किया: -

केंद्रीय गृह मंत्रालय (एमएचए) की साइबर सुरक्षा शाखा I4C ने शनिवार को देश भर में अलर्ट जारी कर लोगों को ऑनलाइन बुकिंग धोखाधड़ी में तेजी से हो रही वृद्धि के बारे में आगाह किया है। इसके शिकार ज्यादातर **धार्मिक तीर्थयात्री** और **अनजान पर्यटक** होते हैं।

भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने अलर्ट में कहा कि साइबर धोखाधड़ी **फर्जी वेबसाइटों, सोशल मीडिया पेजों, व्हाट्सएप अकाउंटों और यहां तक कि गूगल और फेसबुक जैसे प्रमुख प्लेटफार्मों पर प्रायोजित विज्ञापनों के जरिए की जाती है।**

I4C ने ऑनलाइन बुकिंग धोखाधड़ी के बारे में लोगों को **खास तौर पर देश भर में धार्मिक तीर्थयात्रियों और पर्यटकों को निशाना बनाने वालों के बारे में** सचेत किया है, ये धोखाधड़ी फर्जी वेबसाइट, भ्रामक सोशल मीडिया पेज, फेसबुक पोस्ट और गूगल जैसे सर्च इंजन पर पेड(सशुल्क) विज्ञापनों के जरिए की जा रही है।

I4C के अनुसार, ये घोटाले आमतौर पर पीड़ितों को **केदारनाथ और चार धाम यात्रा के लिए हेलीकॉप्टर बुकिंग, गेस्ट हाउस और होटल आवास, ऑनलाइन कैब या टैक्सी सेवाओं और धार्मिक पर्यटन पैकेज** जैसे प्रस्तावों के साथ लुभाते हैं।

2. साइबर धोखाधड़ी

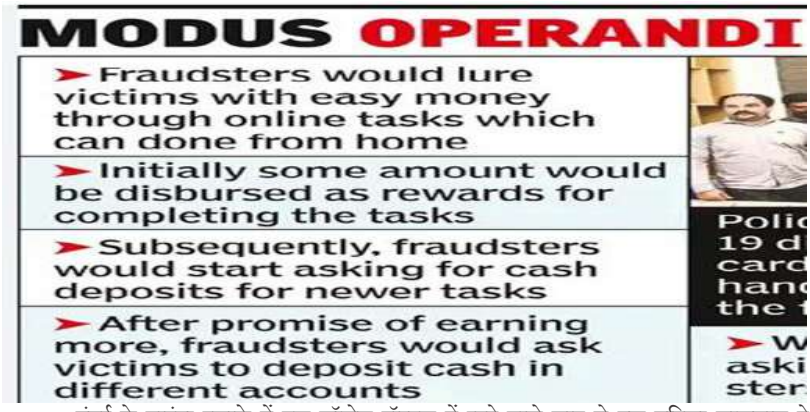
(ए) हैदराबाद साइबर अपराध पुलिस ने साइबर धोखाधड़ी के लिए वैवाहिक साइट Shaadi.com बुक किया: -

हैदराबाद साइबर अपराध पुलिस ने वैवाहिक मंच शादी डॉट कॉम से जुड़े साइबर धोखाधड़ी के एक गंभीर मामले का पर्दाफाश किया है, जहां एक फर्जी प्रोफाइल का इस्तेमाल कर शहर की एक महिला डॉक्टर से 11 लाख रुपये की ठगी की गई, साथ ही जबरन वसूली और ब्लैकमेल की धमकी भी दी गई।

हाल ही में गिरफ्तार किए गए संदिग्ध ने एक अलग नाम से फर्जी प्रोफाइल बनाई थी और पीड़िता से संपर्क करने के लिए प्लेटफॉर्म की प्रीमियम सेवा का फायदा उठाया और शादी का वादा किया। साइबर क्राइम के एक अधिकारी ने कहा, "वित्तीय संकट का दावा करते हुए, उसने पीड़िता को बड़ी राशि ट्रांसफर करने के लिए प्रेरित किया और बाद में उसे व्यक्तिगत सामग्री का इस्तेमाल करने की धमकी दी और ब्लैकमेल किया।"

(बी) कश्मीरी इंजीनियरिंग छात्र से ₹ 4.30 लाख की ऑनलाइन ठगी:-

माटुंगा पुलिस थाने के अधिकारियों ने बताया कि जम्मू-कश्मीर का 20 वर्षीय इंजीनियरिंग छात्र साइबर धोखाधड़ी का शिकार हो गया और "टास्क फ्रॉड" घोटाले में 4.30 लाख रुपये गंवा दिए।



मुंबई के माटुंगा इलाके में एक कॉलेज हॉस्टल में रहने वाले छात्र से एक महिला जालसाज ने **व्हाट्सएप के जरिए संपर्क किया था।** उसने छात्र को ऑनलाइन रिव्यू पोस्ट करके प्रतिदिन 2,000 से 8,000 रुपये कमाने का पार्ट-टाइम काम देने की पेशकश की थी।

शुरुआत में जल्दी कमाई के लालच में आकर छात्र ने इसमें भाग लेने के लिए सहमति दे दी। पीटीआई की रिपोर्ट के अनुसार, फिर उसे एक टेलीग्राम चैनल से जोड़ा गया , जहाँ उसे छोटे-छोटे काम दिए गए और कुछ शुरुआती भुगतान भी किए गए , जिससे उसे आगे बढ़ने का प्रोत्साहन मिला। जैसे-जैसे काम आगे बढ़ा, उसे बड़े कामों के लिए **" सुरक्षा उपाय "** के तौर पर राशि जमा करने के लिए कहा गया। समय के साथ, पीड़ित ने कई ट्रांजेक्शन में कुल 4.30 लाख रुपये जमा कर दिए। जब बिना किसी और भुगतान या स्पष्ट स्पष्टीकरण के और राशि की मांग जारी रही, तो छात्र को संदेह हुआ और उसे एहसास हुआ कि उसके साथ धोखाधड़ी हुई है।

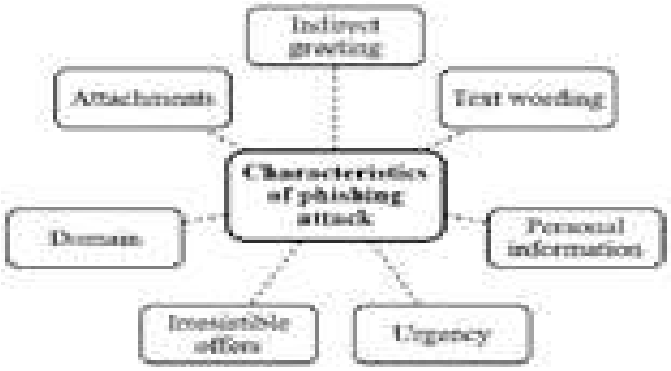
यह मामला भारत में साइबर धोखाधड़ी की बढ़ती घटनाओं में से एक है, जिसमें घोटालेबाज **सोशल मीडिया और मैसेजिंग ऐप का इस्तेमाल करके अनजान व्यक्तियों, खासकर छात्रों और नौकरी चाहने वालों को निशाना बना रहे हैं।** अधिकारियों ने लोगों को सलाह दी है कि वे सतर्क रहें और भाग

लेने से पहले किसी भी ऑनलाइन नौकरी की पेशकश या वित्तीय योजनाओं की पुष्टि करें।

3. इस माह के टिप

1) फ़िशिंग मेल के संबंध में :-

यह देखा गया है कि साइबर खतरों, विशेष रूप से एनआईसी ईमेल खातों के माध्यम से किए जाने वाले फ़िशिंग हमलों में कश्मीर में हाल की स्थिति के बाद उल्लेखनीय वृद्धि देखी गई है।



ये हमलावर अक्सर भ्रामक ईमेल भेजते हैं जो वैध लगते हैं, संवेदनशील जानकारी निकालने, मैलवेयर इंस्टॉल करने या आधिकारिक सिस्टम तक अनधिकृत पहुँच प्राप्त करने का प्रयास करते हैं। सभी उपयोगकर्ताओं को सलाह दी जाती है कि यदि इस प्रकार का फ़िशिंग मेल प्राप्त होता है तो नीचे दिए गए उपायों का पालन करें:-

फ़िशिंग डोमेन का शिकार बनने से बचने के लिए:

1. अवांछित ई-मेल या संदेशों से सावधान रहें: वैध संस्थाएं/संगठन कभी भी ई-मेल या संदेश के माध्यम से संवेदनशील जानकारी नहीं मांगते हैं।

2. डोमेन नाम सत्यापित करें: URL को ध्यानपूर्वक जांचें, डोमेन नाम में गलत वर्तनी, अतिरिक्त वर्ण या भिन्नता की जांच करें।

3. व्याकरणिक त्रुटियों और वर्तनी पर ध्यान दें : वैध वेबसाइटों में आमतौर पर पेशेवर सामग्री होती है।

4. तत्काल या धमकी भरे संदेशों से सावधान रहें: फ़िशिंग डोमेन अक्सर खतरे की भावना पैदा करने की कोशिश करते हैं। उपयोगकर्ताओं को त्वरित कार्रवाई करने के लिए प्रेरित करते हैं।

5. HTTPS और वैध SSL प्रमाणपत्र की जाँच करें: वैध वेबसाइटों में आमतौर पर वैध SSL प्रमाण पत्र होता है तथा वे HTTPS का उपयोग करें.

फ़िशिंग डोमेन से बचाव के लिए:

1. मजबूत एवं अद्वितीय पासवर्ड का उपयोग करें: एक ही पासवर्ड को कई साइटों पर उपयोग करने से बचें।

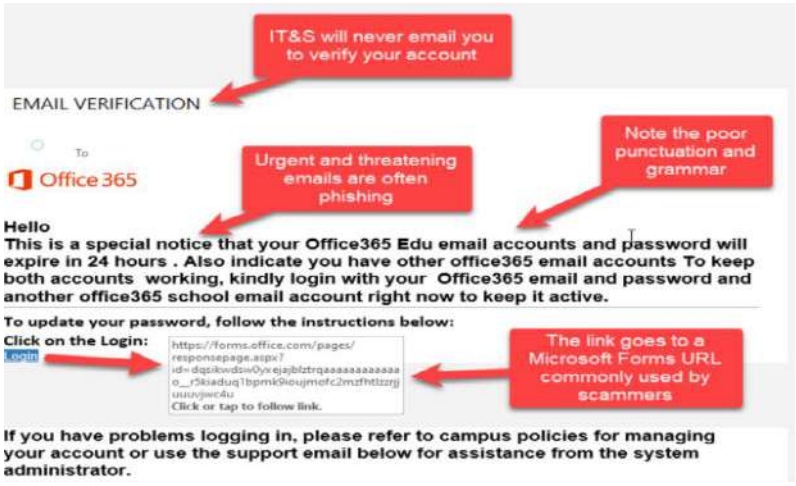
2. दो-कारक प्रमाणीकरण (2FA) सक्षम करें: 2FA सुरक्षा की एक अतिरिक्त परत जोड़ता है ताकि अनधिकृत पहुंच से बचा जा सके।

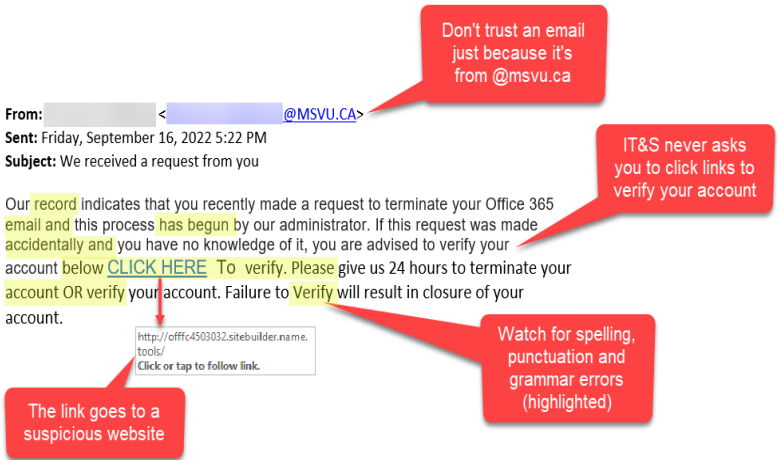
3. अपने सॉफ्टवेयर और ऑपरेटिंग सिस्टम को अद्यतन रखें: सुनिश्चित करें कि आपके पास नवीनतम सुरक्षा पैच और अपडेट हैं।

4. एंटी-वायरस सॉफ़्टवेयर और फ़ायरवॉल का उपयोग करें: अपने डिवाइस को मैलवेयर और अनधिकृत पहुंच / एक्सेस से सुरक्षित रखें।

उपरोक्त उपायों का पालन करके, आप अपने सिस्टम को प्रभावी ढंग से सुग्राही कर सकते हैं और फ़िशिंग मेल पर क्लिक करने से जुड़े संभावित जोखिमों से बच सकते हैं।

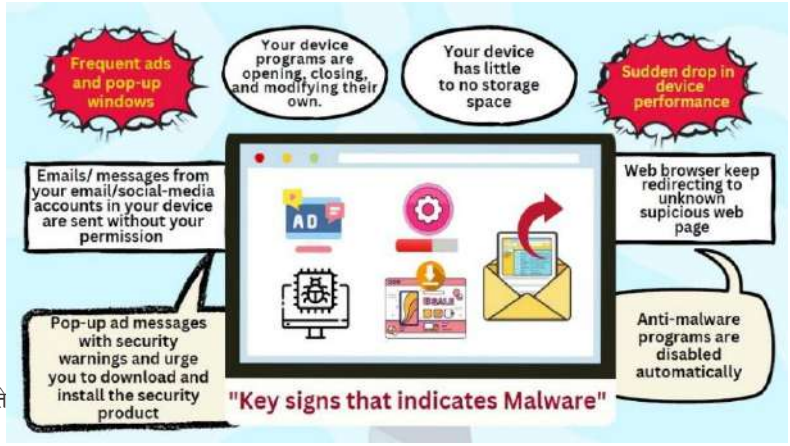
नकली ई-मेल की विशेषताओं को पहचानने के कुछ तरीके:





2) मैलवेयर के मुख्य संकेत और सुरक्षात्मक उपाय: -

अज्ञात स्रोत से आने वाले संदिग्ध ईमेल, लिंक और साइटों पर क्लिक करने से बचें। जैसे ही आप किसी संदिग्ध लिंक पर क्लिक करते हैं तो आपका मोबाइल हैक हो सकता है या आपका डेटा चोरी हो सकता है।



केवल सुरक्षित एवं अधिकृत वेबसाइट को ही ब्राउज़ करें।

- अपने कंप्यूटर सॉफ्टवेयर/ब्राउज़र को सदैव अद्यतन रखें।
- अपने डेटा का नियमित रूप से बैकअप बनाए रखें।
- वेबसाइटों पर प्रदर्शित होने वाले संदिग्ध विज्ञापनों को रोकने के लिए पॉप-अप/एड-ब्लॉकर जैसे सॉफ़्टवेयर इंस्टॉल करें।
- अपने डिवाइस में एंटीवायरस और एंटीमैलवेयर समाधान स्थापित करें और उन्हें अद्यतन रखें।
- वास्तविक लिंक खोजने के लिए छवियों/लिंकों पर माउस घुमाएं।
- चैट या सोशल मीडिया पोस्ट पर प्राप्त लिंक के माध्यम से कोई भी ऐप इंस्टॉल न करें.

3). रैनसमवेयर अपराधी अब अधिकारियों के बच्चों के सिम स्वैप करके उनके माता-पिता पर दबाव बना रहे हैं: -

मैंडिएंट (एक साइबर सुरक्षा कंपनी, जो अब गूगल की सहायक कंपनी है) के अनुसार आरएसएसी रैनसमवेयर संक्रमण "पीड़ित संस्था के खिलाफ एक मनोवैज्ञानिक हमले" में बदल गया है, क्योंकि अपराधी पीड़ितों को भुगतान करने के लिए मजबूर करने के लिए तेजी से व्यक्तिगत और आक्रामक रणनीति का उपयोग करते हैं।

हमने ऐसी परिस्थितियाँ देखी हैं जहाँ धमकी देने वाले लोग अधिकारियों के बच्चों के फोन का सिम स्वैप करते हैं, और उनके बच्चों के फोन नंबर से अधिकारियों को फोन कॉल करना शुरू कर देते हैं। मनोवैज्ञानिक दुविधा जिससे अधिकारी गुजरता है - बच्चों से फोन कॉल देखकर, फोन उठाकर यह सुनना कि यह किसी और की आवाज़ है?

कभी-कभी, यह कॉलर आईडी स्पूफिंग होती है। दूसरी बार, हम परिवार के सदस्यों के सिम स्वैपिंग का प्रदर्शन देखते हैं।" किसी भी तरह से, यह भयावह है। बच्चों से फोन कॉल देखना, फोन उठाना, और सुनना कि यह किसी और की आवाज़ है।

सुझाव:-

- सिम कार्ड लॉक इनेबल करें।
- मजबूत एवं विशिष्ट पासवर्ड का प्रयोग करें।
- मल्टी फैक्टर ऑथैंटिकेशन (MFA) लागू करें।
- एक्जीक्यूटिव्स और उनके परिवारों को शिक्षित करें।
- सुरक्षा सेटिंग्स की नियमित समीक्षा करें और उन्हें अद्यतन करें।
- संदिग्ध गतिविधि के लिए खातों की निगरानी करें।
- व्यक्तिगत जानकारी का प्रकटीकरण सीमित करें।
- अद्यतन सॉफ़्टवेयर से डिवाइस को सुरक्षित रखें।
- संचार प्रोटोकॉल स्थापित करें।
- संदिग्ध गतिविधि की **रिपोर्ट** करें।

वीरता दिवस पदक समारोह 2025

जीसी, नीमच में सांस्कृतिक कार्यक्रम में डीजी सीआरपीएफ

गांधीनगर में 72वीं अखिल भारतीय पुलिस एक्वेटिक्स एवं क्रॉस कंट्री चैम्पियनशिप

86वें सीआरपीएफ दिवस परेड में माननीय गृह मंत्री

86वें सीआरपीएफ दिवस परेड के अवसर पर K9 का प्रदर्शन