सितंबर, 2024

केंद्रीय रिज़र्व पुलिस बल

साइबर बाइट

नया एंड्राइड मैलवेयर एन-गेट

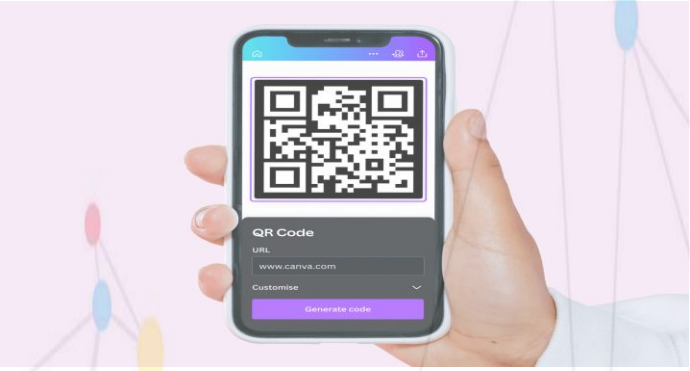
कांटेक्टलेस पेमेंट कार्ड को क्लोन करने के लिए एनएफसी डेटा चुराता है

भारत में अब तक की सबसे बड़ी साइबर धोखाधड़ी

75 वर्षीय व्यक्ति से 13 करोड़ रूपये की ठगी

1.साइबर गीक्स समाचार

क) नया क्यूआर कोड फ़िशिंग अभियान, क्रेडेंशियल्स चुराने के लिए माइक्रोसॉफ्ट स्वे का सहारा लेता है।



एक नया क्यूआर कोड फ़िशिंग अभियान नकली पृष्ठों को होस्ट करने के लिए माइक्रोसॉफ्ट स्वे का उपयोग करता है, पीड़ितों को बरगलाने के लिए इसकी वैधता का फायदा उठाता है। एशिया और उत्तरी अमेरिका में उपयोगकर्ताओं को टारगेट करते हुए, प्रौद्योगिकी, विनिर्माण और वित्त क्षेत्रों पर केंद्रित हैं।

सुझाव:-

- क्यूआर कोड फ़िशिंग हमलों से खुद को बचाने के लिए, ये समझें कि वे कैसे काम करते हैं और कोड स्कैन करते समय अपनी सुरक्षा सुनिश्चित करें।
- स्कैन करने से पहले हमेशा कोड के स्रोत की जांच करें और टाइपिंग की गलतियों, गलत वर्तनियों या संदिग्ध यूआरएल पर नजर रखें।
- विश्वसनीय क्यूआर कोड स्कैनिंग ऐप्स का उपयोग करें और टू स्टेप वेरीफिकेशन करें।
- सुनिश्चित करें कि आपके डिवाइस में एंटीवायरस सॉफ़्टवेयर है।
- जब तक आप आश्वस्त न हों कि वेबसाइट वैध है, तब तक व्यक्तिगत जानकारी कभी साझा न करें।

ख) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Centre) द्वारा साइबर सुरक्षा संबंधी सलाह।

यह देखा गया है कि हमलावर नकली/छिपे हुए ईमेल आईडी, दुर्भावनापूर्ण डोमेन, फ़िशिंग वेब पेज और विशिंग तकनीकों का उपयोग करके सरकारी कर्मियों को निशाना बना रहे हैं।

फ़िशिंग हमलों की कार्यप्रणाली: -

केस 1: स्पीयर-फ़िशिंग ईमेल में एक HTML फ़्रेम होता है जिसमें शीर्षक होता है "keep the same password" और "Skip upto 6 months" क्लिक करने पर, यह एक URL पर रीडायरेक्ट करता है, जो एक फ़िशिंग ईमेल है। फ़ायरफ़ॉक्स और क्रोम ब्राउज़र इस URL को एक खतरनाक साइट के रूप में पहचानते हैं।

केस 2: स्पीयर-फ़िशिंग ईमेल में एक लिंक होता है जो "mod.gov.in" या "ddpdoo.gov.in" की नकल करने वाले क्लोन किए गए पेज पर ले जाता है, जिसमें NIC मेल क्रेडेंशियल के लिए प्रॉम्प्ट होता है। सक्रिय दुर्भावनापूर्ण IP, उपयोगकर्ता का क्रेडेंशियल प्राप्त कर सकता है या मैलवेयर फैला सकता है।

सुझाव:-

- एंटीवायरस सॉफ़्टवेयर इंस्टाल करें और नियमित रूप से अपडेट करें।
- नियमित रूप से अपडेट और पैच इंस्टाल करें।
- नियमित रूप से बैकअप का अभ्यास करें और उन बैकअप को ऑफलाइन या अलग नेटवर्क पर रखें।
- बहु-कारक प्रमाणीकरण (एमएफए) लागू करें।
- अज्ञात स्रोतों से प्राप्त ईमेल अनुलग्नकों पर कभी भी क्लिक न करें और उन्हें निष्पादित न करें।
- सोशल मीडिया पर अज्ञात स्रोतों से साझा किए गए लिंक को कभी न खोलें।
- कभी भी अज्ञात फ़ाइलों को अतिरंजित शीर्षकों के साथ न चलाएँ।

ग) एफबीआई और सीआईएसए ने नए खतरों और रैनसमवेयर को रोकने के तरीके पर संयुक्त सलाह जारी की है।

एफबीआई और सीआईएसए ने संगठनों को रैनसमवेयर से बचाने में मदद करने के लिए अपने चल रहे #Stop Ransomware प्रयास के हिस्से के रूप में एक संयुक्त सलाह जारी की है। नवीनतम सलाह में रैनसमवेयर से साइबर खतरों को कम करने के लिए तीन प्रमुख कार्रवाइयों की रूपरेखा दी गई है: अपडेट जारी होते ही उन्हें इंस्टॉल करना, फ़िशिंग-प्रतिरोधी Multi-Factor Authentication (MFA).एमएफए की आवश्यकता और उपयोगकर्ताओं को प्रशिक्षण देना।

रैंसमवेयर हमलों और डेटा उल्लंघनों के पीड़ितों की संख्या इतनी गहरी हो गई है कि नई साइबर रक्षा चुनौती पीड़ितों के नए हमलों और खुलासों की संख्या के बराबर ही है। यह साइबर-आपराधिक हमले के तरीकों में आश्चर्यजनक प्रगति का परिणाम है, साथ ही कई संगठनों द्वारा नए हमले के तरीकों को समायोजित करने में बहुत धीमी प्रतिक्रिया भी है। जैसा कि अनुमान लगाया गया था, जेनेरेटिव एआई वास्तव में साइबर अपराधियों पर हमला करने वाले संगठनों के लिए गेम चेंजर रहा है और यह साइबर रक्षा रणनीतियों में तत्काल समायोजन को अनिवार्य करता है।

घ) नया एंड्रॉयड मैलवेयर एन - गेट एनएफसी डाटा चुराकर संपर्क रहित भुगतान कार्डों की क्लोनिंग करता है ।

साइबर सुरक्षा शोधकर्ताओं ने एक नए एंड्रॉयड मैलवेयर की खोज की है जो क्रेडिट और डेबिट कार्ड से संपर्क रहित भुगतान डेटा को धोखाधड़ी के लिए हमलावर के डिवाइस पर भेजता है।

एन-गेट मैलवेयर में पीड़ितों के भुगतान कार्ड से डेटा को, उनके एंड्रॉयड डिवाइस पर इंस्टॉल किए गए दुर्भावनापूर्ण ऐप के माध्यम से, हमलावर के रूट किए गए एंड्रॉयड फोन तक पहुंचाने की अद्वितीय क्षमता है। हमलों का अंतिम लक्ष्य एन-गेट का उपयोग करके पीड़ितों के भौतिक भुगतान कार्ड से निकट-क्षेत्र संचार (एनएफसी) डेटा को क्लोन करना और जानकारी को हमलावर डिवाइस तक पहुंचाना है, जो एटीएम से पैसे निकालने के लिए मूल कार्ड का अनुकरण करता है।

सुझाव:-

- अपने कार्डों को आसानी से पहुंच वाली जेबों या बैगों में न रखें, क्योंकि वे जेबकतरों को आकर्षित कर सकते हैं।
- स्कैनिंग उपकरणों को रोकने के लिए अपने बटुए को टिन फॉयल से ढकें, या इसी प्रकार की सुरक्षा के लिए आरएफआईडी अवरोधक वस्तुओं का उपयोग करें।
- भुगतान के समय अपने कार्ड को नज़रों से ओझल न होने दें; इसमें से डेटा चुराया जा सकता है।
- भुगतान के लिए अपना कार्ड मित्रों को न दें; सभी लेन-देन के समय स्वयं उपस्थित रहें।
- यह सुनिश्चित करने के लिए कि आपसे सही राशि ली गई है, रसीद मांगें।
- किसी भी असामान्य गतिविधि को देखने के लिए बैंक स्टेटमेंट और अपनी क्रेडिट रिपोर्ट पर कड़ी नजर रखें ।

2.साइबर धोखाधड़ी

वित्त वर्ष 24 में साइबर धोखाधड़ी से भारत को 177 करोड़ रुपये का नुकसान हुआ:-

भारत में साइबर धोखाधड़ी के कारण होने वाली धनराशि वित्त वर्ष 2023 में 69.68 करोड़ रुपये से बढ़कर वित्त वर्ष 2024 में 177.05 करोड़ रुपये हो गई है। साइबर धोखाधड़ी से होने वाले नुकसानों में वृद्धि एक चिंताजनक प्रवृत्ति है। यदि किसी ग्राहक की लापरवाही के कारण नुकसान होता है, तो उन्हें बैंक को अनधिकृत लेनदेन की सूचना देने तक इसकी भरपाई करनी चाहिए।

भारतीय रिजर्व बैंक (आरबीआई) ने अनधिकृत लेनदेन के कारण ग्राहकों को होने वाले नुकसान को सीमित करने के लिए दिशानिर्देश जारी किए हैं, जिन्हें 3 कार्य दिवसों के भीतर रिपोर्ट करने और बैंक की लापरवाही या अन्य प्रणालीगत दोष साबित होने पर टाला जा सकता है।

यदि कोई ग्राहक 4 से 7 कार्य दिवसों के भीतर अनधिकृत लेनदेन की रिपोर्ट करता है, तो खाते के प्रकार के आधार पर उनकी देयता 5,000 रुपये से लेकर 25,000 रुपये तक हो सकती है। 7 कार्य दिवसों से परे, देयता बैंक की नीति द्वारा नियंत्रित होती है। बैंक को अनधिकृत लेनदेन के लिए ग्राहक की लापरवाही साबित करनी होगी।

भारत में अब तक की सबसे बड़ी साइबर धोखाधड़ी:

तेलंगाना का साइबर सुरक्षा ब्यूरो एक बड़े साइबर वित्तीय घोटाले की जांच कर रहा है, जिसमें 75 वर्षीय सेवानिवृत्त प्रबंधक को 13 करोड़ रुपये का चूना लगाया गया। पीड़ित को व्हाट्सएप के माध्यम से निवेश का अवसर देने वाले घोटालेबाजों ने धोखा दिया था।

उच्च रिटर्न के लालच में आकर, उस व्यक्ति ने 4 करोड़ रुपये का निवेश किया। जब उसका बैलेंस 10 करोड़ रुपये तक पहुंच गया, तो उसने पैसे निकालने की कोशिश की, लेकिन उसे बताया गया कि उसे अतिरिक्त शुल्क देना होगा। यह मानते हुए कि वह अपना निवेश और मुनाफा वापस पा सकता है, उसने अगले 15 दिनों में 9 करोड़ रुपये और ट्रांसफर कर दिए। ईडी ने 25 करोड़ रुपये के साइबर निवेश घोटाले में बेंगलुरु में चार लोगों को गिरफ्तार किया है। वे घोटाले के पैसे को सफेद करने के लिए कंपनियां और बैंक खाते खोलने में सम्मिलित थे।

3. इस माह के टिप

आज की तेज़ रफ़्तार भरी दुनिया में, घोटालेबाज़ निजी फ़ायदे के लिए ताजातरीन घटनाओं का फ़ायदा उठाते हैं। वे समाचारों में होने वाली घटनाओं का इस्तेमाल करके हमें संवेदनशील जानकारी देने के लिए धोखा देते हैं।

डेटा और सिस्टम की सुरक्षा के लिए इन युक्तियों को समझना बहुत ज़रूरी है। हाल की घटनाएं इस बात को उजागर करती हैं कि घोटालेबाज कितनी जल्दी किसी स्थिति का फ़ायदा उठा सकते हैं। इसके तुरंत बाद, घोटालेबाजों ने इन समस्याओं के समाधान का दावा करते हुए फ़िशिंग ईमेल भेजे। उन्होंने प्राप्तकर्ताओं को दुर्भावनापूर्ण लिंक पर क्लिक करने के लिए सोशल इंजीनियरिंग रणनीति का इस्तेमाल किया। इसके

अलावा, वर्तमान घटना घोटाले के अन्य उदाहरणों में शामिल हैं:

प्राकृतिक आपदाएं: राहत प्रयासों के लिए प्राप्त दान को चुराने के लिए साइबर अपराधियों ने दान संस्थाओं का रूप धारण कर लिया है।

प्रमुख डेटा उल्लंघन: अपराधियों ने प्रभावित कंपनियों के रूप में प्रस्तुत होकर उपयोगकर्ताओं से उनके खातों की जानकारी को "सत्यापित" करने का अनुरोध किया है।

सुझाव:-

- तत्काल अनुरोधों के प्रति संशयी रहें।
- घोटालेबाज त्वरित निर्णय लेने के लिए अत्यावश्यकता का उपयोग करते हैं। यदि आपको कोई अत्यावश्यक ईमेल मिलता है, तो रुकें और प्रेषक की पुष्टि करें।
- स्रोत की पुष्टि करें .
- क्लिक करने से पहले प्रेषक के ईमेल और लिंक की जांच कर लें कि कहीं कोई गलत टाइपिंग या संदिग्ध संकेत तो नहीं हैं, क्योंकि ये फ़िशिंग का संकेत हो सकते हैं।
- भावनात्मक हेरफेर से सावधान रहें।
- घोटालेबाज क्लिक हेतु लुभाने के लिए डर, जिज्ञासा या लालच का इस्तेमाल करते हैं। मजबूत भावनात्मक अपील या असाधारण वादों वाले ईमेल से सावधान रहें।

संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ