केंद्रीय रिजर्व पुलिस बल

साइबर बाइट

- वल्चर एंड्रॉइड बैंकिंग ट्रोजन उन्नत रिमोट कंट्रोल क्षमताओं के साथ लौटता है।
- एआई-कॉलिंग:-धोखेबाज नए प्रकार के धोखे के लिए एआई वॉयस क्लोनिंग टूल की ओर रुख करते हैं।
- सिस्को ग्राहक पासवर्ड-स्प्रेइंग हमलों के बारे में चेतावनी देता है जो सिस्को सुरक्षित फ़ायरवॉल उपकरणों की रिमोट एक्सेस वीपीएन (आरएवीपीएन) सेवाओं को लक्षित कर रहे हैं।
- एआई वोर्म, जो डेटा चुरा सकता है : यह क्या है, यह कैसा कार्य करता है और इससे कैसे सुरक्षित रह सकते है।

साइबर बाइट
मई -2024
संस्करण

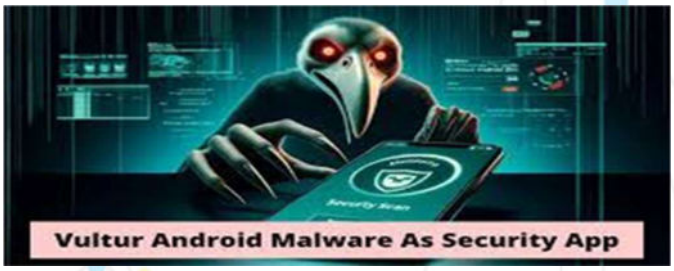
- साइबर फ्रॉड अपडेट्स

ऑनलाइन वितीय धोखाधड़ी
की रिपोर्ट करने के लिए
1930

https://cybercrime.gov.in
पर अपनी शिकायत दर्ज करें

1.साइबर गीक समाचार

क) वल्चर एंड्रॉइड बैंकिंग ट्रोजन उन्नत रिमोट कंट्रोल क्षमताओं के साथ लौटता है।



वल्चर के नाम से जाना जाने वाला एंड्रॉइड बैंकिंग ट्रोजन नई सुविधाओं और बेहतर एंटी-एनालिसिस और डिटेक्शन इवेज़न तकनीकों के साथ फिर से सामने आया है, जो इसके ऑपरेटरों को मोबाइल डिवाइस के साथ दूरस्थ रूप से बातचीत करने और संवेदनशील डेटा एकत्र करने में सक्षम बनाता है। **वल्चर** ने अपने सी-2 संचार को एन्क्रिप्ट करके, तुरंत डिक्रिप्ट किए गए कई एन्क्रिप्टेड पेलोड का उपयोग करके, अपने दुर्भावनापूर्ण कार्यों को अंजाम देने के लिए वैध अनुप्रयोगों की आड़ का उपयोग करके अपनी अधिक दुर्भावनापूर्ण गतिविधियों को छिपाना शुरू कर दिया है।

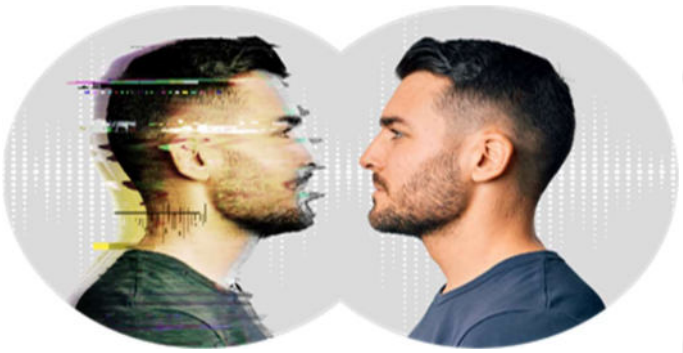
मैलवेयर को **गूगल प्ले स्टोर** पर ट्रोजनाइज्ड ड्रॉपर ऐप्स के माध्यम से वितरित होते देखा गया है, जो प्रमाणीकरणकर्ता और उत्पादकता ऐप्स के रूप में अनजाने उपयोगकर्ताओं को उन्हें इंस्टॉल करने के लिए बरगलाता है।

पहला एसएमएस संदेश पीड़ित को फोन कॉल के लिए मार्गदर्शन करता है। जब पीड़ित उस नंबर पर कॉल करता है, तो जालसाज पीड़ित को एक दूसरा एसएमएस प्रदान करता है जिसमें ड्रॉपर का लिंक शामिल होता है: **मैक्एफ़ी सिक्योरिटी ऐप** [वैध] का एक संशोधित संस्करण।" इंस्टालेशन पर, दुर्भावनापूर्ण ड्रॉपर तीन संबंधित पेलोड (दो एपीके और एक डीईएक्स फ़ाइल) निष्पादित करता है जो बॉट को सी-2 सर्वर के साथ पंजीकृत करता है, अल्फा वीएनसी और एनग्रोक के माध्यम से रिमोट एक्सेस के लिए एक्सेसिबिलिटी सेवाओं की अनुमति प्राप्त करता है, और सी-2 सर्वर से प्राप्त कमांड चलाता है। वल्चर में प्रमुख सुविधाओं में से एक संक्रमित डिवाइस के साथ दूरस्थ रूप से बातचीत करने की क्षमता है, जिसमें एंड्रॉइड की एक्सेसिबिलिटी सेवाओं के माध्यम से क्लिक, स्क्रॉल और स्वाइप करने के साथ-साथ डाउनलोड, अपलोड, डिलीट, इंस्टॉल और फाइलें ढूंढना शामिल है। इसके अलावा, मैलवेयर पीड़ितों को ऐप्स की पूर्व-निर्धारित सूची के साथ बातचीत करने से रोकने, स्टेटस बार में कस्टम नोटिफिकेशन प्रदर्शित करने और यहां तक कि लॉक स्क्रीन सुरक्षा उपायों को बायपास करने के लिए की-गार्ड को अक्षम करने से भी सुसज्जित है।

सुझावः-

- सॉफ्टवेयर अपडेटेड रखें।
- विश्वसनीय सुरक्षा सॉफ्टवेयर का उपयोग करें।
- केवल आधिकारिक स्रोतों से ही ऐप्स डाउनलोड करें।
- ऐप अनुमतियों की समीक्षा करें।
- गूगल प्ले सुरक्षा सक्षम करें।
- डिवाइस लॉकिंग तंत्र लागू करें।
- लिंक एवं अटैचमेंटस के साथ सावधानी बरतें।
- स्वयं एवं दूसरों को शिक्षित करें।
- नियमित रूप से डेटा का बैक-अप रखें।
- खाता गतिविधियों की निगरानी रखें।

ख) एआई-कॉलिंगः- धोखेबाज नए प्रकार के धोखे के लिए एआई वॉयस क्लोनिंग टूल की ओर रुख करते हैं।



साइबर अपराधियों ने नवनिर्मित कृत्रिम बुद्धिमत्ता (एआई) वॉयस क्लोनिंग टूल का सहारा लिया है और धोखे की एक नई किस्म तैयार की है। ऑडियो के एक छोटे से नमूने के साथ, वे लगभग किसी की भी आवाज़ क्लोन कर सकते हैं और वॉइसमेल या वॉइस मैसेजिंग टेक्स्ट द्वारा फर्जी संदेश भेज सकते हैं। उद्देश्य, अक्सर, लोगों को धोखा देकर सैकड़ों, नहीं तो हज़ारों डॉलर ठगना होता है। इसमें तीन सेकंड का ऑडियो ही काफी है। किसी व्यक्ति की आवाज के एक छोटे से नमूने और साइबर अपराधी द्वारा तैयार की गई स्क्रिप्ट के साथ, ये आवाज क्लोन संदेश विश्वसनीय लगते हैं, विश्वव्यापी सर्वेक्षण में 70% लोगों ने कहा कि उन्हें विश्वास नहीं था कि वे क्लोन आवाज और असली के बीच अंतर बता सकते हैं। साइबर अपराधी उस प्रकार के संदेश बनाते हैं जिनकी आप अपेक्षा कर सकते हैं जो तात्कालिकता और संकट से भरे हुए होते है। वे क्लोनिंग टूल का उपयोग किसी पीड़ित के मित्र या परिवार के सदस्य कि ध्वनि संदेश के साथ प्रस्तुत करने के लिए करेंगे, जिसमें कहा जाएगा कि वे एक कार दुर्घटना में शामिल हो गए हैं, या हो सकता है कि उन्हें लूट लिया गया हो या घायल कर दिया गया हो। किसी भी तरह, फर्जी संदेश अक्सर कहता है कि उन्हें

तुरंत पैसे की जरूरत है। कुल मिलाकर, यह दृष्टिकोण अब तक काफी प्रभावी साबित हुआ है। सर्वेक्षण में शामिल दस लोगों में से एक ने कहा कि उन्हें एआई वॉयस क्लोन से एक संदेश मिला है, और उनमें से 77% पीड़ितों ने कहा कि परिणामस्वरूप उन्हें पैसे का नुकसान हुआ है। विचार करें कि लोग यूट्यूब पर अपने वीडियो पोस्ट करते हैं, सोशल मीडिया पर रील साझा करते हैं और शायद पॉडकास्ट में भी भाग लेते हैं। यहां तक कि अपेक्षाकृत सार्वजनिक स्रोतों तक पहुंच करके भी, साइबर अपराधी अपने शस्त्रागार को शक्तिशाली स्रोत सामग्री से भर सकते हैं। सर्वेक्षण उत्तरदाताओं में से लगभग आधे (45%) ने कहा कि वे पैसे की आवश्यकता वाले किसी मित्र या प्रियजन के ध्वनि मेल या ध्वनि संदेश का उत्तर देंगे, खासकर अगर उन्हें लगता है कि अनुरोध उनके साथी या जीवनसाथी से आया है (40%)), माँ (24%), या बच्चा (20%)।

इसके अलावा, उन्होंने बताया कि यदि संदेश भेजने वाला कहता है तो वे संभवतः इनमें से किसी एक संदेश का जवाब देंगे:

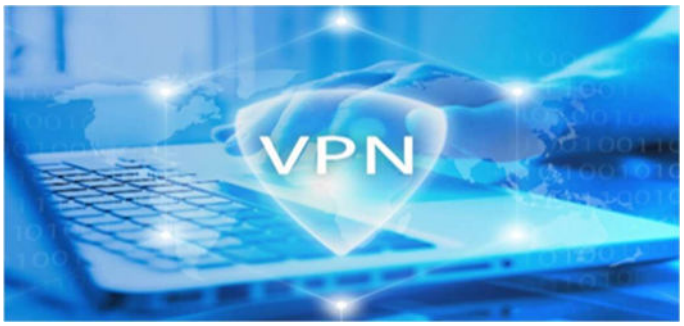
- वे एक कार दुर्घटना में रहे हैं (48%)।
- उन्हें लूट लिया गया है (47%)।
- उन्होंने अपना फ़ोन या वॉलेट खो दिया है (43%)।
- विदेश यात्रा के दौरान उन्हें मदद की ज़रूरत थी (41%)।

ये संदेश लक्षित "स्पीयर फ़िशिंग" हमलों के नवीनतम उदाहरण हैं, जो विशिष्ट जानकारी वाले विशिष्ट लोगों को लक्षित करते हैं जो उस पर कार्रवाई करने के लिए पर्याप्त विश्वसनीय लगते हैं। साइबर अपराधी अक्सर यह जानकारी सार्वजनिक सोशल मीडिया प्रोफाइल और ऑनलाइन अन्य स्थानों से प्राप्त करते हैं, जहां लोग अपने बारे में, अपने परिवार के बारे में, अपनी यात्रा आदि के बारे में पोस्ट करते हैं और फिर मौका भुनाने का प्रयास करते हैं। भुगतान के तरीके अलग-अलग होते हैं, फिर भी साइबर अपराधी अक्सर फॉर्म मांगते हैं जैसे कि उपहार कार्ड, वायर ट्रांसफ़र, पुनः लोड करने योग्य डेबिट कार्ड और यहां तक कि क्रिप्टोकरेंसी जिनका पता लगाना या पुनर्प्राप्त करना मुश्किल है। हमेशा की तरह, इस प्रकार के भुगतान का अनुरोध एक प्रमुख खतरे को दर्शाता हैं। यह बिल्कुल एक घोटाला हो सकता है।

सुझावः-

- बच्चों, परिवार के सदस्यों या विश्वसनीय करीबी दोस्तों के साथ एक मौखिक कोडवर्ड सेट करें।
- हमेशा स्रोत पर सवाल उठाएं।
- क्लिक करने और साझा करने से पहले सोचें।
- अपनी पहचान सुरक्षित रखें।
- डेटा ब्रोकर साइटों से अपना नाम हटाकर करें।

ग) सिस्को, ग्राहकों को पासवर्ड-स्प्रेइंग हमलों के बारे में चेतावनी देता है जो सिस्को सुरक्षित फ़ायरवॉल उपकरणों की रिमोट एक्सेस वीपीएन (आरएवीपीएन) सेवाओं को लक्षित कर रहे हैं।



कंपनी ने रिमोट एक्सेस वीपीएन (आरएवीपीएन) सेवाओं के उद्देश्य से पासवर्ड स्प्रे हमलों के खिलाफ सिफारिशों वाला एक दस्तावेज प्रकाशित किया है। आईटी दिग्गज ने बताया कि हमले तीसरे पक्ष के वीपीएन कंसन्ट्रेटर्स को भी निशाना बना रहे हैं।

"सिस्को को आरएवीपीएन सेवाओं पर लक्षित पासवर्ड स्प्रे अटैक से संबंधित कई रिपोर्टों से अवगत कराया गया था। टैलोस द्वारा यह नोट किया गया है कि ये हमले केवल सिस्को उत्पादों तक ही सीमित नहीं हैं, बल्कि तीसरे पक्ष के वीपीएन कंसंट्रेटर्स को भी प्रभावित करता हैं। रिपोर्ट के अनुसार "आपके वातावरण के आधार पर, हमलों के कारण खाते लॉक हो सकते हैं, जिसके परिणामस्वरूप सेवा से इनकार (डीओएस) जैसी स्थितियाँ उत्पन्न हो सकती हैं।"

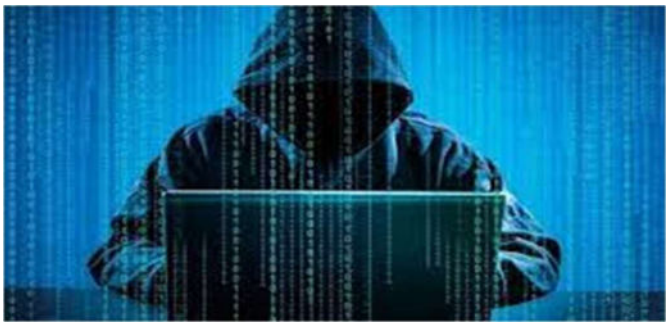
पासवर्ड स्प्रेइंग एक प्रकार का क्रूर बल हमला है। इस हमले में, एक हमलावर एप्लिकेशन पर डिफ़ॉल्ट पासवर्ड वाले उपयोगकर्ता नामों की सूची के आधार पर जबरदस्ती लॉगिन करेगा। उदाहरण के लिए, एक हमलावर खाता लॉकआउट से बचने के लिए एप्लिकेशन पर कई अलग-अलग खातों के खिलाफ एक पासवर्ड (जैसे, सिक्योर@123) का उपयोग करेगा, जो आम तौर पर तब होता है जब एक ही खाते को कई पासवर्ड के साथ मजबूर किया जाता है।

सुझावः-

- मजबूत पासवर्ड नीतियां लागू करें।
- मल्टी फैक्टर प्रमाणीकरण (एमएफए) लागू करें।
- उपकरणों को अपडेट और पैच करें।
- लॉग की निगराना और विश्लेषण करें।
- खाता लॉकआउट नीतियां लागू करें।
- घुसपैठ रोकथाम प्रणालियों (आईपीएस) को सक्षम करें।
- जियो-लोकेशन ब्लॉकिंग लागू करें।
- नियमित सुरक्षा संपरीक्षा करें।

घ) एआई वोर्म, जो निजी डेटा चुरा सकता है :

यह क्या है, यह कैसा कार्य करता है और इससे कैसे सुरक्षित रह सकते है।



डिजिटल दुनिया तेजी से बढ़ रही है और वर्तमान में, इस विकास का शीर्ष राइडर जेनरेटिव एआई-चैट जीपीटी, जेमिनी, कोपायलट इत्यादि है। हम कृत्रिम बुद्धिमत्ता संचालित प्लेटफार्मों के जाल से घिरे हुए हैं जो हमारी अधिकांश समस्याओं का समाधान प्रदान करते हैं। क्या प्रोटेक्टिव योजना की आवश्यकता है? आपको एक अनुकूलित जवाब मिलता है। कोड लिखने के लिए संघर्ष कर रहे हैं? एआई का उपयोग करके पूरा ड्राफ्ट आपकी आंखों के सामने होगा। हालाँकि, एआई इकोसिस्टम पर बढ़ती निर्भरता और इसका प्रसार नए खतरों को भी जन्म दे रहा है जो संभावित रूप से आपको काफी हद तक नुकसान पहुंचा सकते हैं। ऐसा ही एक ख़तरा एआई वर्म्स का विकास है, जो आपका गोपनीय डेटा चुरा सकता है और जेनरेटिव एआई सिस्टम द्वारा बनाई गई सुरक्षा दीवारों को तोड़ सकता है।

एआई वर्म कैसे काम करता है?

आप इस मॉरिस II की कल्पना एक सेंध लगाने वाले कंप्यूटर वर्म की तरह कर सकते हैं। और इसका काम कृत्रिम बुद्धिमत्ता (एआई) का उपयोग करने वाले ईमेल सहायकों के साथ धोखा करना है। सबसे पहले, मॉरिस II "ऐडवेर्सरिअल सेल्फ-रेप्लीकेसन" नामक एक गुप्त चाल का उपयोग करता है। यह ईमेल सिस्टम पर संदेशों की बौछार कर देता है, जिससे वह संदेशों को बार-बार अग्रेषित करके एक घेरे में ले जाता है। इससे ईमेल सहायक के पीछे के एआई मॉडल भ्रमित हो जाते हैं। वे डेटा तक पहुँचना और उसे बदलना समाप्त कर देते हैं। इससे या तो जानकारी चोरी हो सकती है या हानिकारक सामग्री (जैसे मैलवेयर) फैल सकती है। शोधकर्ताओं के अनुसार, मॉरिस II के पास घुसपैठ करने के दो तरीके हैं: टेक्स्ट-आधारित: यह ईमेल के अंदर खराब संकेतों को छुपाता है, सहायक की सुरक्षा को मूर्ख बनाता है। छवि आधारित: यह कृमि को और अधिक फैलाने के लिए गुप्त संकेतों वाली छवियों का उपयोग करता है। सरल शब्दों में, मॉरिस II एक सेंध लगाने वाला कंप्यूटर वर्म है जो पेंचीदा रणनीति का उपयोग करके ईमेल सिस्टम में गड़बड़ी करता है और उनके पीछे की एआई को भ्रमित करता है

सुझाव:-

- सॉफ्टवेयर अपडेटेड रखें।
- एंटीवायरस/एंटी-मैलवेयर सॉफ़्टवेयर तैनात करें I
- नेटवर्क विभाजन लागू करें।
- घुसपैठ का पता लगाने और रोकथाम प्रणाली (आईडीपीएस) सक्षम करें।
- कम से कम विशेषाधिकार का उपयोग करें।
- उपयोगकर्ताओं को शिक्षित करें।
- नेटवर्क ट्रेफिक की निगरानी रखें।
- नियमित डेटा बैक-अप रखें।
- व्यवहार विश्लेषण लागू करें।
- सुरक्षा विशेषज्ञों के साथ सहयोग करें।

2. साइबर फ्रॉड

क) महाराष्ट्र के एक 37 वर्षीय व्यक्ति ने उच्च रिटर्न के वादे के लालच में आकर ऑनलाइन टास्क घोटाले में 10.13 लाख रुपये खो दिए।

महाराष्ट्र के नवी मुंबई के एक 37 वर्षीय व्यक्ति ने कुछ ऑनलाइन कार्यों के लिए उच्च रिटर्न के वादे के लालच में आकर कथित तौर पर ₹ 10.13 लाख खो दिए। नवी मुंबई के साइबर पुलिस स्टेशन ने इस संबंध में चार लोगों के खिलाफ मामला दर्ज किया है। आरोपी ने 16 से 27 जनवरी के बीच ओल्ड पनवेल इलाके के निवासी पीड़ित से संपर्क किया और उसे कुछ ऑनलाइन प्रीपेड कार्य करने की पेशकश की। उन्होंने उसे कुछ लिंक भेजे, कार्य सौंपे और आकर्षक रिटर्न का वादा किया। साइबर पुलिस स्टेशन के एक अधिकारी ने बताया कि इसके बाद, पीड़ित ने निर्देशानुसार बैंक खातों और यूपीआई आईडी के माध्यम से कुल 10,13,005 रुपये का भुगतान किया। हालाँकि, कार्य पूरा करने के बाद, पीड़ित को न तो वादा किया गया रिटर्न मिला और न ही उसका पैसा वापस किया गया। जब उसने आरोपियों से भुगतान मांगा तो उन्होंने गोलमोल जवाब दिया।

ख) वॉइस क्लोनिंग स्कैम: कैसे साइबर अपराधी, माता-पिता को धोखा देने के लिए बच्चों' की आवाज का उपयोग कर रहे हैं।

मान लीजिए कि आपको किसी का फोन आता है और धमकी दी जाती है कि अगर आप उनकी मांगें पूरी नहीं करेंगे तो आपके बच्चे को आपराधिक मामले में फंसा दिया जाएगा। आप यह सोचकर सावधान हो जाते हैं कि कहीं कोई आपको धोखा देने

की कोशिश तो नहीं कर रहा है। हालाँकि, अगले ही मिनट, आप अपने बच्चे को फोन पर रोते हुए सुनते हैं और आपको डर लगता है कि यह सच हो सकता है। और इसलिए आप भुगतान करते हैं - बाद में पता चलता है कि यह वास्तव में एक स्कैम था। आपका बच्चा कभी फ़ोन पर नहीं था, लेकिन परिष्कृत सॉफ़्टवेयर का उपयोग करके उनकी आवाज़ क्लोन कर ली गई थी। पीड़ित, नोएडा सेक्टर 78 में महागुन मॉडर्न अपार्टमेंट का निवासी है, जो दिल्ली नगर निगम में एक अधीक्षण अभियंता के रूप में काम करता है। वह अपने 18 वर्षीय बेटे को जेईई मॉक टेस्ट के लिए राजेंद्र नगर मेट्रो के पास एक केंद्र पर छोड़ने गया था। इसके बाद वह कुछ काम निपटाने के लिए गाजियाबाद में स्टेशन चला गया। एक घंटे बाद, उन्हें +92 देश कोड वाले नंबर से कॉल आया। पीड़िता ने कहा, "फोन करने वाले धोखेबाज, जिसने खुद को पुलिस इंस्पेक्टर बताया, ने कहा कि मेरा बेटा बलात्कारियों के एक गिरोह के साथ पकड़ा गया है...; उसने मुझसे अपना नाम हटाने के लिए तुरंत पेटीएम के माध्यम से 30,000 रुपये का भुगतान करने की मांग की। उन्होंने कहा कि मैं आपके बेटे से भी करा सकता सकता हूं। अगले मिनट, मैंने एक आवाज सुनी, 'पापा कृपया उन्हें भुगतान करें, वे असली पुलिसकर्मी हैं, कृपया मुझे बचाएं'। मुझे एक क्षण के लिए भी संदेह न हो सका कि वह मेरा लड़का नहीं है। बोलने का अंदाज़, रोना... सब कुछ एक जैसा था।" अभी भी संदेह होने पर, पीड़ित ने फोन करने वाले से पूछा कि वह किस पुलिस स्टेशन में तैनात है, लेकिन उस व्यक्ति ने कोई जवाब नहीं दिया। "मैंने उससे कहा कि मैं ऑनलाइन सेवाओं का उपयोग नहीं करता, लेकिन मेरे पास 10,000 रुपये नकद है और मैं उसे व्यक्तिगत रूप से दे सकता हूँ। लेकिन उन्होंने लेने से इनकार कर दिया और जोर देकर कहा कि पैसे ट्रांसफर करने के लिए दुकानदार की मदद लो। मुझे डर था कि कहीं वह अपहरणकर्ता न हो. इसलिए मैंने अपने ड्राइवर को दुकानदार बनने के लिए कहा और उसे 10,000 रुपये भेजने के लिए फोन दे दिया।

3. इस माह के टिप

डेबिट कार्ड/क्रेडिट कार्ड सुरक्षा अनुदेशः-

अपना कार्ड सुरक्षित रखें :- अपने कार्ड को नकदी की तरह समझें। उसे इधर-उधर न छोड़े और न ही किसी को उधार दें।

पिन और पासवर्ड याद रखें :- अपने पिन और पासवर्ड कही पर भी न लिखें। इसे बजाय उन्हें याद रखें।

अपनी निजी जानकारी की रक्षा करें :- अपनी निजी जानकारी साझा करने में सावधान रहें, विशेषकर फोन या ऑनलाइन होने पर। जब आप ऑनलाइन खरीददारी कर रहे हो तो यह सुनिश्चित करें कि आप सुरक्षित वेबसाइटस पर है।

अपने खाता विवरण की नियमित समीक्षा करें :- किसी भी अप्राधिकृत लेनदेन को पता लगाने के लिए अपने खाता विवरण को नियमित अंतराल पर चैक करें।

लेनदेन अलर्ट सक्षम करें :- बहुत से बैंक आपके कार्ड से प्रत्येक लेनदेन के लिए नॉटिफिकेशन प्राप्त करने का विकल्प देते है। अपने कार्ड के उपयोग से अद्यतन रहने के लिए इस फीचर को सक्षम करें।

एटीएम और कार्ड रीडर से सावधान रहें :- एटीएम या कार्ड रीडर का उपयोग करने से पहले उनसे जुड़े किसी भी संदिग्ध उपकरण की जांच कर लें।

सुरक्षित एटीएम का उपयोग करें :- अच्छी रोशनी वाले, सुरक्षित क्षेत्रों में स्थित एटीएम का उपयोग करें। सुनसान या कम रोशनी वाली जगहों के एटीएम का उपयोग ना करें।

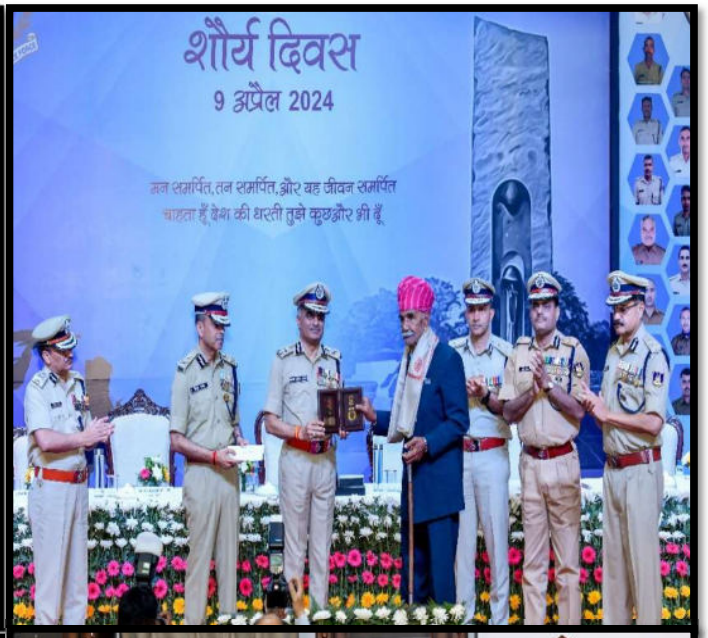
धोखाधड़ी सुरक्षा सेवाओं के लिए साइन अप करें:- कुछ वित्तीय संस्थान फ्रॉड सुरक्षा सेवाएं प्रदान करते हैं जो संदिग्ध गतिविधि के लिए आपके खाते की निगरानी करते हैं और संभावित धोखाधड़ी के प्रति आपको सचेत करते हैं।

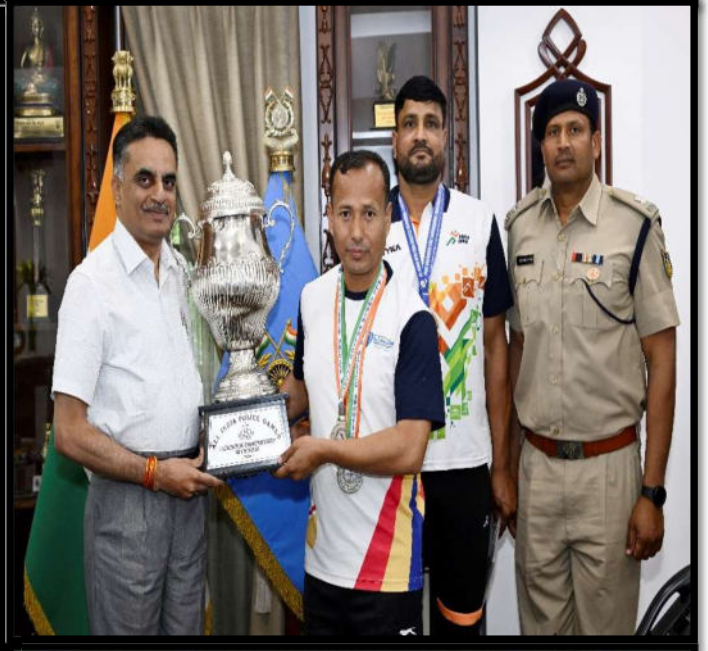
खोए या चोरी हुए कार्ड की तुरंत रिपोर्ट करें:- यदि आपका कार्ड खो जाता है या संदेह है कि यह चोरी हो गया है, तो कार्ड को रद्द करने और बदलने के लिए तुरंत अपने बैंक या क्रेडिट कार्ड उपयोगकर्ता से संपर्क करें।

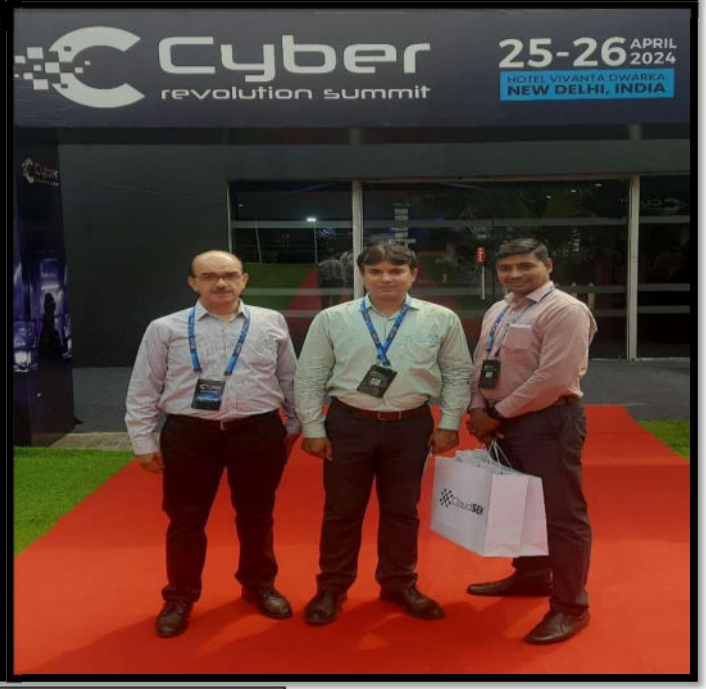
सुरक्षित ऑनलाइन भुगतान विधियों का उपयोग करें:- ऑनलाइन खरीदारी करते समय, पेपैल या वर्चुअल क्रेडिट कार्ड नंबर जैसी सुरक्षित भुगतान विधियों का उपयोग करने पर विचार करें। हमलावरों ने समझौता किए गए सिस्टम में पेलोड भेजने के लिए कोबाल्ट स्ट्राइक एडवर्सरी सिमुलेशन टूल का उपयोग करते हैं।

भारतीय साइबरस्पेस पर हालिया साइबर खतरा।

इंडोनेशिया के हैकिंग ग्रुप **जेनोसेक टीम** ने अपने टेलीग्राम चैनल पर एक चेतावनी जारी की, जिसमें पीएम नरेंद्र मोदी की मुसलमानों को "घुसपैठिया" बताने वाली टिप्पणी के जवाब में हैक्टिविस्ट इंडोनेशिया कि वापसी कि घोषणा की, वे भारतीय साइबरस्पेस को निशाना बनाने के लिए #OPINDIA लॉन्च करने जा रहे हैं।







संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ