

पूर्व सैनिकों और वीर नारियों द्वारा साइबर सुरक्षा धोखाधड़ी से निपटना

कमांडर पी राजगोपाल ताम्पी आईएन (आर)

- एआई और बड़े भाषा मॉडल
- सॉफ्टवेयर और एआई में क्या अंतर है?
- एजेंट क्या होता है?
- एजेंट और एलएलएम में क्या अंतर है?
- एआई के कुछ महत्वपूर्ण लाभ क्या हैं?
    - वैज्ञानिक खोजों में तीव्र प्रगति
    - नए पदार्थ, नए अणु, उत्पादकता में लाभ
    - मौसम पूर्वानुमान
    - सॉफ्टवेयर कोडिंग
    - रोबोट और स्वचालन
- कृत्रिम बुद्धिमत्ता के प्रमुख जोखिम क्या हैं?
    - छल, सत्ता की लालसा और आत्मरक्षा
    - डीपफेक
    - नियंत्रण खोना
    - पुनरावर्ती आत्म-सुधार (RSI)
    - स्व-प्रतिकृति

- हगिंगफेस घटना, एंथ्रोपिक आईओटी भविष्यवाणी
- फ्रांस में प्रशीतन संयंत्रों को हैक करना – अक्टूबर 2026 के मध्य तक
- सरकारी वेबसाइटें ठप (पीएचपी बग के कारण) – 21 अनुसूचित जनजाति अक्टूबर 2026
- यह मूलतः दोहरे उपयोग वाली तकनीक है – स्वायत्त हथियार, सीबीआरएन और युद्धकालीन उपयोग में इसके गंभीर खतरे हैं।
- एआई साइबर सुरक्षा का प्रवर्तक और रक्षक है।
- हमारे मस्तिष्क से भी अधिक शक्तिशाली कंप्यूटिंग इंजन (तेज़ और असीमित संसाधन)।उन्हें समझ पाना या उनके साथ तालमेल बिठा पाना संभव नहीं होगा।
- एजेंट चौबीसों घंटे सातों दिन काम करते हैं और सैकड़ों की संख्या में एन्क्रिप्शन को ब्रूट फोर्स से भेद सकते हैं, सॉफ्टवेयर में बग ढूंढ सकते हैं। • एआई सिस्टम प्रशिक्षण के बाद चालू होते ही पूरी जानकारी के साथ काम करना शुरू कर सकते हैं, कहीं भी माइग्रेट कर सकते हैं और हमें उनका पता तब तक नहीं चलेगा जब तक बहुत देर हो चुकी होगी।
- निकट भविष्य में नुकसान कृत्रिम बुद्धिमत्ता द्वारा इंटरनेट पर नियंत्रण करने और बुनियादी ढांचे

को हैक करने से हो सकता है।प्रणालियाँ और उपयोगिताएँ।

• एआई सिस्टमों के प्रति संदेह और कम भरोसे का भाव रखें:

• सोशल मीडिया से प्राप्त जानकारी पर भरोसा न करें।

• सिरी या इसके समकक्ष वार्तालाप निगरानी ऐप्स को निष्क्रिय रखें।

• यदि आप चैट जीपीटी या क्लाउड जैसे एआई टूल का उपयोग करते हैं, तो "सभी के लिए मॉडल में सुधार करें" विकल्प और स्थान विकल्प को बंद कर दें।

• बाज़ार में उपलब्ध एआई एजेंटों का उपयोग करने से बचें, सिवाय इसके कि आप यह सुनिश्चित कर सकें कि वे आपके व्यक्तिगत डेटा को किस प्रकार संभालते हैं। इसका उपयोग केवल कम जोखिम वाले अनुप्रयोगों के लिए करें, यदि यह अत्यंत आवश्यक हो।

• अपने विचारों और इरादों को किसी भी एआई एजेंट को न सौंपें, विशेषकर अपनी डायरी या निजी जर्नल को। • अपने बैंक खातों, बिलों, भुगतानों, अन्य वित्तीय मामलों और लेन-देन में स्वचालित लेनदेन के लिए एआई एजेंटों को पहुंच न दें।

• अपने फोल्डर, ईमेल सेवाओं और कार्ड की जानकारी तक पहुंच प्रदान न करें।

• हमेशा "खुद सोचें", एआई से अपने लिए सोचने को न कहें।

• अपनी विचार प्रक्रिया को एआई सिस्टम के बजाय किसी भरोसेमंद दोस्त से सत्यापित करें।

• गोपनीयता नियंत्रणों का प्रभावी ढंग से उपयोग करें, चिकित्सा और वित्तीय रिकॉर्ड केवल अपरिहार्य आवश्यकता होने पर

ही अपलोड करें।

• किसी कॉलर पर सिर्फ इसलिए भरोसा न करें क्योंकि उसकी आवाज़ आपके परिवार के सदस्य जैसी लगती है। • अगर कोई आपातकालीन स्थिति में रिश्तेदार होने का दावा करके पैसे मांगता है, तो कॉल काट दें और उस व्यक्ति को उसके पहले से सेव किए गए नंबर पर वापस कॉल करें।

• आपात स्थिति में परिवार के सदस्यों की पहचान सत्यापित करने के लिए एक गोपनीय वाक्यांश पर सहमति बनाएं। इसे सोशल मीडिया पर साझा न करें।मीडिया।

• किसी वीडियो कॉल को सिर्फ इसलिए असली न समझें क्योंकि आप उस व्यक्ति का चेहरा पहचानते हैं। • पैसे, गोपनीयता या तत्काल कार्रवाई के लिए किए गए अनुरोधों को चेतावनी समझें। • पुलिस, सीबीआई, सीमा शुल्क, अदालतों या अन्य अधिकारियों द्वारा की गई किसी भी कार्रवाई का दावा करने वाले संदेशों पर विश्वास न करें।हमने आपको डिजिटल रूप से गिरफ्तार कर लिया है।

• कॉलर आईडी, व्हाट्सएप प्रोफाइल फोटो या प्रदर्शित संगठन के नामों को पहचान के प्रमाण के रूप में न मानें।
• अपने ऑनलाइन डेटा प्रोफाइल और फुटप्रिंट को न्यूनतम संभव स्तर तक कम करें। •
प्रतिरूपण का उदाहरण (नकली वीडियो कॉल अनुमोदन के कारण $25 मिलियन का हस्तांतरण)।

• वैध उद्देश्य के बिना पहचान दस्तावेजों को साझा करने से बचें।
• जहां उपयुक्त हो, पहचान दस्तावेजों की प्रतियों में उद्देश्य-विशिष्ट वॉटरमार्क जोड़ें।• WhatsApp, Facebook, Instagram और अन्य सोशल प्लेटफॉर्म पर गोपनीयता सेटिंग्स की समीक्षा करें।• मैसेजिंग ग्रुप में आपको जोड़ने वालों को सीमित करें और ग्रुप की सदस्यता कम से कम रखने का प्रयास करें। • जहां तक संभव हो, सार्वजनिक रूप से उपलब्ध वॉइस रिकॉर्डिंग और व्यक्तिगत वीडियो को सीमित करें।
• पारिवारिक संबंधों, दिनचर्या और आर्थिक स्थिति के बारे में विस्तृत जानकारी प्रकाशित करने से बचें। • सार्वजनिक ऑनलाइन प्रोफाइल से अनावश्यक व्यक्तिगत जानकारी हटा दें।• जहां आवश्यक हो, UIDAI की आधिकारिक आधार प्रमाणीकरण-इतिहास और बायोमेट्रिक-लॉकिंग सुविधाओं का उपयोग

करें।उपयुक्त।

• जहां उपलब्ध हो, वहां सरकारी दूरसंचार सेवाओं के माध्यम से अपने मोबाइल कनेक्शन की जांच करें।

• कम भरोसेमंद सदस्यता और पंजीकरण के लिए एक अलग ईमेल पते का उपयोग करें।• क्लाउड-शेयरिंग लिंक की समीक्षा करें और आवश्यकता न होने पर सार्वजनिक पहुंच हटा दें।

• अपना बैंकिंग पिन, यूपीआई पिन, एटीएम पिन, सीवीवी, पासवर्ड, जन्मतिथि या ओटीपी कभी भी किसी को न बताएं।• याद रखें: पैसे प्राप्त करने के लिए आपको यूपीआई पिन दर्ज करने की आवश्यकता नहीं है। इसे दर्ज करने से आमतौर पर भुगतान अधिकृत हो जाता है।• किसी अजनबी द्वारा भेजे गए क्यूआर कोड को स्कैन करके कभी भी पैसे प्राप्त न करें।

• अप्रत्याशित यूपीआई भुगतान अनुरोध को कभी भी स्वीकृत न करें।

• एआई का उपयोग करके गारंटीकृत उच्च रिटर्न या असाधारण लाभ का वादा करने वाली निवेश योजनाओं पर भरोसा न करें।• एजेंटों और अजनबियों को कभी भी आपके बैंकिंग एप्लिकेशन को दूर से संचालित करने की अनुमति न दें।

• बैंक कार्ड, चेक या वित्तीय दस्तावेजों की तस्वीरें अनजान लोगों के साथ साझा न करें। • सभी महत्वपूर्ण खातों पर लेनदेन अलर्ट चालू करें।

• यदि आपका बैंक अनुमति देता है, तो अपनी आवश्यकताओं के अनुरूप दैनिक हस्तांतरण सीमा निर्धारित करें।

• कार्ड सुरक्षा: यदि संभव हो तो ऑनलाइन कार्ड विवरण संग्रहीत न करें। कार्ड विवरण की स्वचालित रूप से भरने की प्रक्रिया से बचें।
• जब उच्च सीमा की आवश्यकता न हो, तो क्रेडिट कार्ड की ऑनलाइन लेनदेन सीमा कम कर दें। • आवश्यकता न होने पर अंतर्राष्ट्रीय कार्ड लेनदेन बंद कर दें।
• विदेश यात्रा के दौरान, विशेष रूप से एम्स्टर्डम की घटना के बाद, संपर्क रहित लेनदेन को अक्षम करें। • पर्याप्त बचत राशि को उन खातों से अलग रखें जिनका उपयोग बार-बार ऑनलाइन/यूपीआई भुगतान के लिए किया जाता है।

• बैंकिंग, ईमेल और महत्वपूर्ण खातों के लिए अलग-अलग पासवर्ड का उपयोग करें। • लंबे पासवर्ड या ऐसे वाक्यांशों का उपयोग करें जिनका अनुमान लगाना कठिन हो।
• जहां भी उपलब्ध हो, दो-कारक प्रमाणीकरण या FIDO2 प्रमाणीकरण को सक्षम करें।• अपने फोन को पिन, फिंगरप्रिंट या चेहरे की पहचान से लॉक करें।
• अपने फ़ोन और एप्लिकेशन को नवीनतम संस्करण से अपडेट रखें। • एप्लिकेशन केवल आधिकारिक ऐप स्टोर से ही डाउनलोड करें।
• किसी अज्ञात व्यक्ति द्वारा व्हाट्सएप, एसएमएस या ईमेल के माध्यम से भेजे गए किसी भी एपीके या एप्लिकेशन को इंस्टॉल न करें।

• किसी अजनबी के कहने पर स्क्रीन शेयरिंग या रिमोट एक्सेस एप्लिकेशन इंस्टॉल न करें। • ऐसे किसी भी लिंक पर क्लिक न करें जो यह दावा करे कि आपका केवाईसी, पैन, आधार कार्ड, बैंक खाता, बिजली आपूर्ति या डिलीवरी ब्लॉक कर दी जाएगी।
• संदेशों में दिए गए लिंक पर क्लिक करने के बजाय, आधिकारिक बैंकिंग या सेवा एप्लिकेशन को स्वयं खोलें।

• यदि संभव हो तो खातों के लिए एक बैकअप सुरक्षा कुंजी पंजीकृत करें और उसे सुरक्षित रूप से संग्रहीत करके रखें।
• व्यक्तिगत, पारिवारिक, रिश्ते संबंधी जानकारी और तस्वीरें पोस्ट करने से बचें।सोशल मीडिया पर।
• अपनी यात्रा का कार्यक्रम या दैनिक दिनचर्या सोशल मीडिया पर प्रकाशित न करें।
• अपनी पसंद-नापसंद, राजनीतिक रुझान, वित्तीय खरीदारी और निजी गतिविधियों को सोशल मीडिया पर ज़ाहिर न करें।

• घर के वाईफाई के लिए WPA2 AES या WPA 3 एन्क्रिप्शन का उपयोग करें और मजबूत पासवर्ड का प्रयोग करें।
• यदि आप घर में कैमरे और IoT डिवाइस का उपयोग करते हैं, तो सुनिश्चित करें कि डेटा आपके डेटा कार्ड पर ही रहे। इसे क्लाउड पर स्थानांतरित न करें।
• सोशल मीडिया पर फर्जी खातों को ब्लॉक करें और उनकी रिपोर्ट करें।

मेंधोखाधड़ी होने पर क्या करें?

1. तुरंत 1930 पर कॉल करें - भारत की राष्ट्रीय साइबर वित्तीय धोखाधड़ी हेल्पलाइन।
2. घटना की रिपोर्ट ऑनलाइन करेंराष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
3. तुरंत अपने बैंक से संपर्क करें
4. आवश्यकतानुसार प्रभावित कार्ड, खाते या भुगतान पहुंच को अवरुद्ध करने का अनुरोध करें।5. शीघ्र रिपोर्टिंग से आगे के तबादलों को रोकने का अवसर बेहतर होता है, हालांकि वसूली की गारंटी नहीं है।इसके अलावा ये कदम भी उठाएं:
1. संदिग्ध जालसाज से संपर्क करना बंद कर दें।

2. रिमोट एक्सेस सेशन बंद करें और अनधिकृत सॉफ़्टवेयर हटाने में सहायता लें। 3. किसी विश्वसनीय डिवाइस का उपयोग करके समझौता किए गए पासवर्ड बदलें।
4. आवश्यकतानुसार संदिग्ध लॉगिन सत्रों को रद्द करें और प्रमाणीकरण विधियों को रीसेट करें।5. संदेशों, स्क्रीनशॉट, फ़ोन नंबर, लेन-देन के संदर्भ और अन्य सबूतों को सुरक्षित रखें। 6. फर्जी प्रोफाइल, डीपफेक और प्रतिरूपण सामग्री की सूचना संबंधित प्लेटफॉर्म और अधिकारियों को दें। 7. यदि आपके खाते का उपयोग धोखाधड़ी वाले संदेश भेजने के लिए किया गया है, तो प्रभावित संपर्कों को सूचित करें।

1. स्वतंत्र सत्यापन के बिना किसी भी परिचित आवाज या चेहरे पर कभी भरोसा न करें। 2. कभी भी OTP, PIN, पासवर्ड या बैंकिंग संबंधी जानकारी का खुलासा न करें।
3. धमकियों, अत्यावश्यकता या गोपनीयता के कारण कभी भी पैसे का हस्तांतरण न करें।
4. डिजिटल गिरफ्तारी या पुलिस के सुरक्षित खातों के दावों पर कभी विश्वास न करें।
5. पैसे प्राप्त करने के लिए कभी भी क्यूआर कोड स्कैन न करें या यूपीआई पिन दर्ज न करें।
6. किसी अजनबी के अनुरोध पर कभी भी सॉफ्टवेयर इंस्टॉल न करें या अपनी स्क्रीन साझा न करें।
7. अप्रत्याशित लिंक, निवेश प्रस्तावों या पेंशन संबंधी संदेशों पर कभी भरोसा न करें। 8. अपने फोन को अपडेट रखें और खातों की मज़बूत प्रमाणीकरण सुविधा चालू रखें।

9. असामान्य वित्तीय निर्णय लेने से पहले किसी विश्वसनीय व्यक्ति से सलाह लें।
10. यदि धोखाधड़ी होती है, तो तुरंत अपने बैंक से संपर्क करें और 1930 पर कॉल करें।
11. याद रखने योग्य सबसे प्रभावी सिद्धांत यह है:
12. किसी आवाज, चेहरे, संदेश या वीडियो पर मात्र इसलिए भरोसा न करें क्योंकि वह असली लगता है। कोई भी कार्रवाई करने से पहले पहचान और अनुरोध की स्वतंत्र रूप से पुष्टि करें।

स्वास्थ्य डेटा	नहीं
फ़ोटो और वीडियो	नहीं
शारीरिक गतिविधि	नहीं
सूचनाएं	नहीं
ब्लूटूथ	केवल उपयोग करते सम
एआई ऐप्स	प्रशिक्षण के लिए डेटा क

मोबाइल फोन की	
सेटिंग्स	अनुशंसित सेटिंग
जगह	केवल ऐप का उपयोग
कैमरा	केवल ऐप का उपयोग
माइक्रोफ़ोन	हर बार पूछें
संपर्क और एसएमएस	हर बार पूछें
कैलेंडर	हर बार पूछें

भाग्य वहीं होता है जहाँ अवसर और तैयारी का संगम होता है।

एआईपी रिसर्च वेबसाइट HTTPS:AIPATHFINDER.ORG

अनुप्रयुक्त मानव-केंद्रित एआई –HTTPS://www.amazon.com/dp/B0CYXHYPHC

अपनी बुद्धि को सशक्त बनाएं -https://www.amazon.in/dp/B0D3WZXY99

धन्यवाद!