

माजी सैनिक आणि वीर नारींद्वारे सायबर सुरक्षा फसवणुकीचे हाताळणी

कमांडर पी राजगोपाल टँपी IN (R)

- एआय आणि मोठे भाषा मॉडेल

सॉफ्टवेअर आणि एआय (AI) मध्ये काय फरक आहे?

एजंट म्हणजे काय?

एजंट आणि एलएलएम यांच्यात काय फरक आहे?

- एआयचे काही महत्त्वाचे फायदे कोणते आहेत?
    - वैज्ञानिक शोधांमधील जलद प्रगती
    - नवीन सामग्री, नवीन रेणू, उत्पादकतेतील फायदे
    - हवामानाचा अंदाज
    - सॉफ्टवेअर कोडिंग
    - रोबोट आणि स्वयंचलन
- एआयचे प्रमुख धोके कोणते आहेत?
    - फसवणूक, सत्तालोभ आणि आत्मसंरक्षण
    - डीपफेक्स

    नियंत्रण गमावणे
    - पुनरावर्ती स्व-सुधारणा (आरएसआय)
    - स्व-प्रतिकृती

- हगिंगफेस घटना, मानववंशीय IoT भविष्यवाणी
- फ्रान्समधील रेफ्रिजरेशन प्लांट हॅक करणे – ऑक्टोबर २०२६ च्या मध्यापर्यंत
- सरकारी वेबसाईट्स बंद (PHP मधील त्रुटींमुळे) – २१ सेंट ऑक्टोबर २०२६
- मूलतः दुहेरी वापराचे तंत्रज्ञान – स्वायत्त शस्त्र, सीबीआरएन (CBRN) आणि युद्धकालीन वापरामध्ये मोठे धोके.
- एआय हे सायबरसुरक्षेला सक्षम करणारे आणि तिचे रक्षण करणारे आहे
- आपल्या मेंदूपेक्षा अधिक शक्तिशाली संगणकीय यंत्रणा (अधिक वेगवान आणि अमर्याद संसाधने). आम्हीत्यांच्याशी बरोबरी करू शकणार नाही किंवा त्यांना समजू शकणार नाही.
- एजंट २४x७ कार्यरत असतात आणि शेकडोच्या संख्येने ते एनक्रिप्शनवर ब्रूट फोर्स हल्ला करू शकतात, सॉफ्टवेअरमधील त्रुटी शोधू शकतात. • एआय सिस्टीम्स प्रशिक्षणानंतर पॉवर ऑन करताच पूर्ण ज्ञानासह कार्यरत होऊ शकतात, कुठेही स्थलांतरित होऊ शकतात आणि खूप उशीर होईपर्यंत आपल्याला त्यांचा शोध लागू शकत नाही.
- एआयने इंटरनेटवर ताबा मिळवल्यास आणि पायाभूत सुविधा हॅक केल्यास नजीकच्या काळात नुकसान होऊ शकते.प्रणाली आणि सुविधा.

• एआय प्रणालींकडे संशयाने आणि कमी विश्वासाने पाहा:

• सोशल मीडियावरून मिळालेल्या माहितीवर विश्वास ठेवू नका.

• सिरी किंवा तत्सम संभाषण निरीक्षण ॲप्स बंद ठेवा.

• तुम्ही Chat GPT किंवा Claude सारखी AI साधने वापरत असल्यास, “सर्वांसाठी मॉडेल सुधारा” हा पर्याय आणि स्थानाचा पर्याय बंद करा.

• व्यावसायिकरित्या उपलब्ध असलेले एआय एजंट वापरणे टाळा, मात्र ते तुमच्या वैयक्तिक डेटाला कसे हाताळते याची तुम्ही विश्वसनीयरीत्या पडताळणी करू शकत असाल तरच त्यांचा वापर करा. अत्यंत गरज असेल तरच, कमी जोखमीच्या अनुप्रयोगांसाठी त्याचा वापर करा.

• तुमचे विचार आणि हेतू कोणत्याही एआय एजंटला सोपवू नका, विशेषतः तुमची डायरी किंवा खाजगी रोजनिशी. • तुमच्या बँक खात्यांमधील व्यवहार, बिले, देयके, इतर आर्थिक बाबी आणि व्यवहार स्वयंचलित करण्यासाठी एआय एजंटना प्रवेश देऊ नका.

• तुमच्या फोल्डर्स, ईमेल सेवा आणि कार्ड माहितीचा ॲक्सेस देऊ नका.

• नेहमी स्वतः विचार करा, एआयला तुमच्यासाठी विचार करायला सांगू नका.

• तुमच्या विचारप्रक्रियेची पडताळणी एआय प्रणालींकडून नव्हे, तर एखाद्या विश्वासू मित्राकडून करा.

• गोपनीयता नियंत्रणांचा प्रभावीपणे वापर करा, केवळ अत्यावश्यक गरजेच्या वेळीच वैद्यकीय आणि आर्थिक नोंदी

अपलोड करा.28/10/2026 पी राजगोपाल टंपी 4

• केवळ आवाज कुटुंबातील सदस्यासारखा वाटतो म्हणून फोन करणाऱ्यावर कधीही विश्वास ठेवू नका. • जर कोणी आपत्कालीन परिस्थितीत नातेवाईक असल्याचा दावा करून पैशांची मागणी करत असेल, तर फोन कट करा आणि त्या व्यक्तीला त्यांच्या पूर्वी सेव्ह केलेल्या नंबरवर परत कॉल करा.

• आपत्कालीन परिस्थितीसाठी कुटुंबाच्या खाजगी पडताळणी वाक्यांशावर सहमत व्हा. तो सोशल मीडियावर शेअर करू नका.माध्यमे.

• केवळ समोरच्या व्यक्तीचा चेहरा ओळखीचा आहे म्हणून व्हिडिओ कॉल खरा आहे असे समजू नका. • पैशांची मागणी, गुप्तता किंवा तात्काळ कारवाई यांसारख्या तातडीच्या विनंत्यांना धोक्याची सूचना समजा. • पोलीस, सीबीआय, सीमाशुल्क, न्यायालये किंवा इतर अधिकाऱ्यांनी संपर्क साधल्याचा दावा करणाऱ्या संदेशांवर विश्वास ठेवू नका.तुम्हाला डिजिटल अटकेत ठेवले आहे.

• ओळखीचा पुरावा म्हणून कॉलर आयडी, व्हॉट्सॲप प्रोफाइल फोटो किंवा संस्थेच्या नावांवर विश्वास ठेवू नका.

• तुमचा ऑनलाइन डेटा प्रोफाइल आणि ठसा शक्य तितका कमी करा • बनावट ओळख वापरण्याचे उदाहरण (बनावट व्हिडिओ कॉल मंजुरीमुळे $25 दशलक्ष हस्तांतरित).

• वैध कारणाशिवाय ओळखपत्रे इतरांना देणे टाळा.

• आवश्यक असेल तेथे, ओळखपत्रांच्या प्रतींवर विशिष्ट उद्देशासाठीचा वॉटरमार्क लावा.• व्हॉट्सॲप, फेसबुक, इन्स्टाग्राम आणि इतर सोशल प्लॅटफॉर्मवरील प्रायव्हसी सेटिंग्ज तपासा.• तुम्हाला मेसेजिंग ग्रुपमध्ये कोण जोडू शकेल यावर निर्बंध घाला, ग्रुपमधील सदस्यत्व कमीत कमी ठेवण्याचा प्रयत्न करा. • शक्य असेल तिथे सार्वजनिकरित्या उपलब्ध व्हॉइस रेकॉर्डिंग आणि वैयक्तिक व्हिडिओ मर्यादित ठेवा. • कौटुंबिक संबंध, दिनचर्या आणि आर्थिक परिस्थितीची सविस्तर माहिती प्रकाशित करणे टाळा. • सार्वजनिक ऑनलाइन प्रोफाइलमधून अनावश्यक वैयक्तिक माहिती काढून टाका.• UIDAI च्या अधिकृत आधार प्रमाणीकरण-इतिहास आणि बायोमेट्रिक-लॉकिंग सुविधांचा वापर करा जिथेयोग्य.

• जिथे उपलब्ध असेल तिथे, अधिकृत सरकारी दूरसंचार सेवांद्वारे तुमचे मोबाईल कनेक्शन

तपासा.
• कमी विश्वासार्ह सदस्यता आणि नोंदणीसाठी वेगळा ईमेल पत्ता वापरा.• क्लाउड-शेअरिंग लिंक्सचे पुनरावलोकन करा आणि गरज नसताना सार्वजनिक प्रवेश काढून टाका.

• तुमचा बँकिंग पिन, यूपीआय पिन, एटीएम पिन, सीव्हीव्ही, पासवर्ड, जन्मतारीख किंवा ओटीपी कधीही उघड करू नका.• लक्षात ठेवा: पैसे मिळवण्यासाठी तुम्हाला UPI पिन टाकण्याची आवश्यकता नाही. तो टाकल्याने सामान्यतः पेमेंटला अधिकृतता मिळते.• अनोळखी व्यक्तीने पाठवलेला QR कोड पैसे मिळवण्यासाठी कधीही स्कॅन करू नका.
• अनपेक्षित UPI कलेक्ट रिक्वेस्टला कधीही मंजूर करू नका.
एआयचा वापर करून हमीपूर्वक उच्च परतावा किंवा अफाट नफा मिळवून देण्याचे आश्वासन देणाऱ्या गुंतवणूक योजनांवर विश्वास ठेवू नका.• एजंट आणि अनोळखी व्यक्तींना तुमचे बँकिंग ॲप्लिकेशन दूरस्थपणे चालवण्याची परवानगी कधीही देऊ नका.
• बँक कार्ड, चेक किंवा आर्थिक कागदपत्रांचे फोटो अनोळखी व्यक्तींसोबत शेअर करू नका. • सर्व महत्त्वाच्या खात्यांवर ट्रान्झॅक्शन अलर्ट चालू करा.
• तुमची बँक परवानगी देत असल्यास, तुमच्या गरजेनुसार दैनंदिन हस्तांतरण मर्यादा निश्चित करा.

• कार्डची काळजी: शक्य असल्यास ऑनलाइन कार्डचा तपशील साठवू नका. कार्डचा तपशील आपोआप भरण्याची प्रक्रिया टाळा. • जेव्हा उच्च मर्यादेची आवश्यकता नसेल, तेव्हा क्रेडिट-कार्डच्या ऑनलाइन व्यवहारांची मर्यादा कमी करा. • गरज नसताना आंतरराष्ट्रीय कार्ड व्यवहार बंद करा.

• परदेशात प्रवास करताना, विशेषतः अॅमस्टरडॅम घटनेप्रमाणे, संपर्करहित व्यवहार बंद ठेवा. • वारंवार ऑनलाइन/UPI पेमेंट करण्यासाठी वापरल्या जाणाऱ्या खात्यांपासून मोठी बचत वेगळी ठेवा.28/10/2026 पी राजगोपाल टंपी 7

• बँकिंग, ईमेल आणि महत्त्वाच्या खात्यांसाठी वेगवेगळे पासवर्ड वापरा. • लांब पासवर्ड किंवा अंदाज करणे कठीण असलेले पासफ्रेज वापरा.

• जिथे उपलब्ध असेल तिथे टू-फॅक्टर ऑथेंटिकेशन किंवा FIDO2 ऑथेंटिकेशन सक्षम करा.• तुमचा फोन पिन, फिंगरप्रिंट किंवा फेस ऑथेंटिकेशनने लॉक करा.

• तुमचा फोन आणि ॲप्लिकेशन्स नवीनतम आवृत्तीसह अद्ययावत ठेवा. • ॲप्लिकेशन्स केवळ अधिकृत ॲप स्टोअर्सवरूनच डाउनलोड करा.

• अनोळखी व्यक्तीने व्हॉट्सॲप, एसएमएस किंवा ईमेलद्वारे पाठवलेले कोणतेही एपीके किंवा ॲप्लिकेशन इन्स्टॉल करू नका.

• अनोळखी व्यक्तीच्या सांगण्यावरून स्क्रीन-शेअरिंग किंवा रिमोट-ॲक्सेस ॲप्लिकेशन्स इन्स्टॉल करू नका. • तुमचे केवायसी, पॅन, आधार, बँक खाते, वीजपुरवठा किंवा डिलिव्हरी ब्लॉक

केली जाईल असा दावा करणाऱ्या अनपेक्षित लिंक्सवर क्लिक करू नका.
• संदेशांमधील लिंक्सवर क्लिक करण्याऐवजी स्वतः अधिकृत बँकिंग किंवा सेवा ॲप्लिकेशन उघडा.

• शक्य असल्यास खात्यांसाठी बॅकअप सुरक्षा की नोंदवा आणि ती सुरक्षितपणे संग्रहित करून ठेवा.
• वैयक्तिक, कौटुंबिक, नातेसंबंधांची माहिती आणि छायाचित्रे टाकणे टाळासोशल मीडियावर.
• तुमच्या प्रवासाचा तपशील किंवा दैनंदिन दिनचर्या सोशल मीडियावर प्रकाशित करू नका. • तुमच्या आवडीनिवडी, राजकीय विचार, आर्थिक खरेदी आणि खाजगी घडामोडी सोशल मीडियावर उघड करू नका.
• घरगुती वायफायसाठी मजबूत पासवर्डसह WPA2 AES किंवा WPA 3 एन्क्रिप्शन वापरा.

• तुम्ही घरगुती कॅमेरे आणि IoT उपकरणे वापरत असल्यास, डेटा तुमच्या डेटा कार्डवरच राहील याची खात्री करा. तो क्लाउडवर हस्तांतरित करू नका.
• सोशल मीडियावर बनावट खाती ब्लॉक करा आणि त्यांची तक्रार करा.

मध्येफसवणूक झाली असेल तर काय करावे?

१. तात्काळ १९३० वर कॉल करा - भारताची राष्ट्रीय सायबर आर्थिक फसवणूक हेल्पलाइन.
२. येथे ऑनलाइन घटनेची तक्रार करा[राष्ट्रीय सायबर गुन्हे अहवाल पोर्टल]
३. तुमच्या बँकेशी तात्काळ संपर्क साधा.
4. आवश्यकतेनुसार, प्रभावित कार्ड, खाती किंवा पेमेंट ॲक्सेस ब्लॉक करण्याची विनंती करा.५. लवकर अहवाल दिल्याने पुढील हस्तांतरण थांबवण्याची संधी सुधारते, तथापि वसुलीची हमी नाही.तसेच खालील उपाययोजना करा:
१. संशयित फसवणूक करणाऱ्या व्यक्तीशी संपर्क थांबवा.
२. रिमोट-ॲक्सेस सत्रे डिस्कनेक्ट करा आणि अनधिकृत सॉफ्टवेअर काढून टाकण्यासाठी मदत घ्या.
३. असुरक्षित झालेले पासवर्ड एका विश्वसनीय डिव्हाइसचा वापर करून बदला.
४. संशयास्पद लॉगिन सत्रे रद्द करा आणि आवश्यकतेनुसार प्रमाणीकरण पद्धती रीसेट करा.५. संदेश, स्क्रीनशॉट,

फोन नंबर, व्यवहाराचे संदर्भ आणि इतर पुरावे जतन करा. ६. बनावट प्रोफाइल, डीपफेक आणि बनावट ओळख असलेल्या सामग्रीची संबंधित प्लॅटफॉर्म आणि अधिकाऱ्यांकडे तक्रार करा. ७. जर तुमच्या खात्याचा वापर फसवणुकीचे संदेश पाठवण्यासाठी केला गेला असेल, तर प्रभावित संपर्कांना सावध करा.

१. स्वतंत्र पडताळणी केल्याशिवाय ओळखीच्या आवाजावर किंवा चेहऱ्यावर कधीही विश्वास ठेवू नका. २. ओटीपी, पिन, पासवर्ड किंवा बँकिंग माहिती कधीही उघड करू नका.

३. धमक्या, निकड किंवा गुप्ततेमुळे कधीही पैसे हस्तांतरित करू नका.

४. डिजिटल अटक किंवा पोलिसांच्या सुरक्षित खात्यांच्या दाव्यांवर कधीही विश्वास ठेवू नका.

५. पैसे मिळवण्यासाठी कधीही QR कोड स्कॅन करू नका किंवा UPI पिन टाकू नका.

६. अनोळखी व्यक्तीच्या सांगण्यावरून कधीही सॉफ्टवेअर इन्स्टॉल करू नका किंवा तुमची स्क्रीन शेअर करू नका.

७. अनपेक्षित लिंक्स, गुंतवणुकीच्या ऑफर्स किंवा पेन्शन-संबंधित संदेशांवर कधीही विश्वास ठेवू नका. ८. फोन अद्ययावत ठेवा आणि खात्याचे मजबूत प्रमाणीकरण सक्षम करा.

९. असामान्य आर्थिक निर्णय घेण्यापूर्वी विश्वासू व्यक्तीचा सल्ला घ्या. १०. फसवणूक झाल्यास, तुमच्या बँकेशी संपर्क साधा आणि ताबडतोब १९३० वर कॉल

करा.

११. लक्षात ठेवण्याचे सर्वात प्रभावी तत्त्व हे आहे:

१२. केवळ खरा वाटतो म्हणून कोणत्याही आवाजावर, चेहऱ्यावर, संदेशावर किंवा व्हिडिओवर कधीही विश्वास ठेवू नका. कोणतीही कारवाई करण्यापूर्वी ओळख आणि विनंतीची स्वतंत्रपणे पडताळणी करा.

	मोबाईल फोन सुर
सेटिंग्ज	शिफारसित सेटिंग
स्थान	फक्त अॅप वापरताना
कॅमेरा	फक्त अॅप वापरताना
मायक्रोफोन	प्रत्येक वेळी विचारा
संपर्क आणि एसएमएस	प्रत्येक वेळी विचारा
कॅलेंडर	प्रत्येक वेळी विचारा

आरोग्य डेटा	नाही
फोटो आणि व्हिडिओ	नाही
शारीरिक क्रियाकलाप	नाही
सूचना	नाही
ब्लूटूथ	फक्त वापरताना
एआय अॅप्स	प्रशिक्षणासाठी डेटा वाप

जिथे संधी आणि पूर्वतयारी यांचा संगम होतो, तेच नशीब होय.

एआयपी संशोधन संकेतस्थळ HTTPS:AIPATHFINDER.ORG

उपयोजित मानवकेंद्रित एआय –HTTPS://www.amazon.com/dp/B0CYXHYPHC

आपली बुद्धिमत्ता वाढवाhttps://www.amazon.in/dp/B0D3WZXY99

धन्यवाद!