

படைவீரர்கள் மற்றும் வீர நாரிகளால் இணையப் பாதுகாப்பு மோசடிகளைக் கையாளுதல்

தளபதி பி ராஜகோபால் தம்பி IN (R)

- செயற்கை நுண்ணறிவு மற்றும் பெரிய மொழி மாதிரிகள்

மென்பொருளுக்கும் செயற்கை நுண்ணறிவுக்கும் என்ன வேறுபாடு?

- முகவர் என்பவர் யார்?
- ஒரு முகவர், ஒரு எல்.எல்.எம்-மிடமிருந்து எவ்வாறு வேறுபடுகிறார்?
- செயற்கை நுண்ணறிவின் சில முக்கிய நன்மைகள் என்னென்ன?
  - அறிவியல் கண்டுபிடிப்புகளில் விரைவான முன்னேற்றம்
  - புதிய பொருட்கள், புதிய மூலக்கூறுகள், உற்பத்தித்திறன் நன்மைகள்
  - வானிலை முன்னறிவிப்புகள்
  - மென்பொருள் நிரலாக்கம்
  - ரோபோக்கள் மற்றும் தானியக்கம்
- செயற்கை நுண்ணறிவின் முக்கிய அபாயங்கள் என்னென்ன?
  - ஏமாற்றுதல், அதிகார வேட்கை மற்றும் தற்காப்பு
  - டீப்ஃபேக்குகள்

- கட்டுப்பாட்டை இழத்தல்
- தொடர் சுய முன்னேற்றம் (RSI)
- சுய பிரதிபலிப்பு

- ஹக்கிங்ஃபேஸ் சம்பவம், மானுட IoT கணிப்பு
- பிரான்சில் உள்ள குளிர்பதன ஆலைகளை ஹேக்கிங் செய்தல் – அக்டோபர் 2026 நடுப்பகுதி
- அரசு இணையதளங்கள் செயலிழப்பு (PHP பிழைகள்) – 21வது அக்டோபர் 2026
- இயல்பாகவே இரட்டைப் பயன்பாட்டுத் தொழில்நுட்பம் – தானியங்கி ஆயுதம், CBRN மற்றும் போர்க்காலப் பயன்பாடுகளில் பெரும் அபாயங்களைக் கொண்டது.

• செயற்கை நுண்ணறிவு என்பது இணையப் பாதுகாப்பைச் சாத்தியமாக்குவதாகவும் காப்பதாகவும் விளங்குகிறது.

• நமது மூளையை விட சக்திவாய்ந்த கணினி இயந்திரம் (வேகமானது மற்றும் வரம்பற்ற வளங்களைக் கொண்டது). நாம்அவர்களுடன் ஈடுகொடுக்கவோ அல்லது அவர்களைப் புரிந்துகொள்ளவோ முடியாது.

• முகவர்கள் 24 மணி நேரமும், வாரத்தின் ஏழு நாட்களும் இயங்குகின்றன; நூற்றுக்கணக்கில் அவை குறியாக்கத்தை வலுக்கட்டாயமாக உடைக்கவும், மென்பொருளில் உள்ள பிழைகளைக் கண்டறியவும் முடியும். • செயற்கை நுண்ணறிவு அமைப்புகள், இயக்கப்பட்டவுடன் பயிற்சி பெற்று, முழுமையான அறிவுடன் செயல்படத் தொடங்கிவிடும்; அவை எங்கும் இடம்பெயரக்கூடும், மேலும் காலம் கடந்துவிடும் வரை நம்மால் அவற்றைக் கண்டறிய முடியாமல் போகலாம்.

• செயற்கை நுண்ணறிவு இணையத்தைக் கைப்பற்றுவதாலும், உள்கட்டமைப்புகளை ஹேக் செய்வதாலும் உடனடித் தீங்கு ஏற்படலாம்.அமைப்புகள் மற்றும் பயன்பாடுகள்.

• செயற்கை நுண்ணறிவு அமைப்புகளைச் சந்தேகத்துடனும் குறைந்த அளவிலான நம்பிக்கையுடனும் அணுகவும்:

சமூக ஊடகங்களில் இருந்து பெறப்படும் தகவல்களை நம்பாதீர்கள்.

• Siri அல்லது அதற்கு இணையான உரையாடல் கண்காணிப்பு செயலிகளை முடக்கி வைக்கவும்.

• நீங்கள் Chat GPT அல்லது Claude போன்ற AI கருவிகளைப் பயன்படுத்தினால், “அனைவருக்கும் மாதிரியை மேம்படுத்து” (Improve model for everyone) என்ற விருப்பத்தையும் இருப்பிட விருப்பத்தையும் அணைத்துவிடவும்.

• உங்கள் தனிப்பட்ட தரவை அது கையாளும் விதத்தை உங்களால் நம்பகத்தன்மையுடன் சரிபார்க்க முடிந்தால் தவிர, வணிக ரீதியாகக் கிடைக்கும் செயற்கை நுண்ணறிவு முகவர்களைப் பயன்படுத்துவதைத் தவிர்க்கவும். உங்களுக்கு முற்றிலும் தேவைப்பட்டால் மட்டுமே, குறைந்த அபாயமுள்ள பயன்பாடுகளுக்கு அதைப் பயன்படுத்தவும்.

• உங்கள் எண்ணங்களையும் நோக்கங்களையும் எந்தவொரு செயற்கை நுண்ணறிவு முகவரிடமும் ஒப்படைக்காதீர்கள், குறிப்பாக உங்கள் நாட்குறிப்பு அல்லது தனிப்பட்ட பத்திரிக்கையை. • உங்கள் வங்கிக் கணக்குகள், கட்டணங்கள், கொடுப்பனவுகள், பிற

நிதி விஷயங்கள் மற்றும் பரிவர்த்தனைகளைத் தானியக்கமாக்குவதற்காக செயற்கை நுண்ணறிவு முகவர்களுக்கு அணுகலை வழங்காதீர்கள்.

• உங்கள் கோப்புறைகள், மின்னஞ்சல் சேவைகள் மற்றும் அட்டைத் தகவல்களுக்கான அணுகலை வழங்காதீர்கள்.

• எப்போதும் நீங்களே சுயமாகச் சிந்தியுங்கள், உங்களுக்காகச் சிந்திக்க செயற்கை நுண்ணறிவைக் கேட்காதீர்கள்.

• உங்கள் சிந்தனைப் போக்கை செயற்கை நுண்ணறிவு அமைப்புகளிடம் அல்லாமல், நம்பகமான நண்பரிடம் சரிபார்க்கவும்.

• தனியுரிமைக் கட்டுப்பாடுகளைத் திறம்படப் பயன்படுத்துங்கள்; தவிர்க்க முடியாத

தேவை ஏற்பட்டால் மட்டுமே மருத்துவ மற்றும் நிதிப் பதிவுகளைப்

பதிவேற்றவும்.28/10/2026 பி ராஜகோபால் தம்பி 4

• அழைப்பவரின் குரல் குடும்ப உறுப்பினரின் குரலைப் போலவே இருக்கிறது என்பதற்காக மட்டும் அவரை ஒருபோதும் நம்பாதீர்கள். • யாராவது அவசரத் தேவைக்காக உறவினர் என்று கூறி பணம் கேட்டால், இணைப்பைத் துண்டித்துவிட்டு, அவர்கள் முன்பே சேமித்து வைத்திருக்கும் எண்ணிற்கு மீண்டும் அழைக்கவும்.

• அவசர காலங்களில் பயன்படுத்துவதற்கென ஒரு தனிப்பட்ட குடும்ப சரிபார்ப்பு சொற்றொடரை முடிவு செய்யுங்கள். அதை சமூக வலைத்தளங்களில் பகிர வேண்டாம்.ஊடகங்கள்.

• பேசுபவரின் முகத்தை அடையாளம் கண்டுகொண்டதால் மட்டுமே, அது ஒரு உண்மையான காணொளி அழைப்பு என எண்ணிவிடாதீர்கள். • பணம், இரகசியம் அல்லது உடனடி நடவடிக்கை தொடர்பான அவசரக் கோரிக்கைகளை எச்சரிக்கை அறிகுறிகளாகக் கருதுங்கள். • காவல்துறை, சிபிஐ, சுங்கத்துறை, நீதிமன்றங்கள் அல்லது பிற அதிகாரிகள் இருப்பதாகக்

கூறும் செய்திகளை நம்பாதீர்கள்.உங்களை டிஜிட்டல் காவலில் வைத்துள்ளோம்.

- அழைப்பாளர் அடையாளம், வாட்ஸ்அப் சுயவிவரப் புகைப்படங்கள் அல்லது காட்டப்படும் நிறுவனப் பெயர்களை அடையாளச் சான்றாக நம்பாதீர்கள்.
- உங்கள் ஆன்லைன் தரவு சுயவிவரத்தையும் தடயத்தையும் முடிந்தவரை குறைந்தபட்சமாகக் குறைக்கவும் • ஆள்மாறாட்ட உதாரணம் (போலி வீடியோ அழைப்பு ஒப்புதல் காரணமாக $25 மில்லியன் பரிமாற்றம் செய்யப்பட்டது).

முறையான நோக்கம் இல்லாமல் அடையாள ஆவணங்களைப் பகிர்வதைத் தவிர்க்கவும்.

• பொருத்தமான இடங்களில், அடையாள ஆவணங்களின் நகல்களில் அதற்கேற்ற நீர்முத்திரையைச் சேர்க்கவும்.• வாட்ஸ்அப், ஃபேஸ்புக், இன்ஸ்டாகிராம் மற்றும் பிற சமூக வலைதளங்களில் உள்ள தனியுரிமை அமைப்புகளைச் சரிபார்க்கவும்.• செய்திக் குழுக்களில் உங்களைச் சேர்ப்பவர்களைக் கட்டுப்படுத்துங்கள், குழு உறுப்பினர்களின் எண்ணிக்கையைக் குறைக்க முயலுங்கள். • நடைமுறைக்கு சாத்தியமான இடங்களில், பொதுவில் கிடைக்கும் குரல் பதிவுகள் மற்றும் தனிப்பட்ட காணொளிகளைக் கட்டுப்படுத்துங்கள். • விரிவான குடும்ப உறவுகள், அன்றாடப் பழக்கவழக்கங்கள் மற்றும் நிதிச் சூழ்நிலைகள் போன்றவற்றை வெளியிடுவதைத் தவிர்க்கவும். • பொதுவான இணைய சுயவிவரங்களிலிருந்து தேவையற்ற தனிப்பட்ட தகவல்களை நீக்கவும்.• தேவைப்படும் இடங்களில் UIDAI-இன் அதிகாரப்பூர்வ ஆதார் அங்கீகார வரலாறு மற்றும் பயோமெட்ரிக் பூட்டு வசதிகளைப் பயன்படுத்தவும்.பொருத்தமானது.

• அதிகாரப்பூர்வ அரசு தொலைத்தொடர்பு சேவைகள் கிடைக்கும் பட்சத்தில், உங்கள் அலைபேசி இணைப்புகளைச் சரிபார்த்துக் கொள்ளுங்கள்.

• குறைந்த நம்பகத்தன்மை கொண்ட சந்தாக்கள் மற்றும் பதிவுகளுக்குத் தனி மின்னஞ்சல் முகவரியைப் பயன்படுத்தவும்.•

கிளவுட் பகிர்வு இணைப்புகளை மதிப்பாய்வு செய்து, இனி தேவைப்படாதபோது பொது அணுகலை நீக்கவும்.

28/10/2026 பி ராஜகோபால் தம்பி 6

• உங்கள் வங்கி பின், யுபிஐ பின், ஏடிஎம் பின், சிவிவி, கடவுச்சொல், பிறந்த தேதி அல்லது ஓடிபி ஆகியவற்றை ஒருபோதும் வெளியிடாதீர்கள்.• நினைவில் கொள்ளுங்கள்: பணம் பெறுவதற்கு நீங்கள் UPI PIN எண்ணை உள்ளிடத் தேவையில்லை. அதை உள்ளிடுவது பொதுவாகப் பணப் பரிமாற்றத்திற்கு அங்கீகாரம் அளிக்கும்.• பணம் பெறுவதற்காக, முன்பின் தெரியாதவர் அனுப்பும் QR குறியீட்டை ஒருபோதும் ஸ்கேன் செய்யாதீர்கள்.

• எதிர்பாராத UPI கலெக்ட் கோரிக்கையை ஒருபோதும் அங்கீகரிக்காதீர்கள்.

• செயற்கை நுண்ணறிவைப் பயன்படுத்தி, உத்தரவாதமான அதிக வருமானம் அல்லது அசாதாரண இலாபங்களை வழங்குவதாக உறுதியளிக்கும் முதலீட்டுத் திட்டங்களை நம்பாதீர்கள்.• முகவர்களையும் முன்பின் தெரியாதவர்களையும் உங்கள் வங்கிச் செயலியைத் தொலைவிலிருந்து இயக்க ஒருபோதும் அனுமதிக்காதீர்கள்.

• வங்கி அட்டைகள், காசோலைகள் அல்லது நிதி ஆவணங்களின்

புகைப்படங்களை அறிமுகமில்லாத நபர்களுடன் பகிர வேண்டாம். • அனைத்து முக்கிய கணக்குகளிலும் பரிவர்த்தனை எச்சரிக்கைகளை இயக்கவும்.

• உங்கள் வங்கி அனுமதிக்கும் பட்சத்தில், உங்கள் தேவைகளுக்கு ஏற்ற தினசரி பரிமாற்ற வரம்புகளை அமைத்துக் கொள்ளுங்கள்.

• அட்டைகள் குறித்த கவனிப்பு: முடிந்தால், இணையத்தில் அட்டை விவரங்களைச் சேமிக்க வேண்டாம். அட்டை விவரங்கள் தானாக நிரப்பப்படும் செயல்முறையைத் தவிர்க்கவும். • அதிக வரம்புகள் இனி தேவைப்படாதபோது, கடன் அட்டை இணையப் பரிவர்த்தனை வரம்புகளைக் குறைக்கவும். • தேவைப்படாதபோது சர்வதேச அட்டைப் பரிவர்த்தனைகளை முடக்கவும்.

• வெளிநாடுகளுக்குப் பயணம் செய்யும்போது, குறிப்பாகத் தொடுதலில்லாப் பரிவர்த்தனைகளை முடக்கவும் – ஆம்ஸ்டர்டாம் சம்பவம் • அடிக்கடி ஆன்லைன்/UPI மூலம் பணம் செலுத்துவதற்குப் பயன்படுத்தப்படும் கணக்குகளிலிருந்து கணிசமான சேமிப்பைத் தனியாக வைத்திருக்கவும்.28/10/2026 பி ராஜகோபால் தம்பி 7

• வங்கி, மின்னஞ்சல் மற்றும் முக்கிய கணக்குகளுக்கு வெவ்வேறு கடவுச்சொற்களைப் பயன்படுத்தவும். • யூகிக்கக் கடினமான நீண்ட கடவுச்சொற்களை அல்லது கடவுச்சொற்றொடர்களைப் பயன்படுத்தவும்.

• இரு காரணி அங்கீகாரம் அல்லது FIDO2 அங்கீகாரம் கிடைக்கின்ற இடங்களில் அதைச் செயல்படுத்தவும்.• உங்கள் தொலைபேசியை PIN, கைரேகை அல்லது முக அங்கீகாரம் மூலம் பூட்டவும்.

• உங்கள் தொலைபேசி மற்றும் செயலிகளை சமீபத்திய வெளியீடுகளுடன் புதுப்பித்துக் கொள்ளுங்கள். • அதிகாரப்பூர்வ செயலி அங்காடிகளிலிருந்து மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யுங்கள்.

• அறிமுகமில்லாத நபரால் வாட்ஸ்அப், எஸ்எம்எஸ் அல்லது மின்னஞ்சல் மூலம் அனுப்பப்படும் APK அல்லது செயலியை நிறுவ வேண்டாம்.

• முன்பின் தெரியாத ஒருவரின் வேண்டுகோளின் பேரில், திரை பகிர்வு அல்லது தொலைநிலை அணுகல் செயலிகளை நிறுவ

வேண்டாம். • உங்கள் KYC, PAN, ஆதார், வங்கிக் கணக்கு, மின்சார விநியோகம் அல்லது வீட்டு விநியோகம் முடக்கப்படும் என்று கூறும் எதிர்பாராத இணைப்புகளைச் சொடுக்க வேண்டாம்.

செய்திகளில் உள்ள இணைப்புகளைச் சொடுக்குவதற்குப் பதிலாக, அதிகாரப்பூர்வ வங்கி அல்லது சேவைச் செயலியை நீங்களே திறக்கவும்.

முடிந்தால், கணக்குகளுக்கான காப்புப் பாதுகாப்புச் சாவியைப் பதிவுசெய்து, அதனைப் பாதுகாப்பாகச் சேமித்து வைக்கவும்.

• தனிப்பட்ட, குடும்ப, உறவுமுறை விவரங்கள் மற்றும் புகைப்படங்களைப் பதிவிடுவதைத் தவிர்க்கவும்.சமூக

ஊடகங்களில்.
• உங்கள் பயணத் திட்டத்தையோ அல்லது அன்றாட வழக்கத்தையோ சமூக ஊடகங்களில் வெளியிடாதீர்கள். • உங்களின் விருப்பங்கள், வெறுப்புகள், அரசியல் நிலைப்பாடுகள், நிதி சார்ந்த கொள்முதல்கள் மற்றும் தனிப்பட்ட செயல்பாடுகளை சமூக ஊடகங்களில் வெளிப்படுத்தாதீர்கள்.
• வீட்டு வை◌ைபைக்கு, வலிமையான கடவுச்சொற்களுடன் கூடிய WPA2 AES அல்லது WPA 3 குறியாக்கத்தைப் பயன்படுத்தவும்.
• நீங்கள் வீட்டுக் கேமராக்கள் மற்றும் IoT சாதனங்களைப் பயன்படுத்தினால், தரவுகள் உங்கள் டேட்டா கார்டிலேயே இருப்பதை உறுதிசெய்து கொள்ளுங்கள். அதை கிளவுடிற்கு மாற்ற வேண்டாம்.
• சமூக ஊடகங்களில் ஆள்மாறாட்டக் கணக்குகளைத்

தடுத்து, புகார் அளியுங்கள்.

ஓமோசடி நடந்திருந்தால் என்ன செய்வது?

1. உடனடியாக 1930 என்ற எண்ணை அழைக்கவும் - இது இந்தியாவின் தேசிய இணையவழி நிதி மோசடி உதவி எண்.
2. சம்பவத்தை ஆன்லைனில் புகாரளிக்கவும்தேசிய இணையக் குற்றப் புகாரளிப்பு இணையதளம்
3. உடனடியாக உங்கள் வங்கியைத் தொடர்பு கொள்ளுங்கள்.
4. பாதிக்கப்பட்ட அட்டைகள், கணக்குகள் அல்லது பணம் செலுத்தும் அணுகலைத் தேவைக்கேற்ப முடக்குமாறு கோரவும்.5. முன்கூட்டியே தெரிவிப்பது மேலும் பணப் பரிமாற்றங்களைத் தடுப்பதற்கான வாய்ப்பை மேம்படுத்துகிறது, இருப்பினும் மீட்புக்கு உத்தரவாதம் இல்லை.மேலும் இந்த நடவடிக்கைகளையும் மேற்கொள்ளுங்கள்:
1. மோசடி செய்பவர் என சந்தேகிக்கப்படுபவருடன் தொடர்புகொள்வதை நிறுத்துங்கள்.
2. தொலைநிலை அணுகல் அமர்வுகளைத் துண்டித்து,

அங்கீகரிக்கப்படாத மென்பொருளை அகற்ற உதவி கோரவும். 3.
நம்பகமான சாதனத்தைப் பயன்படுத்தி, பாதிக்கப்பட்ட
கடவுச்சொற்களை மாற்றவும்.
4. சந்தேகத்திற்கிடமான உள்நுழைவு அமர்வுகளை ரத்துசெய்து, தேவைப்பட்டால்
அங்கீகார முறைகளை மீட்டமைக்கவும்.5. செய்திகள், ஸ்கிரீன்ஷாட்கள்,
தொலைபேசி எண்கள், பரிவர்த்தனை குறிப்புகள் மற்றும் பிற ஆதாரங்களைப்
பாதுகாக்கவும். 6. போலி சுயவிவரங்கள், டீப்ஃபேக்குகள் மற்றும் ஆள்மாறாட்ட
உள்ளடக்கங்களை சம்பந்தப்பட்ட தளங்கள் மற்றும் அதிகாரிகளிடம் புகாரளிக்கவும்.
7. மோசடி செய்திகளை அனுப்ப உங்கள் கணக்கு பயன்படுத்தப்பட்டிருந்தால்,
பாதிக்கப்பட்ட தொடர்புகளுக்கு எச்சரிக்கை செய்யவும்.

1. சுய சரிபார்ப்பு இல்லாமல், நன்கு அறிமுகமான
குரலையோ முகத்தையோ ஒருபோதும் நம்பாதீர்கள். 2.
OTP, PIN, கடவுச்சொல் அல்லது வங்கிச் சான்றுகளை

ஒருபோதும் வெளியிடாதீர்கள்.

3. மிரட்டல்கள், அவசரம் அல்லது இரகசியம் காரணமாக ஒருபோதும் பணத்தை அனுப்பாதீர்கள்.

4. டிஜிட்டல் கைது அல்லது காவல்துறை பாதுகாப்புக் கணக்குகள் தொடர்பான கூற்றுகளை ஒருபோதும் நம்பாதீர்கள்.

5. பணம் பெறுவதற்காக ஒருபோதும் QR குறியீட்டை ஸ்கேன் செய்யவோ அல்லது UPI PIN எண்ணை உள்ளிடவோ வேண்டாம்.

6. முன்பின் தெரியாத ஒருவரின் வேண்டுகோளின் பேரில் ஒருபோதும் மென்பொருளை நிறுவவோ அல்லது உங்கள் திரையைப் பகிரவோ வேண்டாம்.

7. எதிர்பாராத இணைப்புகள், முதலீட்டுச் சலுகைகள் அல்லது ஓய்வூதியம் தொடர்பான செய்திகளை ஒருபோதும் நம்பாதீர்கள். 8. கைபேசிகளைப் புதுப்பித்த நிலையில் வைத்திருங்கள் மற்றும் வலுவான கணக்கு அங்கீகாரத்தைச் செயல்படுத்துங்கள்.

9. வழக்கத்திற்கு மாறான நிதி முடிவுகளை எடுப்பதற்கு முன், நம்பகமான ஒருவரிடம் கலந்தாலோசிக்கவும். 10. மோசடி நடந்தால், உடனடியாக உங்கள் வங்கியைத் தொடர்புகொண்டு 1930 என்ற எண்ணிற்கு அழைக்கவும்.

11. நினைவில் கொள்ள வேண்டிய மிகவும் பயனுள்ள ஒரே கொள்கை இதுதான்:

12. ஒரு குரல், முகம், செய்தி அல்லது காணொளி உண்மையானது போல்

தோற்றமளிக்கிறது என்பதற்காக மட்டும் அதை ஒருபோதும் நம்பாதீர்கள். நடவடிக்கை எடுப்பதற்கு முன், அதன் அடையாளத்தையும் கோரிக்கையையும் சுயமாகச் சரிபார்க்கவும்.

நாட்காட்டி	ஒவ்வொரு முை கேளுங்கள்
சுகாதார தரவு	இல்லை
புகைப்படங்கள் மற்றும் வீடியோக்கள்	இல்லை
உடல் செயல்பாடு	இல்லை
அறிவிப்புகள்	இல்லை
புளூடூத்	பயன்படுத்தும்
AI செயலிகள்	பயிற்சிக்காகத் த பயன்படுத்த வே

மொபைல் ஃபோன் பாதுக	
அமைப்புகள்	பரிந்துரைக்கப்ப
இடம்	செயலியைப் ப போது மட்டும்
கேமரா	செயலியைப் ப போது மட்டும்
மைக்ரோசிமென்ட்	ஒவ்வொரு முை கேளுங்கள்
தொடர்புகள் மற்றும் எஸ்எம்எஸ்	ஒவ்வொரு முை கேளுங்கள்

வாய்ப்பும் முன் தயாரிப்பும் சந்திக்கும் இடமே அதிர்ஷ்டம்.

AIP ஆராய்ச்சி வலைத்தளம் HTTPS:AIPATHFINDER.ORG

பயன்பாட்டு மனித மைய செயற்கை நுண்ணறிவு –HTTPS://www.amazon.com/dp/B0CYXHYPHC

உங்கள் அறிவாற்றலை மேம்படுத்துங்கள்https://www.amazon.in/dp/B0D3WZXY99

நன்றி!