इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

certin
Enhancing Cyber Security in India

ISEA
Information Security
Education & Awareness

Digital India
Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

செயற்கை நுண்ணறிவு விழிப்புணர்வு வழிகாட்டி

இணையப் பாதுகாப்புப் பண்பாட்டை உருவாக்குங்கள்

#சைபர்சுகாதாரம்நமதுகலாச்சாரம்

தேசிய இணையப் பாதுகாப்பு விழிப்புணர்வு மாதம் (அக்டோபர் 2026)

பதிப்பாளர்

இந்திய கணினி அவசரகால பதிலளிப்புக் குழு

எங்களைப் பின்தொடருங்கள் : @IndianCERT @cert_india

பொருளடக்கம்

முன்னுரை 3

செயற்கை நுண்ணறிவு மேம்படுத்தப்பட்ட ஃபிஷிங் மற்றும் சமூகப் பொறியியல் 4

குரல் மற்றும் காணொளி டீப்ஃபேக்குகள் (விஷிங்) 5

செயற்கை நுண்ணறிவு உதவியுடனான தீம்பொருள் மற்றும் தானியங்கி தாக்குதல்கள் 6

போலி வலைத்தளங்கள் மற்றும் அடையாளத் திருட்டு 7

அபாயக் குறிகள் சரிபார்ப்புப் பட்டியல் 8

இணையப் பாதுகாப்பு 9

சாதனப் பாதுகாப்பு 10

செயற்கை நுண்ணறிவை பொறுப்புடன் பயன்படுத்துங்கள் 11

நம்பகமான செயலிகளைத் தேர்ந்தெடுக்கவும் 12

சைபர் பாதுகாப்பு சம்பவங்களை CERT-In-க்கு புகாரளிக்கவும். 13

முன்னுரை

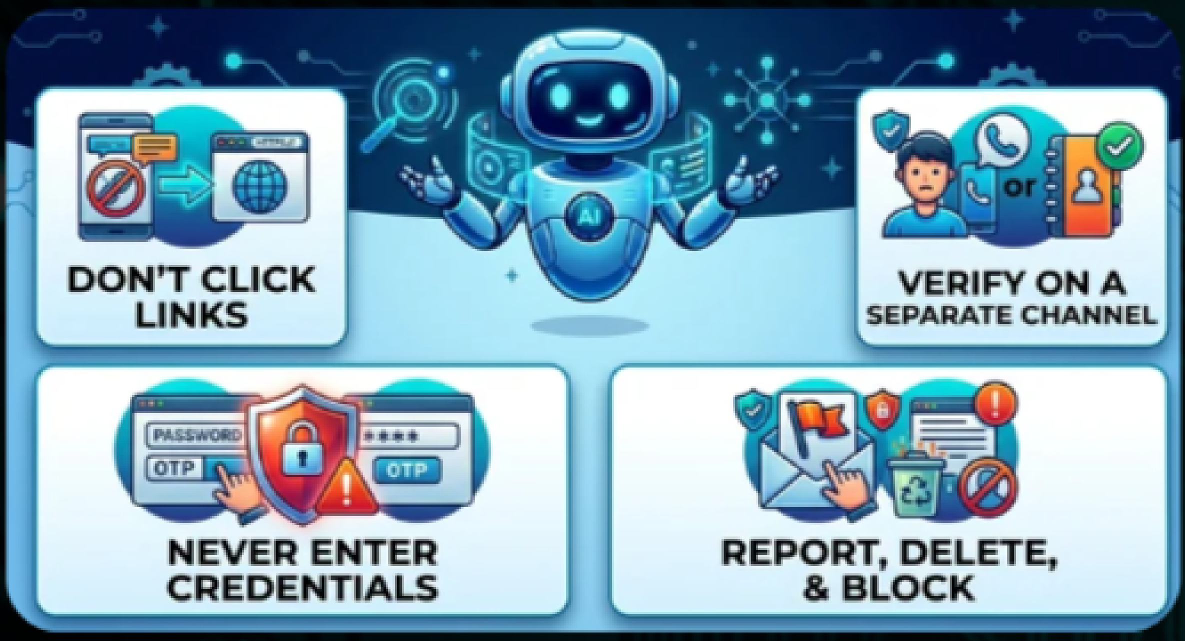
செயற்கை நுண்ணறிவு (AI) நாம் வாழும், பணிபுரியும் மற்றும் தொடர்பு கொள்ளும் முறையை மாற்றியமைத்து வருகிறது. இது புத்தாக்கத்தை சாத்தியமாக்குகிறது, உற்பத்தித்திறனை மேம்படுத்துகிறது, மேலும் பல்வேறு துறைகளில் உள்ள சிக்கலான பிரச்சனைகளைத் தீர்க்க உதவுகிறது. இருப்பினும், இதே தொழில்நுட்பம், அச்சுறுத்தல் செய்பவர்களால் மிகவும் மேம்பட்ட மற்றும் நம்பத்தகுந்த இணைய அச்சுறுத்தல்களை உருவாக்கவும் தவறாகப் பயன்படுத்தப்படுகிறது.

தாக்குதல் நடத்துபவர்களால் இப்போது மிகவும் தத்ரூபமான மின்னஞ்சல்கள், செய்திகள், ஆடியோ, வீடியோக்கள் மற்றும் இணையதளங்களை உருவாக்க முடிவதால், செயற்கை நுண்ணறிவு (AI) டிஜிட்டல் அச்சுறுத்தல்களைக் கண்டறிவதை மேலும் கடினமாக்குகிறது. மோசமான இலக்கணம், வழக்கத்திற்கு மாறான வடிவமைப்பு அல்லது வெளிப்படையான தவறுகள் போன்ற பாரம்பரிய எச்சரிக்கை அறிகுறிகள் இனி நம்பகமான குறிகாட்டிகளாக இல்லாமல் போகலாம். சரிபார்ப்பும் பொறுப்பான டிஜிட்டல் நடைமுறைகளும் முன்னெப்போதையும் விட மிகவும் முக்கியமானதாகிவிட்டன.

நாம் அன்றாடம் பயன்படுத்தும் செயற்கை நுண்ணறிவு கருவிகளும் திறன்மிகு சாதனங்களும் கவனமாகப் பயன்படுத்தப்படாவிட்டால், புதிய தனியுரிமை மற்றும் பாதுகாப்பு அபாயங்களை ஏற்படுத்தக்கூடும். நம்பகமற்ற செயற்கை நுண்ணறிவு செயலிகளுடன் தனிப்பட்ட அல்லது இரகசியத் தகவல்களைப் பகிர்வது, தேவையற்ற அனுமதிகளை வழங்குவது, அல்லது சரிபார்ப்பு இல்லாமல் செயற்கை நுண்ணறிவால் உருவாக்கப்பட்ட தகவல்களைச் சார்ந்திருப்பது போன்றவை தனிநபர்களையும் நிறுவனங்களையும் பாதுகாப்பு அபாயங்களுக்கு உள்ளாக்கக்கூடும்.

இந்திய கணினி அவசரகால பதிலளிப்புக் குழுவின் (CERT-In) “செயற்கை நுண்ணறிவு இணைய விழிப்புணர்வு” குறித்த இந்தக் கையேடு, இணையப் பாதுகாப்பு வல்லுநர்களுக்கு மட்டுமல்லாமல், சாதாரண குடிமக்கள், ஊழியர்கள் மற்றும் டிஜிட்டல் பயனர்களுக்காகவும் வடிவமைக்கப்பட்டுள்ளது. செயற்கை நுண்ணறிவு டிஜிட்டல் அச்சுறுத்தல் சூழலை எவ்வாறு மாற்றுகிறது என்பதை இது விளக்குவதோடு, தனிப்பட்ட தகவல்கள், சாதனங்கள் மற்றும் இணைய அடையாளத்தைப் பாதுகாக்க அனைவரும் பின்பற்றக்கூடிய எளிய, நடைமுறை வழிமுறைகளையும் வழங்குகிறது.

செயற்கை நுண்ணறிவு மேம்படுத்தப்பட்ட ஃபிஷிங் மற்றும் சமூகப் பொறியியல்



இது எவ்வாறு செயல்படுகிறது?

அச்சுறுத்தல் செய்பவர்கள் இப்போது உண்மையானதாகவும் பிழையற்றதாகவும் தோற்றமளிக்கும் மின்னஞ்சல்களையும் குறுஞ்செய்திகளையும் அனுப்புகிறார்கள். செய்திகளைத் தனிப்பட்டவை போல உணர வைப்பதற்காக, அவர்கள் உங்கள் வேலை, நீங்கள் பயன்படுத்தும் சேவைகள் அல்லது சமீபத்திய செயல்பாடுகள் போன்ற உங்களைப் பற்றிய விவரங்களைப் பயன்படுத்துகிறார்கள். இந்தச் செய்திகள் நேர்த்தியாக எழுதப்பட்டிருப்பதால், அவற்றைக் கண்டறிவது மிகவும் கடினமாக இருக்கும்.

எப்படி அடையாளம் காண்பது?

- அந்தச் செய்தி உங்களுக்கே உரியது போல் தோன்றினாலும், அது எதிர்பாராத விதமாக வந்து சேர்கிறது.
- அது அவசரமான அல்லது அச்சுறுத்தும் தொனியைப் பயன்படுத்தி, உடனடி நடவடிக்கை எடுக்கக் கோருகிறது.
- இது ஒரு இணைப்பைக் கிளிக் செய்யவோ, கணக்கைச் சரிபார்க்கவோ, கடவுச்சொல்லை மீட்டமைக்கவோ அல்லது பணம் செலுத்தவோ உங்களைக் கேட்கிறது.
- அனுப்புநரின் முகவரி ஏறக்குறைய சரியாகத் தெரிகிறது, ஆனால் முழுமையாக இல்லை.

பாதுகாப்பாக இருப்பது எப்படி?

- கேட்கப்படாத செய்திகளில் உள்ள இணைப்புகளைச் சொடுக்காதீர்கள். அதற்குப் பதிலாக, நேரடியாக அதிகாரப்பூர்வ இணையதளம் அல்லது செயலிக்குச் செல்லுங்கள்.
- அதிகாரப்பூர்வ தொலைபேசி எண் அல்லது செயலி போன்ற தனிப்பட்ட, நம்பகமான தொடர்பு வழிமுறையின் மூலம் கோரிக்கைகளைச் சரிபார்க்கவும்.
- செய்தி இணைப்பு மூலம் சென்றடையும் பக்கத்தில் ஒருபோதும் அடையாள விவரங்களையோ அல்லது OTP-களையோ உள்ளிடாதீர்கள்.
- சந்தேகத்திற்கிடமான செய்திகளைப் புகாரளித்து நீக்கவும், பின்னர் அனுப்புபவரைத் தடுக்கவும்.

எங்களைப் பின்தொடருங்கள் : @IndianCERT @cert_india

குரல் மற்றும் காணொளி டீப்ஃபேக்குகள் [விஷிங்]

இது எவ்வாறு செயல்படுகிறது?

அச்சுறுத்தல் செய்பவர்கள் குரல்களை நகலெடுக்கலாம் அல்லது உண்மையானது போல் தோற்றமளிக்கும் போலி வீடியோக்களை உருவாக்கலாம். முக்கியமான தகவல்களைப் பகிரும்படி, பணம் அனுப்பும்படி அல்லது விரைவாகச் செயல்படும்படி உங்களை வற்புறுத்துவதற்காக, அவர்கள் குடும்பத்தினர், சக ஊழியர்கள் அல்லது அதிகாரிகள் போல் நடிக்கக்கூடும்.

எப்படி அடையாளம் காண்பது?

- அசாதாரணமான அவசரம், பீதி, அல்லது யாரிடமும் சொல்ல வேண்டாம் என்பது போன்ற இரகசியத்தைக் காக்குமாறு கோருதல்.
- சற்றே மாறுபட்ட தொனி, வேகம், பின்னணி இரைச்சல் அல்லது ஒலித் தரம்.
- சாதாரண சரிபார்ப்பு அல்லது ஒப்புதல் செயல்முறைகளைத் தவிர்ப்பதற்கான கோரிக்கைகள்.
- பரிசு அட்டைகள், கிரிப்டோகரன்சி அல்லது பணப் பரிமாற்றம் மூலமான பணம் செலுத்துவதற்கான கோரிக்கைகள்.

பாதுகாப்பாக இருப்பது எப்படி?

- அழைப்பைத் துண்டித்துவிட்டு, அவருக்குத் தெரிந்த, சேமித்து வைத்த எண்ணிலிருந்து மீண்டும் அழைக்கவும்.
- அவசர காலங்களில் அடையாளத்தைச் சரிபார்க்க, குடும்பம் அல்லது பணியிடத்தில் ஒரு பாதுகாப்புச் சொல்லை அமைக்கவும்.
- அழைப்பு அல்லது காணொளியை மட்டும் அடிப்படையாகக் கொண்டு ஒருபோதும் பணம் செலுத்துவதற்கு அங்கீகாரம் அளிக்காதீர்கள். வேறொரு வழிமுறையின் மூலம் எழுத்துப்பூர்வமாக உறுதிப்படுத்தவும்.
- எதிர்வினையாற்றுவதற்கு முன் சற்று நிதானியுங்கள். அச்சுறுத்தல் செய்பவர்கள், உங்கள் முடிவெடுக்கும் திறனைக் குழப்புவதற்காக பீதியை நம்பியிருக்கிறார்கள்.

செயற்கை நுண்ணறிவு உதவியுடனான தீம்பொருள் மற்றும் தானியங்கி தாக்குதல்கள்

இது எவ்வாறு செயல்படுகிறது?

அச்சுறுத்தல் செய்பவர்கள், தீங்கிழைக்கும் குறியீடுகளை உருவாக்க அல்லது மறைக்கவும், திருடப்பட்ட கடவுச்சொற்களைப் பல தளங்களில் சோதிக்கவும், மற்றும் மேம்படுத்தல்கள் தேவைப்படும் அமைப்புகளைக் கண்டறியவும் செயற்கை நுண்ணறிவு கருவிகளைப் பயன்படுத்துகின்றனர். இது தாக்குதல்களை வேகமாகவும் பரவலாகவும் ஆக்குகிறது.

எப்படி அடையாளம் காண்பது?

- எதிர்பாராத உள்நுழைவு எச்சரிக்கைகள், கடவுச்சொல் மீட்டமைப்பு மின்னஞ்சல்கள் அல்லது நீங்கள் கோராத MFA தூண்டுதல்கள்
- உங்கள் கணக்குச் செயல்பாட்டில் பட்டியலிடப்பட்டுள்ள அறிமுகமில்லாத சாதனங்கள் அல்லது அமர்வுகள்
- வைரஸ் தடுப்பு எச்சரிக்கைகள், பாப்-அப்கள், அல்லது வழக்கத்திற்கு மாறாக மெதுவான சாதனச் செயல்பாடு
- உங்களுக்குத் தெரியாத கோப்புகள், அமைப்புகள் அல்லது உலாவி நீட்டிப்புகள்

பாதுகாப்பாக இருப்பது எப்படி?

- ஒவ்வொரு கணக்கிற்கும் தனித்துவமான, வலிமையான கடவுச்சொல்லைப் பயன்படுத்துங்கள்.
- அனைத்து முக்கிய கணக்குகளிலும் பல காரணி அங்கீகாரத்தை (MFA) இயக்கவும்.
- வைரஸ் தடுப்பு மென்பொருள், அமைப்புகள் மற்றும் செயலிகளைப் புதுப்பித்த நிலையில் வைத்திருங்கள்.
- எதிர்பாராத உள்நுழைவு அல்லது MFA எச்சரிக்கைகள் வந்தால் உடனடியாக நடவடிக்கை எடுக்கவும்.

போலி வலைத்தளங்கள் மற்றும் அடையாளத் திருட்டு

இது எவ்வாறு செயல்படுகிறது?

அச்சுறுத்தல் செய்பவர்கள், உங்கள் உள்நுழைவுச் சான்றுகள், OTP-கள் அல்லது கட்டண விவரங்களைத் திருடுவதற்காக, வங்கி அல்லது ஷாப்பிங் தளங்கள் போன்ற உண்மையானவை போலத் தோற்றமளிக்கும் வலைத்தளங்களையும் சாட்பாட்களையும் உருவாக்கலாம். அவர்கள் போலி அடையாளங்களை உருவாக்குவதற்காக, போலியான புகைப்படங்கள் அல்லது ஆவணங்களையும் பயன்படுத்தக்கூடும்.

எப்படி அடையாளம் காண்பது?

- கூடுதல் எழுத்துக்கள், கோடுகள் அல்லது வேறுபட்ட டொமைன் முடிவு போன்ற சிறிய மாற்றங்களுடன் கூடிய இணையதள முகவரிகள்.
- OTP-கள், PIN-கள் அல்லது முழு அட்டை எண்களைக் கேட்கும் சாட்பாட்கள் அல்லது முகவர்கள்.
- பரிச்சயமான இணையதளத்தில் HTTPS விடுபட்டிருப்பது அல்லது வழக்கத்திற்கு மாறான வடிவமைப்பு முரண்பாடுகள்.

பாதுகாப்பாக இருப்பது எப்படி?

- இணைப்புகளைச் சொடுக்குவதற்குப் பதிலாக, எப்போதும் அதிகாரப்பூர்வ URL-களை நேரடியாகத் தட்டச்சு செய்யவும் அல்லது சரிபார்க்கப்பட்ட புக்மார்க்குகளைப் பயன்படுத்தவும்.
- OTP-கள், PIN எண்கள் அல்லது முழு அட்டை விவரங்களையும் எந்தவொரு சாட்பாட் அல்லது "ஆதரவு முகவருடனும்" ஒருபோதும் பகிர வேண்டாம்.
- எங்கும் உள்நுழைவதற்கு முன், HTTPS உள்ளதா எனச் சரிபார்த்து, டொமைன் பெயரை உன்னிப்பாகக் கவனிக்கவும்.
- உங்கள் வங்கி அறிக்கைகளையும் கடன் அறிக்கையையும், வழக்கத்திற்கு மாறான செயல்பாடுகள் ஏதேனும் உள்ளதா எனத் தவறாமல் கண்காணிக்கவும்.

அபாய எச்சரிக்கைகள் சரிபார்ப்புப் பட்டியல்

செயற்கை நுண்ணறிவு மூலமான தாக்குதலின் இந்த அறிகுறிகளைக் கவனியுங்கள்:

- ☑ பணம், சான்றுகள் அல்லது ஒப்புதலுக்கான அவசரமான, அழுத்தமான கோரிக்கை
- ☑ "அறிந்த" ஒரு நபரிடமிருந்து வரும் அழைப்பு அல்லது வீடியோவில் ஏற்படும் சிறிய ஒலி/ஒளி முரண்பாடுகள்
- ☑ சாதாரண சரிபார்ப்பு/ஒப்புதல் நடைமுறைகளைத் தவிர்ப்பதற்கான கோரிக்கை
- ☑ அறிமுகமில்லாத அனுப்புநர் டொமைன் அல்லது சற்றே மாற்றப்பட்ட URL
- ☑ எதிர்பாராத MFA தூண்டுதல்கள் அல்லது நீங்கள் கோராத OTPகள்
- ☑ அதிகாரப்பூர்வமற்ற இணைப்புகள் வழியாகப் பாதுகாப்பு மென்பொருளை முடக்க அல்லது "சரிபார்க்க" கோரிக்கைகள்
- ☑ முன்பணம் அல்லது தனிப்பட்ட நிதி விவரங்கள் தேவைப்படும் வேலை/முதலீட்டுச் சலுகைகள்

சந்தேகம் ஏற்படும்போது – சற்று நிறுத்தி, சுயமாகச் சரிபார்த்துக் கொள்ளுங்கள், மேலும் அழுத்தத்தின் காரணமாகச் செயல்படாதீர்கள்.

இணையப் பாதுகாப்பு

உங்கள் கணக்குகளைப் பாதுகாக்கவும்

- ஒவ்வொரு கணக்கிற்கும் வலிமையான மற்றும் தனித்துவமான கடவுச்சொற்களைப் பயன்படுத்துங்கள்; அவற்றை பாதுகாப்பாக சேமிக்க கடவுச்சொல் மேலாளரைப் பயன்படுத்துங்கள்.
- பல காரணி அங்கீகாரத்தை (MFA) செயல்படுத்தவும்.
- OTPகள், PINகள், கடவுச்சொற்கள் அல்லது பாதுகாப்புக் குறியீடுகளை யாருடனும் ஒருபோதும் பகிராதீர்கள்.
- கூடுதல் பாதுகாப்பு அடுக்காக பயோமெட்ரிக் அங்கீகாரத்தை (கைரேகை/முக அடையாளம் காணுதல்) பயன்படுத்தவும்.

மின்னஞ்சல் மற்றும் இணையத்தைப் பயன்படுத்தும்போது பாதுகாப்பாக இருங்கள்

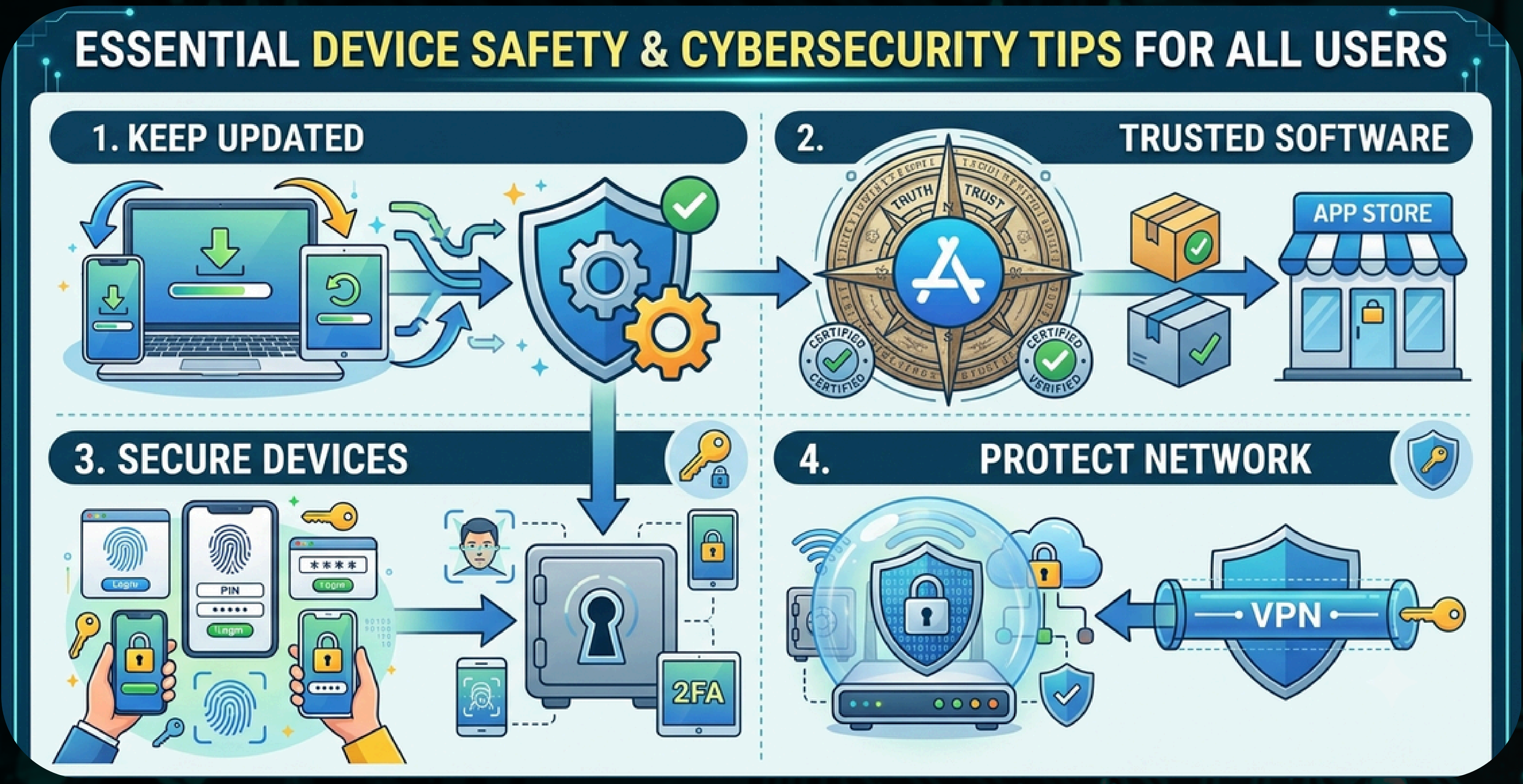
- சந்தேகத்திற்கிடமான அல்லது ஒரே மாதிரியான மின்னஞ்சல் முகவரிகள் உள்ளதா என அனுப்புநர் விவரங்களைக் கவனமாகச் சரிபார்க்கவும்.
- இணைப்புகளைச் சொடுக்குவதற்கு முன் சரிபார்க்கவும், எதிர்பாராத இணைப்புகளைத் திறப்பதைத் தவிர்க்கவும்.
- உள்நுழைவு அல்லது நிதி விவரங்களை உள்ளிடுவதற்கு முன் இணையதளத்தின் நம்பகத்தன்மையை உறுதிப்படுத்தவும்.
- சந்தேகம் ஏற்படும்போது, செயல்படுவதற்கு முன் நிறுத்திச் சரிபார்க்கவும்.

ஏதேனும் தவறு நடப்பதற்கு முன் தயாராகுங்கள்

- ஆஃப்லைனில் அல்லது பாதுகாப்பான கிளவுட் சேவையில் சேமிக்கப்பட்ட முக்கியமான கோப்புகளின் காப்புப்பிரதிகளைத் தவறாமல் பராமரிக்கவும்.
- கணக்கு மீட்புத் தகவல்களை (மின்னஞ்சல்/தொலைபேசி) புதுப்பித்து, பாதுகாப்பாக வைத்திருக்கவும்.

எங்களைப் பின்தொடருங்கள் : @IndianCERT @cert_india

சாதன பாதுகாப்பு



⋙ சாதனங்களைப் புதுப்பித்த நிலையில் வைத்திருங்கள்

- அறியப்பட்ட பாதிப்புகளைச் சரிசெய்ய, இயக்க முறைமைகள், செயலிகள், உலாவிகள் மற்றும் பாதுகாப்பு மென்பொருட்களைத் தவறாமல் புதுப்பிக்கவும்.
- முடிந்தவரை தானியங்கு புதுப்பிப்புகளைச் செயல்படுத்தவும்.

⋙ நம்பகமான மென்பொருளை மட்டும் நிறுவவும்

- அசல் மென்பொருளைப் பயன்படுத்துங்கள் மற்றும் அதிகாரப்பூர்வ ஆப் ஸ்டோர்கள் அல்லது நம்பகமான மூலங்களிலிருந்து மட்டுமே பயன்பாடுகளை நிறுவவும்.
- நம்பகமான வைரஸ் தடுப்பு அல்லது பாதுகாப்பு தீர்வுகளைப் பயன்படுத்தி, அவற்றை அவ்வப்போது புதுப்பித்துக் கொள்ளுங்கள்.

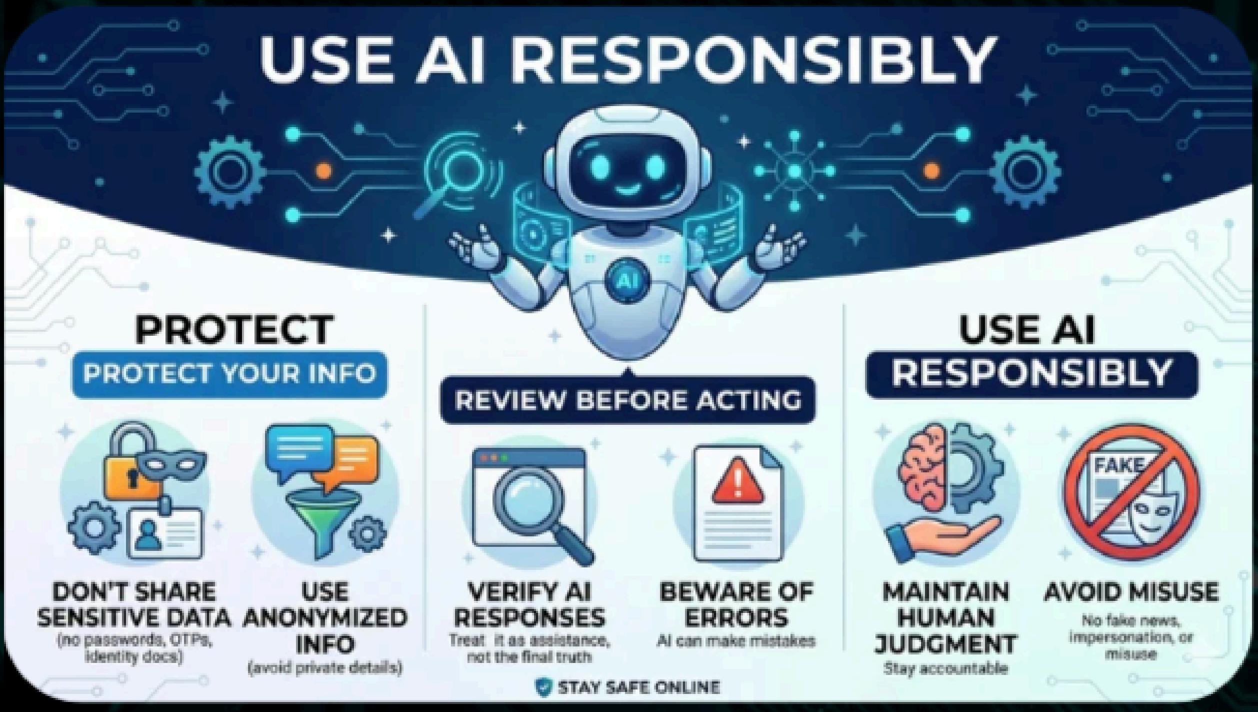
⋙ உங்கள் சாதனங்களையும் கணக்குகளையும் பாதுகாக்கவும்

- அனைத்து சாதனங்களிலும் வலிமையான கடவுச்சொற்களை அல்லது திரைப்பூட்டுகளைப் பயன்படுத்துங்கள்.
- சாதனக் குறியாக்க மற்றும் பாதுகாப்பு அம்சங்கள் கிடைக்கும்போதெல்லாம் அவற்றைச் செயல்படுத்தவும்.
- தேவையற்ற விண்ணப்பங்களையும் அனுமதிகளையும் மதிப்பாய்வு செய்து அகற்றவும்.

⋙ உங்கள் நெட்வொர்க் இணைப்பைப் பாதுகாக்கவும்

- உங்கள் Wi-Fi-ஐ வலிமையான கடவுச்சொல் மூலம் பாதுகாத்து, இயல்புநிலை ரூட்டர் சான்றுகளை மாற்றவும்.
- புதுப்பிக்கப்பட்ட ரூட்டர் ஃபார்ம்வேரையும் பாதுகாப்பான நெட்வொர்க் அமைப்புகளையும் பயன்படுத்தவும்.
- பாதுகாப்பற்ற வலையமைப்புகள் வழியாக முக்கியமான கணக்குகளை அணுகுவதையோ அல்லது இரகசியத் தகவல்களைப் பகிர்வதையோ தவிர்க்கவும்.

செயற்கை நுண்ணறிவை பொறுப்புடன் பயன்படுத்துங்கள்



உங்கள் தனிப்பட்ட தகவல்களைப் பாதுகாக்கவும்

- தனிப்பட்ட, நிதி, உடல்நலம், அலுவல் அல்லது இரகசியத் தகவல்களைப் பொது செயற்கை நுண்ணறிவுக் கருவிகளிலோ அல்லது அறியப்படாத இணையச் சேவைகளிலோ உள்ளிடாதீர்கள்.
- கடவுச்சொற்கள், OTP-கள், கணக்கு எண்கள், அடையாள ஆவணங்கள், வாடிக்கையாளர் தரவுகள் அல்லது தனிப்பட்ட உரையாடல்கள் போன்ற முக்கியமான விவரங்களைப் பகிர்வதைத் தவிர்க்கவும்.
- செயற்கை நுண்ணறிவு கருவிகளிடம் உதவி கேட்கும்போது, அடையாளம் மறைக்கப்பட்ட அல்லது பொதுவான தகவல்களைப் பயன்படுத்தவும்.

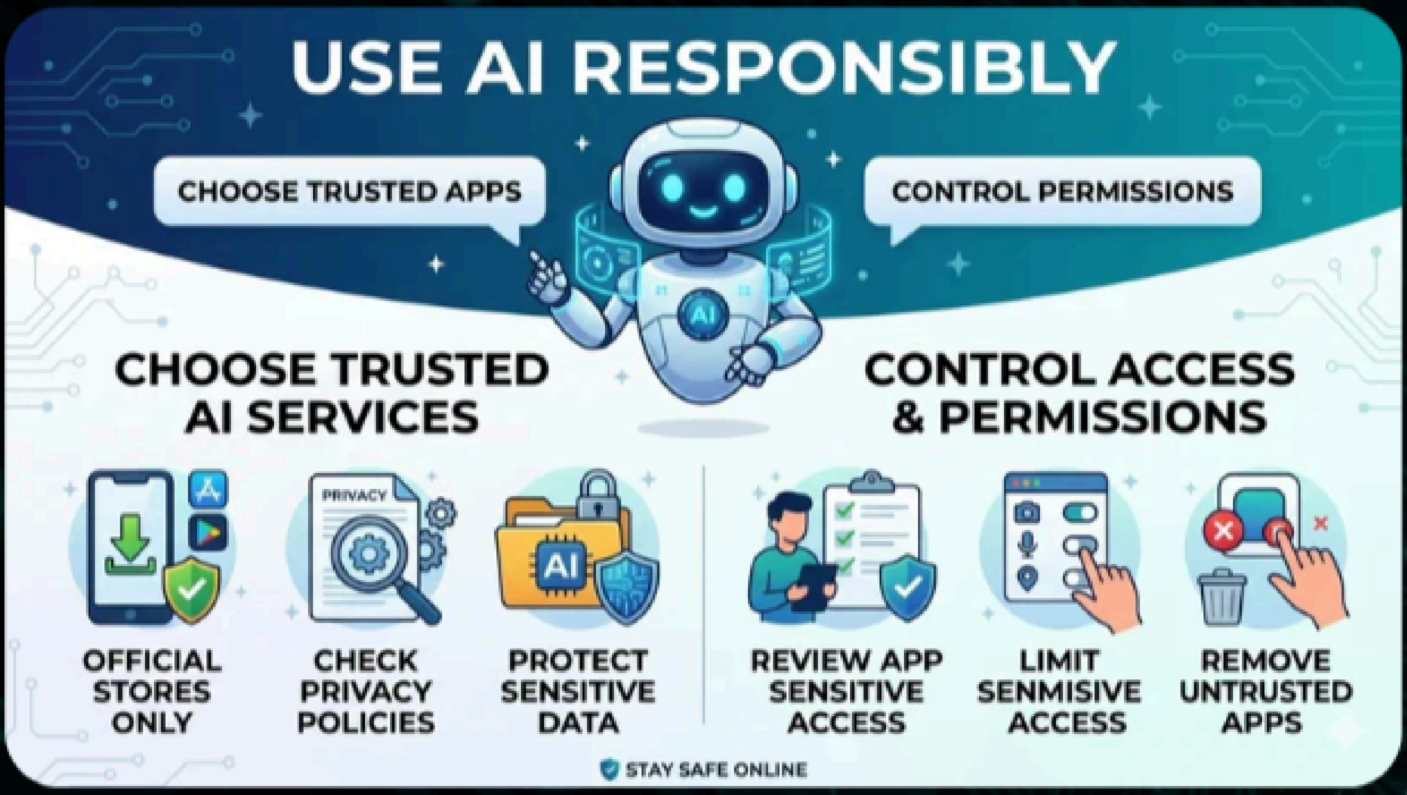
பகிர்வதற்கு அல்லது செயல்படுவதற்கு முன் மதிப்பாய்வு செய்யவும்

- செயற்கை நுண்ணறிவால் உருவாக்கப்படும் பதில்களை உதவியாகக் கருதுங்கள், இறுதி உண்மை ஆதாரமாகக் கருதாதீர்கள்.
- நிதி, சட்ட, தொழில்முறை அல்லது தனிப்பட்ட முடிவுகளுக்காக முக்கியமான தகவல்களைப் பயன்படுத்துவதற்கு முன்பு அவற்றைச் சரிபார்க்கவும்.
- செயற்கை நுண்ணறிவு கருவிகள் தவறான, முழுமையற்ற அல்லது தவறாக வழிநடத்தும் தகவல்களை உருவாக்கக்கூடும் என்பதை நினைவில் கொள்ளுங்கள்.

செயற்கை நுண்ணறிவு கருவிகளைப் பொறுப்புடன் பயன்படுத்துங்கள்

- உங்கள் பணி மற்றும் கற்றலுக்கு ஆதரவளிக்க செயற்கை நுண்ணறிவைப் பயன்படுத்துங்கள், ஆனால் மனித பகுத்தறிவையும் பொறுப்புணர்வையும் பேணுங்கள்.
- தவறான தகவல்களை உருவாக்கவோ பரப்பவோ, மற்றவர்களைப் போல் ஆள்மாறாட்டம் செய்யவோ, அல்லது ஒருவரின் தனிப்பட்ட தரவுகளைத் தவறாகப் பயன்படுத்தவோ செயற்கை நுண்ணறிவைப் பயன்படுத்தாதீர்கள்.

நம்பகமான செயலிகளைத் தேர்ந்தெடுக்கவும்



செயலி அணுகல் மற்றும் அனுமதிகளைக் கட்டுப்படுத்துதல்

- செயற்கை நுண்ணறிவுப் பயன்பாடுகள் மற்றும் டிஜிட்டல் உதவியாளர்களுக்கு வழங்கப்பட்ட அனுமதிகளை மதிப்பாய்வு செய்யவும்.
- கேமரா, மைக்ரோஃபோன், தொடர்புகள் அல்லது இருப்பிடம் போன்ற அம்சங்களுக்குத் தேவைப்படும்போது மட்டும் அணுகலை அனுமதிக்கவும்.
- தேவையற்ற அனுமதிகளை நீக்குங்கள் மற்றும் நம்பகமற்ற மூலங்களிலிருந்து வரும் செயலிகளை நிறுவல் நீக்கம் செய்யுங்கள்.

நம்பகமான AI சேவைகளைத் தேர்ந்தெடுக்கவும்

- நம்பகமான வழங்குநர்களின் AI செயலிகளைப் பயன்படுத்துங்கள், மேலும் அவற்றை அதிகாரப்பூர்வ ஆப் ஸ்டோர்களில் இருந்து மட்டுமே பதிவிறக்கம் செய்யுங்கள்.
- செயற்கை நுண்ணறிவு சேவைகளைப் பயன்படுத்துவதற்கு முன், தனியுரிமை அமைப்புகள், பயன்பாட்டு விதிமுறைகள் மற்றும் தரவு கையாளும் நடைமுறைகளை மதிப்பாய்வு செய்யவும்.
- பாதுகாப்புக் கட்டுப்பாடுகள் சரிபார்க்கப்படும் வரை, AI கருவிகளை முக்கியமான கணக்குகள் அல்லது கோப்புகளுடன் இணைப்பதைத் தவிர்க்கவும்.

Report Cyber Security Incidents to CERT-In

For reporting Cyber Security Incidents to CERT-In:

Visit website: ***https://www.cert-in.org.in***

Email: ***incident@cert-in.org.in***

Toll Free Phone: ***+91-1800-11-4949***

Toll Free Fax: ***+91-1800-11-6969***

Information Desk

Phone: ***+91-11-22902657***

Follow us :

@IndianCERT

@cert_india

WEBSITE
https://www.cert-in.org.in/

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Awareness Booklet
https://cert-in.org.in/AwarenessBooklets.jsp

Security Tools
https://www.csk.gov.in/security-tools.html