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

एआई जागरूकता गाइड

साइबर स्वच्छता की संस्कृति का विकास करें

#साइबरहाइजीनहमारीसंस्कृति



राष्ट्रीय साइबर सुरक्षा जागरूकता माह (अक्टूबर 2026)

द्वारा आयोजित किया गया

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया समूह

हमारे पृष्ठ का अनुसरण करें :

@IndianCERT

@cert_india

विषयसूची

प्रस्तावना 3

एआई-आधारित फ़िशिंग और सामाजिक इंजीनियरिंग । 4

आवाज और वीडियो डीपफेक (विशिंग) । 5

कृत्रिम बुद्धिमत्ता की मदद से संचालित मैलवेयर और स्वचालित हमले । 6

फर्जी वेबसाइटें और पहचान की चोरी । 7

खतरे के संकेतों की पहचान की सूची । 8

ऑनलाइन सुरक्षा प्रणाली । 9

उपकरणों की सुरक्षा । 10

एआई का उत्तरदायी उपयोग करें । 11

विश्वसनीय ऐप्स का चयन करें । 12

साइबर सुरक्षा से संबंधित घटनाओं की सूचना CERT-In को दें। 13

प्रस्तावना

कृत्रिम बुद्धिमत्ता (एआई) हमारे जीवन, कार्य और संवाद के तरीकों में परिवर्तन ला रही है। यह नवाचार को प्रोत्साहित करती है, उत्पादकता को बढ़ाती है और विभिन्न क्षेत्रों में जटिल समस्याओं के समाधान में सहायता करती है। हालांकि, इस तकनीक का दुरुपयोग भी खतरा उत्पन्न करने वाले तत्वों द्वारा अधिक उन्नत और विश्वसनीय साइबर खतरों को उत्पन्न करने के लिए किया जा रहा है।

कृत्रिम बुद्धिमत्ता (एआई) के कारण डिजिटल खतरों की पहचान करना अधिक चुनौतीपूर्ण हो गया है, क्योंकि हमलावर अब अत्यधिक यथार्थवादी ईमेल, संदेश, ऑडियो, वीडियो और वेबसाइट बना सकते हैं। व्याकरण की गलतियाँ, असामान्य प्रारूपण या स्पष्ट त्रुटियाँ जैसे पारंपरिक चेतावनी संकेत अब विश्वसनीय संकेतक नहीं रह गए हैं। सत्यापन और जिम्मेदार डिजिटल व्यवहार पहले से कहीं अधिक आवश्यक हो गए हैं।

हम हर दिन जिन एआई उपकरणों और स्मार्ट डिवाइसों का उपयोग करते हैं, यदि उनका सावधानीपूर्वक उपयोग नहीं किया गया, तो इससे गोपनीयता और सुरक्षा से संबंधित नए जोखिम उत्पन्न हो सकते हैं। अविश्वसनीय एआई एप्लिकेशनों के साथ व्यक्तिगत या गोपनीय जानकारी साझा करना, अनावश्यक अनुमतियाँ देना, या बिना सत्यापन के एआई द्वारा उत्पन्न जानकारी पर भरोसा करना व्यक्तियों और संगठनों को सुरक्षा जोखिमों में डाल सकता है।

इंडियन कंप्यूटर इमरजेंसी रिस्पांस टीम (CERT-In) द्वारा तैयार की गई "एआई साइबर जागरूकता" पर यह पुस्तिका सामान्य नागरिकों, कर्मचारियों और डिजिटल उपयोगकर्ताओं के लिए है, न कि केवल साइबर सुरक्षा विशेषज्ञों के लिए। यह स्पष्ट करती है कि एआई किस प्रकार डिजिटल खतरों के परिदृश्य को परिवर्तित कर रहा है और व्यक्तिगत जानकारी, उपकरणों और ऑनलाइन पहचान की सुरक्षा के लिए सरल, व्यावहारिक कदम सुझाती है जिनका पालन सभी कर सकते हैं।

एआई-समर्थित फ़िशिंग और सामाजिक इंजीनियरिंग



यह प्रक्रिया किस प्रकार कार्य करती है?

आजकल, अपराधी ऐसे ईमेल और टेक्स्ट संदेश भेजते हैं जो देखने में वास्तविक और त्रुटिहीन लगते हैं। वे आपके बारे में जानकारी, जैसे कि आपका पेशा, आपके द्वारा उपयोग की जाने वाली सेवाएं या हाल की गतिविधियां, का उपयोग करके संदेशों को व्यक्तिगत बनाते हैं। चूंकि ये संदेश अच्छी तरह से लिखे गए होते हैं, इसलिए इन्हें पहचानना बहुत कठिन हो जाता है।

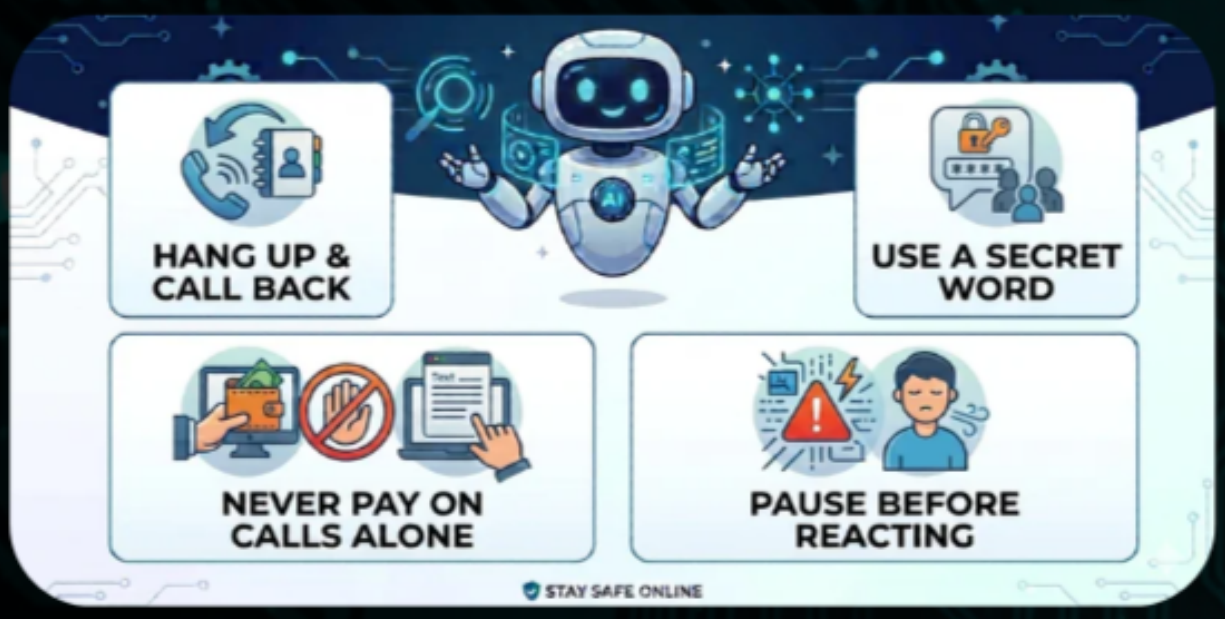
पहचान कैसे की जाए?

- यह संदेश आपको अत्यंत विशिष्ट प्रतीत होता है, लेकिन यह अचानक आता है।
- इसमें एक महत्वपूर्ण या धमकी भरा स्वरूप अपनाया जाता है और तात्कालिक कार्रवाई की आवश्यकता होती है।
- यह आपसे किसी लिंक पर क्लिक करने, खाते की पुष्टि करने, पासवर्ड को रीसेट करने या भुगतान करने के लिए अनुरोध करता है।
- प्रेषक का पता लगभग सही प्रतीत हो रहा है, लेकिन पूरी तरह से नहीं।

सुरक्षित रहने के उपाय क्या हैं?

- अनचाहे संदेशों में शामिल लिंक पर क्लिक न करें। इसके बजाय सीधे आधिकारिक वेबसाइट या ऐप पर जाएं।
- अनुरोधों को किसी अलग, विश्वसनीय संपर्क माध्यम, जैसे कि आधिकारिक फोन नंबर या एप्लिकेशन के माध्यम से सत्यापित करें।
- किसी संदेश लिंक के माध्यम से खोले गए पृष्ठ पर कभी भी क्रेडेंशियल या ओटीपी दर्ज न करें।
- संदिग्ध संदेशों की सूचना दें और उन्हें हटा दें, फिर भेजने वाले को अवरुद्ध कर दें।

आवाज और वीडियो डीपफेक (विशिंग)



यह प्रक्रिया किस प्रकार कार्य करती है?

खतरा उत्पन्न करने वाले व्यक्ति आवाज की नकल कर सकते हैं या ऐसे नकली वीडियो बना सकते हैं जो देखने और सुनने में वास्तविक प्रतीत होते हैं। वे परिवार के सदस्य, सहकर्मी या अधिकारी के रूप में सामने आकर आपको संवेदनशील जानकारी साझा करने, पैसे भेजने या तात्कालिक कार्रवाई करने के लिए मजबूर कर सकते हैं।

पहचान कैसे की जाए?

- असामान्य जल्दी, चिंता, या गोपनीयता बनाए रखने का अनुरोध, जैसे कि किसी को न बताना।
- आवाज का स्वर, गति, पृष्ठभूमि का शोर या ऑडियो गुणवत्ता में थोड़ी असंगति।
- सामान्य सत्यापन या अनुमोदन प्रक्रियाओं को अनदेखा करने के लिए अनुरोध।
- उपहार कार्ड, क्रिप्टोकरेंसी या वायर ट्रांसफर के जरिए भुगतान के लिए अनुरोध।

सुरक्षित रहने के उपाय क्या हैं?

- फोन काट दें और उस व्यक्ति को उनके ज्ञात, सहेजे गए नंबर पर वापस कॉल करें।
- आपातकालीन स्थिति में पहचान की पुष्टि करने के लिए परिवार या कार्यस्थल पर एक सुरक्षित शब्द निर्धारित करें।
- केवल कॉल या वीडियो कॉल के आधार पर भुगतान को कभी भी स्वीकृत न करें। किसी अन्य तरीके से लिखित रूप में इसकी पुष्टि करें।
- प्रतिक्रिया देने से पहले कुछ क्षण रुकें। हमलावर आपकी चिंता का लाभ उठाकर आपके निर्णय लेने की क्षमता को प्रभावित करते हैं।

एआई-समर्थित मैलवेयर और स्वचालित हमले



यह प्रक्रिया किस प्रकार कार्य करती है?

हमलावर दुर्भावनापूर्ण कोड बनाने या छिपाने, कई साइटों पर चुराए गए पासवर्ड का परीक्षण करने और अपडेट की आवश्यकता वाले सिस्टम की पहचान करने के लिए एआई उपकरण का उपयोग करते हैं। इससे हमले तेज़ और व्यापक हो जाते हैं।

पहचान कैसे की जाए?

- अप्रत्याशित लॉगिन चेतावनी, पासवर्ड रीसेट ईमेल, या ऐसे मल्टी-फैक्टर प्रमाणीकरण संकेत जो आपने नहीं मांगे हों
- आपके खाते की गतिविधि में अनजान उपकरण या सत्र शामिल हैं।
- एंटीवायरस अलर्ट, पॉप-अप या डिवाइस का असामान्य रूप से धीमा प्रदर्शन
- ऐसी फ़ाइलें, सेटिंग्स या ब्राउज़र एक्सटेंशन जिन्हें आप पहचानते नहीं हैं

सुरक्षित रहने के उपाय क्या हैं?

- हर खाते के लिए एक विशिष्ट, मजबूत पासवर्ड का उपयोग करें।
- सभी महत्वपूर्ण खातों पर बहु-कारक प्रमाणीकरण (एमएफए) सक्रिय करें।
- एंटीवायरस सॉफ़्टवेयर, सिस्टम और ऐप्स को निरंतर अपडेट करते रहें।
- अप्रत्याशित लॉगिन या एमएफए अलर्ट प्राप्त होने पर तुरंत प्रतिक्रिया दें।

फर्जी वेबसाइटें और पहचान की चोरी



यह प्रक्रिया किस प्रकार कार्य करती है?

अपराधी आपके लॉगिन क्रेडेंशियल, ओटीपी या भुगतान विवरण चुराने के लिए बैंकिंग या शॉपिंग पोर्टल जैसी दिखने वाली मिलती-जुलती वेबसाइटें और चैटबॉट बना सकते हैं। वे धोखाधड़ी पहचान बनाने के लिए नकली तस्वीरें या दस्तावेज़ों का भी उपयोग कर सकते हैं।

पहचान कैसे की जाए?

- वेबसाइट के यूआरएल में छोटे परिवर्तन, जैसे अतिरिक्त अक्षर, हाइफ़न या डोमेन के अंत में कोई भिन्न नाम।
- चैटबॉट या एजेंट ओटीपी, पिन या संपूर्ण कार्ड नंबर मांग रहे हैं।
- किसी परिचित वेबसाइट पर HTTPS की अनुपस्थिति या असामान्य डिज़ाइन संबंधी असंगतियाँ होना।

सुरक्षित रहने के उपाय क्या हैं?

- लिंक पर क्लिक करने के बजाय हमेशा आधिकारिक यूआरएल को सीधे टाइप करें या सत्यापित बुकमार्क का उपयोग करें।
- किसी भी चैटबॉट या "सहायता एजेंट" के साथ कभी भी ओटीपी, पिन या कार्ड की संपूर्ण जानकारी साझा न करें।
- किसी भी साइट पर लॉग इन करने से पहले HTTPS की पुष्टि करें और डोमेन नाम पर ध्यान दें।
- अपने बैंक स्टेटमेंट और क्रेडिट रिपोर्ट पर नियमित रूप से ध्यान दें ताकि किसी भी अनजान गतिविधि का पता लगाया जा सके।

खतरे के संकेतों की सूची

कृत्रिम बुद्धिमत्ता के माध्यम से होने वाले हमलों के इन संकेतों पर ध्यान दें:

- धन, प्रमाण पत्र या अनुमोदन के लिए तात्कालिक, दबावयुक्त अनुरोध
- किसी "पहचाने गए" व्यक्ति के कॉल या वीडियो में ऑडियो/वीडियो में छोटी विसंगतियां
- सामान्य सत्यापन/अनुमोदन प्रक्रियाओं को नजरअंदाज करने का अनुरोध
- अज्ञात प्रेषक डोमेन या थोड़ा परिवर्तित यूआरएल
- अप्रत्याशित MFA प्रॉम्प्ट या OTP जिसे आपने अनुरोध नहीं किया था
- सुरक्षा सॉफ़्टवेयर को बंद करने या अनधिकृत लिंक के माध्यम से "सत्यापित" करने के लिए अनुरोध
- नौकरी/निवेश के प्रस्ताव जिनमें अग्रिम भुगतान या व्यक्तिगत वित्तीय जानकारी की आवश्यकता होती है

जब संदेह हो, तो रुकें, स्वतंत्र रूप से सत्यापित करें और दबाव में आकर कोई निर्णय न लें।

ऑनलाइन सुरक्षा प्रणाली



अपने खातों की सुरक्षा सुनिश्चित करें|

- प्रत्येक खाते के लिए एक मजबूत और अद्वितीय पासवर्ड का चयन करें; उन्हें सुरक्षित रूप से संग्रहित करने के लिए पासवर्ड प्रबंधक का उपयोग करें।
- जहां भी संभव हो, मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए) को सक्रिय करें।
- कभी भी किसी के साथ ओटीपी, पिन, पासवर्ड या सुरक्षा कोड साझा मत करें।
- अतिरिक्त सुरक्षा स्तर के रूप में बायोमेट्रिक प्रमाणीकरण (फिंगरप्रिंट/चेहरे की पहचान) का उपयोग करें।

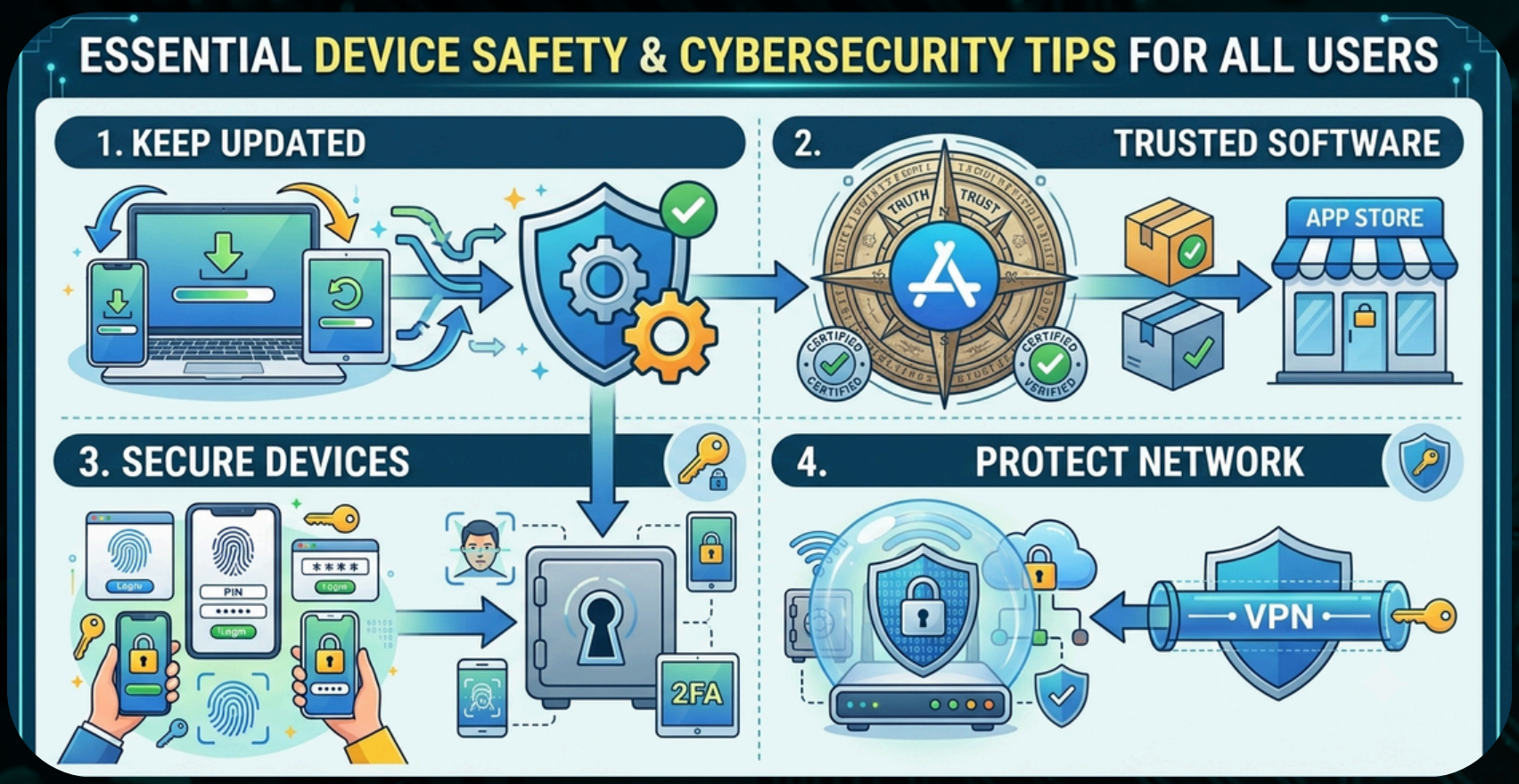
ईमेल और इंटरनेट का उपयोग करते समय सुरक्षा का ध्यान रखें|

- संदिग्ध या समान ईमेल पतों के लिए प्रेषक की जानकारी की बारीकी से जांच करें।
- लिंक पर क्लिक करने से पहले उसकी जांच करें और अनजान अटैचमेंट खोलने से बचें।
- लॉगिन या वित्तीय जानकारी दर्ज करने से पहले वेबसाइट की विश्वसनीयता की जांच करें।
- जब संदेह हो, तो कार्य करने से पहले ठहरें और पुष्टि करें।

कुछ गलत होने से पहले तैयारी कर लें।

- महत्वपूर्ण फाइलों का नियमित रूप से बैकअप लें और उन्हें ऑफलाइन या किसी सुरक्षित क्लाउड सेवा में संग्रहित करें।
- खाता पुनर्प्राप्ति से संबंधित जानकारी (ईमेल/फ़ोन) को अपडेट और सुरक्षित रखें।

उपकरणों की सुरक्षा



उपकरणों को अद्यतित रखें

- **ज्ञात कमजोरियों को समाप्त करने के लिए ऑपरेटिंग सिस्टम, एप्लिकेशन, ब्राउज़र और सुरक्षा सॉफ़्टवेयर को समय-समय पर अपडेट करें।**
- जहां भी संभव हो, स्वचालित अपडेट सक्रिय करें।

केवल विश्वसनीय सॉफ़्टवेयर स्थापित करें

- असली सॉफ़्टवेयर का उपयोग करें और केवल आधिकारिक ऐप स्टोर या विश्वसनीय स्रोतों से एप्लिकेशन स्थापित करें।
- विश्वसनीय एंटीवायरस या सुरक्षा समाधान का उपयोग करें और उन्हें नियमित रूप से अपडेट करते रहें।

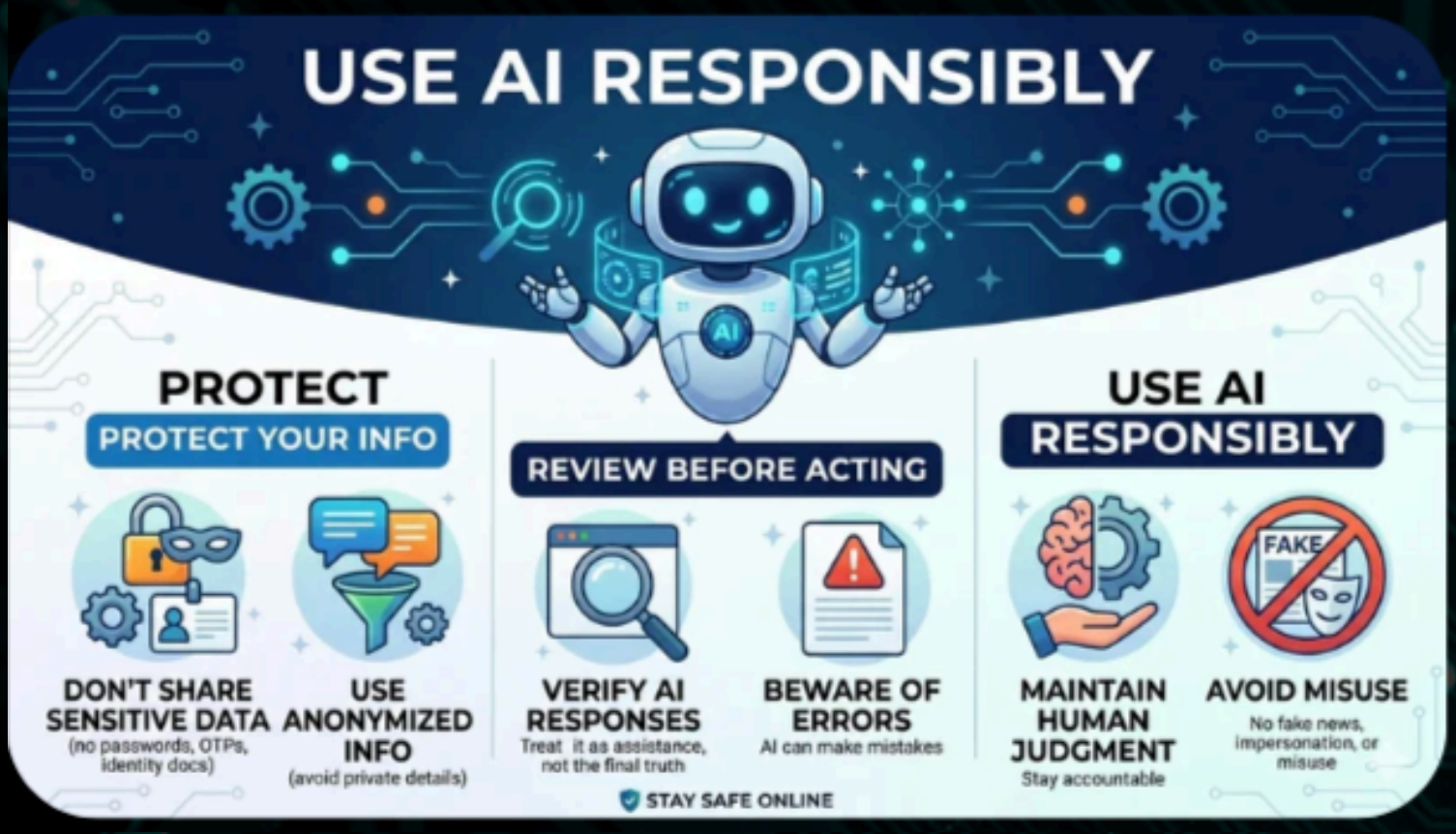
अपने उपकरणों और खातों की सुरक्षा सुनिश्चित करें

- सभी उपकरणों पर मजबूत पासवर्ड या स्क्रीन लॉक का उपयोग करना आवश्यक है।
- जब भी संभव हो, डिवाइस एन्क्रिप्शन और सुरक्षा विशेषताओं को सक्रिय करें।
- अनावश्यक एप्लिकेशन और अनुमतियों की जाँच करें और उन्हें हटा दें।

अपने नेटवर्क कनेक्शन की सुरक्षा सुनिश्चित करें।

- अपने वाई-फाई को एक मजबूत पासवर्ड से सुरक्षित करें और राउटर के डिफ़ॉल्ट लॉगिन विवरण को बदलें।
- राउटर के नवीनतम फर्मवेयर और सुरक्षित नेटवर्क सेटिंग्स का उपयोग करें।
- असुरक्षित नेटवर्क पर संवेदनशील खातों तक पहुँचने या गोपनीय जानकारी साझा करने से बचना चाहिए।

एआई का उत्तरदायी उपयोग करें



अपनी व्यक्तिगत जानकारी की सुरक्षा सुनिश्चित करें

- **सार्वजनिक एआई उपकरणों या अज्ञात ऑनलाइन सेवाओं में व्यक्तिगत, वित्तीय, स्वास्थ्य संबंधी, आधिकारिक या गोपनीय जानकारी न डालें।**
- पासवर्ड, ओटीपी, खाता संख्या, पहचान पत्र, ग्राहक जानकारी या व्यक्तिगत संवाद जैसी संवेदनशील जानकारी साझा करने से बचें।
- एआई उपकरणों से सहायता मांगते समय गुमनाम या सामान्य जानकारी का उपयोग करें।

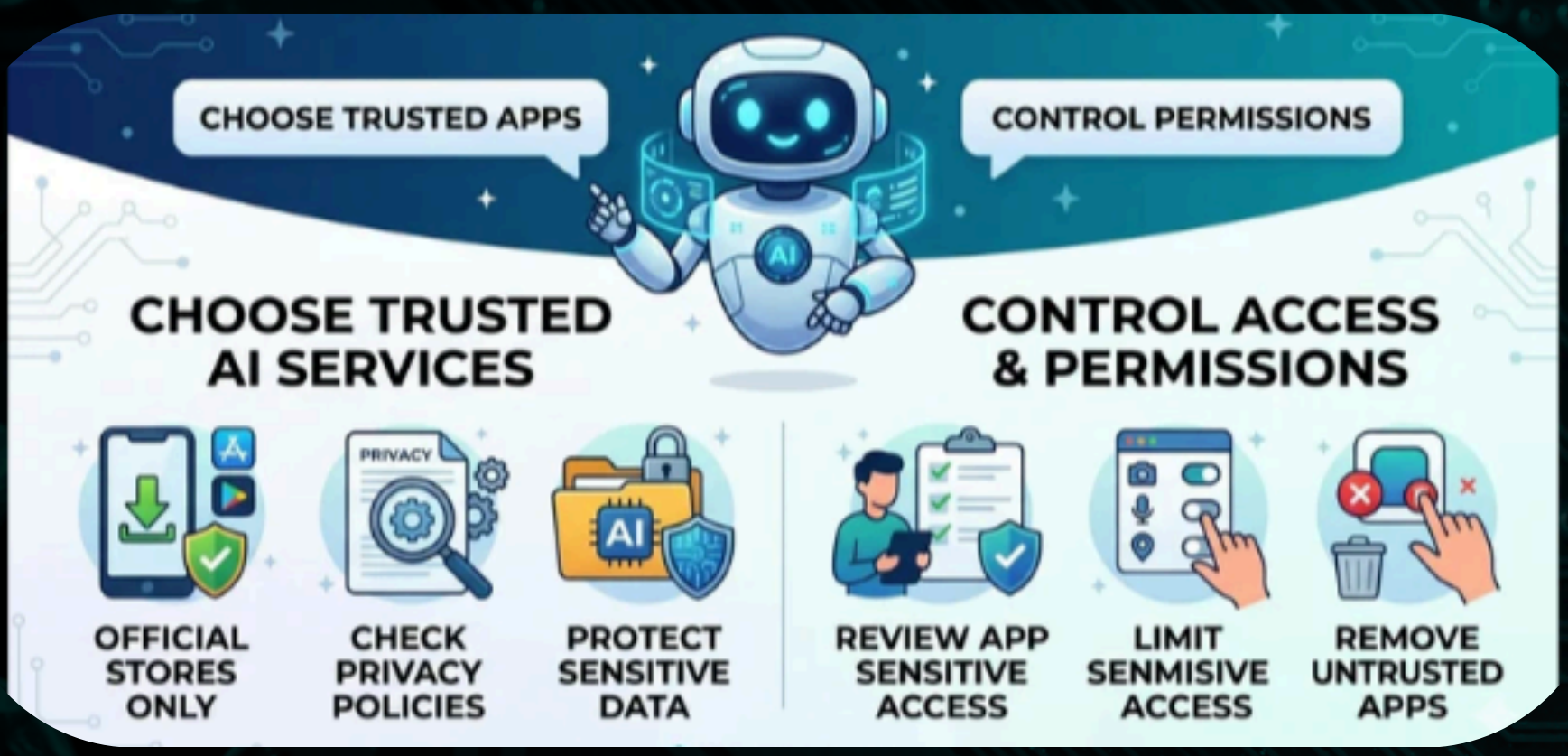
साझा करने या क्रिया करने से पहले समीक्षा करें

- **कृत्रिम बुद्धिमत्ता द्वारा उत्पन्न प्रतिक्रियाओं को एक सहायता के रूप में समझें, न कि सत्य के अंतिम स्रोत के रूप में।**
- वित्तीय, कानूनी, व्यावसायिक या व्यक्तिगत निर्णय लेने से पहले महत्वपूर्ण जानकारी की पुष्टि अवश्य कर लें।
- ध्यान दें कि एआई उपकरण गलत, अधूरी या भ्रामक जानकारी उत्पन्न कर सकते हैं।

एआई उपकरणों का जिम्मेदारी से उपयोग करें

- अपने कार्य और अध्ययन में सहायता के लिए एआई का उपयोग करें, लेकिन मानव निर्णय और उत्तरदायित्व को बनाए रखें।
- कृत्रिम बुद्धिमत्ता का उपयोग गलत जानकारी उत्पन्न करने या फैलाने, दूसरों की पहचान अपनाने या किसी के व्यक्तिगत डेटा का दुरुपयोग करने के लिए नहीं किया जाना चाहिए।

विश्वसनीय ऐप्स का चयन करें|



ऐप की पहुंच और अनुमतियों का प्रबंधन करें

- एआई अनुप्रयोगों और डिजिटल सहायकों को प्रदान की गई अनुमतियों का मूल्यांकन करें।
- कैमरा, माइक्रोफोन, संपर्क या स्थान जैसी सुविधाओं तक पहुंच की अनुमति केवल तब दें जब यह आवश्यक हो।
- अनावश्यक अनुमतियाँ समाप्त करें और अविश्वसनीय स्रोतों से ऐप्स को हटा दें।

विश्वसनीय एआई सेवाओं का चयन करें।

- प्रतिष्ठित प्रदाताओं के एआई एप्लिकेशन का उपयोग करें और उन्हें केवल अधिकृत ऐप स्टोर से डाउनलोड करें।
- एआई सेवाओं का उपयोग करने से पूर्व गोपनीयता सेटिंग्स, उपयोग की शर्तें और डेटा प्रबंधन नीतियों की जांच करें।
- सुरक्षा नियंत्रणों की पुष्टि किए बिना एआई उपकरणों को संवेदनशील खातों या फ़ाइलों से जोड़ने से बचें।

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

certin Enhancing Cyber Security in India

ISEA Information Security Education & Awareness

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

Digital India Power To Empower

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

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