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

AI जागरूकता गाइड

साइबर स्वच्छता के संस्कृति बनाये |

#साइबरस्वच्छताअपनी संस्कृति



राष्ट्रीय साइबर सुरक्षा जागरूकता माह (अक्टूबर 2026)

प्रकाशक

भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया टीम

हमरा सब के फॉलो करू :

@IndianCERT

@cert_india

विषयवस्तु तालिका

भूमिका 3

AI-बढ़ा फिशिंग एवं सोशल इंजीनियरिंग 4

आवाज एवं वीडियो deepfakes (vishing) 5

AI-सहायता प्राप्त मैलवेयर एवं स्वचालित हमला 6

नकली वेबसाइट एवं पहचान चोरी 7

लाल झंडा चेकलिस्ट 8

ऑनलाइन सुरक्षा 9

डिवाइस सुरक्षा 10

AI के जिम्मेदारी से प्रयोग करे | 11

विश्वसनीय ऐप्स चुनू 12

साइबर सुरक्षा घटनाक कें सीईआरटी-इन कें रिपोर्ट करूं 13

भूमिका

आर्टिफिशियल इंटेलिजेंस (AI) हमरऽ जीबै, काम करै, आरू संवाद करै के तरीका मं बदलाव लानी रहलऽ छै । इ नवाचार कें सक्षम बनायत छै, उत्पादकता मे सुधार करयत छै, आ विभिन्न क्षेत्रक मे जटिल समस्याक कें हल करय मे मदद करयत छै. लेकिन, वही तकनीक के दुरुपयोग खतरा अभिनेता सिनी द्वारा भी करलौ जाय रहलौ छै ताकि आरू उन्नत आरू आश्वस्त करै वाला साइबर खतरा पैदा करलौ जाय सकै ।

AI डिजिटल खतरा कें पहचान करनाय मुश्किल बना रहल छै, कियाकि हमलावर आब अत्यधिक यथार्थवादी ईमेल, संदेश, ऑडियो, वीडियो, आ वेबसाइट बना सकय छै. पारंपरिक चेतावनी संकेत, जेना कि खराब व्याकरण, असामान्य प्रारूपण, या स्पष्ट गलती, आब विश्वसनीय संकेतक नहि भ सकय छै. सत्यापन आ जिम्मेदार डिजिटल प्रथा पहिले सं बेसि महत्वपूर्ण भ गेल छै.

AI टूल आ स्मार्ट डिवाइस जे हम रोज उपयोग करय छी, यदि ओकर सावधानी सं उपयोग नहि कैल जाय त नव गोपनीयता आ सुरक्षा जोखिम कें शुरूआत कयर सकय छै. अविश्वसनीय AI अनुप्रयोगक कें साथ व्यक्तिगत या गोपनीय जानकारी साझा करनाय, अनावश्यक अनुमति देनाय, या बिना सत्यापन कें AI उत्पन्न जानकारी पर भरोसा करनाय व्यक्ति आ संगठनक कें सुरक्षा जोखिम कें सामना कयर सकय छै.

“AI साइबर जागरूकता” पर भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (सीईआरटी-इन) कें इ पुस्तिका केवल साइबर सुरक्षा पेशेवरक कें लेल नहि, बल्कि रोजमर्रा कें नागरिकक, कर्मचारीक, आ डिजिटल उपयोगकर्ताक कें लेल डिजाइन कैल गेल छै. इ बतायत छै की AI डिजिटल खतरा परिदृश्य कें कोना बदल रहल छै आ सरल, व्यावहारिक कदम प्रदान करयत छै जेकर पालन सब लोग व्यक्तिगत जानकारी, उपकरणक आ ऑनलाइन पहचान कें सुरक्षा कें लेल कयर सकय छै.

AI-एन्हांसड फिशिंग एवं सोशल इंजीनियरिंग



ई कोना काज करैत अछि ?

आब धमकी देबय वाला कलाकार एहन ईमेल आओर टेक्स्ट भेजय छथिन्ह जे असली आओर त्रुटि मुक्त लगैत अछि. ओ अहां कें बारे मे विवरण कें उपयोग करएयत छै, जेना अहां कें नौकरी, सेवाक कें उपयोग करएयत छै, या हाल कें गतिविधियक, संदेशक कें व्यक्तिगत महसूस करएय कें लेल. चूँकि ई संदेश नीक लिखल गेल अछि, तेँ एकरा देखब बहुत कठिन भ' सकैत अछि.

पहचान कोना करब ?

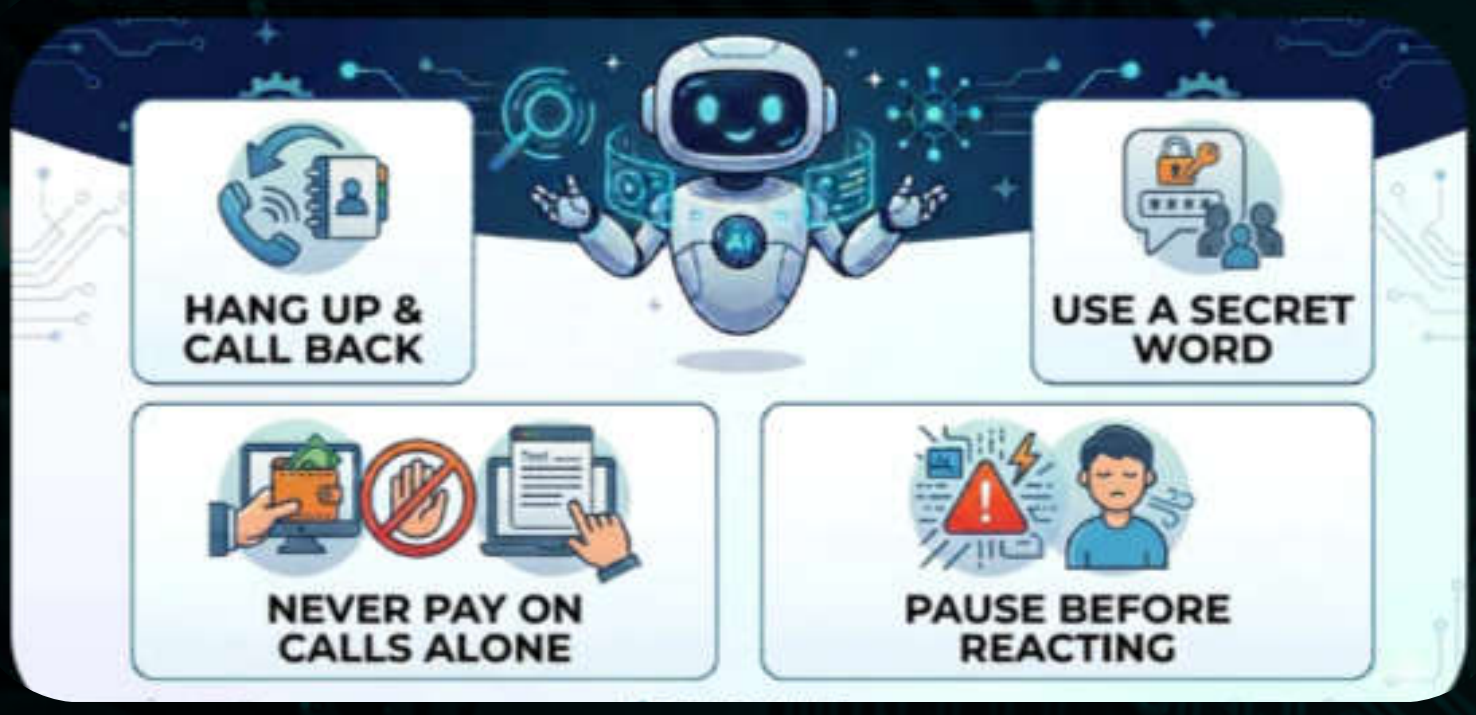
- संदेश अहां के लेल बेहद विशिष्ट लगैत अछि मुदा अप्रत्याशित रूप सं पहुंचैत अछि.
- एहि मे जरूरी या धमकी भरल स्वर के प्रयोग कयल गेल अछि आ तत्काल कार्रवाई के मांग कयल गेल अछि।
- इ अहां सं कोनों लिंक पर क्लिक करय, कोनों खाता कें सत्यापन करय, पासवर्ड रीसेट करय या भुगतान करय कें लेल कहय छै.
- प्रेषक’क पता लगभग सही लगैत छैक, मुदा एकदम सही नहि.

सुरक्षित कोना रहब ?

- अवांछित संदेश मे लिंक पर क्लिक नहि करू. एकर बदला मे सीधा आधिकारिक वेबसाइट या ऐप पर जाउ।
- कोनों अलग, विश्वसनीय संपर्क चैनल कें माध्यम सं अनुरोधक कें सत्यापन करूं, जेना कोनों आधिकारिक फोन नंबर या ऐप.
- संदेश लिंक कें माध्यम सं पहुंचल गेल पन्ना पर कहियो क्रेडेंशियल या ओटीपी नहि दर्ज करूं.
- संदिग्ध संदेशक रिपोर्ट करू आ मेटा दियौक, फेर प्रेषक कैं ब्लॉक करू।

हमरा सब के फॉलो करू :
@IndianCERT
@cert_india

स्वर आ वीडियो बनावटी छल [विषिंग]



ई कोना काज करैत अछि ?

धमकी देबय वाला अभिनेता आवाज के क्लोन क सकय छै या नकली वीडियो बना सकय छै जे असली दिखय आ सुनय मे आबि सकय छै. ओ परिवार, सहयोगी या अधिकारी कें रूप मे दिखावा कयर सकय छै जे अहां कें संवेदनशील जानकारी साझा करय, पैसा भेजय या जल्दी सं काज करय कें लेल दबाव बना सकय छै.

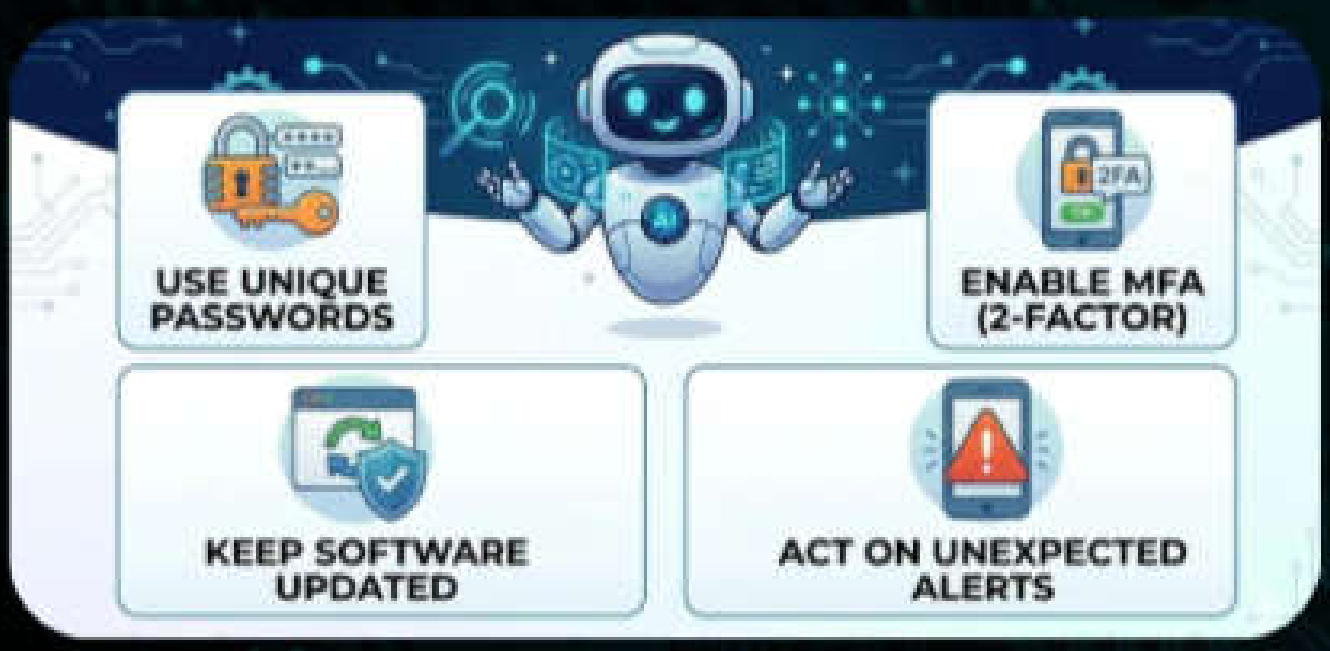
पहचान कोना करब ?

- असामान्य तात्कालिकता, घबराहट, वा गोपनीयताक आग्रह, जेना ककरो नहि कहब.
- कनि ऑफ टोन, पेसिंग, बैकग्राउंड नॉइज, या ऑडियो क्वालिटी।
- सामान्य सत्यापन या स्वीकृति प्रक्रिया कें बाईपास करय कें अनुरोध.
- उपहार कार्ड, क्रिप्टोकरेंसी, या तार स्थानांतरण कें माध्यम सं भुगतान कें लेल अनुरोध.

सुरक्षित कोना रहब ?

- फोन राखू आ ओहि व्यक्ति कें ओकर ज्ञात, सेव नंबर कें उपयोग करयत वापस फोन करूं.
- आपातकालीन स्थिति मे पहचान कें सत्यापन कें लेल परिवार या कार्यस्थल कें सुरक्षित शब्द सेट करूं.
- केवल कॉल या वीडियो कें आधार पर भुगतान कें अधिकृत नहि करूं. अलग चैनल के माध्यम स लिखित रूप स पुष्टि करू।
- प्रतिक्रिया देबासँ पहिने रुकि जाउ। धमकी देबय वाला अभिनेता अहां के निर्णय पर बादल मचाबय लेल घबराहट पर निर्भर रहैत छथिन्ह.

AI-सहायता प्राप्त मालवेयर एवं स्वचालित हमला



ई कोना काज करैत अछि ?

खतरा अभिनेताक AI उपकरणक कें उपयोग दुर्भावनापूर्ण कोड बनावा या छिपावा कें लेल, कईटा साइट पर चोरी कैल गेल पासवर्ड कें परीक्षण करय आ ओय सिस्टम कें पहचान करय कें लेल करय छै जेकरा अपडेट कें जरूरत छै. एहि सं हमला तेजी सं आओर व्यापक भ जाएत अछि.

पहचान कोना करब ?

- अप्रत्याशित लॉगिन अलर्ट, पासवर्ड रीसेट ईमेल, या एमएफए प्रॉम्प्ट जे अहां अनुरोध नहि केने रही
- अहां कें खाता गतिविधि मे सूचीबद्ध अपरिचित डिवाइस या सत्र
- एंटीवायरस चेतावनी, पॉप-अप, या असामान्य रूप सं धीमा डिवाइस प्रदर्शन
- फाइल, सेटिंग, या ब्राउज़र एक्सटेंशन जे अहाँ नहि चिन्हैत छी

सुरक्षित कोना रहब ?

- हर खाता कें लेल एकटा अद्वितीय, मजबूत पासवर्ड कें उपयोग करूं.
- सबटा महत्वपूर्ण खाताक पर बहु कारक प्रमाणीकरण (एमएफए) सक्षम करू.
- एंटीवायरस सॉफ्टवेयर, सिस्टम, आ ऐप कें अद्यतन राखूं.
- अप्रत्याशित लॉगिन या एमएफए अलर्ट पर तुरंत कार्य करू.

हमरा सब के फॉलो करू :
@IndianCERT
@cert_india

नकली वेबसाइट एवं पहचान चोरी



ई कोना काज करैत अछि ?

खतरा अभिनेताक अहां कें लॉगिन क्रेडेंशियल, ओटीपी, या भुगतान विवरण चोरी करय कें लेल एकटा समान देखाय वाला वेबसाइट आ चैटबोट बना सकय छै जे असली प्रतीत होयत छै, जेना बैंकिंग या खरीदारी पोर्टल. ओ गलत पहचान बनाबय लेल फर्जी फोटो या दस्तावेज के इस्तेमाल सेहो क सकय छथिन्ह.

पहचान कोना करब ?

- कनि बदलल गेल वेबसाइट यूआरएल, जेना अतिरिक्त अक्षर, हाइफन, या कोनो अलग डोमेन अंत.
- ओटीपी, पिन, या पूरा कार्ड नंबर मांगय वाला चैटबोट या एजेंट.
- कोनों परिचित साइट पर HTTPS या असामान्य डिजाइन असंगति गायब.

सुरक्षित कोना रहब ?

- हमेशा आधिकारिक यूआरएल सीधा टाइप करू या सत्यापित बुकमार्क के उपयोग करू, लिंक पर क्लिक करय के बजाय
- कोनों चैटबॉट या "सपोर्ट एजेंट" कें साथ कहियो ओटीपी, पिन, या पूरा कार्ड कें विवरण साझा नहि करूं.
- एचटीटीपीएस कें जांच करूं आ कतहु लॉग इन करय सं पहिले डोमेन नाम कें ध्यान सं देखूं
- अपरिचित गतिविधि कें लेल नियमित रूप सं अपन बैंक स्टेटमेंट आ क्रेडिट रिपोर्ट कें निगरानी करूं.

हमरा सब के फॉलो करू :
@IndianCERT
@cert_india

लाल झंडे चेकलिस्ट

AI-सक्षम हमलाक ई संकेत देखू:

- पैसा, साख, या मंजूरी कें लेल तत्काल, दबाव वाला अनुरोध
- कोनों "ज्ञात" व्यक्ति कें कॉल या वीडियो मे हल्का ऑडियो/वीडियो असंगति
- सामान्य सत्यापन/ स्वीकृति प्रक्रिया कें बाईपास करय कें अनुरोध
- अपरिचित प्रेषक डोमेन अथवा कनेक बदलल यूआरएल
- अप्रत्याशित एमएफए प्रॉम्प्ट या ओटीपी जे अहाँ अनुरोध नहि केने रही
- सुरक्षा सॉफ्टवेयर कें अक्षम करय कें लेल या अनौपचारिक लिंक कें माध्यम सं "सत्यापन" करय कें अनुरोध
- नौकरी/निवेश प्रस्तावक कें लेल अपफ्रंट भुगतान या व्यक्तिगत वित्तीय विवरण कें आवश्यकता होयत छै

जखन संदेह होयत तखन — रुकू, स्वतंत्र रूप सं सत्यापन करू, आ दबाव मे काज नहि करू.

ऑनलाइन सुरक्षा



अपन खाता के रक्षा करू

- हर खाता कें लेल मजबूत आ अद्वितीय पासवर्ड कें उपयोग करूं; ओकरा सुरक्षित रूप सं संग्रहीत करय कें लेल पासवर्ड प्रबंधक कें उपयोग करूं.
- जतय उपलब्ध होयत बहु-कारक प्रमाणीकरण (एमएफए) सक्षम करू.
- ओटीपी, पिन, पासवर्ड, या सुरक्षा कोड कें कखनो ककरो सं साझा नहि करूं.
- बायोमेट्रिक प्रमाणीकरण (फिंगरप्रिंट/चेहरा पहचान) कें उपयोग एकटा अतिरिक्त सुरक्षा परत कें रूप मे करूं.

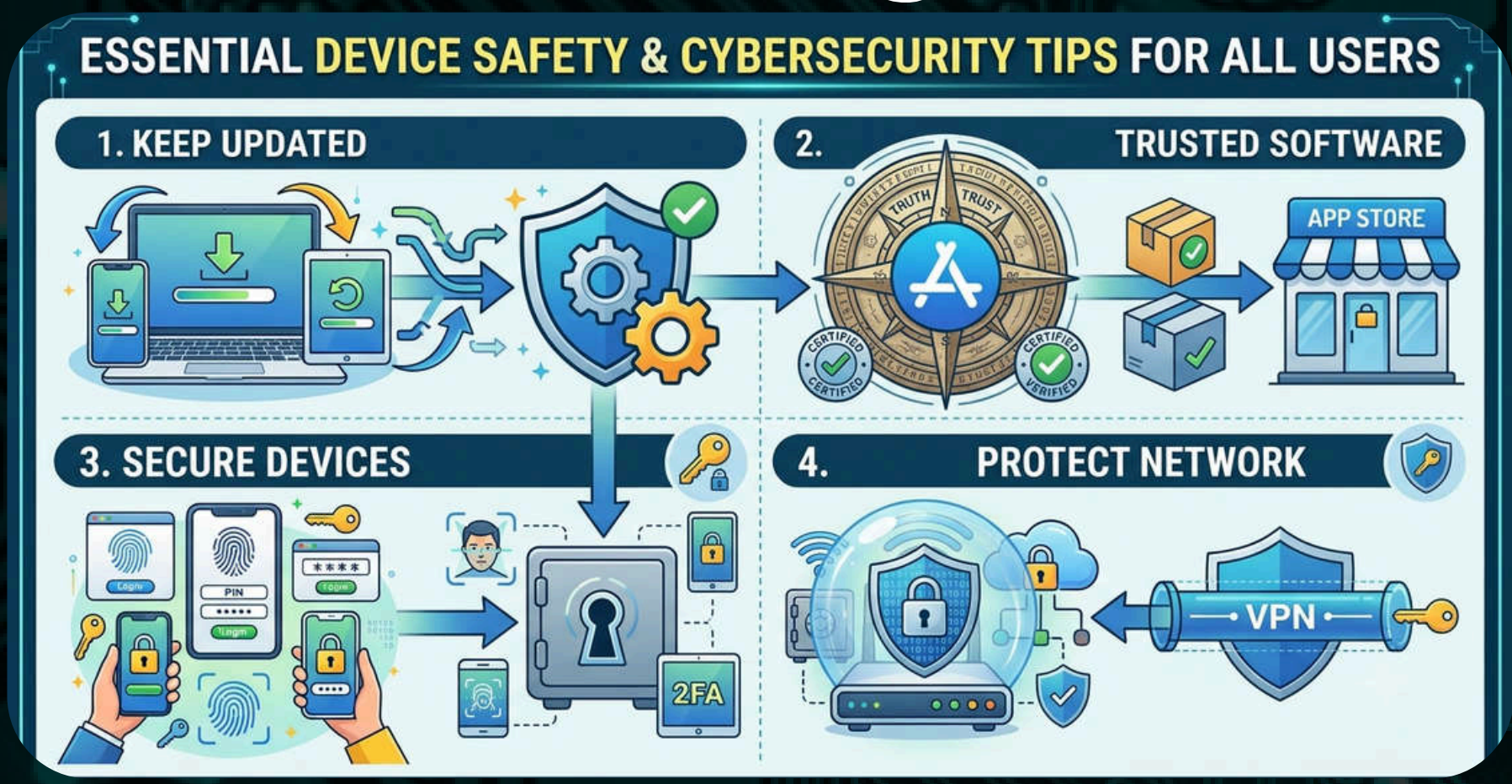
ईमेल एवं इंटरनेट का उपयोग करते समय सुरक्षित रहे |

- संदिग्ध या एक समान ईमेल पता कें लेल प्रेषक कें विवरण कें ध्यान सं जांचूं.
- क्लिक करय सं पहिने लिंक के सत्यापन करू आओर अप्रत्याशित संलग्नक खोलय सं बचू.
- लॉगिन या वित्तीय विवरण दर्ज करय सं पहिने वेबसाइट के प्रामाणिकता के पुष्टि करू.
- जखन संदेह होयत तखन रुकि क' सत्यापन करू आ काज करय सं पहिने.

किछु गड़बड़ हेबा स पहिने तैयारी करू

- महत्वपूर्ण फाइल कें नियमित बैकअप बनाक राखूं, जे ऑफलाइन या सुरक्षित क्लाउड सेवा मे संग्रहीत कैल गेल छै
- खाता वसूली कें जानकारी (ईमेल/फोन) कें अपडेट आ सुरक्षित राखूं

डिवाइस सुरक्षा



डिवाइस अपडेट राखू

- ज्ञात कमजोरी कें ठीक करय कें लेल ऑपरेटिंग सिस्टम, एप्लीकेशन, ब्राउज़र, आ सुरक्षा सॉफ्टवेयर कें नियमित रूप सं अपडेट करूं.
- जतय संभव होएत स्वचालित अपडेट सक्षम करू.

केवल विश्वसनीय सॉफ्टवेयर इंस्टॉल करू

- असली सॉफ्टवेयर कें उपयोग करूं आ केवल आधिकारिक ऐप स्टोर या विश्वसनीय स्रोत सं एप्लीकेशन इंस्टॉल करूं.
- विश्वसनीय एंटीवायरस या सुरक्षा समाधान कें उपयोग करूं आ ओकरा अपडेट राखूं.

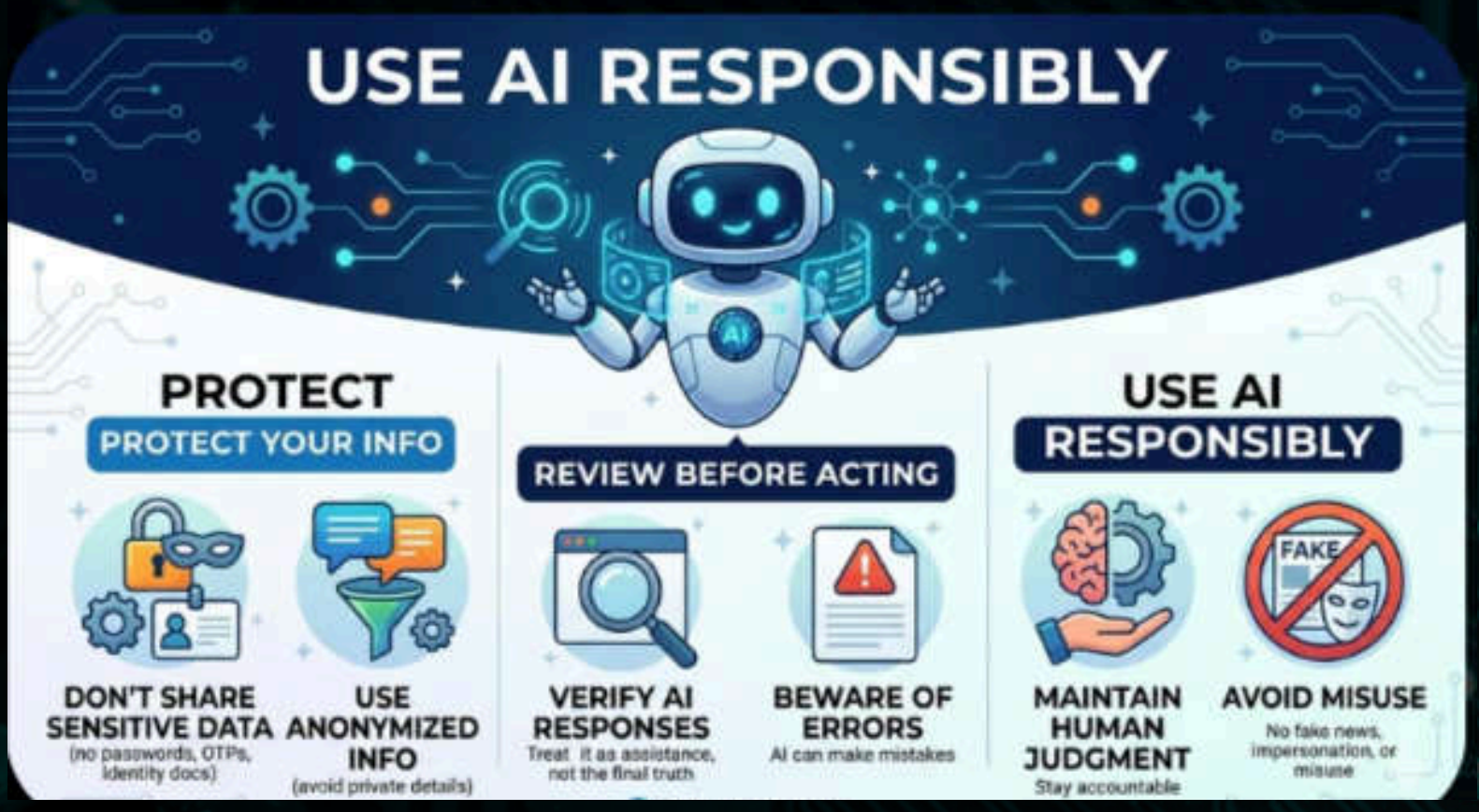
अपन डिवाइस आ खाता सुरक्षित करू

- सब डिवाइस पर मजबूत पासवर्ड या स्क्रीन लॉक कें उपयोग करूं.
- जखन कखनो उपलब्ध होयत तखन डिवाइस एन्क्रिप्शन आ सुरक्षा सुविधाक कें सक्षम करू.
- अनावश्यक आवेदन आ अनुमतियक कें समीक्षा आ हटाउ.

अपन नेटवर्क कनेक्शन के सुरक्षा करू

- अपन वाई-फाई कें मजबूत पासवर्ड सं सुरक्षित करूं आ डिफ़ॉल्ट राउटर क्रेडेंशियल बदलूं.
- अपडेट राउटर फर्मवेयर आ सुरक्षित नेटवर्क सेटिंग्स कें उपयोग करूं.
- संवेदनशील खाताक कें एक्सेस करय सं बचूं या असुरक्षित नेटवर्क पर गोपनीय जानकारी साझा करय सं बचूं.

AI जिम्मेदार ढंग स उपयोग करू



अपन व्यक्तिगत जानकारीक रक्षा करू

- सार्वजनिक *AI* उपकरणक या अज्ञात ऑनलाइन सेवाक मे व्यक्तिगत, वित्तीय, स्वास्थ्य, आधिकारिक, या गोपनीय जानकारी नहि दर्ज करूं.
- संवेदनशील विवरण जेना पासवर्ड, ओटीपी, खाता नंबर, पहचान दस्तावेज, ग्राहक डाटा, या निजी बातचीत कें साझा करय सं बचूं.
- AI उपकरण सं सहायता कें लेल पूछएय कें समय बेनामी या सामान्य जानकारी कें उपयोग करूं.

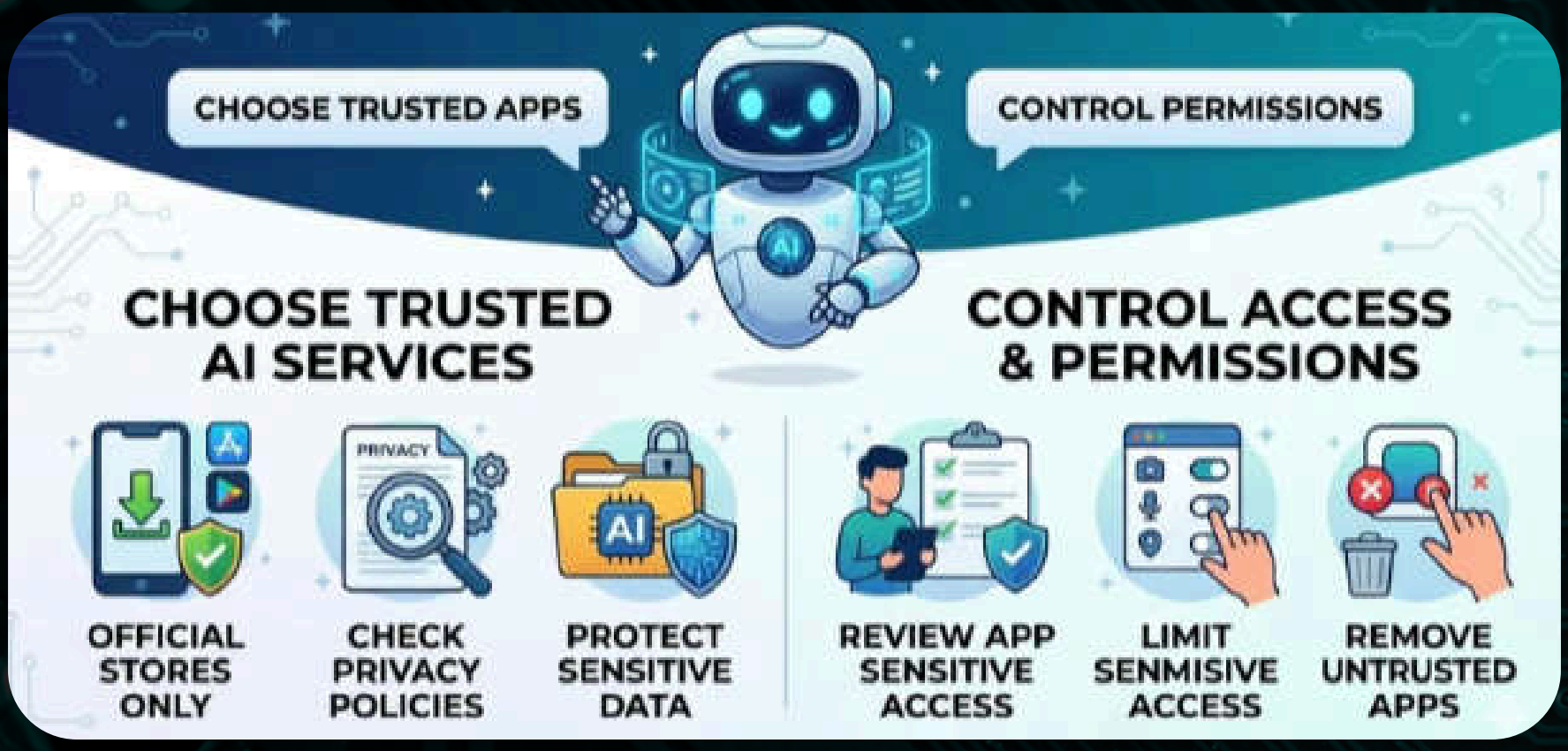
शेयर या एक्ट करबा स पहिने समीक्षा करू

- AI सं उत्पन्न प्रतिक्रियाक कें सहायता कें रूप मे देखूं, सत्य कें अंतिम स्रोत कें रूप मे नहि.
- वित्तीय, कानूनी, पेशेवर, या व्यक्तिगत निर्णय कें लेल उपयोग करय सं पहिले महत्वपूर्ण जानकारी कें सत्यापन करूं.
- ध्यान राखूं कि AI उपकरण गलत, अपूर्ण या भ्रामक जानकारी पैदा कयर सकय छै.

AI टूल के जिम्मेदारी स उपयोग करू

- अपन काज आ सीखय के समर्थन करय लेल AI के उपयोग करू, मुदा मानवीय निर्णय आ जवाबदेही बना क राखू.
- गलत जानकारी बनावा या फैलाबै, दोसर कें नकल करय, या ककरो व्यक्तिगत डेटा कें दुरुपयोग करय कें लेल AI कें उपयोग नहि करूं.

विश्वसनीय ऐप्स चुनू



ऐप पहुँच एवं अनुमति नियंत्रण

- AI एप्लीकेशन आ डिजिटल सहायक कें देल गेल अनुमतियक कें समीक्षा करूं.
- केवल तखनहि पहुंच कें अनुमति दिअ जखन कैमरा, माइक्रोफोन, संपर्क, या स्थान जैना सुविधाक कें लेल आवश्यक होय.
- अनावश्यक अनुमति हटाउ आ अविश्वसनीय स्रोत सं ऐप अनइंस्टॉल करू.

विश्वसनीय AI सेवा चुनू

- प्रतिष्ठित प्रदाता सं AI एप्लीकेशन कें उपयोग करूं आ ओकरा केवल आधिकारिक ऐप स्टोर सं डाउनलोड करूं.
- AI सेवाक कें उपयोग करय सं पहिले गोपनीयता सेटिंग्स, उपयोग कें शर्तक, आ डाटा हैंडलिंग प्रथाक कें समीक्षा करूं.
- AI उपकरणक कें संवेदनशील खाता या फाइल सं जोड़य सं बचूं जखन तइक सुरक्षा नियंत्रण कें सत्यापन नहि कैल जायत छै.

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