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 स्वच्छताको संस्कृति निर्माण गर्नुहोस्

#साइबर स्वच्छताहाम्रो संस्कृति



राष्ट्रिय साइबर सुरक्षा जागरूकता महिना (अक्टोबर २०२६)

प्रकाशक

भारतीय कम्प्युटर आपतकालीन प्रतिक्रिया टोली

हामीलाई पछ्याउनुहोस् :

@IndianCERT

@cert_india

सामग्रीको तालिका

प्रस्तावना ३

AI-उन्नत फिसिङ र सामाजिक इन्जिनियरिङ ४

भ्वाइस र भिडियो डिपफेक (भिसिङ) ५

AI-सहायता प्राप्त मालवेयर र स्वचालित आक्रमणहरू ६

नक्कली वेबसाइट र पहिचान चोरी ७

रातो झण्डा चेकलिस्ट ८

अनलाइन सुरक्षा ९

उपकरण सुरक्षा १०

AIलाई जिम्मेवारीपूर्वक प्रयोग गर्नुहोस् ११

विश्वसनीय एपहरू छनौट गर्नुहोस् १२

साइबर सुरक्षा घटनाहरू CERT-In लाई रिपोर्ट गर्नुहोस् १३

प्रस्तावना

आर्टिफिसियल इन्टेलिजेन्स (AI) ले हाम्रो जीवन, काम र सञ्चार गर्ने तरिकालाई रूपान्तरण गरिरहेको छ। यसले नवप्रवर्तनलाई सक्षम बनाउँछ, उत्पादकता सुधार गर्छ र विभिन्न क्षेत्रहरूमा जटिल समस्याहरू समाधान गर्न मद्दत गर्छ। यद्यपि, उही प्रविधिलाई खतरा अभिनेताहरूले अझ उन्नत र विश्वस्त साइबर खतराहरू सिर्जना गर्न दुरुपयोग गरिरहेका छन्।

AIले डिजिटल खतराहरू पहिचान गर्न अझ गाह्रो बनाउँदैछ किनभने आक्रमणकारीहरूले अब अत्यधिक यथार्थपरक इमेल, सन्देश, अडियो, भिडियो र वेबसाइटहरू सिर्जना गर्न सक्छन्। परम्परागत चेतावनी संकेतहरू, जस्तै कमजोर व्याकरण, असामान्य ढाँचा, वा स्पष्ट गल्तीहरू, अब भरपर्दो सूचक नहुन सक्छन्। प्रमाणीकरण र जिम्मेवार डिजिटल अभ्यासहरू पहिलेभन्दा बढी महत्त्वपूर्ण भएका छन्।

हामीले हरेक दिन प्रयोग गर्ने AI उपकरणहरू र स्मार्ट उपकरणहरू सावधानीपूर्वक प्रयोग नगरिएमा नयाँ गोपनीयता र सुरक्षा जोखिमहरू ल्याउन सक्छन्। अविश्वसनीय AI अनुप्रयोगहरूसँग व्यक्तिगत वा गोप्य जानकारी साझा गर्ने, अनावश्यक अनुमतिहरू प्रदान गर्ने, वा प्रमाणीकरण बिना AI द्वारा उत्पन्न जानकारीमा भर पर्दा व्यक्ति र संस्थाहरूलाई सुरक्षा जोखिममा पार्न सक्छ।

भारतीय कम्प्युटर आपतकालीन प्रतिक्रिया टोली (CERT-In) द्वारा "AI साइबर जागरूकता" मा प्रस्तुत गरिएको यो पुस्तिका साइबर सुरक्षा पेशेवरहरू मात्र नभई दैनिक नागरिकहरू, कर्मचारीहरू र डिजिटल प्रयोगकर्ताहरूका लागि डिजाइन गरिएको हो। यसले AI ले डिजिटल खतराको परिदृश्यलाई कसरी परिवर्तन गरिरहेको छ भनेर वर्णन गर्दछ र व्यक्तिगत जानकारी, उपकरणहरू र अनलाइन पहिचान सुरक्षित गर्न सबैले पालना गर्न सक्ने सरल, व्यावहारिक कदमहरू प्रदान गर्दछ।

AI-एन्हांस्ड फिसिङ र सामाजिक इन्जिनियरिङ



यो कसरी काम गर्छ?

धम्की दिने कलाकारहरूले अब वास्तविक र त्रुटिरहित देखिने इमेल र सन्देशहरू पठाउँछन्। तिनीहरूले तपाईंको बारेमा विवरणहरू प्रयोग गर्छन्, जस्तै तपाईंको काम, तपाईंले प्रयोग गर्ने सेवाहरू, वा हालसालैका गतिविधिहरू, सन्देशहरूलाई व्यक्तिगत महसुस गराउन। यी सन्देशहरू राम्रोसँग लेखिएका हुनाले, तिनीहरूलाई पत्ता लगाउन धेरै गाह्रो हुन सक्छ।

कसरी पहिचान गर्ने?

- सन्देश तपाईंलाई एकदमै विशिष्ट लाग्छ तर अप्रत्याशित रूपमा आउँछ।
- यसले तत्काल वा धम्कीपूर्ण स्वर प्रयोग गर्दछ र तुरुन्तै कारबाहीको माग गर्दछ।
- यसले तपाईंलाई लिङ्कमा क्लिक गर्न, खाता प्रमाणित गर्न, पासवर्ड रिसेट गर्न वा भुक्तानी गर्न सोध्छ।
- पठाउनेको ठेगाना लगभग सही देखिन्छ, तर पूर्ण रूपमा होइन।

कसरी सुरक्षित रहने?

- अनावश्यक सन्देशहरूमा भएका लिङ्कहरूमा क्लिक नगर्नुहोस्। बरु सिधै आधिकारिक वेबसाइट वा एपमा जानुहोस्।
- आधिकारिक फोन नम्बर वा एप जस्ता छुट्टै, विश्वसनीय सम्पर्क च्यानल मार्फत अनुरोधहरू प्रमाणित गर्नुहोस्।
- सन्देश लिङ्क मार्फत प्राप्त पृष्ठमा कहिल्यै पनि प्रमाणपत्र वा OTP प्रविष्ट नगर्नुहोस्।
- शंकास्पद सन्देशहरू रिपोर्ट गर्नुहोस् र मेटाउनुहोस्, त्यसपछि पठाउनेलाई ब्लक गर्नुहोस्।

हामीलाई पछ्याउनुहोस् :
@IndianCERT
@cert_india

भ्वाइस र भिडियो डिपफेक [भिसिङ]



यो कसरी काम गर्छ?

धम्की दिने कलाकारहरूले आवाज क्लोन गर्न सक्छन् वा वास्तविक देखिने र सुनिने नक्कली भिडियोहरू सिर्जना गर्न सक्छन्। तिनीहरूले तपाईंलाई संवेदनशील जानकारी साझा गर्न, पैसा पठाउन वा छिटो कदम चाल्न दबाब दिन परिवार, सहकर्मी वा अधिकारीको रूपमा प्रस्तुत गर्न सक्छन्।

कसरी पहिचान गर्ने?

- असामान्य जरुरीता, आतंक, वा गोपनीयताको लागि अनुरोध, जस्तै कसैलाई नभन्नु।
- अलिकति फरक स्वर, गति, पृष्ठभूमिको आवाज, वा अडियो गुणस्तर।
- सामान्य प्रमाणीकरण वा अनुमोदन प्रक्रियाहरू बाइपास गर्न अनुरोधहरू।
- उपहार कार्ड, क्रिप्टोकरेन्सी, वा वायर ट्रान्सफर मार्फत भुक्तानीको लागि अनुरोधहरू।

कसरी सुरक्षित रहने?

- फोन काट्नुहोस् र व्यक्तिलाई उनको ज्ञात, सेभ गरिएको नम्बर प्रयोग गरेर फिर्ता कल गर्नुहोस्।
- आपतकालीन अवस्थामा पहिचान प्रमाणित गर्न परिवार वा कार्यस्थल सुरक्षित शब्द सेट गर्नुहोस्।
- कल वा भिडियोको आधारमा मात्र भुक्तानीहरू कहिल्यै अधिकृत नगर्नुहोस्। छुट्टै माध्यमबाट लिखित रूपमा पुष्टि गर्नुहोस्।
- प्रतिक्रिया दिनुअघि रोकिनुहोस्। धम्की दिने व्यक्तिहरू तपाईंको निर्णय क्षमतालाई धमिलो बनाउन आतंकमा भर पर्छन्।

AI-सहायता प्राप्त मालवेयर र स्वचालित आक्रमणहरू



यो कसरी काम गर्छ?

धम्की दिने व्यक्तिहरूले दुर्भावनापूर्ण कोड सिर्जना गर्न वा लुकाउन, धेरै साइटहरूमा चोरी भएका पासवर्डहरू परीक्षण गर्न र अद्यावधिकहरू आवश्यक पर्ने प्रणालीहरू पहिचान गर्न AI उपकरणहरू प्रयोग गर्छन्। यसले आक्रमणहरूलाई छिटो र व्यापक बनाउँछ।

कसरी पहिचान गर्ने?

- तपाईंले अनुरोध नगरेका अप्रत्याशित लगइन अलर्टहरू, पासवर्ड रिसेट इमेलहरू, वा MFA प्रम्प्टहरू
- तपाईंको खाता गतिविधिमा सूचीबद्ध अपरिचित यन्त्र वा सत्रहरू
- एन्टिभाइरस चेतावनी, पप-अप, वा असामान्य रूपमा ढिलो उपकरण प्रदर्शन
- तपाईंले नचिनेका फाइल, सेटिङ वा ब्राउजर एक्सटेन्सनहरू

कसरी सुरक्षित रहने?

- प्रत्येक खाताको लागि एउटा अद्वितीय, बलियो पासवर्ड प्रयोग गर्नुहोस्।
- सबै महत्त्वपूर्ण खाताहरूमा बहु-कारक प्रमाणीकरण (MFA) सक्षम गर्नुहोस्।
- एन्टिभाइरस सफ्टवेयर, प्रणाली र एपहरूलाई अद्यावधिक राख्नुहोस्।
- अप्रत्याशित लगइन वा MFA अलर्टहरूमा तुरुन्तै कारबाही गर्नुहोस्।

नक्कली वेबसाइट र पहिचान चोरी



यो कसरी काम गर्छ?

धम्की दिने व्यक्तिहरूले तपाईंको लगइन प्रमाणहरू, OTP हरू, वा भुक्तानी विवरणहरू चोर्न बैंकिङ वा किनमेल पोर्टलहरू जस्ता वास्तविक देखिने वेबसाइटहरू र च्याटबटहरू सिर्जना गर्न सक्छन्। तिनीहरूले नक्कली पहिचान सिर्जना गर्न नक्कली फोटो वा कागजातहरू पनि प्रयोग गर्न सक्छन्।

कसरी पहिचान गर्ने?

- थोरै परिवर्तन गरिएका वेबसाइट URL हरू, जस्तै अतिरिक्त अक्षरहरू, हाइफनहरू, वा फरक डोमेनको अन्त्य।
- OTP, PIN, वा पूरा कार्ड नम्बरहरू माग्ने च्याटबट वा एजेन्टहरू।
- परिचित साइटमा HTTPS हराइरहेको छ वा असामान्य डिजाइन असंगतिहरू छन्।

कसरी सुरक्षित रहने?

- लिङ्कहरूमा क्लिक गर्नुको सट्टा सधैं आधिकारिक URL हरू सिधै टाइप गर्नुहोस् वा प्रमाणित बुकमार्कहरू प्रयोग गर्नुहोस्।
- कुनै पनि च्याटबट वा "समर्थन एजेन्ट" सँग कहिल्यै पनि OTP, PIN, वा पूरा कार्ड विवरणहरू साझा नगर्नुहोस्।
- कतै लग इन गर्नु अघि HTTPS जाँच गर्नुहोस् र डोमेन नामलाई ध्यानपूर्वक हेर्नुहोस्।
- अपरिचित गतिविधिको लागि आफ्नो बैंक स्टेटमेन्ट र क्रेडिट रिपोर्ट नियमित रूपमा निगरानी गर्नुहोस्।

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

रातो झण्डाको सूची

AI-सक्षम आक्रमणका यी संकेतहरू हेर्नुहोस्:

- पैसा, प्रमाणपत्र वा स्वीकृतिको लागि तत्काल, दबाबपूर्ण अनुरोध
- "परिचित" व्यक्तिको कल वा भिडियोमा थोरै अडियो/भिडियो असंगतिहरू
- सामान्य प्रमाणीकरण/अनुमोदन प्रक्रियाहरू बाइपास गर्न अनुरोध
- अपरिचित प्रेषक डोमेन वा थोरै परिवर्तन गरिएको URL
- तपाईंले अनुरोध नगर्नुभएका अप्रत्याशित MFA प्रम्प्ट वा OTP हरू
- सुरक्षा सफ्टवेयर असक्षम पार्न वा अनौपचारिक लिङ्कहरू मार्फत "प्रमाणित" गर्न अनुरोधहरू
- अग्रिम भुक्तानी वा व्यक्तिगत वित्तीय विवरण आवश्यक पर्ने जागिर/लगानी प्रस्तावहरू

शंका लागेमा — रोक्नुहोस्, स्वतन्त्र रूपमा प्रमाणित गर्नुहोस्, र दबाबमा काम नगर्नुहोस्।

हामीलाई पछ्याउनुहोस् :
@IndianCERT
@cert_india

अनलाइन सुरक्षा



आफ्नो खाताहरू सुरक्षित गर्नुहोस्

- प्रत्येक खाताको लागि बलियो र अद्वितीय पासवर्डहरू प्रयोग गर्नुहोस्; तिनीहरूलाई सुरक्षित रूपमा भण्डारण गर्न पासवर्ड प्रबन्धक प्रयोग गर्नुहोस्।
- उपलब्ध भएसम्म बहु-कारक प्रमाणीकरण (MFA) सक्षम गर्नुहोस्।
- कहिल्यै पनि कसैसँग OTP, PIN, पासवर्ड वा सुरक्षा कोडहरू साझा नगर्नुहोस्।
- अतिरिक्त सुरक्षा तहको रूपमा बायोमेट्रिक प्रमाणीकरण (औंठाछाप/अनुहार पहिचान) प्रयोग गर्नुहोस्।

इमेल र इन्टरनेट प्रयोग गर्दा सुरक्षित रहनुहोस्

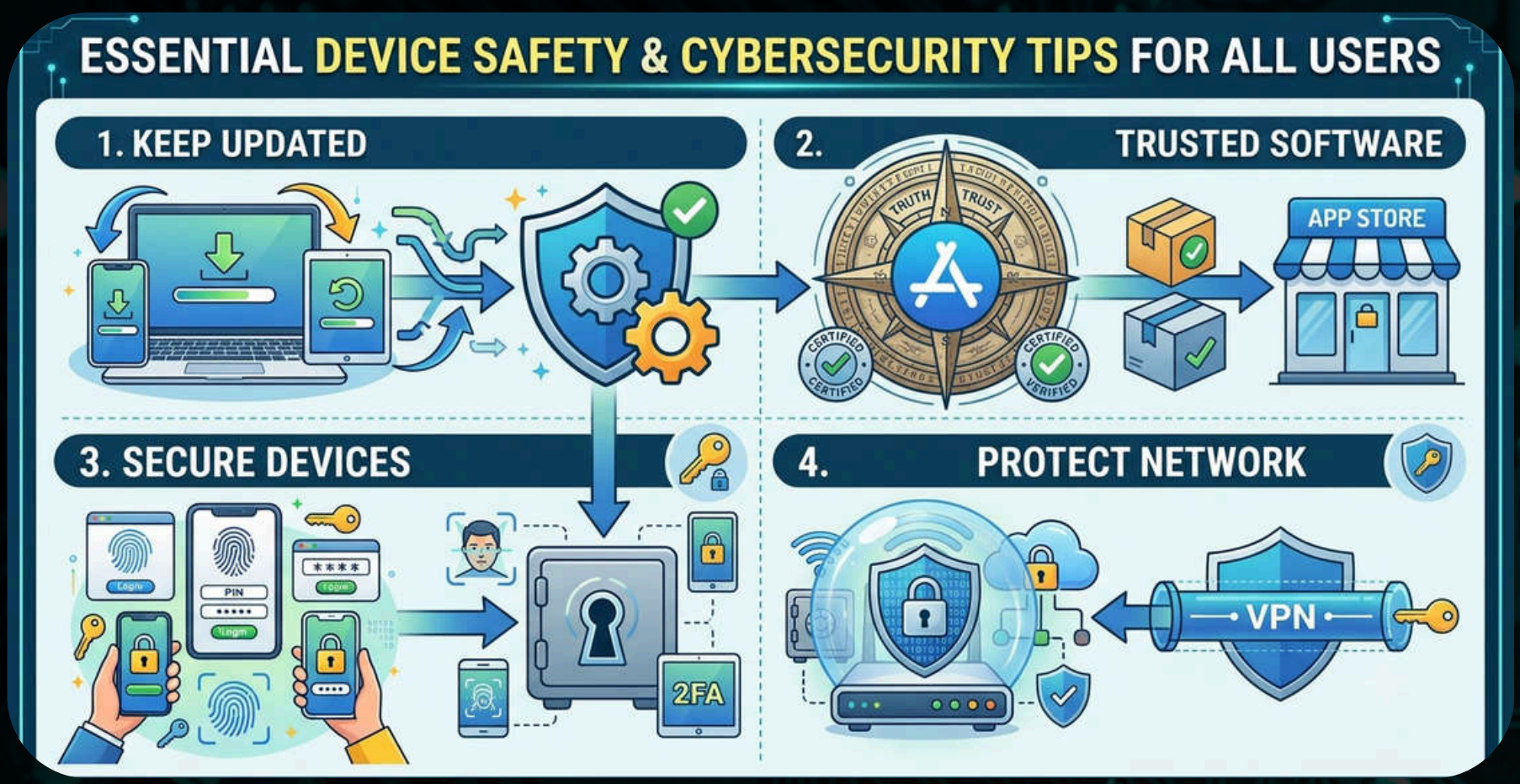
- शंकास्पद वा उस्तै देखिने इमेल ठेगानाहरूको लागि प्रेषकको विवरणहरू ध्यानपूर्वक जाँच गर्नुहोस्।
- क्लिक गर्नु अघि लिङ्कहरू प्रमाणित गर्नुहोस् र अप्रत्याशित संलग्नकहरू नखोल्नुहोस्।
- लगइन वा वित्तीय विवरणहरू प्रविष्ट गर्नु अघि वेबसाइटको प्रामाणिकता पुष्टि गर्नुहोस्।
- शंका लागेमा, काम गर्नु अघि रोक्नुहोस् र प्रमाणित गर्नुहोस्।

केही गलत हुनु अघि नै तयारी गर्नुहोस्

- अफलाइन वा सुरक्षित क्लाउड सेवामा भण्डारण गरिएका महत्त्वपूर्ण फाइलहरूको नियमित ब्याकअप राख्नुहोस्।
- खाता रिकभरी जानकारी (इमेल/फोन) अद्यावधिक र सुरक्षित राख्नुहोस्।

हामीलाई पछ्याउनुहोस् : @IndianCERT @cert_india

उपकरण सुरक्षा



उपकरणहरू अद्यावधिक राख्नुहोस्

- ज्ञात कमजोरीहरू समाधान गर्न अपरेटिङ सिस्टम, एप्लिकेसन, ब्राउजर र सुरक्षा सफ्टवेयर नियमित रूपमा अपडेट गर्नुहोस्।
- सम्भव भएसम्म स्वचालित अपडेटहरू सक्षम गर्नुहोस्।

विश्वसनीय सफ्टवेयर मात्र स्थापना गर्नुहोस्

- वास्तविक सफ्टवेयर प्रयोग गर्नुहोस् र आधिकारिक एप स्टोर वा विश्वसनीय स्रोतहरूबाट मात्र एपहरू स्थापना गर्नुहोस्।
- भरपर्दो एन्टिभाइरस वा सुरक्षा समाधानहरू प्रयोग गर्नुहोस् र तिनीहरूलाई अद्यावधिक राख्नुहोस्।

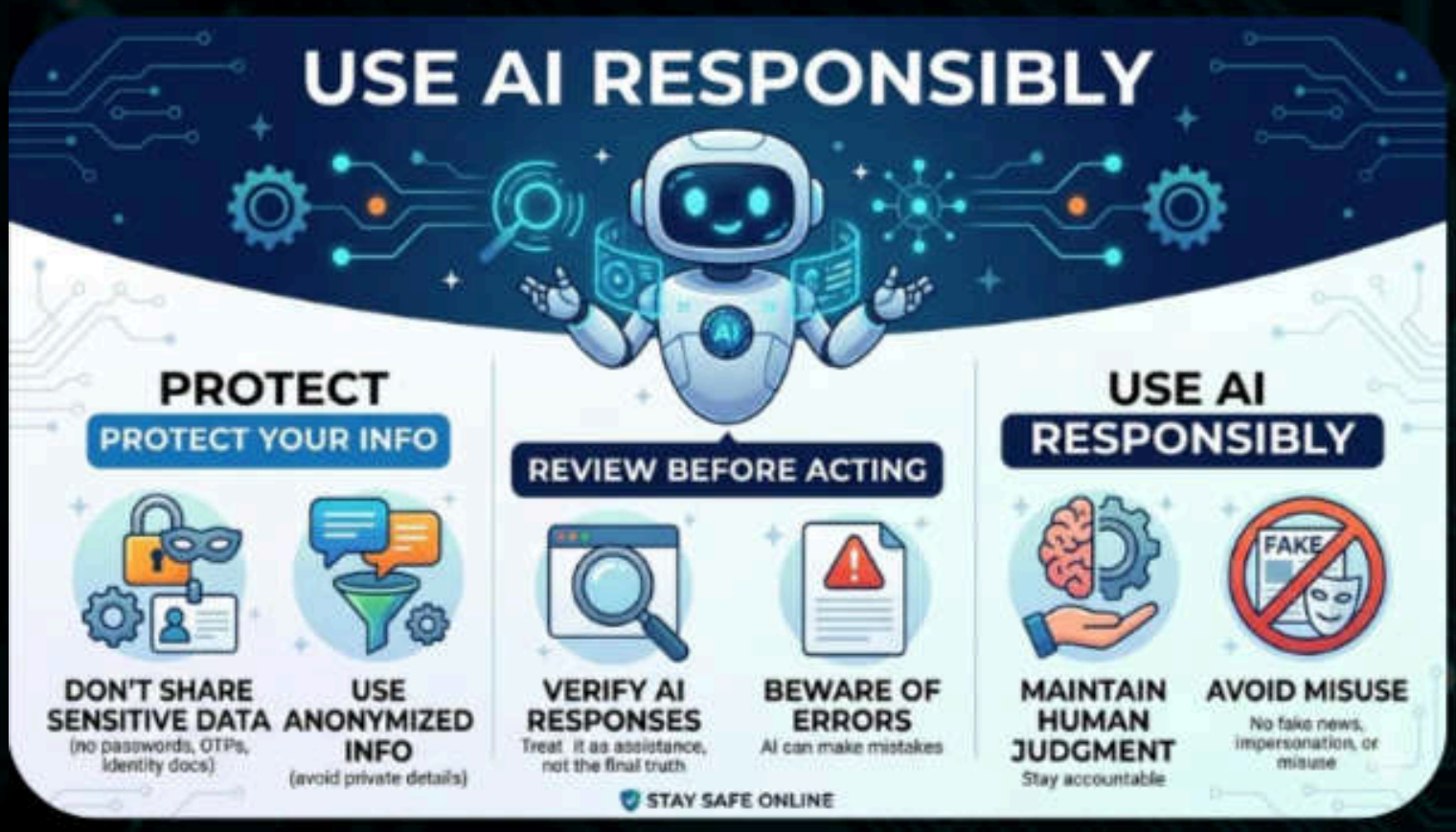
आफ्ना यन्त्रहरू र खाताहरू सुरक्षित गर्नुहोस्

- सबै उपकरणहरूमा बलियो पासवर्ड वा स्क्रिन लकहरू प्रयोग गर्नुहोस्।
- उपलब्ध भएसम्म उपकरण इन्क्रिप्सन र सुरक्षा सुविधाहरू सक्षम गर्नुहोस्।
- अनावश्यक अनुप्रयोगहरू र अनुमतिहरूको समीक्षा गर्नुहोस् र हटाउनुहोस्।

आफ्नो नेटवर्क जडान सुरक्षित गर्नुहोस्

- बलियो पासवर्डको साथ आफ्नो Wi-Fi सुरक्षित गर्नुहोस् र पूर्वनिर्धारित राउटर प्रमाणहरू परिवर्तन गर्नुहोस्।
- अपडेट गरिएको राउटर फर्मवेयर र सुरक्षित नेटवर्क सेटिङहरू प्रयोग गर्नुहोस्।
- असुरक्षित नेटवर्कहरूमा संवेदनशील खाताहरू पहुँच गर्न वा गोप्य जानकारी साझा गर्नबाट बच्नुहोस्।

जिम्मेवारीपूर्वक AI प्रयोग गर्नुहोस्



आफ्नो व्यक्तिगत जानकारी सुरक्षित गर्नुहोस्

- सार्वजनिक AI उपकरणहरू वा अज्ञात अनलाइन सेवाहरूमा व्यक्तिगत, वित्तीय, स्वास्थ्य, आधिकारिक, वा गोप्य जानकारी प्रविष्ट नगर्नुहोस्।
- पासवर्ड, OTP, खाता नम्बर, पहिचान कागजात, ग्राहक डेटा, वा निजी कुराकानी जस्ता संवेदनशील विवरणहरू साझा नगर्नुहोस्।
- AI उपकरणहरूसँग सहयोग माग्दा बेनामी वा सामान्य जानकारी प्रयोग गर्नुहोस्।

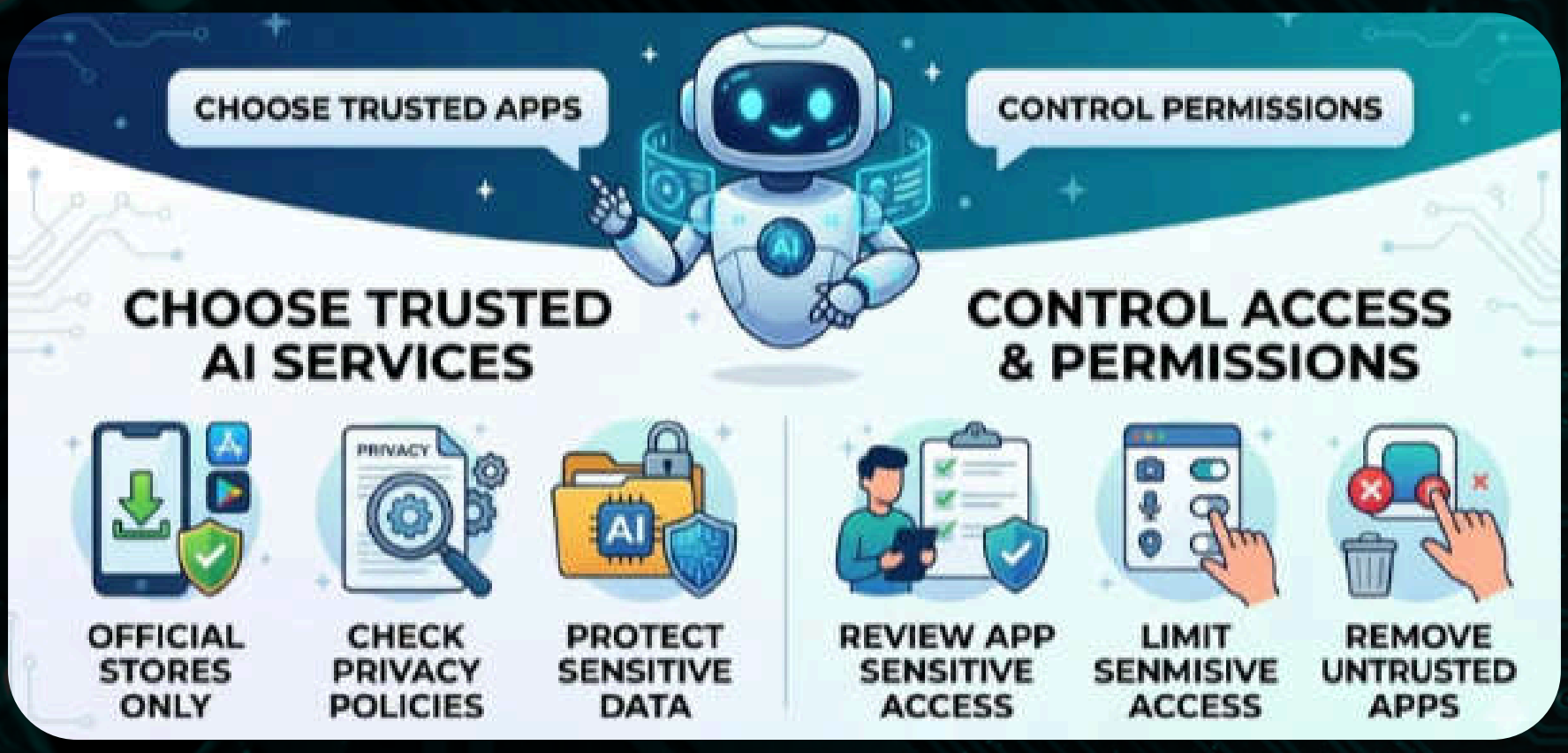
साझा गर्नु वा कार्य गर्नु अघि समीक्षा गर्नुहोस्

- AI-उत्पन्न प्रतिक्रियाहरूलाई सत्यको अन्तिम स्रोतको रूपमा होइन, सहयोगको रूपमा व्यवहार गर्नुहोस्।
- वित्तीय, कानुनी, व्यावसायिक, वा व्यक्तिगत निर्णयहरूको लागि प्रयोग गर्नु अघि महत्त्वपूर्ण जानकारी प्रमाणित गर्नुहोस्।
- AI उपकरणहरूले गलत, अपूर्ण, वा भ्रामक जानकारी उत्पादन गर्न सक्छन् भन्ने कुरामा सचेत रहनुहोस्।

AI उपकरणहरू जिम्मेवारीपूर्वक प्रयोग गर्नुहोस्

- आफ्नो काम र सिकाइलाई समर्थन गर्न AI प्रयोग गर्नुहोस्, तर मानवीय निर्णय र जवाफदेहिता कायम राख्नुहोस्।
- गलत जानकारी सिर्जना गर्न वा फैलाउन, अरूको नक्कल गर्न, वा कसैको व्यक्तिगत डेटाको दुरुपयोग गर्न AI प्रयोग नगर्नुहोस्।

विश्वसनीय एपहरू छनौट गर्नुहोस्



एप पहुँच र अनुमतिहरू नियन्त्रण गर्नुहोस्

- AI अनुप्रयोगहरू र डिजिटल सहायकहरूलाई दिइएको अनुमतिहरूको समीक्षा गर्नुहोस्।
- क्यामेरा, माइक्रोफोन, सम्पर्क वा स्थान जस्ता सुविधाहरूमा आवश्यक पर्दा मात्र पहुँच अनुमति दिनुहोस्।
- अनावश्यक अनुमतिहरू हटाउनुहोस् र अविश्वसनीय स्रोतहरूबाट एपहरू अनइन्स्टल गर्नुहोस्।

विश्वसनीय AI सेवाहरू छनौट गर्नुहोस्

- प्रतिष्ठित प्रदायकहरूबाट AI अनुप्रयोगहरू प्रयोग गर्नुहोस् र तिनीहरूलाई आधिकारिक एप स्टोरहरूबाट मात्र डाउनलोड गर्नुहोस्।
- AI सेवाहरू प्रयोग गर्नु अघि गोपनीयता सेटिङहरू, प्रयोगका सर्तहरू, र डेटा ह्यान्डलिङ अभ्यासहरूको समीक्षा गर्नुहोस्।
- सुरक्षा नियन्त्रणहरू प्रमाणित नभएसम्म संवेदनशील खाता वा फाइलहरूमा AI उपकरणहरू जडान नगर्नुहोस्।

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