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 मार्गदर्शिका

साइबर स्वच्छतायाः संस्कृतिं निर्मायताम्

#साइबरस्वच्छताअपनीसंस्कृति



राष्ट्रीय साइबर सुरक्षा जागरूकता मास (अक्टोबर 2026)

प्रकाशक

भारतीय कम्प्यूटर आपत्कालीन प्रतिक्रिया दल

अस्मान् अनुसरणं कुर्वन्तु :

@IndianCERT

@cert_india

विषयसूची

प्रस्तावना ३

AI-वर्धितं फिशिंग् & सामाजिक-इञ्जिनीयरिङ्गम् ४

स्वर-चित्र-छलप्रपञ्चः (विषिङ्ग्) ५

AI-सहायतायुक्ताः दुर्गन्धयुक्ताः & स्वचालिताः आक्रमणाः ६

नकली वेबसाइट एवं पहचान चोरी ७

लालध्वजानां जाँचसूची ८

ऑनलाइन सुरक्षा ९

यन्त्रसुरक्षा १०

AI इत्यस्य उत्तरदायित्वपूर्वकं उपयोगं कुर्वन्तु ११

विश्वसनीयान् अनुप्रयोगान् चिनुत १२

CERT-In इत्यस्मै साइबरसुरक्षाघटनानां सूचनां ददातु १३

प्रस्तावना

कृत्रिमबुद्धिः (AI) अस्माकं जीवनस्य, कार्यस्य, संवादस्य च मार्गं परिवर्तयति । एतत् नवीनतां सक्षमं करोति, उत्पादकतायां सुधारं करोति, विभिन्नक्षेत्रेषु जटिलसमस्यानां समाधानं कर्तुं च साहाय्यं करोति । परन्तु अधिका उन्नताः प्रत्ययप्रदाः च साइबरधमकीः निर्मातुं धमकी-अभिनेतृभिः अपि एतस्याः एव प्रौद्योगिक्याः दुरुपयोगः क्रियते ।

AI डिजिटल-धमकीनां पहिचानं अधिकं कठिनं करोति यतोहि आक्रमणकारिणः इदानीं अत्यन्तं यथार्थं ईमेल, सन्देशं, श्रव्यं, भिडियो, वेबसाइट् च निर्मातुम् अर्हन्ति । पारम्परिकाः चेतावनीचिह्नानि, यथा दुर्बलव्याकरणं, असामान्यस्वरूपणं, स्पष्टदोषाः वा, विश्वसनीयसूचकाः न भवेयुः । सत्यापनम्, उत्तरदायी डिजिटलप्रथाः च पूर्वस्मात् अपि अधिकं महत्त्वपूर्णाः अभवन् ।

AI-उपकरणाः स्मार्ट-यन्त्राणि च वयं प्रतिदिनं उपयुञ्ज्महे, यदि तेषां सावधानीपूर्वकं उपयोगः न क्रियते तर्हि नूतनानि गोपनीयता-सुरक्षा-जोखिमानि प्रवर्तयितुं शक्नुवन्ति । अविश्वसनीय-AI-अनुप्रयोगैः सह व्यक्तिगत-गोपनीय-सूचनाः साझाकरणं, अनावश्यक-अनुमति-प्रदानं, अथवा सत्यापन-रहित-AI-जनित-सूचनायाः उपरि अवलम्बनं, व्यक्तिं संस्थानां च सुरक्षा-जोखिमानां कृते उजागरं कर्तुं शक्नोति

“AI Cyber Awareness” इति विषये भारतीय कम्प्यूटर आपत्कालीनप्रतिक्रियादलस्य (CERT-In) इयं पुस्तिका न केवलं साइबरसुरक्षाव्यावसायिकानां कृते न तु दैनन्दिननागरिकाणां, कर्मचारिणां, डिजिटलप्रयोक्तृणां च कृते विनिर्मिता अस्ति। एतत् व्याख्यायते यत् AI कथं डिजिटल-धमकी-परिदृश्यं परिवर्तयति तथा च सरल-व्यावहारिक-पदार्थान् प्रदाति, येषां अनुसरणं सर्वे व्यक्तिगत-सूचनाः, उपकरणानि, ऑनलाइन-परिचयः च कर्तुं शक्नुवन्ति

कृत्रिमबुद्ध्या संवर्धितः जालच्छलः च सामाजिकयोजना च



कथं कार्यं करोति ?

इदानीं धमकी-अभिनेतारः ईमेल-पाठान् प्रेषयन्ति ये वास्तविकाः त्रुटिरहिताः च दृश्यन्ते । ते भवतः विषये विवरणानि, यथा भवतः कार्यं, भवता उपयुज्यमानाः सेवाः, अथवा अद्यतनक्रियाकलापाः, सन्देशान् व्यक्तिगतरूपेण अनुभूयन्ते इति उपयुञ्जते । एते सन्देशाः सुलिखिताः इति कारणतः तेषां दर्शनं बहु कठिनं भवितुम् अर्हति ।

कथं परिचयः करणीयः ?

- सन्देशः भवतः कृते अत्यन्तं विशिष्टः इति अनुभूयते परन्तु अप्रत्याशितरूपेण आगच्छति।
- तत् तात्कालिकं वा धमकीकृतं वा स्वरं प्रयुङ्क्ते, तत्कालं कार्यं कर्तुं आग्रहं च करोति ।
- एतत् भवन्तं कञ्चन लिङ्क् क्लिक् कर्तुं, खातं सत्यापयितुं, गुप्तशब्दं पुनः सेट् कर्तुं, अथवा भुक्तिं कर्तुं पृच्छति ।
- प्रेषकस्य सम्बोधनं प्रायः सम्यक् दृश्यते, परन्तु सर्वथा न ।

कथं सुरक्षितं स्थातव्यम् ?

- अयाचितसन्देशेषु लिङ्कानि न क्लिक् कुर्वन्तु। तस्य स्थाने प्रत्यक्षतया आधिकारिकजालस्थलं वा एप् वा गच्छन्तु।
- पृथक्, विश्वसनीयसम्पर्कचैनलद्वारा अनुरोधानाम् सत्यापनम्, यथा आधिकारिकफोनसङ्ख्या अथवा एप्।
- सन्देशलिङ्कद्वारा प्राप्ते पृष्ठे कदापि प्रमाणपत्राणि वा OTPs वा न प्रविशन्तु ।
- शङ्कितान् सन्देशान् निवेदयन्तु, विलोपयन्तु च, ततः प्रेषकं अवरुद्धयन्तु ।

अस्मान् अनुसरणं कुर्वन्तु : @IndianCERT @cert_india

स्वर-चित्र-छलप्रपञ्च: [विषिङ्ग्]



कथं कार्यं करोति ?

धमकी-अभिनेतारः स्वरं क्लोन् कर्तुं वा नकली-वीडियो-निर्माणं कर्तुं शक्नुवन्ति ये वास्तविकरूपेण दृश्यन्ते, ध्वनितुं च शक्नुवन्ति । ते भवन्तं संवेदनशीलसूचनाः साझां कर्तुं, धनं प्रेषयितुं, शीघ्रं कार्यं कर्तुं वा दबावं दातुं परिवारस्य, सहकारिणः, अधिकारिणः वा इव अभिनयं कुर्वन्ति ।

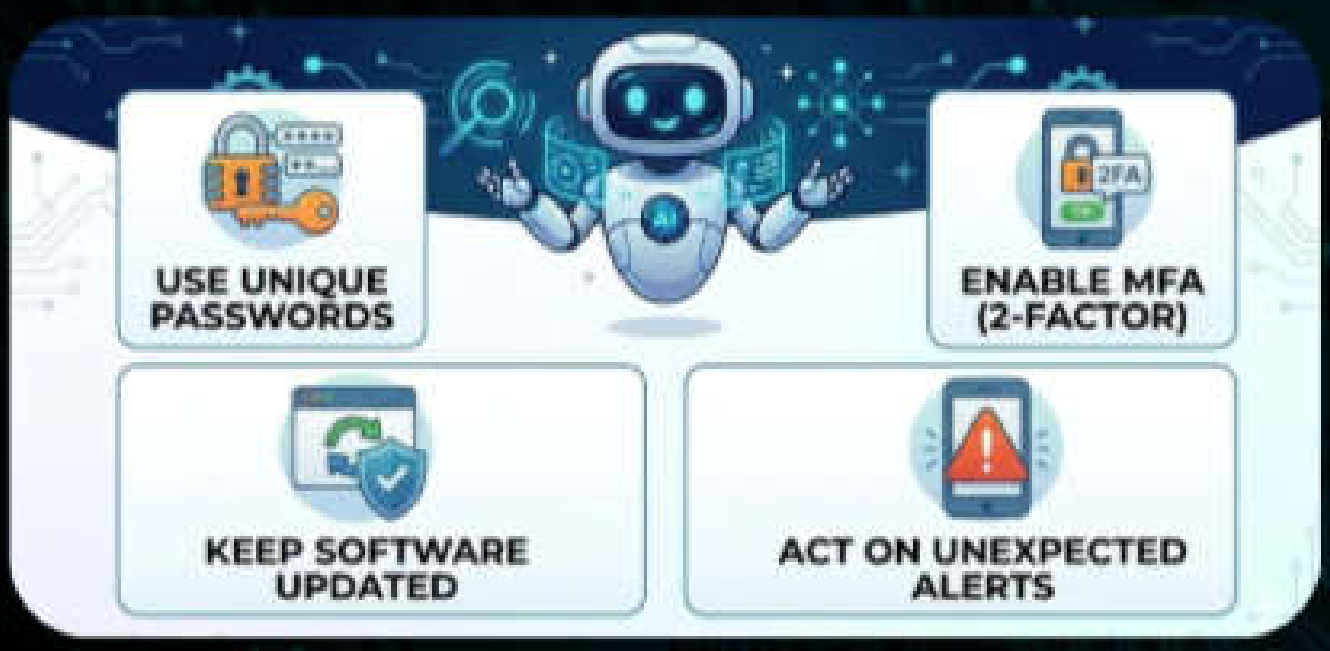
कथं परिचयः करणीयः ?

- असामान्यं तात्कालिकता, आतङ्कः, गोपनीयतायाः अनुरोधः वा यथा कस्मै अपि न वदतु ।
- किञ्चित् अवरुद्धः स्वरः, गतिः, पृष्ठभूमिकोलाहलः, श्रव्यगुणवत्ता वा ।
- सामान्यसत्यापनं वा अनुमोदनप्रक्रियाः वा बाईपासं कर्तुं अनुरोधः।
- उपहारकार्डद्वारा, क्रिप्टोमुद्राद्वारा, तारस्थानान्तरणद्वारा वा भुगतानस्य अनुरोधः।

कथं सुरक्षितं स्थातव्यम् ?

- दूरभाषं स्थापयित्वा व्यक्तिं तस्य ज्ञातं, रक्षितं सङ्ख्यां उपयुज्य पुनः आह्वयन्तु।
- आपत्काले परिचयस्य सत्यापनार्थं परिवारस्य वा कार्यस्थलस्य वा सुरक्षितशब्दं निर्धारयन्तु।
- केवलं कालस्य अथवा वीडियो इत्यस्य आधारेण कदापि भुगतानं न अधिकृत्यताम्। पृथक् मार्गेण लिखितरूपेण पुष्टिं कुर्वन्तु।
- प्रतिक्रियां कर्तुं पूर्वं विरामं कुर्वन्तु। धमकी-नटः भवतः निर्णयं मेघं कर्तुं आतङ्कस्य उपरि अवलम्बन्ते ।

कृत्रिमबुद्ध्या सहायितं दुष्टसॉफ्ट्वेअरम् च स्वयंचालिताः आक्रमणाः



कथं कार्यं करोति ?

धमकी-अभिनेतारः दुर्भावनापूर्ण-सङ्केतं निर्मातुं वा गोपनार्थं वा, बहु-साइट्-मध्ये चोरित-गुप्तशब्दानां परीक्षणाय, अद्यतनस्य आवश्यकतां विद्यमानानाम् प्रणालीनां परिचयाय च AI-उपकरणानाम् उपयोगं कुर्वन्ति । अनेन आक्रमणानि शीघ्रं व्यापकं च भवन्ति ।

कथं परिचयः करणीयः ?

- अप्रत्याशितप्रवेशसचेतनाः, गुप्तशब्दपुनर्स्थापन-ईमेलाः, अथवा MFA-प्रोम्प्ट्-आदयः भवता न अनुरोधिताः
- भवतः खातेः क्रियाकलापस्य सूचीकृतानि अपरिचितयन्त्राणि वा सत्राणि वा
- एण्टीवायरसचेतावनी, पॉप-अप, अथवा असामान्यतया मन्दयन्त्रस्य कार्यक्षमता
- सञ्चिकाः, सेटिङ्ग्स्, ब्राउजर्-विस्तारः वा भवन्तः न परिचिनुवन्ति

कथं सुरक्षितं स्थातव्यम् ?

- प्रत्येकं खातेः कृते अद्वितीयं, दृढं गुप्तशब्दं उपयुज्यताम् ।
- सर्वेषु महत्त्वपूर्णलेखेषु बहुकारकप्रमाणीकरणं (MFA) सक्षमं कुर्वन्तु ।
- एण्टीवायरस सॉफ्टवेयर, सिस्टम्, एप्स् च अद्यतनं कुर्वन्तु।
- अप्रत्याशितप्रवेशस्य अथवा MFA अलर्टस्य तत्क्षणमेव कार्यं कुर्वन्तु।

नकली वेबसाइट एवं पहचान चोरी



कथं कार्यं करोति ?

धमकी-अभिनेतारः भवतः प्रवेशप्रमाणपत्राणि, OTPs, अथवा भुक्तिविवरणं चोरयितुं समानरूपेण दृश्यमानानि वेबसाइट्-चैटबोट्-इत्येतत् निर्मातुम् अर्हन्ति ये वास्तविकरूपेण दृश्यन्ते, यथा बैंकिंग् अथवा शॉपिंग-पोर्टल्-इत्येतत् ते मिथ्यापरिचयस्य निर्माणार्थं नकलीचित्रं वा दस्तावेजं वा उपयोक्तुं शक्नुवन्ति।

कथं परिचयः करणीयः ?

- किञ्चित् परिवर्तिताः वेबसाइट् URL, यथा अतिरिक्ताक्षराणि, हाइफन्, अथवा भिन्नः डोमेन् समाप्तिः।
- OTPs, PINs, अथवा पूर्णकार्डसङ्ख्यां याचमानाः Chatbots अथवा एजेण्ट्।
- परिचितस्थले HTTPS अथवा असामान्यडिजाइनविसंगतयः अनुपलब्धाः।

कथं सुरक्षितं स्थातव्यम् ?

- सदैव आधिकारिक-URL प्रत्यक्षतया टङ्कयन्तु अथवा सत्यापितपुस्तकचिह्नानां उपयोगं कुर्वन्तु, न तु लिङ्क् क्लिक् कर्तुं
- कदापि कस्यचित् चैट्बोट् अथवा "समर्थन एजेण्ट्" इत्यनेन सह OTPs, PINs, अथवा पूर्णकार्डविवरणं न साझां कुर्वन्तु।
- HTTPS इति पश्यन्तु तथा च कुत्रापि प्रवेशात् पूर्वं डोमेननाम सम्यक् पश्यन्तु
- अपरिचितक्रियाकलापस्य कृते नियमितरूपेण स्वस्य बैंकविवरणानां ऋणप्रतिवेदनानां च निरीक्षणं कुर्वन्तु।

अस्मान् अनुसरणं कुर्वन्तु : @IndianCERT @cert_india

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

RED FLAGS CHECKLIST

AI-सक्षम-आक्रमणस्य एतानि लक्षणानि पश्यन्तु:

- धनस्य, प्रमाणपत्रस्य, अनुमोदनस्य वा त्वरितम्, दबावपूर्ण अनुरोधम्
- "ज्ञातस्य" व्यक्तिस्य आह्वानस्य वा भिडियो वा मामूली श्रव्य/वीडियो असङ्गतिः
- सामान्यसत्यापन/ अनुमोदनप्रक्रियाः बाईपासं कर्तुं अनुरोधः
- अपरिचितं प्रेषकक्षेत्रं वा किञ्चित् परिवर्तितं URL वा
- अप्रत्याशित MFA प्रॉम्प्ट् अथवा OTPs भवता अनुरोधः न कृतः
- सुरक्षासॉफ्टवेयरं निष्क्रियं कर्तुं अथवा अनधिकृतलिङ्कद्वारा "सत्यापनं" कर्तुं अनुरोधं करोति
- अग्रिमभुक्तिं वा व्यक्तिगतवित्तीयविवरणं वा आवश्यकं कार्यं/निवेशप्रस्तावः

यदा संशयः भवति तदा — विरामं कुरुत, स्वतन्त्रतया सत्यापयन्तु, दबावेन न कार्यं कुर्वन्तु ।

अस्मान् अनुसरणं कुर्वन्तु :
@IndianCERT
@cert_india

ऑनलाइन सुरक्षा



स्वस्य खातानां रक्षणं कुर्वन्तु

- प्रत्येकं खातेः कृते दृढं अद्वितीयं च गुप्तशब्दं उपयुज्यताम्; तान् सुरक्षितरूपेण संग्रहीतुं गुप्तशब्दप्रबन्धकस्य उपयोगं कुर्वन्तु ।
- यत्र यत्र उपलब्धं तत्र बहुकारकप्रमाणीकरणं (MFA) सक्षमं कुर्वन्तु ।
- कदापि कस्यचित् सह OTP, PIN, गुप्तशब्दाः, सुरक्षासङ्केताः वा न साझाः कुर्वन्तु ।
- अतिरिक्तसुरक्षास्तररूपेण बायोमेट्रिकप्रमाणीकरणस्य (अङ्गुलिचिह्न/मुखपरिचयः) उपयोगं कुर्वन्तु ।

ईमेल & अन्तर्जालस्य उपयोगं कुर्वन् सुरक्षिताः तिष्ठन्तु

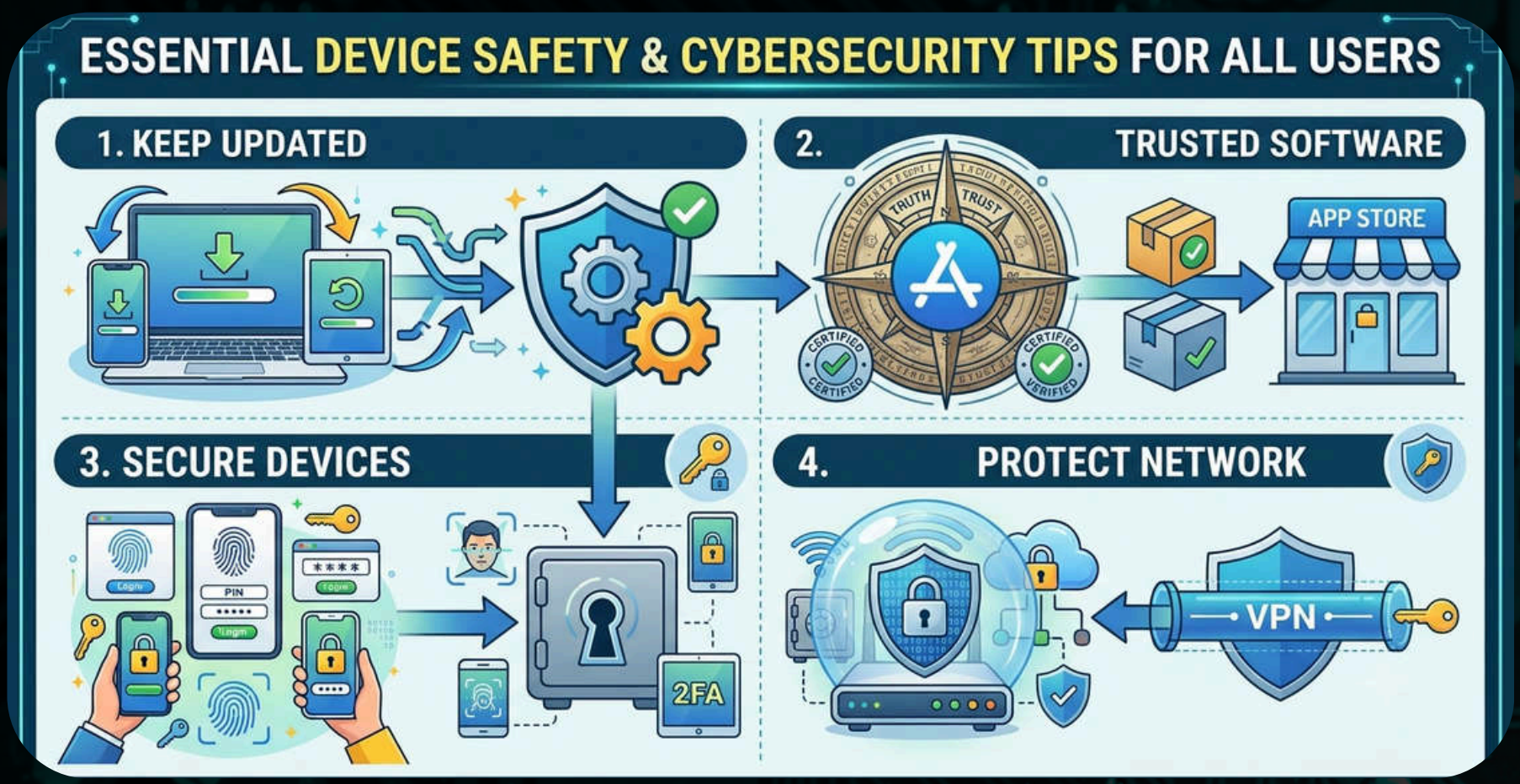
- संदिग्धानां अथवा समानरूपस्य ईमेल-सङ्केतानां कृते प्रेषकस्य विवरणं सावधानीपूर्वकं पश्यन्तु ।
- क्लिक् करणात् पूर्वं लिङ्कानि सत्यापयन्तु, अप्रत्याशित-संलग्नकानि उद्घाटयितुं परिहरन्तु ।
- प्रवेशं वा वित्तीयविवरणं वा प्रविष्टुं पूर्वं वेबसाइट् प्रामाणिकतायाः पुष्टिं कुर्वन्तु।
- यदा संशयः भवति तदा कार्यं कर्तुं पूर्वं निवर्त्य सत्यापयन्तु।

किमपि भ्रष्टं भवितुं पूर्वं सज्जतां कुर्वन्तु

- अफलाइन अथवा सुरक्षितमेघसेवायां संगृहीतानां महत्त्वपूर्णसञ्चिकानां नियमितरूपेण बैकअपं निर्वाहयन्तु
- खातापुनर्प्राप्तिसूचनाः (ईमेल/फोनः) अद्यतनं सुरक्षितं च कुर्वन्तु

अस्मान् अनुसरणं कुर्वन्तु : @IndianCERT @cert_india

उपकरण सुरक्षा



उपकरणानि अद्यतनं कुर्वन्तु

- ज्ञातानि दुर्बलतानि निवारयितुं नियमितरूपेण प्रचालनतन्त्राणि, अनुप्रयोगाः, ब्राउजर्, सुरक्षासॉफ्टवेयरं च अद्यतनं कुर्वन्तु ।
- यत्र सम्भवं तत्र स्वचालितं अद्यतनं सक्षमं कुर्वन्तु।

केवलं विश्वसनीयं सॉफ्टवेयरं संस्थापयन्तु

- वास्तविकसॉफ्टवेयरस्य उपयोगं कुर्वन्तु तथा च केवलं आधिकारिक एप्लिकेशनभण्डारतः अथवा विश्वसनीयस्रोतात् अनुप्रयोगाः संस्थापयन्तु।
- विश्वसनीयं एण्टीवायरसं वा सुरक्षासमाधानं वा उपयुज्य तान् अद्यतनं कुर्वन्तु।

स्वयन्त्राणि खातानि च सुरक्षितानि कुर्वन्तु

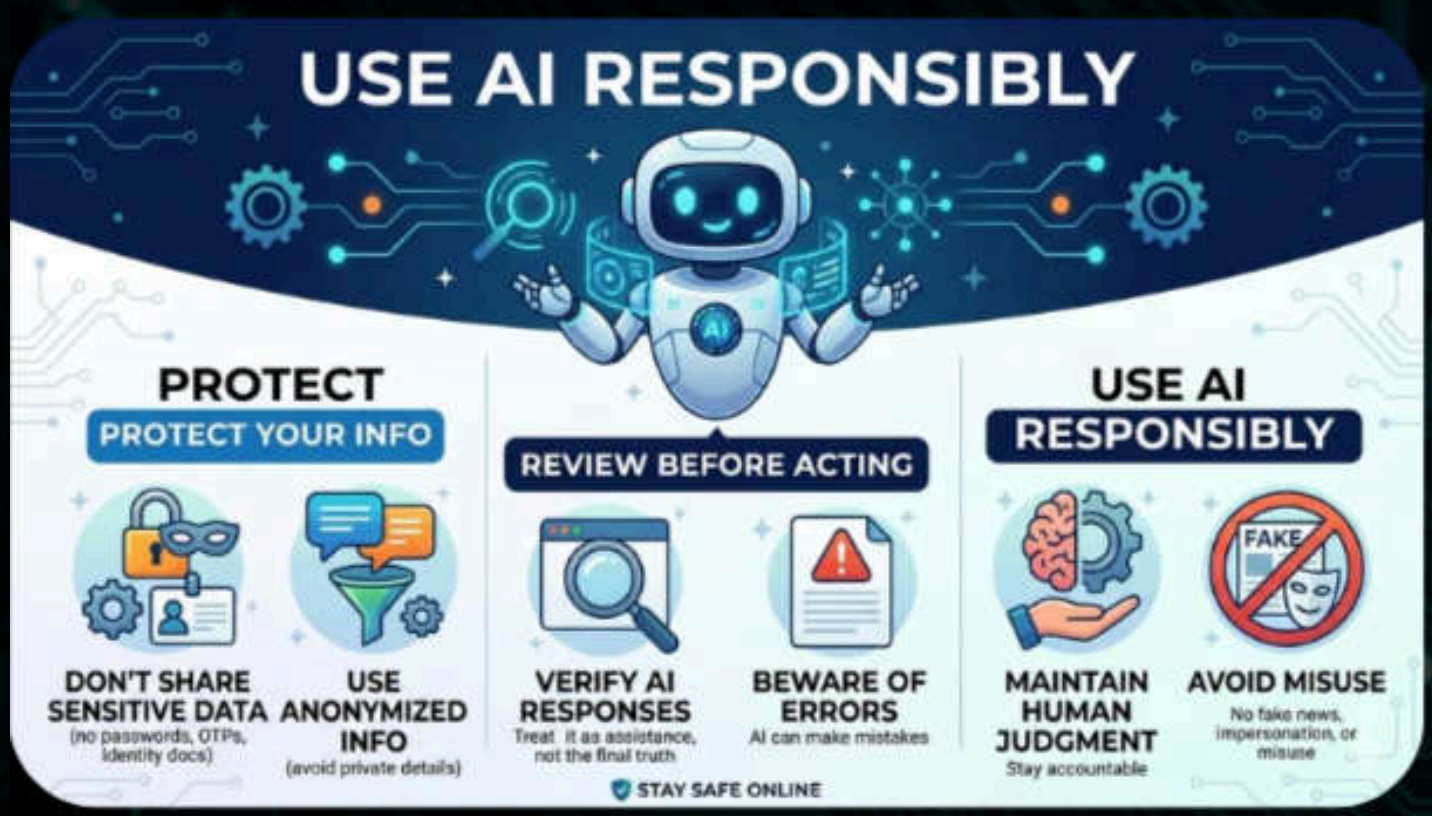
- सर्वेषु उपकरणेषु दृढगुप्तशब्दानां अथवा स्क्रीन-लॉक्-प्रयोगं कुर्वन्तु ।
- यदा यदा उपलब्धं भवति तदा तदा यन्त्रगुप्तीकरणं सुरक्षाविशेषताश्च सक्षमं कुर्वन्तु ।
- अनावश्यक-अनुप्रयोगानाम् अनुमतिनां च समीक्षां कृत्वा निष्कासयन्तु।

स्वस्य संजालसंयोजनस्य रक्षणं कुर्वन्तु

- दृढगुप्तशब्देन स्वस्य Wi-Fi सुरक्षितं कुर्वन्तु तथा च पूर्वनिर्धारितरूटरप्रमाणपत्रं परिवर्तयन्तु।
- अद्यतनं रूटर फर्मवेयरं सुरक्षितं संजालसेटिंग्स् च उपयुज्यताम् ।
- संवेदनशीललेखानां प्रवेशं वा असुरक्षितजालपुटेषु गोपनीयसूचनाः साझाकरणं वा परिहरन्तु ।

अस्मान् अनुसरणं कुर्वन्तु : @IndianCERT @cert_india

कृत्रिमबुद्धिं उत्तरदायित्वेन उपयोजयतु



स्वस्य व्यक्तिगतसूचनाः रक्षन्तु

- सार्वजनिक AI उपकरणेषु अथवा अज्ञातेषु ऑनलाइनसेवासु व्यक्तिगतं, वित्तीयं, स्वास्थ्यं, आधिकारिकं, गोपनीयं वा सूचनां न प्रविशन्तु।
- गुप्तशब्दाः, OTPs, खातासङ्ख्याः, परिचयदस्तावेजाः, ग्राहकदत्तांशः, निजीवार्तालापः इत्यादीनां संवेदनशीलविवरणानां साझेदारी परिहरन्तु ।
- AI-उपकरणानाम् सहायतां याचन्ते सति अनामिका वा सामान्यसूचनाः उपयुज्यताम् ।

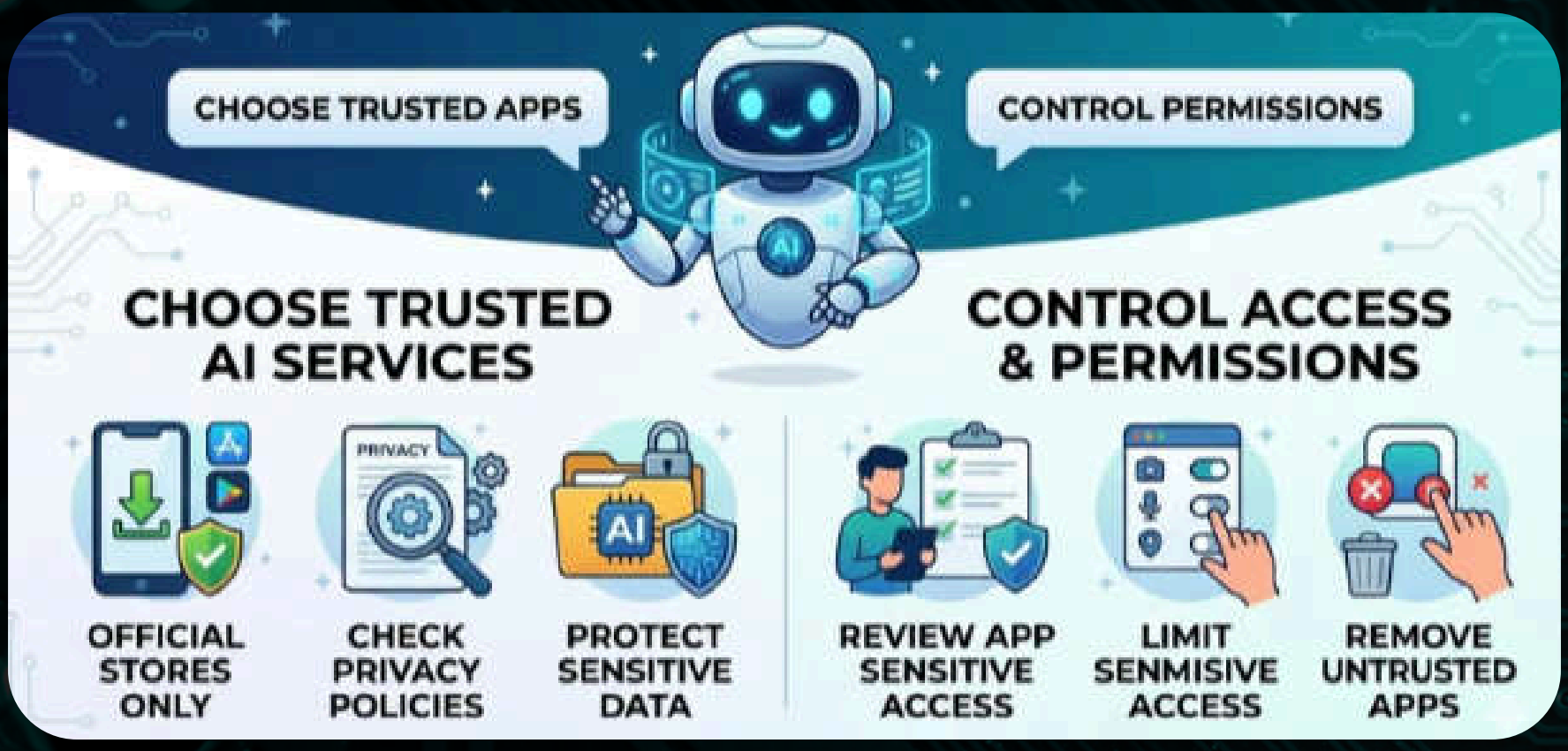
भवन्तः साझां कर्तुं वा कार्यं कर्तुं वा पूर्वं समीक्षां कुर्वन्तु

- AI-जनितप्रतिक्रियाः सहायतारूपेण व्यवहरन्तु, न तु सत्यस्य अन्तिमस्रोतरूपेण।
- वित्तीय, कानूनी, व्यावसायिक, अथवा व्यक्तिगतनिर्णयानां कृते उपयोगात् पूर्वं महत्त्वपूर्णसूचनाः सत्यापयन्तु।
- AI-उपकरणैः अशुद्धा, अपूर्णा, भ्रामकसूचना वा उत्पद्यन्ते इति अवगच्छन्तु ।

AI Tools इत्यस्य उत्तरदायित्वपूर्वकं उपयोगं कुर्वन्तु

- स्वस्य कार्यस्य शिक्षणस्य च समर्थनार्थं AI इत्यस्य उपयोगं कुर्वन्तु, परन्तु मानवीयविवेकं उत्तरदायित्वं च निर्वाहयन्तु।
- मिथ्यासूचनानिर्माणार्थं प्रसारयितुं वा, अन्येषां अनुकरणाय, कस्यचित् व्यक्तिगतदत्तांशस्य दुरुपयोगाय वा AI इत्यस्य उपयोगं न कुर्वन्तु ।

विश्वसनीयान् अनुप्रयोगान् चिनुत



अनुप्रयोगप्रवेशं अनुमतिं च नियच्छतु

- AI अनुप्रयोगेभ्यः डिजिटलसहायकेभ्यः च प्रदत्तानां अनुमतिनां समीक्षां कुर्वन्तु।
- यदा कॅमेरा, माइक्रोफोन, सम्पर्कः, स्थानं वा इत्यादीनां विशेषतानां आवश्यकता भवति तदा एव प्रवेशं अनुमन्यताम् ।
- अनावश्यकं अनुमतिं निष्कास्य अविश्वसनीयस्रोताभ्यः एप्स् विस्थापयन्तु।

विश्वसनीयाः AI सेवाः चिनोतु

- प्रतिष्ठितप्रदातृभ्यः AI-अनुप्रयोगानाम् उपयोगं कुर्वन्तु तथा च केवलं आधिकारिक-एप्-भण्डारतः तान् डाउनलोड् कुर्वन्तु ।
- AI सेवानां उपयोगात् पूर्वं गोपनीयतासेटिंग्स्, उपयोगस्य नियमाः, आँकडानिबन्धनप्रथाः च समीक्षयन्तु ।
- यावत् सुरक्षानियन्त्रणानि सत्यापितं न भवन्ति तावत् AI-उपकरणानाम् संवेदनशीललेखानां वा सञ्चिकानां वा संयोजनं परिहरन्तु ।

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