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 मार्गदर्शक

## सायबर स्वच्छतेची संस्कृती निर्माण करा

#सायबरस्वच्छताआमचीसंस्कृती



# राष्ट्रीय सायबर सुरक्षा जागरूकता महिना (ऑक्टोबर २०२६)

प्रकाशक

**भारतीय संगणक आपत्कालीन प्रतिसाद पथक**

आम्हाला फॉलो करा :

@IndianCERT

@cert_india

# अनुक्रमणिका

प्रस्तावना ३

AI-वर्धित फिशिंग आणि सोशल इंजिनिअरिंग ४

व्हॉइस आणि व्हिडिओ डीपफेक (विशिंग) ५

AI-सहाय्यित मालवेअर आणि स्वयंचलित हल्ले ६

बनावट वेबसाइट्स आणि ओळख चोरी ७

धोक्याच्या चिन्हांची तपासणी सूची ८

ऑनलाइन सुरक्षितता ९

उपकरणाची सुरक्षितता १०

AIचा जबाबदारीने वापर करा ११

विश्वसनीय ॲप्स निवडा १२

सायबर सुरक्षा घटनांची माहिती CERT-In ला द्या. १३

# प्रस्तावना

कृत्रिम बुद्धिमत्ता (AI) आपल्या जगण्याची, काम करण्याची आणि संवाद साधण्याची पद्धत बदलत आहे. यामुळे नवनिर्मितीला चालना मिळते, उत्पादकता सुधारते आणि विविध क्षेत्रांतील गुंतागुंतीच्या समस्या सोडवण्यास मदत होते. तथापि, याच तंत्रज्ञानाचा गैरवापर धोकादायक घटकांकडून अधिक प्रगत आणि विश्वासार्ह सायबर धोके निर्माण करण्यासाठी देखील केला जात आहे.

AI मुळे डिजिटल धोके ओळखणे अधिक कठीण होत आहे, कारण हल्लेखोर आता अत्यंत वास्तववादी ईमेल, संदेश, ऑडिओ, व्हिडिओ आणि वेबसाइट्स तयार करू शकतात. खराब व्याकरण, असामान्य मांडणी किंवा उघड चुका यांसारखी पारंपरिक धोक्याची चिन्हे आता विश्वसनीय निर्देशक ठरू शकत नाहीत. पडताळणी आणि जबाबदार डिजिटल पद्धती पूर्वीपेक्षा अधिक महत्त्वाच्या झाल्या आहेत.

आपण दररोज वापरत असलेली AI साधने आणि स्मार्ट उपकरणे काळजीपूर्वक न वापरल्यास गोपनीयतेचे आणि सुरक्षेचे नवीन धोके निर्माण करू शकतात. अविश्वसनीय AI ॲप्लिकेशन्ससोबत वैयक्तिक किंवा गोपनीय माहिती शेअर करणे, अनावश्यक परवानग्या देणे, किंवा पडताळणी न करता AI ने तयार केलेल्या माहितीवर अवलंबून राहणे, यामुळे व्यक्ती आणि संस्था सुरक्षेच्या धोक्यात येऊ शकतात.

इंडियन कॉम्प्युटर इमर्जन्सी रिस्पॉन्स टीम (CERT-In) द्वारे प्रकाशित “AI सायबर जागरूकता” या विषयावरील ही पुस्तिका केवळ सायबर सुरक्षा व्यावसायिकांसाठीच नाही, तर सर्वसामान्य नागरिक, कर्मचारी आणि डिजिटल वापरकर्त्यांसाठी तयार करण्यात आली आहे. AI डिजिटल धोक्याचे स्वरूप कसे बदलत आहे हे यात स्पष्ट केले आहे आणि वैयक्तिक माहिती, उपकरणे व ऑनलाइन ओळख यांचे संरक्षण करण्यासाठी प्रत्येकजण अवलंब करू शकतील अशा सोप्या, व्यावहारिक पायऱ्या दिल्या आहेत.

# AI-वर्धित फिशिंग आणि सोशल इंजिनिअरिंग




## हे कसे काम करते?

धोका निर्माण करणारे आता असे ईमेल आणि मजकूर पाठवतात जे खरे आणि त्रुटीरहित दिसतात. संदेश वैयक्तिक वाटावेत यासाठी ते तुमच्याबद्दलची माहिती, जसे की तुमची नोकरी, तुम्ही वापरत असलेल्या सेवा किंवा अलीकडील घडामोडी, वापरतात. हे संदेश अतिशय चांगल्या प्रकारे लिहिलेले असल्यामुळे, त्यांना ओळखणे खूप कठीण होऊ शकते.

## कसे ओळखावे?

- तो संदेश तुम्हाला अत्यंत विशिष्ट वाटतो, पण तो अनपेक्षितपणे येतो.
- त्यात तातडीचा किंवा धमकीवजा सूर असतो आणि त्वरित कृतीची मागणी केली जाते.
- ते तुम्हाला लिंकवर क्लिक करण्यास, खाते सत्यापित करण्यास, पासवर्ड रीसेट करण्यास किंवा पेमेंट करण्यास सांगते.
- प्रेषकाचा पत्ता जवळपास बरोबर वाटतो, पण पूर्णपणे नाही.

## सुरक्षित कसे राहावे?

- न मागवलेल्या संदेशांमधील लिंक्सवर क्लिक करू नका. त्याऐवजी थेट अधिकृत वेबसाइट किंवा ॲपवर जा.
- अधिकृत फोन नंबर किंवा ॲपसारख्या वेगळ्या, विश्वसनीय संपर्क माध्यमाद्वारे विनंत्यांची पडताळणी करा.
- मेसेज लिंकद्वारे पोहोचलेल्या पेजवर कधीही क्रेडेन्शियल्स किंवा ओटीपी टाकू नका.
- संशयास्पद संदेशांची तक्रार करा आणि ते हटवा, त्यानंतर पाठवणाऱ्याला ब्लॉक करा.

# व्हॉइस आणि व्हिडिओ डीपफेक्स [विशिंग]




## हे कसे काम करते?

धमकी देणारे घटक आवाज क्लोन करू शकतात किंवा खरे वाटतील असे बनावट व्हिडिओ तयार करू शकतात. ते तुमच्यावर संवेदनशील माहिती देण्यासाठी, पैसे पाठवण्यासाठी किंवा त्वरित कृती करण्यासाठी दबाव टाकण्याकरिता कुटुंब, सहकारी किंवा अधिकारी असल्याचे भासवू शकतात.

## कसे ओळखावे?

- असामान्य तातडी, घबराट किंवा 'कोणालाही सांगू नका' यासारख्या गुप्ततेच्या विनंत्या.
- थोडासा विसंगत सूर, गती, पार्श्वभूमीतील आवाज किंवा ऑडिओची गुणवत्ता.
- सामान्य पडताळणी किंवा मंजुरी प्रक्रिया वगळण्याची विनंती.
- गिफ्ट कार्ड, क्रिप्टोकरन्सी किंवा वायर ट्रान्सफरद्वारे पेमेंट करण्याची विनंती.

## सुरक्षित कसे राहावे?

- फोन ठेवा आणि त्या व्यक्तीला त्यांच्या ओळखीच्या, सेव्ह केलेल्या नंबरवरून परत कॉल करा.
- आणीबाणीच्या परिस्थितीत ओळख पटवण्यासाठी कुटुंबासाठी किंवा कामाच्या ठिकाणी एक सुरक्षित शब्द निश्चित करा.
- केवळ कॉल किंवा व्हिडिओच्या आधारावर पेमेंटला कधीही मंजुरी देऊ नका. एका वेगळ्या माध्यमाद्वारे लेखी स्वरूपात पुष्टी करा.
- प्रतिक्रिया देण्यापूर्वी थांबा. धोका निर्माण करणारे तुमच्या निर्णयक्षमतेवर परिणाम करण्यासाठी तुमच्यातील घबराटीचा फायदा घेतात.

# AI-सहाय्यित मालवेअर आणि स्वयंचलित हल्ले




## हे कसे काम करते?

हल्लेखोर दुर्भावनापूर्ण कोड तयार करण्यासाठी किंवा लपवण्यासाठी, चोरलेले पासवर्ड अनेक साइट्सवर तपासण्यासाठी आणि अद्ययावतीकरणाची आवश्यकता असलेल्या प्रणाली ओळखण्यासाठी AI साधनांचा वापर करतात. यामुळे हल्ले अधिक जलद आणि व्यापक होतात.

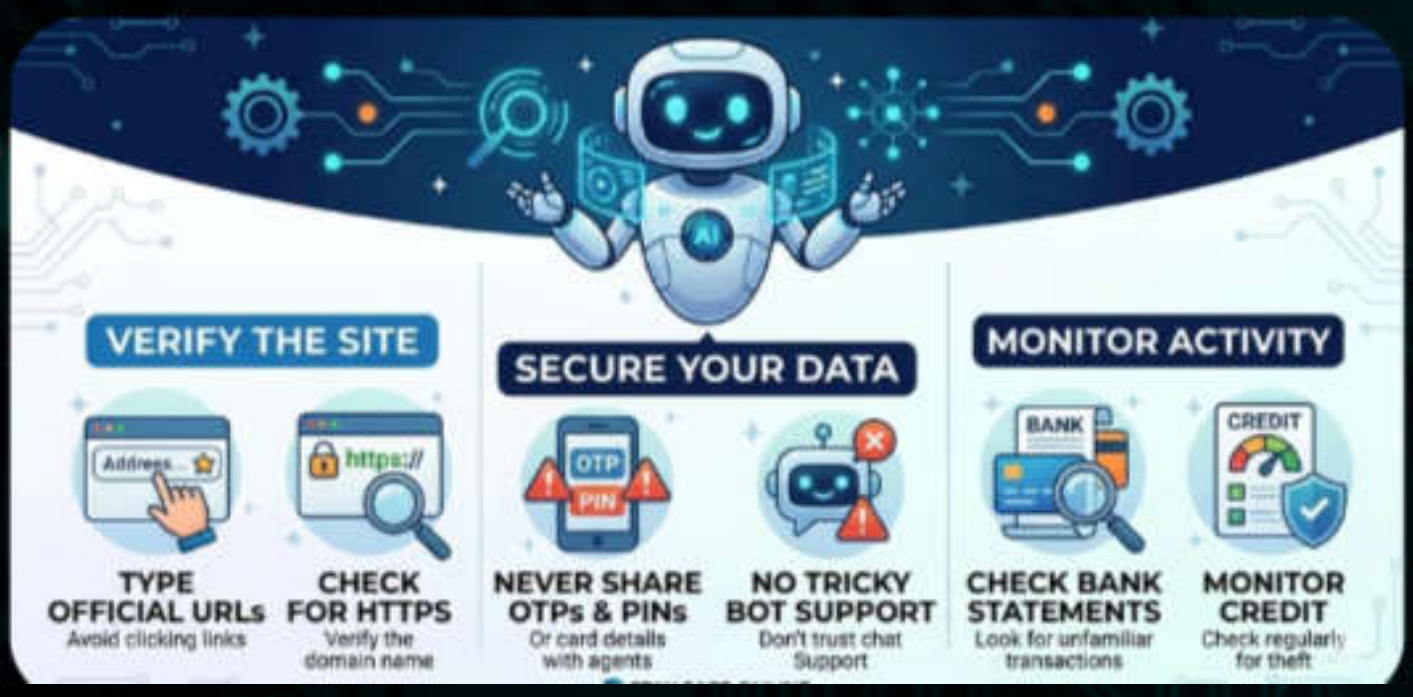
## कसे ओळखावे?

- अनपेक्षित लॉगिन अलर्ट, पासवर्ड रीसेट ईमेल किंवा तुम्ही विनंती न केलेले MFA प्रॉम्प्ट
- तुमच्या खात्याच्या हालचालींमध्ये सूचीबद्ध केलेली अपरिचित उपकरणे किंवा सत्रे
- अँटीव्हायरस चेतावण्या, पॉप-अप किंवा डिव्हाइसची असामान्यपणे मंद कामगिरी
- तुम्हाला अपरिचित असलेल्या फाइल्स, सेटिंग्स किंवा ब्राउझर एक्सटेंशन्स

## सुरक्षित कसे राहावे?

- प्रत्येक खात्यासाठी एकच आणि मजबूत पासवर्ड वापरा.
- सर्व महत्त्वाच्या खात्यांवर मल्टी फॅक्टर ऑथेंटिकेशन (MFA) सक्षम करा.
- अँटीव्हायरस सॉफ्टवेअर, सिस्टीम आणि ॲप्स अद्ययावत ठेवा.
- अनपेक्षित लॉगिन किंवा एमएफए (MFA) अलर्ट आल्यास तात्काळ कारवाई करा.

# बनावट वेबसाइट्स आणि ओळख चोरी




## हे कसे काम करते?

धोका निर्माण करणारे घटक तुमचे लॉगिन क्रेडेन्शियल्स, ओटीपी किंवा पेमेंट तपशील चोरण्यासाठी, बँकिंग किंवा शॉपिंग पोर्टल्ससारख्या खऱ्या वाटणाऱ्या बनावट वेबसाइट्स आणि चॅटबॉट्स तयार करू शकतात. ते खोटी ओळख निर्माण करण्यासाठी बनावट फोटो किंवा कागदपत्रांचा वापर देखील करू शकतात.

## कसे ओळखावे?

- वेबसाइटच्या URL मध्ये थोडे बदल, जसे की अतिरिक्त अक्षरे, हायफन किंवा वेगळा डोमेन शेवट.
- चॅटबॉट्स किंवा एजंट ओटीपी, पिन किंवा संपूर्ण कार्ड नंबर मागत आहेत.
- परिचित साइटवर HTTPS चा अभाव किंवा डिझाइनमधील असामान्य विसंगती.

## सुरक्षित कसे राहावे?

- लिंक्सवर क्लिक करण्याऐवजी, नेहमी अधिकृत युआरएल थेट टाईप करा किंवा सत्यापित बुकमार्क्स वापरा.
- कोणत्याही चॅटबॉट किंवा 'सपोर्ट एजंट'ला ओटीपी, पिन किंवा कार्डचा संपूर्ण तपशील कधीही देऊ नका.
- कुठेही लॉग इन करण्यापूर्वी HTTPS तपासा आणि डोमेन नावाचे काळजीपूर्वक निरीक्षण करा.
- तुमच्या बँक स्टेटमेंट आणि क्रेडिट रिपोर्टमध्ये काही अनोळखी व्यवहार होत आहेत का, हे नियमितपणे तपासा.

# धोक्याच्या चिन्हांची तपासणी सूची

## AI-सक्षम हल्ल्याची ही चिन्हे लक्षात ठेवा:

- पैसे, पात्रता किंवा मंजुरीसाठी केलेली तातडीची, दबावपूर्ण मागणी
- 'ओळखीच्या' व्यक्तीकडून आलेल्या कॉल किंवा व्हिडिओमध्ये ऑडिओ/व्हिडिओमधील किरकोळ विसंगती
- सामान्य पडताळणी/मंजुरी प्रक्रियेला वगळण्याची विनंती
- अनोळखी प्रेषक डोमेन किंवा किंचित बदललेला URL
- अनपेक्षित MFA प्रॉम्प्ट्स किंवा तुम्ही विनंती न केलेले OTP
- सुरक्षा सॉफ्टवेअर निष्क्रिय करण्याच्या किंवा अनधिकृत लिंकद्वारे "सत्यापित" करण्याच्या विनंत्या
- नोकरी/गुंतवणुकीच्या ऑफर्स ज्यासाठी आगाऊ रक्कम किंवा वैयक्तिक आर्थिक तपशील आवश्यक असतो

**शंका असल्यास — थांबा, स्वतंत्रपणे पडताळणी करा आणि दबावाखाली कृती करू नका.**

# ऑनलाइन सुरक्षितता



## तुमची खाती सुरक्षित ठेवा

- प्रत्येक खात्यासाठी मजबूत आणि वेगवेगळे पासवर्ड वापरा; ते सुरक्षितपणे साठवण्यासाठी पासवर्ड मॅनेजरचा वापर करा.
- जिथे जिथे उपलब्ध असेल तिथे मल्टी-फॅक्टर ऑथेंटिकेशन (MFA) सक्षम करा.
- ओटीपी, पिन, पासवर्ड किंवा सुरक्षा कोड कोणासोबतही कधीही शेअर करू नका.
- सुरक्षेचा अतिरिक्त स्तर म्हणून बायोमेट्रिक प्रमाणीकरणाचा (बोटांचे ठसे/चेहऱ्याची ओळख) वापर करा.

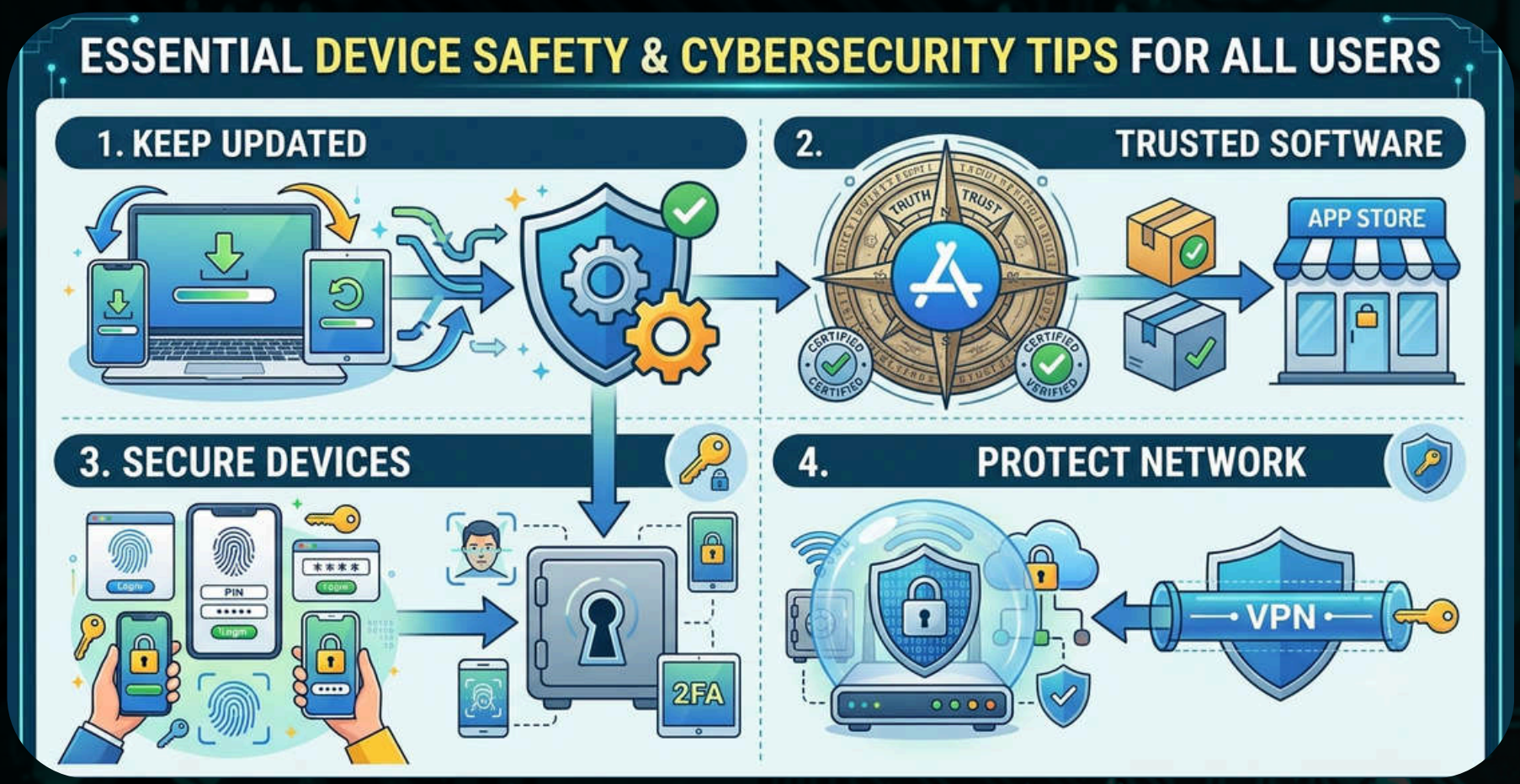
## ईमेल आणि इंटरनेट वापरताना सुरक्षित रहा

- संशयास्पद किंवा सारख्या दिसणाऱ्या ईमेल ॲड्रेससाठी प्रेषकाचा तपशील काळजीपूर्वक तपासा.
- लिंकवर क्लिक करण्यापूर्वी त्या तपासा आणि अनपेक्षित संलग्नक उघडणे टाळा.
- लॉगिन किंवा आर्थिक तपशील प्रविष्ट करण्यापूर्वी वेबसाइटच्या सत्यतेची खात्री करा.
- शंका असल्यास, कृती करण्यापूर्वी थांबा आणि पडताळणी करा.

## काहीतरी चुकीचे होण्यापूर्वी तयारी करा

- महत्त्वाच्या फाईल्सचा नियमित बॅकअप ऑफलाइन किंवा सुरक्षित क्लाउड सेवेमध्ये साठवून ठेवा.
- खाते पुनर्प्राप्तीची माहिती (ईमेल/फोन) अद्ययावत आणि सुरक्षित ठेवा.

# उपकरणाची सुरक्षितता




## उपकरणे अद्ययावत ठेवा

- ज्ञात त्रुटी दूर करण्यासाठी ऑपरेटिंग सिस्टीम, ॲप्लिकेशन्स, ब्राउझर्स आणि सुरक्षा सॉफ्टवेअर नियमितपणे अद्ययावत करा.
- शक्य असेल तिथे स्वयंचलित अद्यतने चालू करा.

## केवळ विश्वसनीय सॉफ्टवेअरच स्थापित करा.

- अस्सल सॉफ्टवेअर वापरा आणि केवळ अधिकृत ॲप स्टोअर्स किंवा विश्वसनीय स्त्रोतांकडूनच ॲप्लिकेशन्स इन्स्टॉल करा.
- विश्वसनीय अँटीव्हायरस किंवा सुरक्षा प्रणाली वापरा आणि त्यांना अद्ययावत ठेवा.

## तुमची उपकरणे आणि खाती सुरक्षित करा

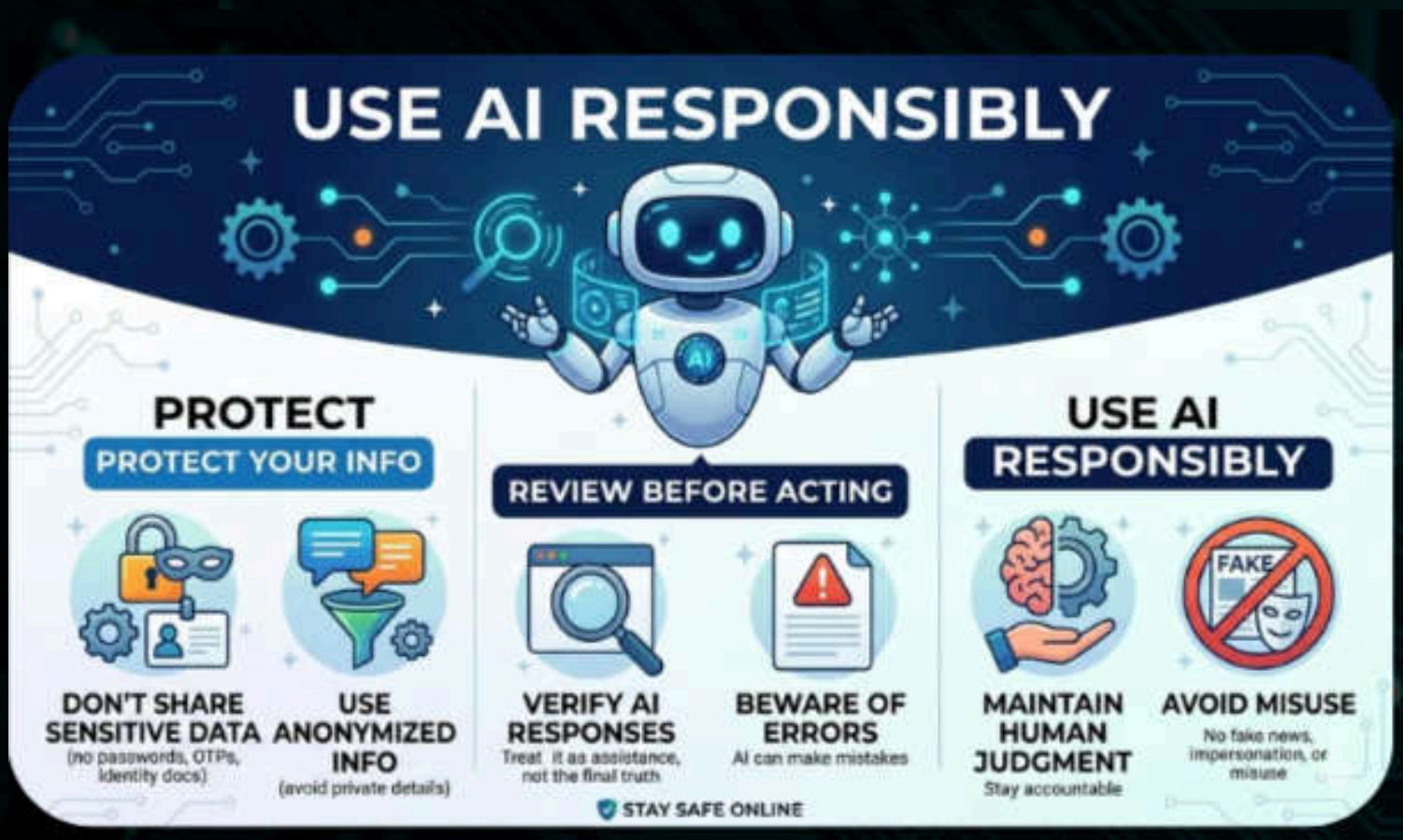
- सर्व उपकरणांवर मजबूत पासवर्ड किंवा स्क्रीन लॉक वापरा.
- जेव्हा उपलब्ध असतील तेव्हा डिव्हाइस एन्क्रिप्शन आणि सुरक्षा वैशिष्ट्ये सक्षम करा.
- अनावश्यक अनुप्रयोग आणि परवानग्या तपासा आणि काढून टाका.

## तुमचे नेटवर्क कनेक्शन सुरक्षित ठेवा.

- तुमचा वाय-फाय एका मजबूत पासवर्डने सुरक्षित करा आणि राउटरची डीफॉल्ट क्रेडेन्शियल्स बदला.
- अद्ययावत राउटर फर्मवेअर आणि सुरक्षित नेटवर्क सेटिंग्ज वापरा.
- असुरक्षित नेटवर्कवरून संवेदनशील खात्यांमध्ये प्रवेश करणे किंवा गोपनीय माहिती शेअर करणे टाळा.

आम्हाला फॉलो करा :
@IndianCERT
@cert_india

# AIचा जबाबदारीने वापर करा




## तुमची वैयक्तिक माहिती सुरक्षित ठेवा

- सार्वजनिक AI साधनांमध्ये किंवा अज्ञात ऑनलाइन सेवांमध्ये वैयक्तिक, आर्थिक, आरोग्यविषयक, अधिकृत किंवा गोपनीय माहिती प्रविष्ट करू नका.
- पासवर्ड, ओटीपी, खाते क्रमांक, ओळखपत्रे, ग्राहक माहिती किंवा खाजगी संभाषणे यांसारखी संवेदनशील माहिती इतरांना देणे टाळा.
- AI साधनांकडे मदत मागताना अनामिक किंवा सामान्य माहितीचा वापर करा.

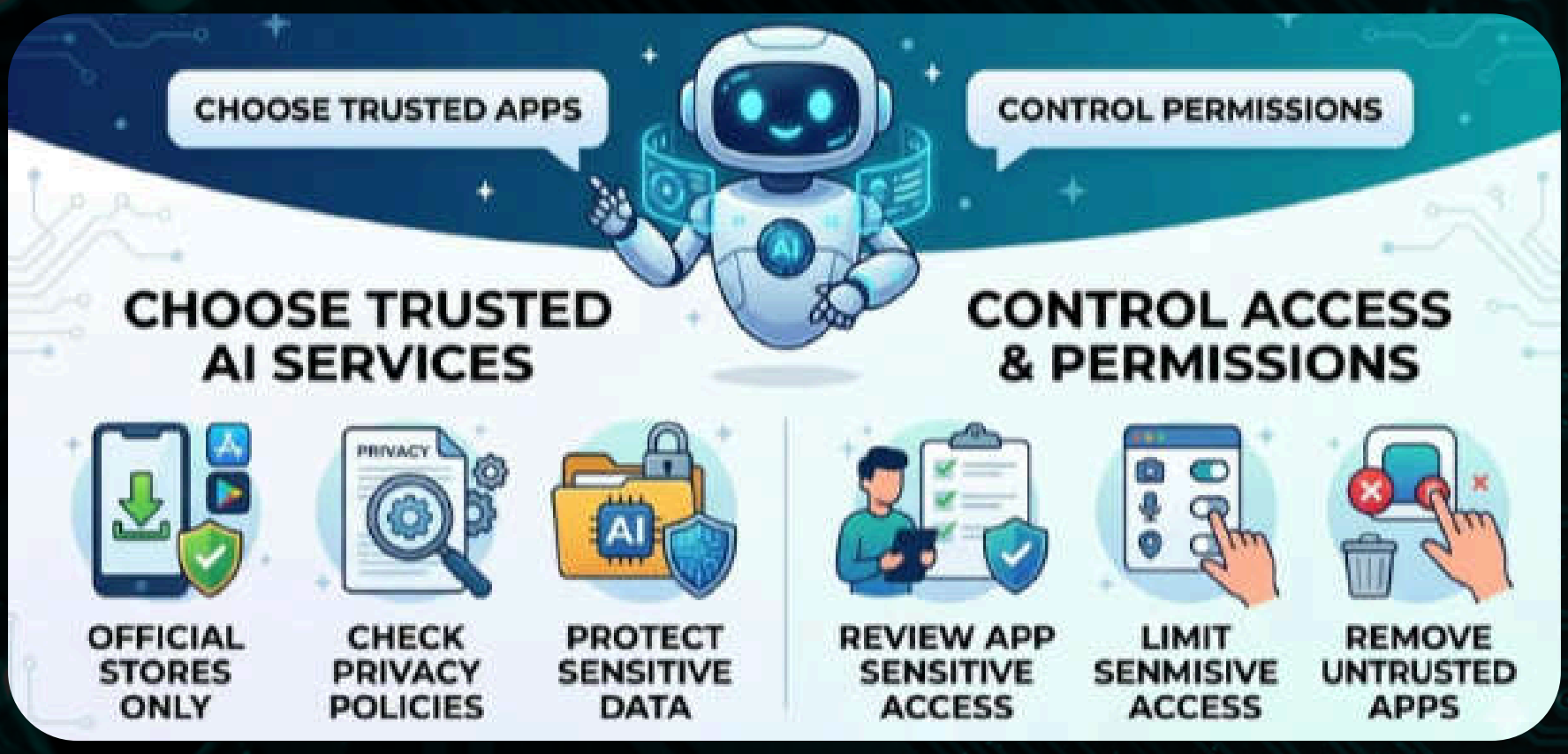
## शेअर करण्यापूर्वी किंवा कृती करण्यापूर्वी पुनरावलोकन करा.

- AI ने दिलेल्या प्रतिसादांना मदत म्हणून माना, अंतिम सत्य स्रोत म्हणून नव्हे.
- आर्थिक, कायदेशीर, व्यावसायिक किंवा वैयक्तिक निर्णयांसाठी महत्त्वाची माहिती वापरण्यापूर्वी तिची पडताळणी करा.
- हे लक्षात ठेवा की AI साधने चुकीची, अपूर्ण किंवा दिशाभूल करणारी माहिती देऊ शकतात.

## AI साधनांचा जबाबदारीने वापर करा

- तुमच्या कामात आणि शिकण्यात साहाय्य मिळवण्यासाठी AIचा वापर करा, पण मानवी विवेकबुद्धी आणि उत्तरदायित्व कायम ठेवा.
- खोटी माहिती तयार करण्यासाठी किंवा पसरवण्यासाठी, इतरांचे सोंग घेण्यासाठी किंवा एखाद्याच्या वैयक्तिक माहितीचा गैरवापर करण्यासाठी AIचा वापर करू नका.

# विश्वसनीय ॲप्स निवडा




## ॲपचा प्रवेश आणि परवानग्या नियंत्रित करा

- AI ॲप्लिकेशन्स आणि डिजिटल असिस्टंट्सना दिलेल्या परवानग्यांचे पुनरावलोकन करा.
- कॅमेरा, मायक्रोफोन, संपर्क किंवा स्थान यांसारख्या वैशिष्ट्यांसाठी केवळ आवश्यक असेल तेव्हाच प्रवेशास परवानगी द्या.
- अनावश्यक परवानग्या काढून टाका आणि अविश्वसनीय स्त्रोतांकडून आलेले ॲप्स अनइन्स्टॉल करा.

## विश्वसनीय AI सेवा निवडा

- प्रतिष्ठित प्रदात्यांकडून AI ॲप्लिकेशन्स वापरा आणि ती केवळ अधिकृत ॲप स्टोअर्सवरूनच डाउनलोड करा.
- AI सेवा वापरण्यापूर्वी गोपनीयता सेटिंग्ज, वापराच्या अटी आणि डेटा हाताळणीच्या पद्धतींचे पुनरावलोकन करा.
- सुरक्षा नियंत्रणांची पडताळणी झाल्याशिवाय AI साधनांना संवेदनशील खात्यांशी किंवा फाईल्सशी जोडणे टाळा.

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