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 آگاہی گائیڈ

سائبر حفظان صحت کا کلچر بنائیں

#CyberHygieneOurCulture



نیشنل سائبر سیکیورٹی بیداری کا مہینہ (اکتوبر 2026)

پبلشر

ہندوستانی کمپیوٹر ایمرجنسی رسپانس ٹیم

ہماری پیروی کریں:

@IndianCERT

@cert_india

مندرجات کا جدول

3 دیباچہ

4 AI سے بہتر فشنگ اور سوشل انجینئرنگ

5 آواز اور ویڈیو ڈیپ فیکس (ویشنگ)

6 AI کی مدد سے مالویئر اور خودکار حملے

7 جعلی ویب سائٹس اور شناخت کی چوری۔

8 سرخ جھنڈوں کی چیک لسٹ

9 آن لائن حفاظت

10 ڈیوائس کی حفاظت

11 AI کو ذمہ داری سے استعمال کریں۔

12 بھروسہ مند ایپس کا انتخاب کریں۔

13 سائبر سیکیورٹی کے واقعات کی اطلاع CERT-In کو دیں۔

دیباچہ

مصنوعی ذہانت (AI) ہمارے رہنے، کام کرنے اور بات چیت کرنے کے طریقے کو بدل رہی ہے۔ یہ جدت کو قابل بناتا ہے، پیداواری صلاحیت کو بہتر بناتا ہے، اور مختلف شعبوں میں پیچیدہ مسائل کو حل کرنے میں مدد کرتا ہے۔ تاہم، اسی ٹیکنالوجی کو مزید جدید اور قابل اعتماد سائبر خطرات پیدا کرنے کے لیے دھمکی دینے والے عناصر بھی غلط استعمال کر رہے ہیں۔

AI ڈیجیٹل خطرات کی نشاندہی کرنا مزید مشکل بنا رہا ہے کیونکہ حملہ آور اب انتہائی حقیقت پسندانہ ای میلز، پیغامات، آڈیو، ویڈیوز اور ویب سائٹس بنا سکتے ہیں۔ روایتی انتباہی علامات، جیسے ناقص گرامر، غیر معمولی فارمیٹنگ، یا واضح غلطیاں، اب قابل اعتماد اشارے نہیں رہ سکتے ہیں۔ تصدیق اور ذمہ دار ڈیجیٹل طرز عمل پہلے سے کہیں زیادہ اہم ہو گئے ہیں۔

AI ٹولز اور سمارٹ ڈیوائسز جو ہم ہر روز استعمال کرتے ہیں اگر انہیں احتیاط سے استعمال نہ کیا جائے تو وہ نئے رازداری اور حفاظتی خطرات کو متعارف کروا سکتے ہیں۔ غیر بھروسہ مند AI ایپلی کیشنز کے ساتھ ذاتی یا خفیہ معلومات کا اشتراک کرنا، غیر ضروری اجازتیں دینا، یا بغیر تصدیق کے AI سے تیار کردہ معلومات پر انحصار کرنا افراد اور تنظیموں کو سیکورٹی کے خطرات سے دوچار کر سکتا ہے۔

ہندوستانی کمپیوٹر ایمرجنسی رسپانس ٹیم (CERT-In) کی طرف سے "AI سائبر آگاہی" پر یہ کتابچہ نہ صرف سائبر سیکیورٹی پیشہ ور افراد بلکہ روزمرہ کے شہریوں، ملازمین اور ڈیجیٹل صارفین کے لیے ڈیزائن کیا گیا ہے۔ یہ بتاتا ہے کہ کس طرح AI ڈیجیٹل خطرے کے منظر نامے کو تبدیل کر رہا ہے اور آسان، عملی اقدامات فراہم کرتا ہے جن کی پیروی ہر کوئی ذاتی معلومات، آلات اور آن لائن شناخت کے تحفظ کے لیے کر سکتا ہے۔

AI بڑھا ہوا فشنگ اور سوشل انجینئرنگ



یہ کیسے کام کرتا ہے؟

دھمکی آمیز اداکار اب ای میلز اور متن بھیجتے ہیں جو حقیقی اور غلطی سے پاک نظر آتے ہیں۔ پیغامات کو ذاتی محسوس کرنے کے لیے وہ آپ کے بارے میں تفصیلات کا استعمال کرتے ہیں، جیسے آپ کی ملازمت، خدمات جو آپ استعمال کرتے ہیں، یا حالیہ سرگرمیاں۔ چونکہ یہ پیغامات اچھی طرح سے لکھے گئے ہیں، اس لیے انہیں تلاش کرنا بہت مشکل ہو سکتا ہے۔

شناخت کیسے کریں؟

- پیغام آپ کے لیے انتہائی مخصوص محسوس ہوتا ہے لیکن غیر متوقع طور پر پہنچ جاتا ہے۔
- یہ ایک فوری یا دھمکی آمیز لہجہ استعمال کرتا ہے اور فوری کارروائی کا مطالبہ کرتا ہے۔
- یہ آپ سے کسی لنک پر کلک کرنے، اکاؤنٹ کی تصدیق کرنے، پاس ورڈ دوبارہ ترتیب دینے، یا ادائیگی کرنے کو کہتا ہے۔
- بھیجنے والے کا پتہ لگ بھگ درست لگتا ہے، لیکن بالکل نہیں۔

محفوظ کیسے رہیں؟

- غیر منقولہ پیغامات میں لنکس پر کلک نہ کریں۔ اس کے بجائے براہ راست آفیشل ویب سائٹ یا ایپ پر جائیں۔
- ایک علیحدہ، بھروسہ مند رابطہ چینل، جیسے کہ آفیشل فون نمبر یا ایپ کے ذریعے درخواستوں کی تصدیق کریں۔
- کسی میسج لنک کے ذریعے پہنچنے والے صفحہ پر کبھی بھی اسناد یا OTP داخل نہ کریں۔
- مشکوک پیغامات کی اطلاع دیں اور حذف کریں، پھر بھیجنے والے کو بلاک کریں۔

آواز اور ویڈیو ڈیپ فیکس (ویشنگ)



یہ کیسے کام کرتا ہے؟

دھمکی آمیز اداکار آوازوں کو کلون کر سکتے ہیں یا جعلی ویڈیوز بنا سکتے ہیں جو حقیقی لگتی ہیں۔ وہ آپ کو حساس معلومات کا اشتراک کرنے، رقم بھیجنے، یا جلدی سے کام کرنے کے لیے دباؤ ڈالنے کے لیے خاندان، ساتھیوں، یا اہلکاروں کے طور پر ظاہر کر سکتے ہیں۔

شناخت کیسے کریں؟

- غیر معمولی عجلت، گھبراہٹ، یا رازداری کی درخواستیں، جیسے کسی کو نہ بتائیں۔
- تھوڑا سا آف ٹون، پیسنگ، بیک گراؤنڈ شور، یا آڈیو کوالٹی۔
- عام تصدیق یا منظوری کے عمل کو نظرانداز کرنے کی درخواستیں۔
- گفٹ کارڈز، کرپٹو کرنسی، یا وائر ٹرانسفر کے ذریعے ادائیگی کی درخواستیں۔

محفوظ کیسے رہیں؟

- بند کریں اور اس شخص کو ان کے معلوم، محفوظ کردہ نمبر کا استعمال کرکے واپس کال کریں۔
- ہنگامی حالات میں شناخت کی توثیق کرنے کے لیے خاندان یا کام کی جگہ پر محفوظ لفظ متعین کریں۔
- صرف کال یا ویڈیو کی بنیاد پر ادائیگیوں کی اجازت نہ دیں۔ ایک علیحدہ چینل کے ذریعے تحریری طور پر تصدیق کریں۔
- رد عمل ظاہر کرنے سے پہلے توقف کریں۔ دھمکی دینے والے اداکار آپ کے فیصلے پر بادل ڈالنے کے لیے گھبراہٹ پر انحصار کرتے ہیں۔

AI کی مدد سے مالویئر اور خودکار حملے



یہ کیسے کام کرتا ہے؟

دھمکی آمیز کوڈ بنانے یا چھپانے، متعدد سائٹس پر چوری شدہ پاس ورڈز کی جانچ کرنے، اور ایسے سسٹمز کی نشاندہی کرنے کے لیے جن کو اپ ڈیٹ کی ضرورت ہوتی ہے، دھمکی دینے والے AI ٹولز کا استعمال کرتے ہیں۔ یہ حملوں کو تیز اور زیادہ وسیع بناتا ہے۔

شناخت کیسے کریں؟

- غیر متوقع لاگ ان الرٹس، پاس ورڈ دوبارہ ترتیب دینے والی ای میلز، یا MFA پرامپٹس جن کی آپ نے درخواست نہیں کی۔
- آپ کے اکاؤنٹ کی سرگرمی میں درج غیر مانوس آلات یا سیشنز
- اینٹی وائرس وارننگز، پاپ اپس، یا آلہ کی غیر معمولی سست کارکردگی
- فائلیں، ترتیبات، یا براؤزر ایکسٹینشنز جنہیں آپ نہیں پہچانتے ہیں۔

محفوظ کیسے رہیں؟

- ہر اکاؤنٹ کے لیے ایک منفرد، مضبوط پاس ورڈ استعمال کریں۔
- تمام اہم اکاؤنٹس پر ملٹی فیکٹر توثیق (MFA) کو فعال کریں۔
- اینٹی وائرس سافٹ ویئر، سسٹمز اور ایپس کو اپ ٹو ڈیٹ رکھیں۔
- غیر متوقع لاگ ان یا MFA الرٹس پر فوری طور پر کارروائی کریں۔

جعلی ویب سائٹس اور شناخت کی چوری۔



یہ کیسے کام کرتا ہے؟

دھمکی دینے والے اداکار آپ کے لاگ ان کی اسناد، OTPs، یا ادائیگی کی تفصیلات چرانے کے لیے ایک جیسی ویب سائٹس اور چیٹ بوٹس بنا سکتے ہیں جو کہ حقیقی دکھائی دیتے ہیں، جیسے کہ بینکنگ یا شاپنگ پورٹلز۔ وہ جعلی شناخت بنانے کے لیے جعلی تصاویر یا دستاویزات بھی استعمال کر سکتے ہیں۔

شناخت کیسے کریں؟

- تھوڑا سا تبدیل شدہ ویب سائٹ یو آر ایل، جیسے اضافی حروف، ہائفنز، یا ایک مختلف ڈومین کا اختتام۔
- چیٹ بوٹس یا ایجنٹس جو PINs، OTPs، یا مکمل کارڈ نمبر مانگ رہے ہیں۔
- ایک مانوس سائٹ پر HTTPS غائب یا غیر معمولی ڈیزائن میں تضادات۔

محفوظ کیسے رہیں؟

- ہمیشہ آفیشل یو آر ایل براہ راست ٹائپ کریں یا لنکس پر کلک کرنے کے بجائے تصدیق شدہ بک مارکس کا استعمال کریں۔
- کسی بھی چیٹ بوٹ یا "سپورٹ ایجنٹ" کے ساتھ کبھی بھی PINs، OTPs، یا کارڈ کی مکمل تفصیلات کا اشتراک نہ کریں۔
- HTTPS چیک کریں اور کہیں بھی لاگ ان کرنے سے پہلے ڈومین کے نام کو قریب سے دیکھیں
- غیر مانوس سرگرمی کے لیے اپنے بینک اسٹیٹمنٹس اور کریڈٹ رپورٹ کی باقاعدگی سے نگرانی کریں۔

ریڈ فلیگ چیک لسٹ

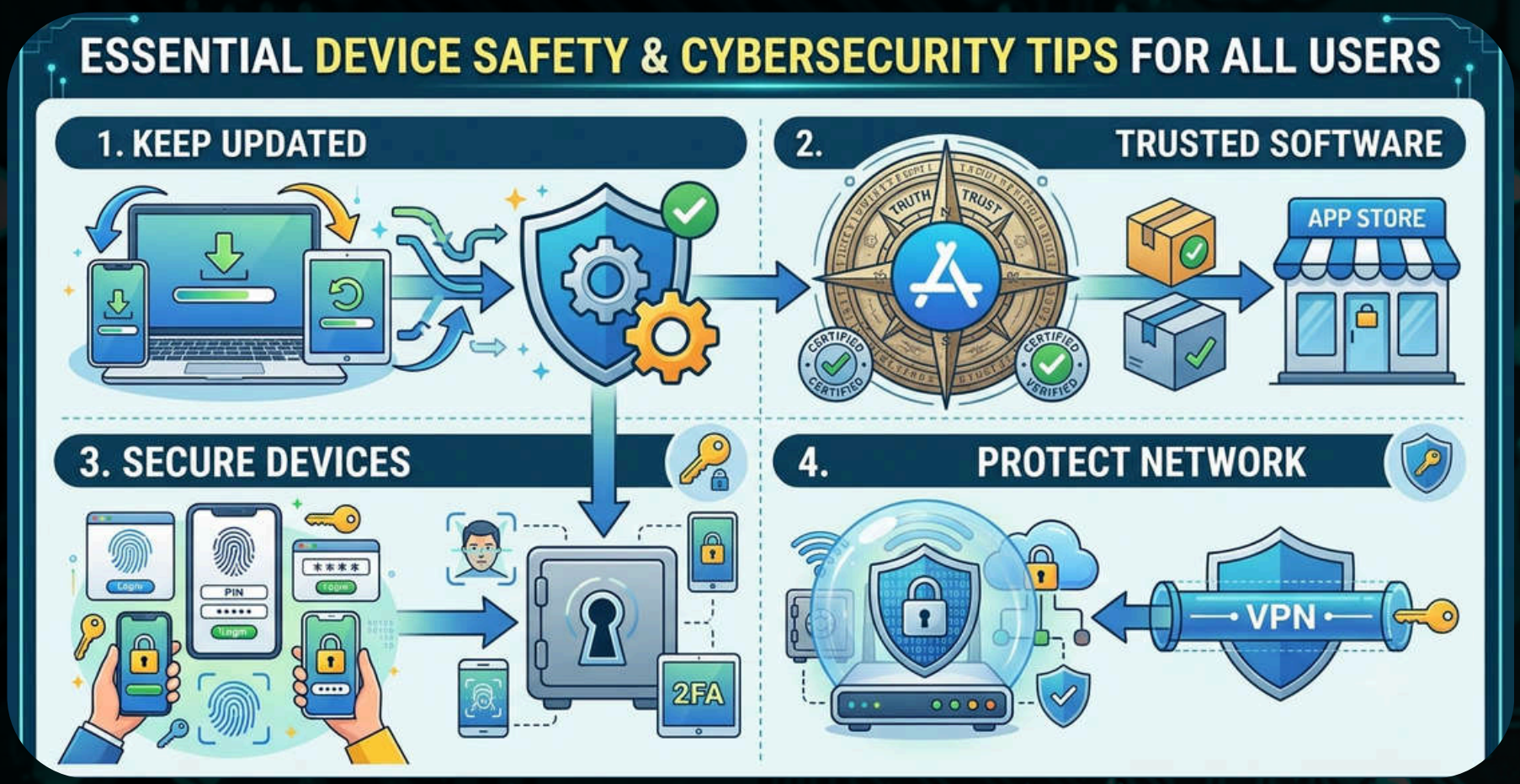
AI سے چلنے والے حملے کی ان علامات کو دیکھیں:

- رقم، اسناد، یا منظوری کے لیے فوری، دباؤ والی درخواست
- "معروف" شخص کی کال یا ویڈیو میں معمولی آڈیو/ویڈیو تضادات
- عام تصدیق / منظوری کے طریقہ کار کو نظرانداز کرنے کی درخواست
- غیر مانوس مرسل ڈومین یا تھوڑا سا تبدیل شدہ URL
- غیر متوقع MFA پرامپٹس یا OTPs جن کی آپ نے درخواست نہیں کی۔
- سیکیورٹی سافٹ ویئر کو غیر فعال کرنے یا غیر سرکاری لنکس کے ذریعے "تصدیق" کرنے کی درخواستیں۔
- جاب/سرمایہ کاری کی پیشکش پیشگی ادائیگی یا ذاتی مالی تفصیلات کی ضرورت ہوتی ہے۔

جب شک ہو — توقف کریں، آزادانہ طور پر تصدیق کریں، اور دباؤ میں کام نہ کریں۔

ہماری پیروی کریں:
@IndianCERT
@cert_india

ڈیوائس کی حفاظت



آلات کو اپ ڈیٹ رکھیں

- آپریٹنگ سسٹمز، ایپلیکیشنز، براؤزرز، اور سیکیورٹی سافٹ ویئر کو معلوم کمزوریوں کو دور کرنے کے لیے باقاعدگی سے اپ ڈیٹ کریں۔
- جہاں بھی ممکن ہو خودکار اپ ڈیٹس کو فعال کریں۔

صرف بھروسہ مند سافٹ ویئر انسٹال کریں۔

- حقیقی سافٹ ویئر استعمال کریں اور ایپلیکیشنز کو صرف آفیشل ایپ اسٹورز یا قابل اعتماد ذرائع سے انسٹال کریں۔
- قابل اعتماد اینٹی وائرس یا حفاظتی حل استعمال کریں اور انہیں اپ ڈیٹ رکھیں۔

اپنے آلات اور اکاؤنٹس کو محفوظ بنائیں

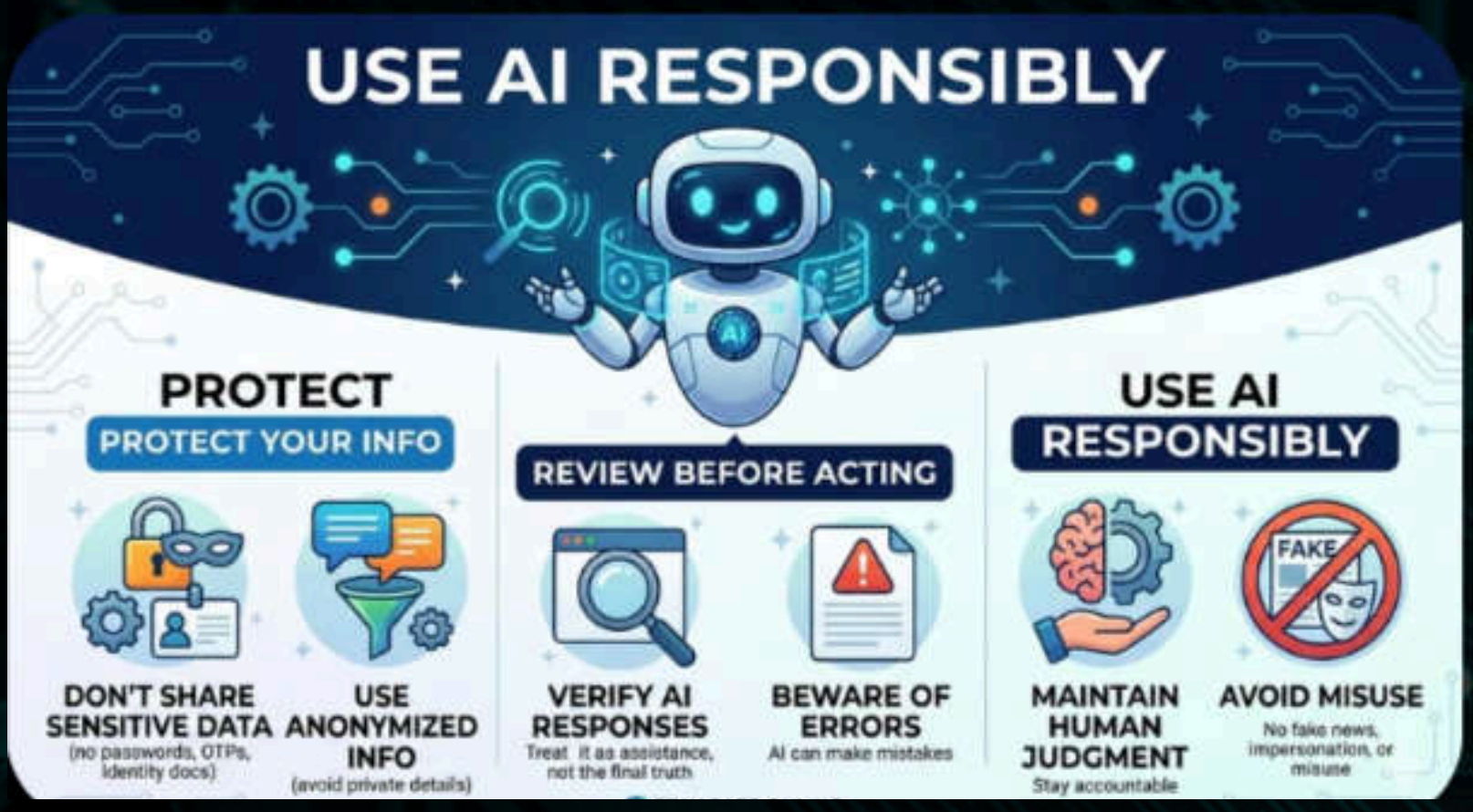
- تمام آلات پر مضبوط پاس ورڈز یا اسکرین لاک استعمال کریں۔
- جب بھی دستیاب ہو آلہ کی خفیہ کاری اور حفاظتی خصوصیات کو فعال کریں۔
- غیر ضروری درخواستوں اور اجازتوں کا جائزہ لیں اور ہٹا دیں۔

اپنے نیٹ ورک کنکشن کی حفاظت کریں۔

- اپنے وائی فائی کو مضبوط پاس ورڈ کے ساتھ محفوظ کریں اور ڈیفالٹ روٹر کی اسناد کو تبدیل کریں۔
- اپ ڈیٹ شدہ راؤٹر فرم ویئر اور محفوظ نیٹ ورک سیٹنگز استعمال کریں۔
- حساس اکاؤنٹس تک رسائی حاصل کرنے یا غیر محفوظ نیٹ ورکس پر خفیہ معلومات شیئر کرنے سے گریز کریں۔

ہماری پیروی کریں: @IndianCERT @cert_india

AI کو ذمہ داری سے استعمال کریں۔



اپنی ذاتی معلومات کی حفاظت کریں۔

- **عوامی *AI* ٹولز یا نامعلوم آن لائن سروسز میں ذاتی، مالی، صحت، سرکاری، یا خفیہ معلومات درج نہ کریں۔**
- پاس ورڈز، OTPs، اکاؤنٹ نمبرز، شناختی دستاویزات، کسٹمر ڈیٹا، یا نجی گفتگو جیسی حساس تفصیلات کا اشتراک کرنے سے گریز کریں۔
- AI ٹولز سے مدد مانگتے وقت گمنام یا عام معلومات استعمال کریں۔

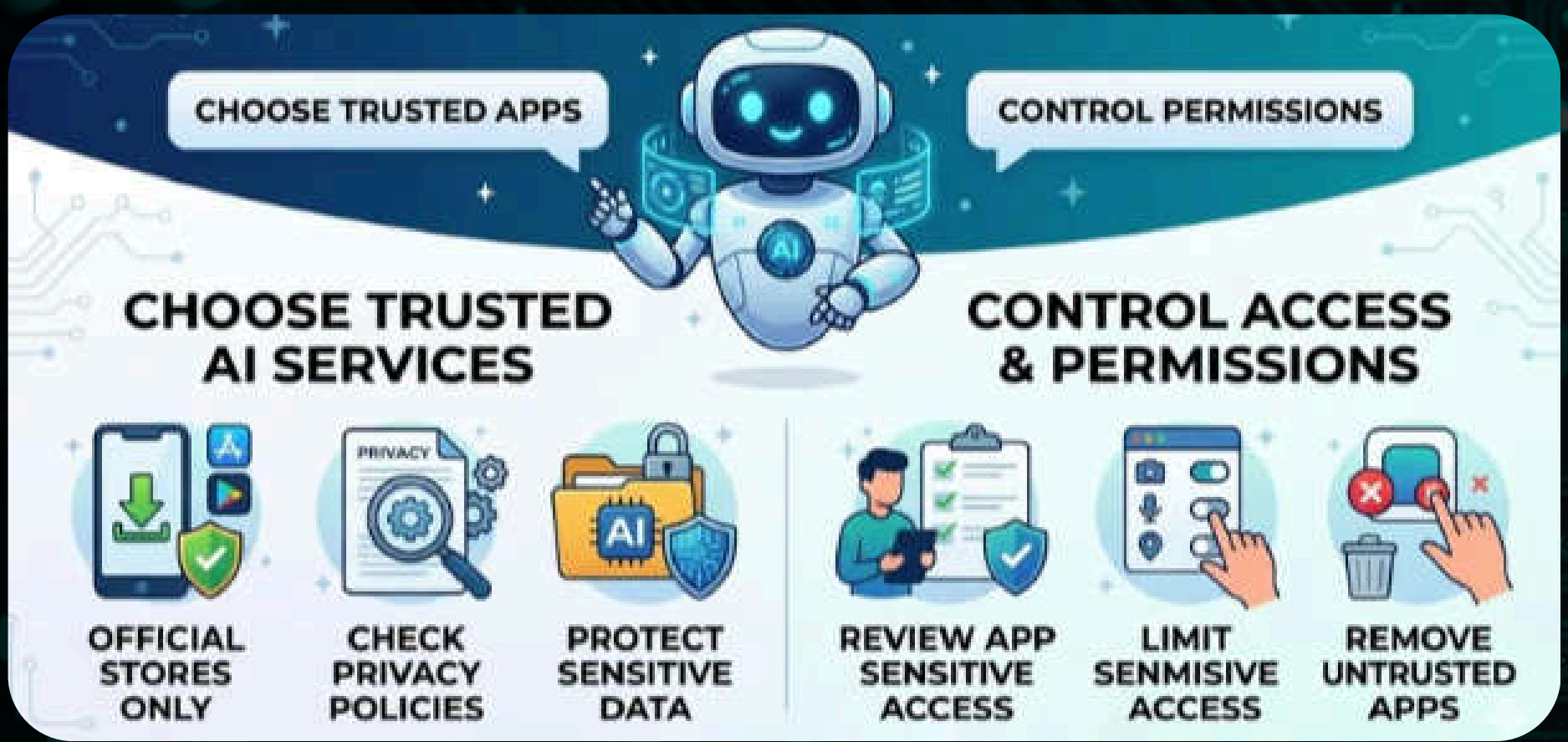
اشتراک کرنے یا عمل کرنے سے پہلے جائزہ لیں۔

- **AI سے تیار کردہ جوابات کو مدد کے طور پر سمجھیں، سچائی کے حتمی ذریعہ کے طور پر نہیں۔**
- اہم معلومات کو مالی، قانونی، پیشہ ورانہ یا ذاتی فیصلوں کے لیے استعمال کرنے سے پہلے اس کی تصدیق کریں۔
- آگاہ رہیں کہ AI ٹولز غلط، نامکمل یا گمراہ کن معلومات پیدا کر سکتے ہیں۔

AI ٹولز کو ذمہ داری سے استعمال کریں۔

- اپنے کام اور سیکھنے میں مدد کے لیے AI کا استعمال کریں، لیکن انسانی فیصلے اور جوابدہی کو برقرار رکھیں۔
- غلط معلومات بنانے یا پھیلانے، دوسروں کی نقالی کرنے یا کسی کے ذاتی ڈیٹا کا غلط استعمال کرنے کے لیے AI کا استعمال نہ کریں۔

بھروسہ مند ایپس کا انتخاب کریں۔



ایپ تک رسائی اور اجازتوں کو کنٹرول کریں۔

- AI ایپلیکیشنز اور ڈیجیٹل اسسٹنٹس کو دی گئی اجازتوں کا جائزہ لیں۔
- صرف اس وقت تک رسائی کی اجازت دیں جب کیمرہ، مائیکروفون، رابطے یا مقام جیسی خصوصیات تک ضروری ہو۔
- غیر ضروری اجازتوں کو ہٹا دیں اور ناقابل اعتماد ذرائع سے ایپس کو ان انسٹال کریں۔

ٹرسٹڈ AI سروسز کا انتخاب کریں۔

- معروف فراہم کنندگان سے ***AI*** ایپلیکیشنز استعمال کریں اور انہیں صرف آفیشل ایپ اسٹورز سے ڈاؤن لوڈ کریں۔
- ***AI*** سروسز استعمال کرنے سے پہلے رازداری کی ترتیبات، استعمال کی شرائط، اور ڈیٹا ہینڈلنگ کے طریقوں کا جائزہ لیں۔
- ***AI*** ٹولز کو حساس اکاؤنٹس یا فائلوں سے منسلک کرنے سے گریز کریں جب تک کہ سیکیورٹی کنٹرولز کی تصدیق نہ ہو جائے۔

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