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

آگاهي گائيڊ AI

سائبر صفائي جي ثقافت پيدا ڪريو

سائبر صفائي اسان جي ثقافت#



قومي سائبر سيڪيورٽي آگاهي مهينو
(آڪٽوبر 2026)

ناشر

هندستاني ڪمپيوٽر ايمرجنسي ريسپانس ٽيم

اسان جي تابعداري ڪريو:

@IndianCERT

@cert_india

مواد جي جدول

ديباچو 3

اي آءِ سان بهتر کيل فشنگ ۽ سوشل انجنيئرنگ 4

وائيس ۽ وڊيو ڊيپ فيڪس (وِشنگ) 5

اي آءِ جي مدد سان مالويئر ۽ خودڪار حملا 6

جعلي ويب سائيٽون ۽ سڃاڻپ جي چوري 7

ڳاڙهي جھنڊن جي چيڪ لسٽ 8

آن لائن حفاظت 9

ڊوائيس جي حفاظت 10

AI کي ذميواري سان استعمال ڪريو 11

قابل اعتماد ائپس چونڊيو 12

CERT-In کي سائبر سيڪيورٽي واقعن جي رپورٽ ڪريو. 13

ديباچو

اسان جي رهڻ، ڪم ڪرڻ ۽ رابطي جي طريقي کي تبديل ڪري (AI) مصنوعي ذهانت رهي آهي. اهو جدت کي فعال بڻائي ٿو، پيداوار کي بهتر بڻائي ٿو، ۽ مختلف شعبن ۾ پيچيده مسئلن کي حل ڪرڻ ۾ مدد ڪري ٿو. جڏهن ته، ساڳئي ٽيڪنالاجي کي خطري جي اداڪارن پاران وڌيڪ ترقي يافته ۽ قائل ڪندڙ سائبر خطرا پيدا ڪرڻ لاءِ غلط استعمال ڪيو پيو وڃي.

اي آءِ ڊجيٽل خطرن کي سڃاڻڻ ۾ وڌيڪ ڏکيائي پيدا ڪري رهيو آهي ڇاڪاڻ ته حملي آور هاڻي انتهائي حقيقي اي ميلون، پيغام، آڊيو، وڊيوز ۽ ويب سائيٽون ٺاهي سگهن ٿا. روايتي خبرداري جا نشان، جهڙوڪ خراب گرامر، غير معمولي فارميٽنگ، يا واضح غلطيون، هاڻي قابل اعتماد اشارا نه ٿي سگهن ٿيون. تصديق ۽ ذميوار ڊجيٽل طريقا اڄي ڪان وڌيڪ اهم ٿي ويا آهن.

اوزار ۽ سمارٽ ڊوائيسز جيڪي AI جيڪڏهن احتياط سان استعمال نه ڪيو وڃي ته اسان هر روز استعمال ڪندا آهيون، اهي نوان رازداري ۽ سيڪيورٽي خطرا متعارف ايپليڪيشنن سان ذاتي يا رازداري معلومات AI ڪرائي سگهن ٿا. غير قابل اعتماد پاران ٺاهيل معلومات AI شيئر ڪرڻ، غير ضروري اجازتون ڏيڻ، يا تصديق کان سواءِ تي پروسو ڪرڻ فردن ۽ تنظيمن کي سيڪيورٽي خطرن ۾ مبتلا ڪري سگهي ٿو.

سائبر آگاهي" تي هي AI" پاران (CERT-In) انڊين ڪمپيوٽر ايمرجنسي رسپانس ٽيم ڪتابچو روزمره جي شهرين، ملازمن ۽ ڊجيٽل استعمال ڪندڙن لاءِ ٺاهيو ويو آهي، نه ڊجيٽل AI رڳو سائبر سيڪيورٽي پروفيشنلز لاءِ. اهو وضاحت ڪري ٿو ته ڪيئن خطري جي منظرنامي کي تبديل ڪري رهيو آهي ۽ سادو، عملي قدم فراهم ڪري ٿو جيڪي هرڪو ذاتي معلومات، ڊوائيسز ۽ آن لائن سڃاڻپ جي حفاظت لاءِ پيروي ڪري سگهي ٿو.

اي آءِ-ايلَهالَسبِ فشلَگ ۽ سوشل اِنجلَيئرلَگ



اهو ڪيئَن ڪم ڪري ٿو؟

ڏمڪي ڏيندڙ اداڪار هاڻي اي ميلون ۽ ٽيڪسٽ موڪليندا آهن جيڪي حقيقي ۽ غلطي کان پاڪ نظر اچن ٿا. اهي توهان جي باري ۾ تفصيل استعمال ڪندا آهن، جهڙوڪ توهان جي نوڪري، توهان جون خدمتون، يا تازيون سرگرميون، پيغامن کي ذاتي محسوس ڪرائڻ لاءِ. جيئن ته اهي پيغام سڌي نموني سان لکيل آهن، انهن کي ڳولڻ تمام ڏکيو ٿي سگهي ٿو.

سڃاڻپ ڪيئَن ڪجي؟

- پيغام توهان لاءِ تمام خاص محسوس ٿئي ٿو پر اوچتو پهچي ٿو.
- اهو هڪ تڪڙي يا ڏمڪي واري لهجي استعمال ڪري ٿو ۽ فوري ڪارروائي جو مطالبو ڪري ٿو.
- اهو توهان کي هڪ لنڪ تي ڪلڪ ڪرڻ، اڪائونٽ جي تصديق ڪرڻ، پاسورڊ ري سيٽ ڪرڻ، يا ادائيگي ڪرڻ لاءِ چوندو.
- موڪلينڈڙ جو پتو لڳ ڀڳ صحيح لڳي ٿو، پر بلڪل نه.

ڪيئَن محفوظ رهجي؟

- غير گهربل پيغامن ۾ لنڪس تي ڪلڪ نه ڪريو. ان جي بدران سڌو سرڪاري ويب سائيٽ يا ايپ تي وڃو.
- درخواستن جي تصديق هڪ الڳ، قابل اعتماد رابطي چينل ذريعي ڪريو، جهڙوڪ سرڪاري فون نمبر يا ايپ.
- داخل نه OTP پيغام جي لنڪ ذريعي پهچندڙ صفحي تي ڪڏهن به سندون يا ڪريو.
- مشڪوڪ پيغامن جي رپورٽ ڪريو ۽ ڊليٽ ڪريو، پوءِ موڪلينڈڙ کي بلاڪ ڪريو.

اسان جي تابعداري ڪريو:
@IndianCERT
@cert_india

وائيس ۽ وڊيو ڊيپ فيڪس [وِشلَنگ]



اهو ڪيئن ٿو؟

ڈمڪيون ڈينڈڙ اداڪار آوازن کي ڪلون ڪري سگھن ٿا يا جعلي وڊيوز ٺاهي سگھن ٿا جيڪي حقيقي نظر اچن ٿا. اهي شايد خاندان، ساٿين، يا آفيسرن جي روپ ۾ پيش ڪن ته جيئن توهان کي حساس معلومات شيئر ڪرڻ، پئسا موڪلڻ، يا جلدي ڪم ڪرڻ لاءِ دٻاءُ وجهي سگھن.

سڃاڻپ ڪيئن ڪجي؟

- غير معمولي تڪڙ، خوف، يا رازداري جي درخواست، جھڙوڪ ڪنهن کي نه ٻڌايو.
- ٿورو بند سر، رفتار، پس منظر جو شور، يا آڊيو معيار.
- عام تصديق يا منظوري جي عملن کي نظرانداز ڪرڻ جون درخواستون.
- گفٽ ڪارڊ، ڪرپٽو ڪرنسي، يا وائر ٽرانسفر ذريعي ادائيگي لاءِ درخواستون.

ڪيئن محفوظ رهجي؟

- فون بند ڪريو ۽ ان شخص کي سندس سڃاتل، محفوظ ڪيل نمبر استعمال ڪندي واپس ڪال ڪريو.
- هنگامي حالتن ۾ سڃاڻپ جي تصديق لاءِ خاندان يا ڪم جي جڳھ لاءِ محفوظ لفظ مقرر ڪريو.
- ڪڏهن به صرف ڪال يا وڊيو جي بنياد تي ادائيگي جي اجازت نه ڏيو. هڪ الگ چينل ذريعي تحريري طور تي تصديق ڪريو.
- رد عمل ڏيڻ کان اڳ رڪجو. ڈمڪي ڈينڈڙ ماڻهو توهان جي فيصلي کي ڊڪٽ لاءِ خوف تي پروسو ڪندا آهن.

اسان جي تابعداري ڪريو: @IndianCERT @cert_india

مصلَوعي ذهاڻت جي مدد سانَ مالويئر ۽ خودڪار حملا



اهو ڪيئَن ڪم ڪري ٿو؟

ٽولز استعمال ڪندا آهن ته جيئن خراب ڪوڊ ٺاهي يا لڪايو AI ڏمڪي ڏيندڙ اداڪار وڃي، ڪيترن ئي سائيٽن تي چوري ٿيل پاسورڊ جي جانچ ڪئي وڃي، ۽ سسٽم جي سڃاڻپ ڪئي وڃي جن کي اپڊيٽ جي ضرورت آهي. اهو حملن کي تيز ۽ وڏيڪ وسيع بڻائي ٿو.

سڃاڻپ ڪيئَن ڪجي؟

- پرامپٽس جيڪي توهان MFA غير متوقع لاگ ان الرٽ، پاسورڊ ري سيٽ اي ميلون، يا درخواست نه ڪيا هئا
- توهان جي اڪائونٽ سرگرمي ۾ درج ٿيل اڻ واقف ڊوائيسز يا سيشن
- اينٽي وائرس ڊيجارينڊز، پاپ اپ، يا غير معمولي طور تي سست ڊوائيس جي ڪارڪردگي
- فائلون، سيٽنگون، يا برائوزر ايڪسٽينشن جيڪي توهان نٿا سڃاڻو

ڪيئَن محفوظ رهجي؟

- هر اڪائونٽ لاءِ هڪ منفرد، مضبوط پاسورڊ استعمال ڪريو.
- جي فعال ڪريو (MFA) سڀني اهم اڪائونٽس تي ملٽي فيڪٽر تصديق.
- اينٽي وائرس سافٽ ويئر، سسٽم ۽ ايپس کي اپڊيٽ رکو.
- غير متوقع لاگ ان يا ايم ايف اي الرٽس تي فوري طور تي عمل ڪريو.

اسان جي تابعداري ڪريو:
@IndianCERT
@cert_india

جعلي ويب سائيٽولاءِ سچاٽپ جي چوري



اهو ڪيئن ٿو؟

ڏمڪي ڏيندڙ اداڪار هڪجهڙا ويب سائيٽون ۽ چيٽ بوٽ ٺاهي سگهن ٿا جيڪي حقيقي نظر اچن ٿا، جهڙوڪ بينڪنگ يا شاپنگ پورٽل، توهان جي لاگ ان سندون، او ٽي پي، يا ادائيگي جي تفصيل چوري ڪرڻ لاءِ. اهي جعلي سچاٽپ ٺاهڻ لاءِ جعلي تصويرون يا دستاويز پڻ استعمال ڪري سگهن ٿا.

سچاٽپ ڪيئن ڪجي؟

- جهڙوڪ اضافي اکر، هائفن، يا هڪ مختلف ڊومين جي آخر ۾ URLs، ٿوري تبديل ٿيل ويب سائيٽ.
- چيٽ بوٽس يا ايجنٽ جيڪي او ٽي پي، پن، يا مڪمل ڪارڊ نمبر پڇن ٿا.
- غائب آهي يا غير معمولي ڊيزائن ۾ تضاد آهن HTTPS ڪنهن واقف سائيٽ تي.

ڪيئن محفوظ رهجي؟

- ٽائيپ ڪريو يا تصديق URL لنڪ تي ڪلڪ ڪرڻ بدران هميشه سڌو سنئون سرڪاري ٿيل بُڪ مارڪ استعمال ڪريو.
- يا مڪمل ڪارڊ، PIN، OTP ڪڏهن به ڪنهن به چيٽ بوٽ يا "سپورٽ ايجنٽ" سان تفصيل شيئر نه ڪريو.
- جي جانچ ڪريو ۽ ڊومين جي نالي کي غور سان HTTPS ڪٽي به لاگ ان ٽيڪ ڪان اڳ ڏسو.
- اڻ ڄاتل سرگرمي لاءِ پنهنجي بينڪ استيٽمينٽس ۽ ڪريڊٽ رپورٽ جي باقاعدي نگراني ڪريو.

اسان جي تابعداري ڪريو:
@IndianCERT
@cert_india

گاڙهي جهلڻ ڊيلا جي چيڪ لسٽ

فعال حملي جي انهن نشانين تي نظر رکو-AI:

- پئسن، سند، يا منظوري لاءِ تڪڙي، دٻاءُ واري درخواست
- ڪنهن "سڃاتل" شخص جي ڪال يا وڊيو ۾ ٿوري آڊيو/وڊيو ۾ تضاد
- عام تصديق / منظوري جي طريقيڪار کي نظرانداز ڪرڻ جي درخواست
- URL اڻ واقف موڪلينڊڻ ڊومين يا ٿورو تبديل ٿيل
- جيڪي توهان درخواست نه ڪيا هئا OTPs پرامپٽس يا MFA غير متوقع
- سيڪيورٽي سافٽ ويئر کي غير فعال ڪرڻ يا غير رسمي لنڪس ذريعي تصديق" ڪرڻ جون درخواستون"
- نوڪري/سيڙپڪاري جون آڇون جيڪي اڳواٽ ادائيگي يا ذاتي مالي تفصيلن جي ضرورت هوندیون آهن

جڏهن شڪ هجي - روڪيو، آزادانه طور تي تصديق ڪريو، ۽ دٻاءُ هيٺ ڪم نه ڪريو.

اسان جي تابعداري ڪريو: @IndianCERT @cert_india



آن لائن حفاظت

پنهنجا اڪائونٽ محفوظ ڪريو

- هر اڪائونٽ لاءِ مضبوط ۽ منفرد پاسورڊ استعمال ڪريو؛ انهن کي محفوظ طريقي سان محفوظ ڪرڻ لاءِ پاسورڊ مئنيجر استعمال ڪريو.
- جتي به موجود هجي، ملٽي فيڪٽر تصديق (MFA) کي فعال ڪريو.
- پن، پاسورڊ، يا سيڪيورٽي ڪوڊ، OTP ڪڏهن به ڪنهن سان به شيئر نه ڪريو.
- اضافي سيڪيورٽي پرت جي طور تي بايوميٽرڪ تصديق (فنگر پرنٽ/ چهري جي سڃاڻپ) استعمال ڪريو.

اي ميل ۽ انٽرنيٽ استعمال ڪندي محفوظ رهو

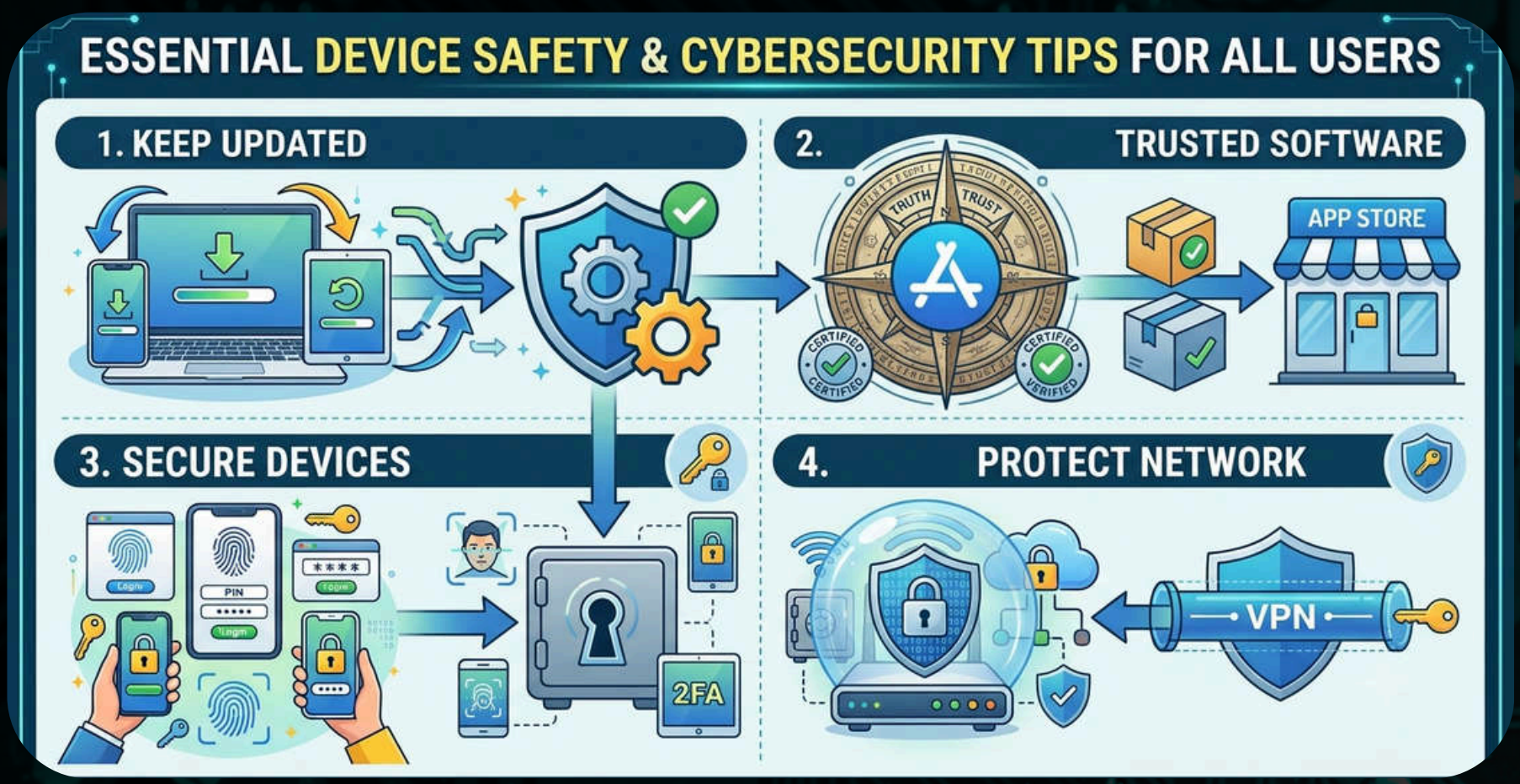
- موڪلينڊڙ جي تفصيلن کي احتياط سان چيڪ ڪريو ته ڇا مشڪوڪ يا هڪجهڙا اي ميل پتا آهن.
- ڪلڪ ڪرڻ کان اڳ لنڪس جي تصديق ڪريو ۽ غير متوقع اٽيچمينٽ کولڻ کان پاسو ڪريو.
- لاگ ان يا مالي تفصيل داخل ڪرڻ کان اڳ ويب سائيٽ جي صداقت جي تصديق ڪريو.
- جڏهن شڪ هجي، روڪيو ۽ عمل ڪرڻ کان اڳ تصديق ڪريو.

ڪجهه غلط ٿيڻ کان اڳ تياري ڪريو

- آف لائن يا محفوظ ڪلائوڊ سروس ۾ محفوظ ڪيل اهم فائلن جو باقاعده بيڪ اپ رکو.
- اڪائونٽ جي بحالي جي معلومات (اي ميل/فون) کي اپڊيٽ ۽ محفوظ رکو.

اسان جي تابعداري ڪريو: @IndianCERT @cert_india

ڈوائيس جي حفاظت



ڈوائيسز کي اپڈيٽ رکو

- سڀاڻ ڪمزورين کي درست ڪرڻ لاءِ آپريٽنگ سسٽم، ايپليڪيشنون، برائوزر، ۽ سيڪيورٽي سافٽ ويئر کي باقاعدي طور تي اپڈيٽ ڪريو.
- جتي به ممڪن هجي خودڪار اپڈيٽس کي فعال ڪريو.

صرف قابل اعتماد سافٽ ويئر انسٽال ڪريو

- حقيقي سافٽ ويئر استعمال ڪريو ۽ صرف سرڪاري ايپ اسٽورن يا قابل اعتماد ذريعن مان ايپليڪيشنون انسٽال ڪريو.
- قابل اعتماد اينٽي وائرس يا سيڪيورٽي حل استعمال ڪريو ۽ انهن کي اپڈيٽ رکو.

پنهنجا ڈوائيسز ۽ اڪائونٽس محفوظ ڪريو

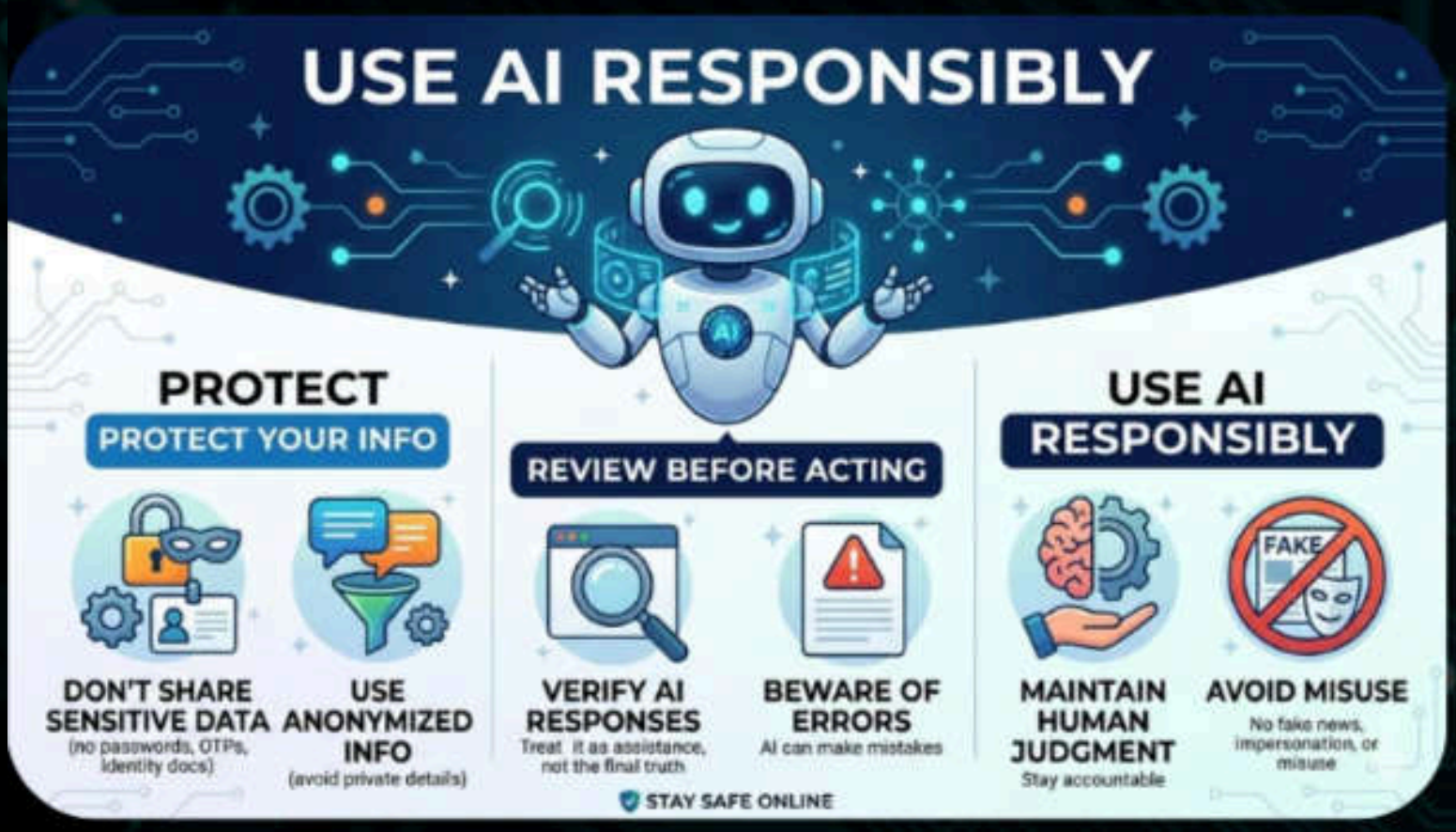
- سڀني ڈوائيسز تي مضبوط پاسورڈ يا اسڪرين لاڪ استعمال ڪريو.
- جڏهن به دستياب هجي ته ڈوائيس انڪرپشن ۽ سيڪيورٽي خاصيتون فعال ڪريو.
- غير ضروري ايپليڪيشنن ۽ اجازتن جو جائزو وٺو ۽ هٽايو.

پنهنجي نيٽ ورڪ ڪنيڪشن کي محفوظ ڪريو

- پنهنجي وائي فائي کي مضبوط پاسورڈ سان محفوظ ڪريو ۽ ڈفالٽ روٽر سيٽنگون تبديل ڪريو.
- اپڈيٽ ٿيل روٽر فرم ويئر ۽ محفوظ نيٽ ورڪ سيٽنگون استعمال ڪريو.
- غير محفوظ نيٽ ورڪن تي حساس اڪائونٽس تائين رسائي يا رازداري معلومات شيئر ڪرڻ کان پاسو ڪريو.

اسان جي تابعداري ڪريو: @IndianCERT @cert_india

AI کي ذميواري سان استعمال ڪريو



پنهنجي ذاتي معلومات جي حفاظت ڪريو

- اوزارن يا نامعلوم آن لائن خدمتن ۾ ذاتي، مالي، صحت، سرڪاري، يا رازداري معلومات *AI* عوامي داخل نه ڪريو.
- حساس تفصيلن جهڙوڪ پاسورڊ، او ٽي پي، اڪائونٽ نمبر، سڃاڻپ دستاويز، گراهڪ ڈيٽا، يا خانگي گفتگو شيئر ڪرڻ کان پاسو ڪريو.
- اوزارن کان پڇڻ وقت گمنام يا عام معلومات استعمال ڪريو AI مدد لاءِ.

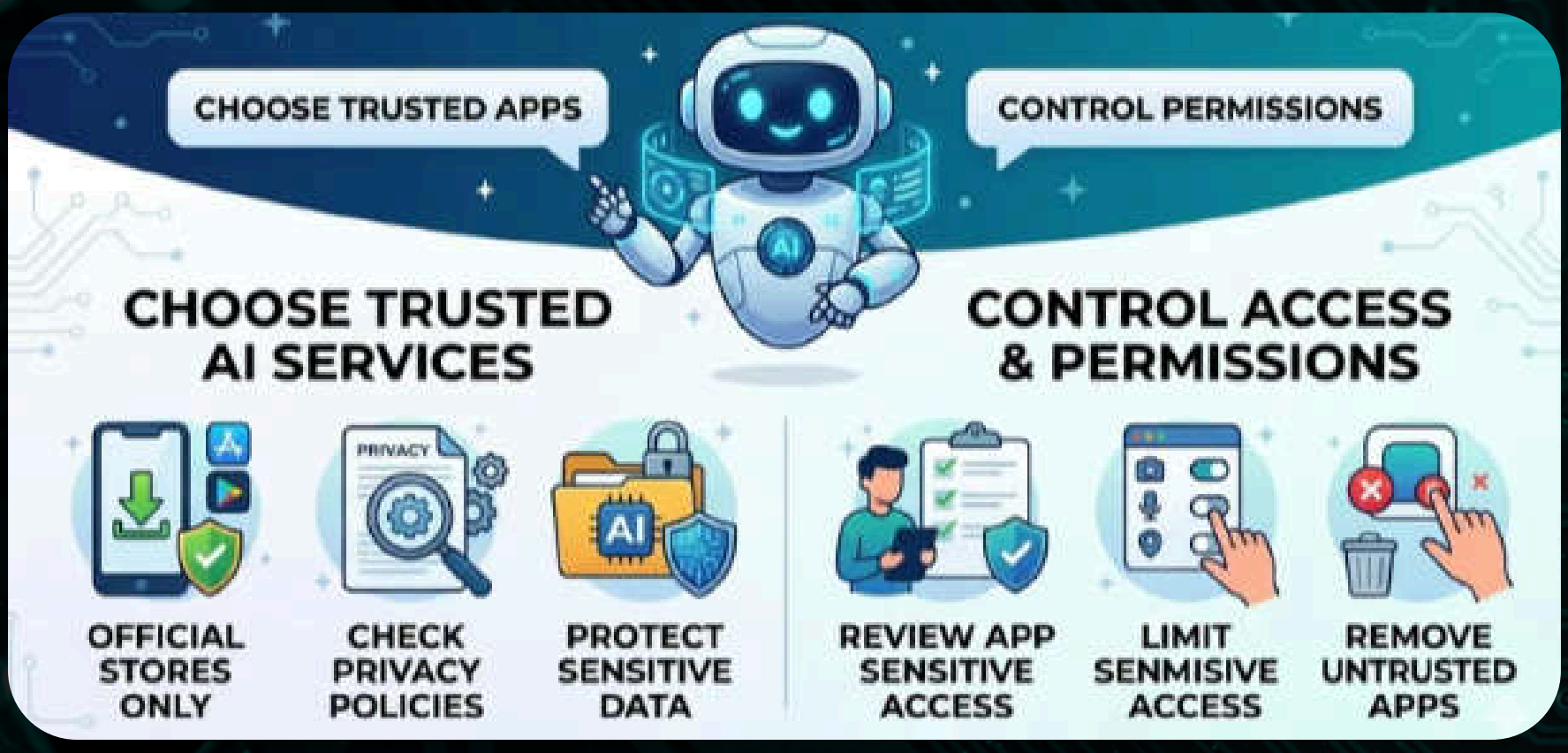
شيئر ڪرڻ يا عمل ڪرڻ کان اڳ جائزو وٺو

- **اي آءِ ياران تيار ڪيل جوابن کي مدد طور سمجهو، سچائي جي آخري ذريعن طور نه.**
- مالي، قانوني، پيشه ورانه، يا ذاتي فيصلن لاءِ استعمال ڪرڻ کان اڳ اهم معلومات جي تصديق ڪريو.
- اوزار غلط، نامڪمل، يا گمراهه ڪندڙ معلومات پيدا ڪري سگهن ٿا AI آگاهه رهو ته.

اوزارن کي ذميواري سان استعمال ڪريو AI

- استعمال ڪريو، پر انساني فيصلي ۽ جوابدهي کي AI پنهنجي ڪم ۽ سکيا جي مدد لاءِ برقرار رکو.
- غلط معلومات ٺاهڻ يا پکيڙڻ، ٻين جي نقل ڪرڻ، يا ڪنهن جي ذاتي ڈيٽا جي غلط استعمال لاءِ AI استعمال نه ڪريو.

قابل اعتماد ائپس چونڊيو



ايپ رسائي ۽ اجازتن کي ڪنٽرول ڪريو

- ايپليڪيشنن ۽ ڊجيٽل اسسٽنٽس کي ڏنل اجازتن جو جائزو ونو AI.
- ڪئميرا، مائڪروفون، رابطا، يا مقام جهڙين خاصيتن تائين رسائي جي اجازت صرف تڏهن ڏيو جڏهن ضروري هجي.
- غير ضروري اجازتون هٽايو ۽ غير قابل اعتماد ذريعن مان ايپس کي انسٽال ڪريو.

خدمتون چونڊيو AI قابل اعتماد

- ايپليڪيشنون استعمال ڪريو ۽ انهن کي صرف AI معتبر فراهم ڪندڙن کان سرڪاري ايپ اسٽورن تان ڊائون لوڊ ڪريو.
- سروسز استعمال ڪرڻ کان اڳ رازداري سيٽنگون، استعمال جون شرطون، ۽ ڊيٽا AI هينڊلنگ جي طريقن جو جائزو ونو.
- اي آءِ ٽولز کي حساس اڪائونٽس يا فائلن سان ڳنڍڻ کان پاسو ڪريو جيستائين سيڪيورٽي ڪنٽرول تصديق نه ٿين.

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