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 সচেতনতা নির্দেশিকা

সাইবার স্বাস্থ্যবিধির সংস্কৃতি গড়ে তুলুন

#সাইবারস্বাস্থ্যবিধিআমাদেরসংস্কৃতি



জাতীয় সাইবার নিরাপত্তা সচেতনতা মাস (অক্টোবর ২০২৬)

প্রকাশক

ভারতীয় কম্পিউটার জরুরি প্রতিক্রিয়া দল

আমাদের অনুসরণ করুন :

@IndianCERT

@cert_india

সূচিপত্র

ভূমিকা ৩

AI-বর্ধিত ফিশিং এবং সোশ্যাল ইঞ্জিনিয়ারিং ৪

ভয়েস ও ভিডিও ডিপফেক (ভিশিং) ৫

AI-সহায়তাযুক্ত ম্যালওয়্যার এবং স্বয়ংক্রিয় আক্রমণ ৬

ভুয়া ওয়েবসাইট এবং পরিচয় চুরি ৭

বিপদ সংকেতের চেকলিস্ট ৮

অনলাইন নিরাপত্তা ৯

ডিভাইসের নিরাপত্তা ১০

দায়িত্বশীলভাবে AI ব্যবহার করুন ১১

বিশ্বস্ত অ্যাপ বেছে নিন ১২

সাইবার নিরাপত্তা সংক্রান্ত ঘটনা CERT-In-কে জানান। ১৩

ভূমিকা

কৃত্রিম বুদ্ধিমত্তা (AI) আমাদের জীবনযাপন, কাজ এবং যোগাযোগের পদ্ধতিকে বদলে দিচ্ছে। এটি উদ্ভাবনকে সম্ভব করে, উৎপাদনশীলতা বাড়ায় এবং বিভিন্ন ক্ষেত্রে জটিল সমস্যা সমাধানে সহায়তা করে। তবে, এই একই প্রযুক্তিকে হুমকিদাতারা আরও উন্নত ও বিশ্বাসযোগ্য সাইবার হুমকি তৈরির জন্য অপব্যবহার করছে।

কৃত্রিম বুদ্ধিমত্তা ডিজিটাল হুমকি শনাক্ত করাকে আরও কঠিন করে তুলছে, কারণ আক্রমণকারীরা এখন অত্যন্ত বাস্তবসম্মত ইমেল, বার্তা, অডিও, ভিডিও এবং ওয়েবসাইট তৈরি করতে পারে। প্রচলিত সতর্কীকরণ চিহ্ন, যেমন দুর্বল ব্যাকরণ, অস্বাভাবিক বিন্যাস বা সুস্পষ্ট ভুল, এখন আর নির্ভরযোগ্য সূচক নাও হতে পারে। যাচাইকরণ এবং দায়িত্বশীল ডিজিটাল অভ্যাস আগের চেয়ে অনেক বেশি গুরুত্বপূর্ণ হয়ে উঠেছে।

আমরা প্রতিদিন যে AI টুল এবং স্মার্ট ডিভাইস ব্যবহার করি, সেগুলো সতর্কতার সাথে ব্যবহার না করা হলে নতুন গোপনীয়তা ও নিরাপত্তা ঝুঁকি তৈরি করতে পারে। অবিশ্বস্ত AI অ্যাপ্লিকেশনের সাথে ব্যক্তিগত বা গোপনীয় তথ্য শেয়ার করা, অপ্রয়োজনীয় অনুমতি প্রদান করা, অথবা যাচাই-বাছাই ছাড়াই AI দ্বারা তৈরি তথ্যের উপর নির্ভর করা ব্যক্তি ও প্রতিষ্ঠানকে নিরাপত্তা ঝুঁকির মুখে ফেলতে পারে।

ইন্ডিয়ান কম্পিউটার ইমার্জেন্সি রেসপন্স টিম (CERT-In) কর্তৃক প্রকাশিত “AI সাইবার অ্যাওয়ারনেস” শীর্ষক এই পুস্তিকাটি শুধুমাত্র সাইবার নিরাপত্তা পেশাদারদের জন্য নয়, বরং সাধারণ নাগরিক, কর্মচারী এবং ডিজিটাল ব্যবহারকারীদের জন্য তৈরি করা হয়েছে। এতে ব্যাখ্যা করা হয়েছে কীভাবে AI ডিজিটাল হুমকির প্রেক্ষাপটকে বদলে দিচ্ছে এবং ব্যক্তিগত তথ্য, ডিভাইস ও অনলাইন পরিচয় সুরক্ষিত রাখার জন্য এমন কিছু সহজ ও বাস্তবসম্মত পদক্ষেপ দেওয়া হয়েছে যা প্রত্যেকেই অনুসরণ করতে পারে।

AI-বর্ধিত ফিশিং এবং সোশ্যাল ইঞ্জিনিয়ারিং



এটি কীভাবে কাজ করে?

হুমকিদাতারা এখন এমন ইমেল এবং টেক্সট পাঠায় যা দেখতে আসল এবং ত্রুটিমুক্ত মনে হয়। বার্তাগুলোকে ব্যক্তিগত করে তোলার জন্য তারা আপনার চাকরি, ব্যবহৃত পরিষেবা বা সাম্প্রতিক কার্যকলাপের মতো বিবরণ ব্যবহার করে। যেহেতু এই বার্তাগুলো ভালোভাবে লেখা হয়, তাই এগুলো শনাক্ত করা অনেক বেশি কঠিন হতে পারে।

কীভাবে শনাক্ত করবেন?

- বার্তাটি আপনার জন্য অত্যন্ত সুনির্দিষ্ট বলে মনে হলেও তা অপ্রত্যাশিতভাবে এসে পৌঁছায়।
- এতে একটি জরুরি বা ভীতিপ্রদ সুর ব্যবহার করা হয় এবং অবিলম্বে পদক্ষেপ নেওয়ার দাবি জানানো হয়।
- এটি আপনাকে একটি লিঙ্কে ক্লিক করতে, অ্যাকাউন্ট যাচাই করতে, পাসওয়ার্ড রিসেট করতে বা অর্থ প্রদান করতে বলে।
- প্রেরকের ঠিকানাটি প্রায় সঠিক মনে হচ্ছে, কিন্তু পুরোপুরি নয়।

কীভাবে সুরক্ষিত থাকবেন?

- অযাচিত মেসেজে থাকা লিঙ্কে ক্লিক করবেন না। এর পরিবর্তে সরাসরি অফিসিয়াল ওয়েবসাইট বা অ্যাপে যান।
- একটি পৃথক ও নির্ভরযোগ্য যোগাযোগ মাধ্যম, যেমন প্রাতিষ্ঠানিক ফোন নম্বর বা অ্যাপের মাধ্যমে অনুরোধগুলো যাচাই করুন।
- মেসেজ লিঙ্কের মাধ্যমে পৌঁছানো কোনো পেজে কখনোই ক্রেডেনশিয়াল বা ওটিপি প্রবেশ করাবেন না।
- সন্দেহজনক বার্তাগুলো রিপোর্ট করে মুছে ফেলুন, তারপর প্রেরককে ব্লক করুন।

ভয়েস ও ভিডিও ডিপফেক [ভিশিং]



এটি কীভাবে কাজ করে?

হুমকিদাতারা কণ্ঠস্বর নকল করতে পারে বা এমন নকল ভিডিও তৈরি করতে পারে যা দেখতে ও শুনতে আসল মনে হয়। তারা সংবেদনশীল তথ্য শেয়ার করতে, টাকা পাঠাতে বা দ্রুত কোনো পদক্ষেপ নিতে আপনাকে চাপ দেওয়ার জন্য পরিবার, সহকর্মী বা কর্মকর্তা সেজে থাকতে পারে।

কীভাবে শনাক্ত করবেন?

- অস্বাভাবিক তাড়া, আতঙ্ক, অথবা গোপনীয়তা রক্ষার অনুরোধ, যেমন কাউকে বলবেন না।
- কণ্ঠস্বরের সামান্য অস্বাভাবিকতা, পায়চারি, পারিপার্শ্বিক কোলাহল বা অডিওর মান।
- সাধারণ যাচাই বা অনুমোদন প্রক্রিয়া এড়িয়ে যাওয়ার অনুরোধ।
- গিফট কার্ড, ক্রিপ্টোকারেন্সি বা ওয়্যার ট্রান্সফারের মাধ্যমে অর্থ প্রদানের অনুরোধ।

কীভাবে সুরক্ষিত থাকবেন?

- ফোন রেখে দিন এবং তার পরিচিত ও সেভ করা নম্বরটি ব্যবহার করে তাকে আবার ফোন করুন।
- জরুরি অবস্থায় পরিচয় যাচাই করার জন্য পরিবার বা কর্মক্ষেত্রে একটি নিরাপদ শব্দ (সেফ ওয়ার্ড) সেট করুন।
- শুধুমাত্র ফোন কল বা ভিডিওর ভিত্তিতে কখনো পেমেন্টের অনুমোদন দেবেন না। আলাদা কোনো মাধ্যমে লিখিতভাবে নিশ্চিত করুন।
- প্রতিক্রিয়া দেখানোর আগে থামুন। হুমকিদাতারা আপনার বিচারবুদ্ধিকে আচ্ছন্ন করার জন্য আতঙ্কের উপর নির্ভর করে।

AI-সহায়তাযুক্ত ম্যালওয়্যার এবং স্বয়ংক্রিয় আক্রমণ



এটি কীভাবে কাজ করে?

আক্রমণকারীরা ক্ষতিকারক কোড তৈরি বা লুকানোর জন্য, একাধিক সাইটে চুরি করা পাসওয়ার্ড পরীক্ষা করার জন্য এবং যেসব সিস্টেমের আপডেট প্রয়োজন তা শনাক্ত করার জন্য AI টুল ব্যবহার করে। এর ফলে আক্রমণগুলো আরও দ্রুত এবং ব্যাপক হয়ে ওঠে।

কীভাবে শনাক্ত করবেন?

- অপ্রত্যাশিত লগইন অ্যালার্ট, পাসওয়ার্ড রিসেট ইমেল, অথবা আপনার অনুরোধ ছাড়াই এমএফএ (MFA) প্রম্পট।
- আপনার অ্যাকাউন্ট কার্যকলাপে অপরিচিত ডিভাইস বা সেশন তালিকাভুক্ত করা হয়েছে।
- অ্যান্টিভাইরাস সতর্কতা, পপ-আপ, বা ডিভাইসের অস্বাভাবিক ধীর গতি
- ফাইল, সেটিংস, বা ব্রাউজার এক্সটেনশন যা আপনি চিনতে পারছেন না

কীভাবে সুরক্ষিত থাকবেন?

- প্রতিটি অ্যাকাউন্টের জন্য একটি স্বতন্ত্র ও শক্তিশালী পাসওয়ার্ড ব্যবহার করুন।
- আপনার সকল গুরুত্বপূর্ণ অ্যাকাউন্টে মাল্টি ফ্যাক্টর অথেন্টিকেশন (MFA) চালু করুন।
- অ্যান্টিভাইরাস সফটওয়্যার, সিস্টেম ও অ্যাপস হালনাগাদ রাখুন।
- অপ্রত্যাশিত লগইন বা এমএফএ অ্যালার্ট পেলে অবিলম্বে ব্যবস্থা নিন।

ভুয়া ওয়েবসাইট এবং পরিচয় চুরি



এটি কীভাবে কাজ করে?

আক্রমণকারীরা আপনার লগইন তথ্য, ওটিপি বা পেমেন্টের বিবরণ চুরি করার জন্য ব্যাংকিং বা শপিং পোর্টালের মতো আসল দেখতে ওয়েবসাইট এবং চ্যাটবট তৈরি করতে পারে। তারা ভুয়া পরিচয় তৈরি করতে নকল ছবি বা নথিও ব্যবহার করতে পারে।

কীভাবে শনাক্ত করবেন?

- ওয়েবসাইটের ইউআরএল-এ সামান্য পরিবর্তন, যেমন অতিরিক্ত অক্ষর, হাইফেন বা ডোমেইনের শেষে ভিন্ন কিছু যোগ করা।
- চ্যাটবট বা এজেন্টরা ওটিপি, পিন বা সম্পূর্ণ কার্ড নম্বর জানতে চাইছে।
- একটি পরিচিত সাইটে HTTPS-এর অনুপস্থিতি অথবা ডিজাইনে অস্বাভাবিক অসঙ্গতি।

কীভাবে সুরক্ষিত থাকবেন?

- লিঙ্কে ক্লিক করার পরিবর্তে সর্বদা সরাসরি অফিসিয়াল ইউআরএল টাইপ করুন অথবা যাচাইকৃত বুকমার্ক ব্যবহার করুন।
- কোনো চ্যাটবট বা 'সাপোর্ট এজেন্ট'-এর সাথে কখনো OTP, PIN বা কার্ডের সম্পূর্ণ বিবরণ শেয়ার করবেন না।
- যেকোনো জায়গায় লগ ইন করার আগে HTTPS আছে কিনা তা পরীক্ষা করুন এবং ডোমেইন নামটি ভালোভাবে দেখে নিন।
- কোনো অস্বাভাবিক কার্যকলাপের জন্য আপনার ব্যাংক স্টেটমেন্ট ও ক্রেডিট রিপোর্ট নিয়মিত পর্যবেক্ষণ করুন।

বিপদ সংকেতের চেকলিস্ট

AI-চালিত আক্রমণের এই লক্ষণগুলোর দিকে নজর রাখুন:

- ☑ টাকা, পরিচয়পত্র বা অনুমোদনের জন্য জরুরি ও চাপযুক্ত অনুরোধ।
- ☑ কোনো 'পরিচিত' ব্যক্তির কাছ থেকে আসা কল বা ভিডিওতে সামান্য অডিও/ভিডিও অসঙ্গতি
- ☑ সাধারণ যাচাই/অনুমোদন প্রক্রিয়া এড়িয়ে যাওয়ার অনুরোধ
- ☑ অপরিচিত প্রেরক ডোমেইন বা সামান্য পরিবর্তিত URL
- ☑ অপ্রত্যাশিত এমএফএ প্রম্পট অথবা আপনার অনুরোধ না করা ওটিপি
- ☑ নিরাপত্তা সফটওয়্যার নিষ্ক্রিয় করার বা অনানুষ্ঠানিক লিঙ্কের মাধ্যমে 'যাচাই' করার অনুরোধ।
- ☑ চাকরি/বিনিয়োগের প্রস্তাব, যার জন্য অগ্রিম অর্থ প্রদান বা ব্যক্তিগত আর্থিক বিবরণের প্রয়োজন হয়।

সন্দেহ হলে — থামুন, নিজে থেকে যাচাই করে নিন এবং চাপের মুখে কোনো কাজ করবেন না।

অনলাইন নিরাপত্তা



আপনার অ্যাকাউন্টগুলো সুরক্ষিত রাখুন

- প্রতিটি অ্যাকাউন্টের জন্য শক্তিশালী ও স্বতন্ত্র পাসওয়ার্ড ব্যবহার করুন; সেগুলো নিরাপদে সংরক্ষণ করতে একটি পাসওয়ার্ড ম্যানেজার ব্যবহার করুন।
- যেখানে যেখানে মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) উপলব্ধ, সেখানে তা সক্রিয় করুন।
- কখনো কারো সাথে ওটিপি, পিন, পাসওয়ার্ড বা সিকিউরিটি কোড শেয়ার করবেন না।
- অতিরিক্ত নিরাপত্তা স্তর হিসেবে বায়োমেট্রিক প্রমাণীকরণ (আঙুলের ছাপ/মুখমণ্ডল শনাক্তকরণ) ব্যবহার করুন।

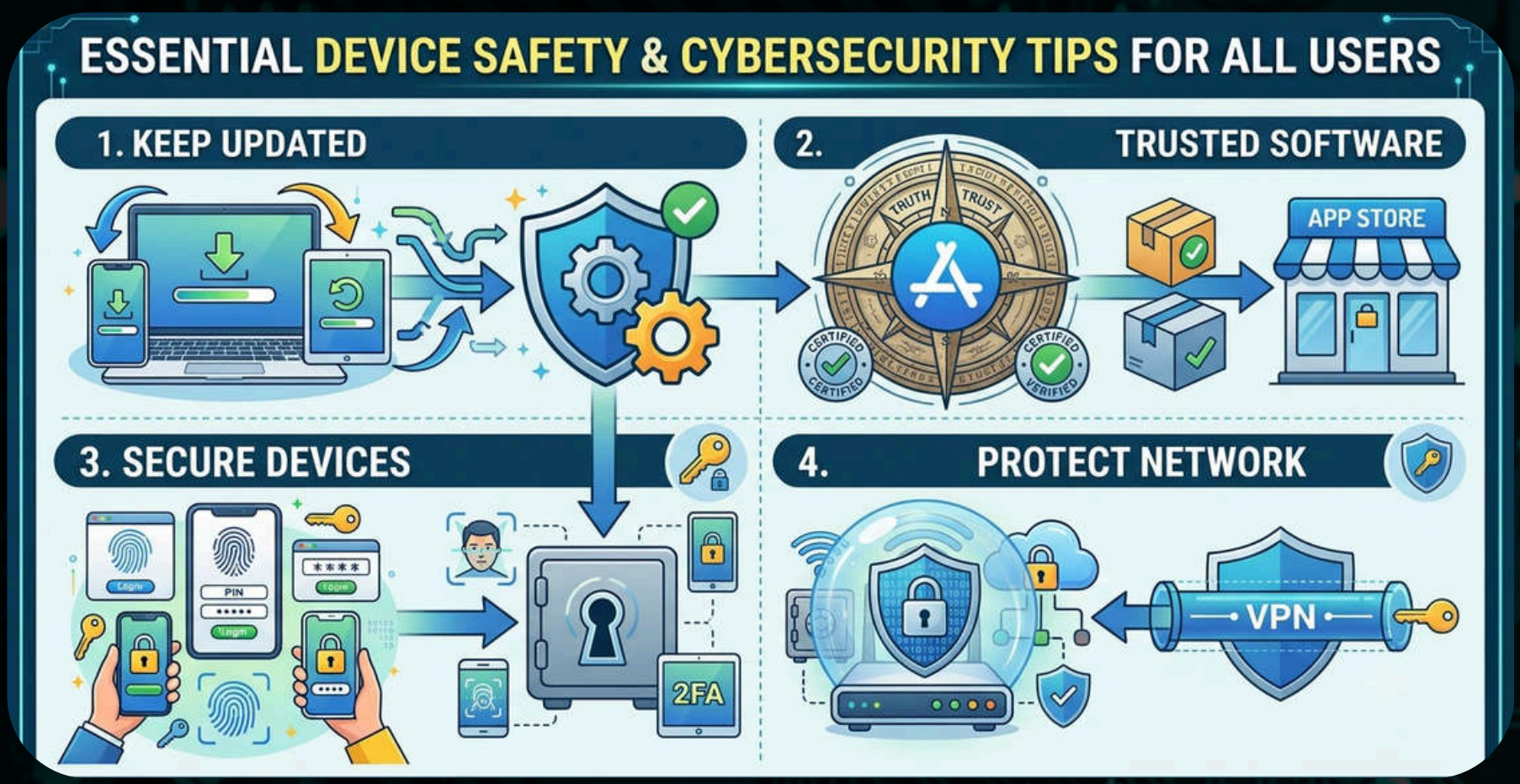
ইমেল ও ইন্টারনেট ব্যবহার করার সময় সুরক্ষিত থাকুন

- সন্দেহজনক বা সাদৃশ্যপূর্ণ ইমেল ঠিকানার ক্ষেত্রে প্রেরকের বিবরণ সাবধানে যাচাই করুন।
- ক্লিক করার আগে লিঙ্কগুলো যাচাই করুন এবং অপ্রত্যাশিত অ্যাটাচমেন্ট খোলা থেকে বিরত থাকুন।
- লগইন বা আর্থিক বিবরণ দেওয়ার আগে ওয়েবসাইটের সত্যতা যাচাই করুন।
- সন্দেহ হলে, কোনো পদক্ষেপ নেওয়ার আগে থামুন এবং যাচাই করে নিন।

কোনো কিছু ভুল হওয়ার আগেই প্রস্তুতি নিন

- গুরুত্বপূর্ণ ফাইলগুলোর নিয়মিত ব্যাকআপ রাখুন, যা অফলাইনে অথবা কোনো সুরক্ষিত ক্লাউড সার্ভিসে সংরক্ষণ করা থাকবে।
- অ্যাকাউন্ট পুনরুদ্ধারের তথ্য (ইমেল/ফোন) হালনাগাদ ও সুরক্ষিত রাখুন।

ডিভাইসের নিরাপত্তা



ডিভাইসগুলো আপডেট রাখুন

- পরিচিত দুর্বলতাগুলো দূর করার জন্য অপারেটিং সিস্টেম, অ্যাপ্লিকেশন, ব্রাউজার এবং নিরাপত্তা সফটওয়্যার নিয়মিত আপডেট করুন।
- যেখানে সম্ভব স্বয়ংক্রিয় আপডেট চালু করুন।

শুধুমাত্র বিশ্বস্ত সফটওয়্যার ইনস্টল করুন

- আসল সফটওয়্যার ব্যবহার করুন এবং শুধুমাত্র অফিসিয়াল অ্যাপ স্টোর বা বিশ্বস্ত উৎস থেকে অ্যাপ্লিকেশন ইনস্টল করুন।
- নির্ভরযোগ্য অ্যান্টিভাইরাস বা নিরাপত্তা সমাধান ব্যবহার করুন এবং সেগুলোকে হালনাগাদ রাখুন।

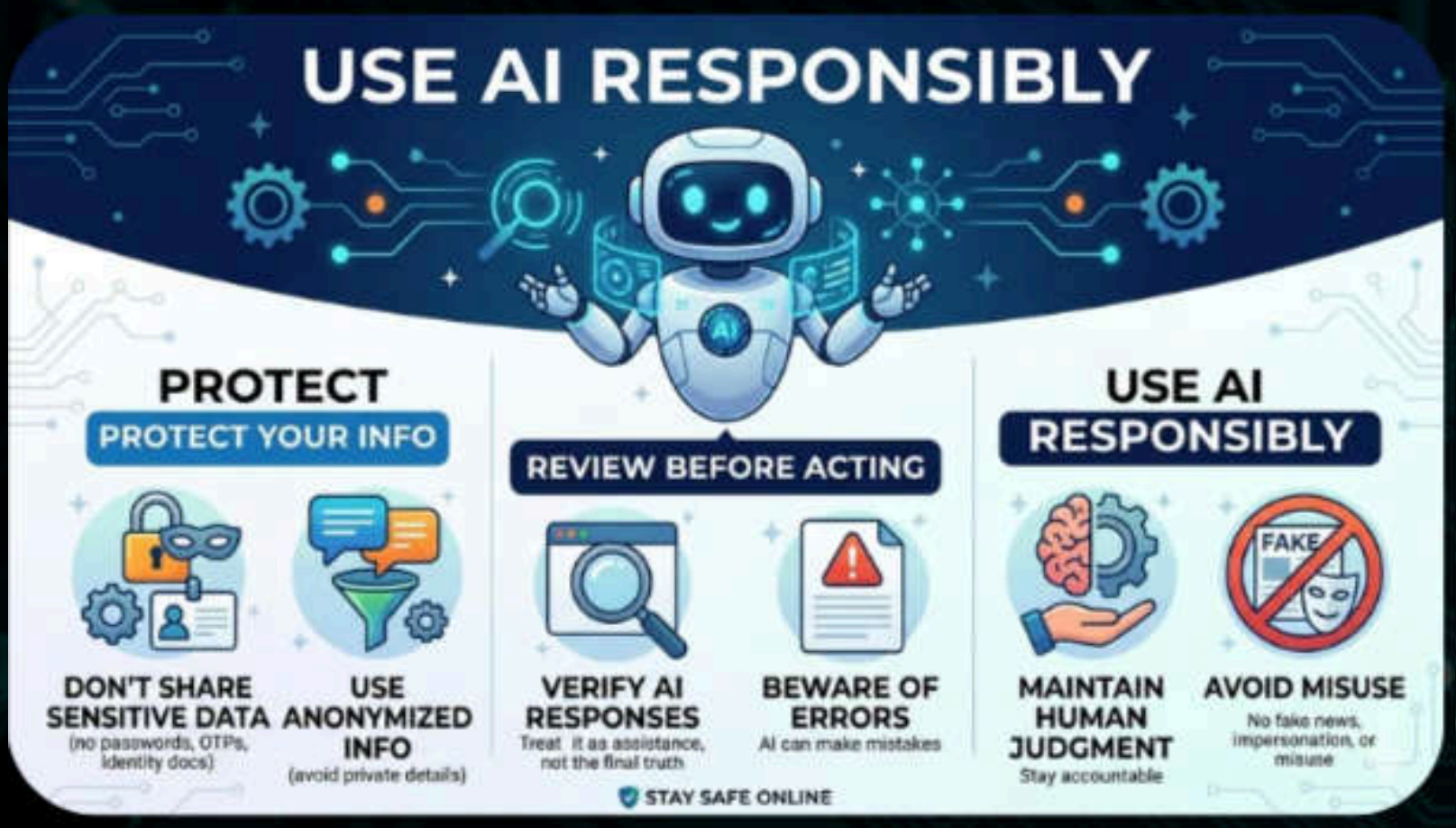
আপনার ডিভাইস ও অ্যাকাউন্ট সুরক্ষিত করুন

- সব ডিভাইসে শক্তিশালী পাসওয়ার্ড বা স্ক্রিন লক ব্যবহার করুন।
- যখনই সম্ভব, ডিভাইসের এনক্রিপশন এবং নিরাপত্তা বৈশিষ্ট্যগুলো সক্রিয় করুন।
- অপ্রয়োজনীয় অ্যাপ্লিকেশন এবং অনুমতিগুলো পর্যালোচনা করে মুছে ফেলুন।

আপনার নেটওয়ার্ক সংযোগ সুরক্ষিত রাখুন

- একটি শক্তিশালী পাসওয়ার্ড দিয়ে আপনার ওয়াই-ফাই সুরক্ষিত করুন এবং রাউটারের ডিফল্ট ক্রেডেনশিয়াল পরিবর্তন করুন।
- আপডেট করা রাউটার ফার্মওয়্যার এবং সুরক্ষিত নেটওয়ার্ক সেটিংস ব্যবহার করুন।
- অসুরক্ষিত নেটওয়ার্কের মাধ্যমে সংবেদনশীল অ্যাকাউন্টে প্রবেশ করা বা গোপনীয় তথ্য শেয়ার করা থেকে বিরত থাকুন।

দায়িত্বের সাথে AI ব্যবহার করুন



আপনার ব্যক্তিগত তথ্য সুরক্ষিত রাখুন

- সর্বজনীন *AI* টুল বা অজানা অনলাইন পরিষেবাগুলিতে ব্যক্তিগত, আর্থিক, স্বাস্থ্য, দাপ্তরিক বা গোপনীয় তথ্য প্রবেশ করাবেন না।
- পাসওয়ার্ড, ওটিপি, অ্যাকাউন্ট নম্বর, পরিচয়পত্র, গ্রাহকের তথ্য বা ব্যক্তিগত কথোপকথনের মতো সংবেদনশীল বিবরণ শেয়ার করা থেকে বিরত থাকুন।
- AI টুলের কাছে সাহায্য চাওয়ার সময় পরিচয় গোপন রেখে বা সাধারণ তথ্য ব্যবহার করুন।

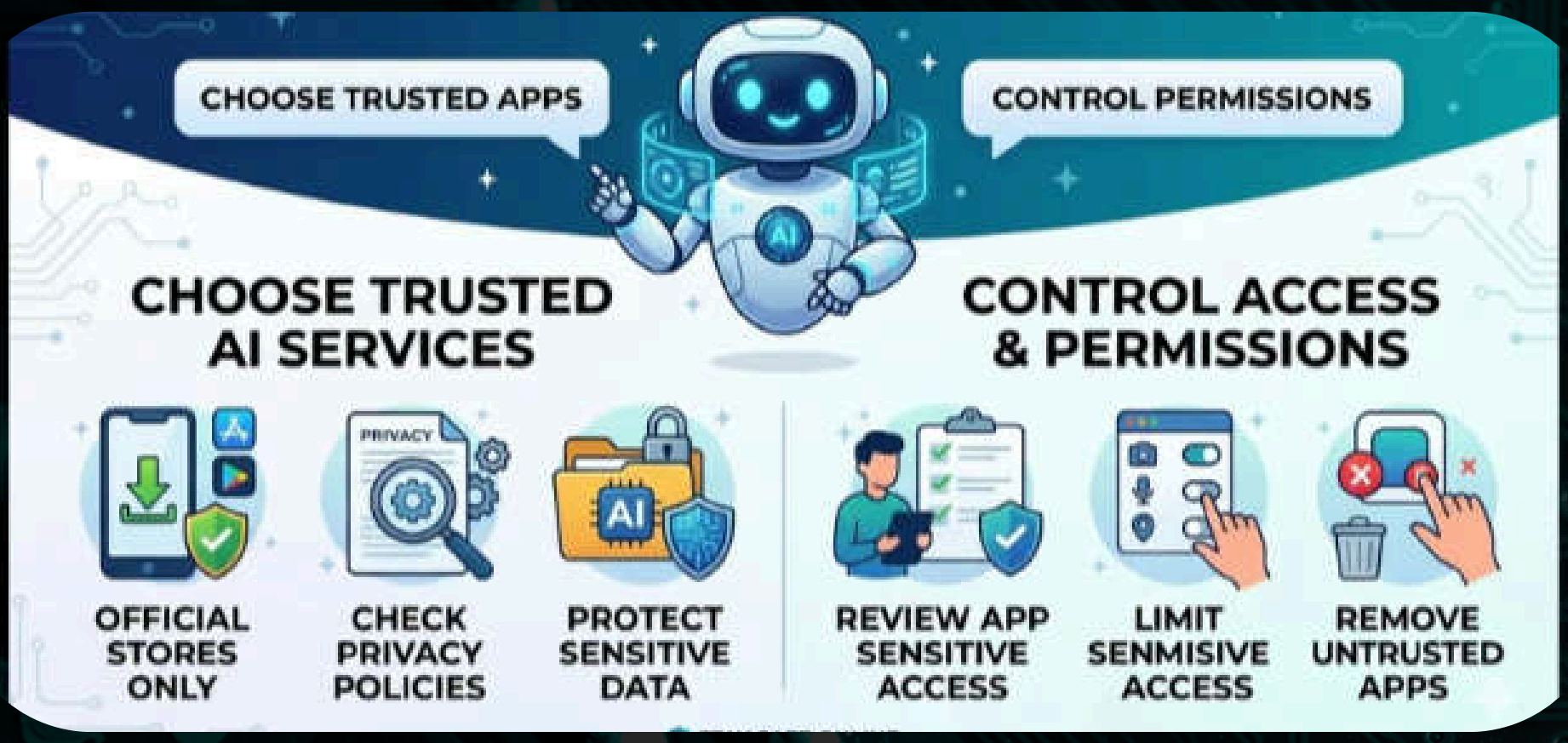
শেয়ার বা কোনো পদক্ষেপ নেওয়ার আগে পর্যালোচনা করুন।

- **AI**-প্রদত্ত প্রতিক্রিয়াগুলোকে সহায়তা হিসেবে বিবেচনা করুন, চূড়ান্ত সত্যের উৎস হিসেবে নয়।
- আর্থিক, আইনি, পেশাগত বা ব্যক্তিগত সিদ্ধান্তের জন্য গুরুত্বপূর্ণ তথ্য ব্যবহার করার আগে তা যাচাই করে নিন।
- মনে রাখবেন যে, AI টুলগুলো ভুল, অসম্পূর্ণ বা বিভ্রান্তিকর তথ্য তৈরি করতে পারে।

দায়িত্বের সাথে AI টুল ব্যবহার করুন

- আপনার কাজ ও শেখার ক্ষেত্রে AI ব্যবহার করুন, কিন্তু মানবিক বিচারবুদ্ধি ও জবাবদিহিতা বজায় রাখুন।
- মিথ্যা তথ্য তৈরি বা ছড়াতে, অন্যের ছদ্মবেশ ধারণ করতে, অথবা কারও ব্যক্তিগত তথ্যের অপব্যবহার করতে AI ব্যবহার করবেন না।

বিশ্বস্ত অ্যাপ বেছে নিন



অ্যাপ অ্যাক্সেস এবং অনুমতি নিয়ন্ত্রণ করুন

- AI অ্যাপ্লিকেশন ও ডিজিটাল অ্যাসিস্ট্যান্টদের দেওয়া অনুমতিগুলো পর্যালোচনা করুন।
- ক্যামেরা, মাইক্রোফোন, কন্টাক্ট বা লোকেশনের মতো ফিচারগুলো শুধু প্রয়োজন হলেই ব্যবহারের অনুমতি দিন।
- অপ্রয়োজনীয় অনুমতিগুলো মুছে ফেলুন এবং অবিশ্বস্ত উৎস থেকে অ্যাপ আনইনস্টল করুন।

বিশ্বস্ত AI পরিষেবা বেছে নিন

- স্বনামধন্য সরবরাহকারীদের AI অ্যাপ্লিকেশন ব্যবহার করুন এবং শুধুমাত্র অফিসিয়াল অ্যাপ স্টোর থেকেই সেগুলো ডাউনলোড করুন।
- AI পরিষেবা ব্যবহার করার আগে গোপনীয়তা সেটিংস, ব্যবহারের শর্তাবলী এবং ডেটা পরিচালনার পদ্ধতি পর্যালোচনা করুন।
- নিরাপত্তা নিয়ন্ত্রণগুলো যাচাই না করা পর্যন্ত সংবেদনশীল অ্যাকাউন্ট বা ফাইলের সাথে AI টুল সংযুক্ত করা থেকে বিরত থাকুন।

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