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 बेदारी मार्गदर्शिका

साइबर सफ़ाई तहज़ीब तैयार करिव

#CyberHygieneOurCulture



राष्ट्रीय साइबर सुरक्षा बेदारी माह (अक्टूबर 2026)

प्रकाशक

इंडियन कंप्यूटर इमरजेंसी रिस्पॉन्स टीम

Follow us :

@IndianCERT

@cert_india

मौज़ुआतुक फ़हरिस्त

- पेश लफ़्ज़ 3
- ए.आई. पर आधारित फ़िशिंग तँथ सोशल इंजीनियरिंग 4
- आवाज़ तँथ वीडियो डीपफेक (विशिंग) 5
- ए.आई. सँत मदद याफ्ता मैलवेयर तँथ खुदकार हमले 6
- नकली वेबसाइट तँथ शनाख़्त चोरी 7
- ख़तरे चिन्हन ह्यंद फ़हरिस्त 8
- ऑनलाइन सुरक्षा 9
- डिवाइस सुरक्षा 10
- ए.आई. ज़िम्मेदारी सँत इस्तिमाल करिव 11
- भरोसेमंद ऐप चुनिव 12
- CERT-In कॅरिव साइबर सुरक्षा हादसन ह्यंद खबर 13

पेश लफ़्ज़

आर्टिफिशियल इंटेलिजेंस (AI) असि जिंदगी, कामकाज तॅं आपसी राबितन ह्यंद तरीक़ा बदलोवान छॅं। यिम नवाचारس (Innovation) فروغ दवान छॅं, पैदावारीयत (Productivity) बढ़ावान छॅं तॅं मुख्तलिफ़ शोबन मंज़ मुश्किल मसअलन हल करनस मंज़ मदद दवान छॅं। मगर यॅंछॅं टेक्नोलॉजी खतरा पैदा करन वालन (Threat Actors) तरफ़स मंज़ ग़लत तौर पुर इस्तेमाल गछान छॅं ताकि वॅं ज़्यादा तरक़्क़ी याफ्ता तॅं यक़ीन दिलावन वालॅं साइबर खतरे तयार करि सकोन।

AI डिजिटल खतरण चिन्हनस मंज़ वुच्छन हिकायत मुश्किल बनावान छॅं, क्याहकि हमलावर वुछ यथ वख्त बहुत असल लगन वालॅं ई-मेल, पैगाम, ऑडियो, वीडियो तॅं वेबसाइट तयार करि सकोन। पुरानॅं खबरदारी निशान, जिमिस मंज़ खराब ग्रामर, ग़ैरमामूली फ़ॉर्मेटिंग या साफ़ ग़लतियाँ शुमार छॅं, अब यक़ीनी निशान नॅं रहि सकोन। यिम सूरतहाल मंज़ तस्दीक (Verification) तॅं ज़िम्मेदार डिजिटल रवैय्या अख ज़रूरी चीज़ बनि गयो छॅं।

असि रोज़मर्रा इस्तिमाल करन वालॅं AI टूल्स तॅं स्मार्ट डिवाइस, अगर एहतियात सॅंत नॅं इस्तेमाल गछि, तॅं नई निजता (Privacy) तॅं सुरक्षा ख़तरे पैदा करि सकोन। गैर-भरोसेमंद AI एप्लिकेशनन सॅंत निजी या राज़दाराना मालूमात साझा करुन, गैर-ज़रूरी अनुमतियाँ (Permissions) द्युन, या तस्दीक बगैर AI तयार करन वालि मालूमात पुर भरोसा करुन, अफ़रादन तॅं इदारनॅं ऽ सुरक्षा खतरण हवालॅं करि सकोन।

इंडियन कंप्यूटर इमरजेंसी रिस्पॉन्स टीम (CERT-In) ह्यंद यॅं बुकलेट “AI साइबर बेदारी” रोज़मर्रा नागरिकन, मुलाज़िमन तॅं डिजिटल इस्तेमाल करन वालनॅंतर तैयार करन आय छॅं, न कि सिर्फ़ साइबर सुरक्षा माहिरनॅंतर। यॅं वज़ाहत करान छॅं कि AI कॅंस तरह डिजिटल खतरण ह्यंद मंज़रनामा बदलावान छॅं तॅंसथि सरल, अमली कदम फराहम करान छॅं यिम हरेक शख्स अपनावि सॅंकान, ताकि अपनी निजी मालूमात, डिवाइस तॅं ऑनलाइन पहचान सुरक्षित राखि सॅंकान।

ए.आई. पुर आधारित फ़िशिंग तँथ सोशल इंजीनियरिंग



यँ कॅसे काम करान छँ?

खतरा पैदा करन वालॅ (Threat Actors) वुच्छ वख्त ऐसे ई-मेल तॅं टेक्स्ट पैगाम भेजान छि यिम असल तॅं गलती रहित लगान छि। वॅं छि तोहंदि बारे मंज़ तफ़सील, मसलन तोहंदॅं नौकरी, तोहंद्यॅं इस्तेमाल करन वॅल सेवाव, या हालिया सरगर्मियाँ इस्तेमाल करान ताकि पैगाम ज़्यादा निजी तॅं यक़ीन योग्य महसूस गछि।
चूंकि यिम पैगाम बहुत अच्छी तरह लिखित असान, तेमिस वजह सॅंत यिमस फ़िशिंग या धोखाधड़ी पैगामस पहचानन छॅं बहुते ज़्यादा मुश्किल बनान।

यँ कॅसे पहचानिव?

- पैगाम تॅ چھ़ंदॅं خॅص तौर पुर तैयार लगान, मगर बगैर उम्मीद س موصول गछान।
- यिमس मंज़ जल्दबाज़ी या धमकी दॅंवन वालि ज़बान इस्तेमाल गछि ॅت फ़ौरी कार्रवाई کرنس کر مطالبہ गछि।
- यँ تॅह्यॅं लिंक पुर क्लिक करन، अकाउंट तस्दीक करन، पासवर्ड रीसेट करन या रक़म जमा करन ॅخ तर करान छॅं।
- भेजन वाल्युक (Sender) पता تقریب ॅن ठीक लगान छॅं, मगर पूरी तरह असल नॅं होवान।

महफ़ूज़ कॅसे रहिव?

- बगैर मांगन आयॅं पैगामन मंज़ दियॅं गयॅं लिंक पुर क्लिक नॅं करिव। यिमस बदले सीधे आधिकारिक वेबसाइट या ऐपس पुर जाएव।
- हर दरख़ास्तुक तस्दीक अलग तॅं भरोसेमंद ज़रिया सॅंत करिव, मसलन आधिकारिक फोन नंबर या ऐप।
- पैगामस मंज़ दियॅं गयॅं लिंक पुर खुलन वाल्यॅं पेजस पुर कदापि अपनी क्रेडेन्शियल्स या OTP दाख़िल नॅं करिव।
- शक पैदा करन वालॅं पैगामन ह्यंद रिपोर्ट करिव तॅं तिम डिलीट करिव، □□त□□क बाद भेजन वाल्यॅं (Sender) बंद करिव (Block करिव)।

आवाज़ तॅंथ वीडियो डीपफेक [विशिंग]



यॅं कॅंसे काम करान छॅं?

खतरा पैदा करन वालॅं (Threat Actors) आवाज़ ڈاون करि सकोन या ऐसे नकली वीडियो (Fake Videos) तयार करि सकोन यिम वुच्छनस तॅं सुननस मंज़ बिल्कुल असल लगान छि। वॅं छि तोहंदॅं खानदान, साथी कारीगर (Colleagues) या अफ़सर बनि कर तोहॅं दबावस मंज़ आनान ताकि ہۆ حساس (Sensitive) मालूमात द्यिव, रक़म भेजिव یا फ़ौरन कोई कदम उठाविव।
यिम आवाज़ तॅं वीडियो एतह असल तॅं यक़ीनयोग्य लगान छि कि यिमस नकली या धोखाधड़ी हॅंद रूपस मंज़ पहचानन बहुते मुश्किल बनान छॅं।

यॅं कॅंसे पहचानिव?

- ग़ैर मामूली जल्दबाज़ी, घबराहट या राज़दारी ह्यॅंद मांग, मसलन "यॅं कॅंन्हिस नॅं वणिव"।
- आवाज़ुक लहजा, गुफ़्तगूयुक रफ़्तार, पॅंठ्यम शोर (Background Noise) या ऑडियो क्वालिटी मंज़ हल्की गड़बड़।
- मामूल ह्यंद तस्दीक (Verification) या मंज़ूरी (Approval) अमलस दरकिनार करन ह्यॅंद दरख़ास्त।
- गिफ्ट कार्ड, क्रिप्टोकरेंसी या वायर ट्रांसफ़र ज़रियॅं पेमेंट करन ह्यॅंद मांग।

महफ़ूज़ कॅंसे रहिव?

- फोन कॅंट करिव तॅं तिमिस शख्सस तेमिसच सहेजॅं गयॅं या मालूम नंबर पुर दुबारा कॉल करिव।
- हंगामी (Emergency) हालतन मंज़ पहचान तस्दीक करन ॅंतर अपने खानदान या दफ़्तर س मंज़ अख "सेफ़ वर्ड" तय करिव।
- सिर्फ़ कॉल या वीडियो पुर भरोसा करि कदापि पेमेंट मंज़ूरी नॅं द्यिव। अलग तॅं भरोसेमंद ज़रिया सॅंत लिखित रूपस मंज़ तस्दीक करिव।
- फ़ौरी प्रतिक्रिया द्युनस पुठॅं थोड़ी देर रुकिव। खतरा पैदा करन वालॅं (Threat Actors) ہۆहंदॅं फ़ैसलॅं पुर असर करनॅं ॅंतर घबराहट तॅं जल्दबाज़ी □□र भरोसा करान छि।

ए.आई.-मदद याफ्ता मालवेर तँथ खुदकार हमले



यँ कँसे काम करान छँ?

ख़तरनाक हमलावर (Threat Actors) ए.आई. टूलन हंद इस्तेमाल करान खराब या नुकसानदायक कोड तयार करनस खातर, या तिम लुकावनस खातर, चोरमुत पासवर्ड मुख़तलिफ वेबसाइटन पेठ आज़मावनस खातर, तेह तिम सिस्टम पहचाननस खातर यिमन अपडेटन हंद ज़रूरत छि। यस कारण हमले वॉन तेज़ तेह वुसीअ पैमानस पेठ फैलान।

यँ कँसे पहचानिव?

- बग़ैर तुहंदि दरख़ास्ति लॉगिन अलर्ट, पासवर्ड रीसेट ईमेल, या MFA प्रॉम्प्ट हासिल गछुन।
- अकाउंट एक्टिविटी मंज़ अजनबी डिवाइस या सेशन नज़र आवुन।
- एंटीवायरस चेतावनियाँ, पॉप-अप्स, या डिवाइस हंद गैर-मामूली सुस्त काम करुन।
- ऐसी फाइल, सेटिंग, या ब्राउज़र एक्सटेंशन दिखुन यिम तुहंदि पहचान मंज़ न छि।

महफ़ूज़ कँसे रहिव?

- हर अकाउंट खातर इस्तेमाल करिव एक अलग तेह मज़बूत पासवर्ड।
- तमाम अहम अकाउंटन पेठ मल्टी-फैक्टर ऑथेंटिकेशन (MFA) चालू करिव।
- एंटीवायरस सॉफ्टवेयर, सिस्टम तेह एप्स हमेशा अपडेट रखिव।
- गैर-मुतवक्के लॉगिन या MFA अलर्ट मिलिथ तुरंत कार्रवाई करिव।

नकली वेबसाइट्स तेह पहचान चोरी



यॅं कॅंसे काम करान छॅं?

ख़तरनाक हमलावर अख़ वेबसाइट तेह चैटबॉट तैयार करि सकान यिम असली लगान, मसलन बैंकिंग या ऑनलाइन खरीदारी पोर्टल। तिम छि तुहंदे लॉगिन क्रेडेंशियल्स, OTP, या पेमेंट डिटेल्स चुरावन्युक कोशिश करान। तिम फर्जी फोटो या दस्तावेज़ इस्तेमाल करि नकली पहचान तइयार करिथ पानस असली दिखावन्युक कोशिश तिम करान।

यॅं कॅंसे पहचानिव?

- वेबसाइट URL मंज़ हल्का बदलाव, मसलन ज़्यादा अक्षर, हाइफ़न, या कोई अलग डोमेन एंडिंग।
- चैटबॉट या एजेंट यिम OTP, PIN, या कार्ड नंबर पॉरि तरह पृछन।
- जान-पहचान वाली वेबसाइट पॅठ HTTPS न हॉवन, या डिज़ाइन मंज़ अजीब तेह गैर-मामूली फर्क नज़र आवुन।

महफ़ूज़ कॅंसे रहिव?

- हमेशा आधिकारिक (Official) URL खुद टाइप करिव या भरोसेमंद बुकमार्क इस्तेमाल करिव, लिंकन पॅठ क्लिक करनस बजाय।
- कदापि OTP, PIN, या पूरे कार्ड विवरण किसी चैटबॉट या "सपोर्ट एजेंट" सॅत साझा न करिव।
- लॉगिन करनस पॅठे पहले HTTPS जांचिव तेह डोमेन नाव ध्यान सॅत देखिव।
- अपने बैंक स्टेटमेंट तेह क्रेडिट रिपोर्ट नियमित तौर पॅठ जांचिव, ताकि कोई अजनबी या संदिग्ध गतिविधि पकड़ी जा सके।

रेड फ्लैग्स चेकलिस्ट [ख़तरे हंद निशान]

AI-सक्षम हमलस हंद ये संकेत पॅठ नज़र रखिव:

- पैसा, क्रेडेंशियल्स, या मंज़ूरी हासिल करनस खातर फ़ौरी तॅह दबाव वाली दरख़ास्त।
- किसी "जान-पहचान" वाले शख़्स हंद कॉल या वीडियो मंज़ आवाज़ या वीडियो से संबंधित मामूली गैर-मामूली फर्क नज़र आवुन।
- आम तस्दीक (Verification) या मंज़ूरी (Approval) हंद तरीक़ा नज़रअंदाज़ करन्युक या बाइपास करन्युक दरख़ास्त करुन।
- अजनबी या गैर-मालूम भेजनहार (Sender) हुंद डोमेन, या थोड़ा बदला हुआ URL नज़र आवुन।
- गैर-मुतवक्के MFA प्रॉम्प्ट या OTP हासिल गछुन, यिम तुहंदी तरफ़ सॅत दरख़ास्त न करिथ आसिन।
- सुरक्षा सॉफ्टवेयर बंद करन्युक, या गैर-आधिकारिक (Unofficial) लिंकन ज़रिये "तस्दीक" (Verify) करन्युक दरख़ास्त करुन।
- ऐसे नौकरी या निवेश (Investment) ऑफर यिमन मंज़ पहले पैसा जमा करन्युक या निजी वित्तीय जानकारी (Personal Financial Details) द्युन्युक तकाज़ा करन।

अगर शक पैदा गछे, तॅह ठहरिव, जानकारी स्वतंत्र तौर पॅठ तस्दीक करिव, तॅह दबाव हेठ कॉई फ़ैसला या कार्रवाई न करिव।

ऑनलाइन सुरक्षा



पनुन अकाउंट सुरक्षित रखिव

- हर अकाउंट खातर मज़बूत तेह अलग पासवर्ड इस्तेमाल करिव; तिमन सुरक्षित तौर पेठ संभाल्नस खातर पासवर्ड मैनेजर इस्तेमाल करिव।
- जत्थे उपलब्ध आसि, तेत्ते मल्टी-फैक्टर ऑथेंटिकेशन (MFA) सक्रिय करिव।
- कदापि OTP, PIN, पासवर्ड, या सुरक्षा कोड कुसुहिं सेत साझा न करिव।
- अतिरिक्त सुरक्षा तह (Layer) खातर बायोमेट्रिक प्रमाणीकरण (फिंगरप्रिंट/ चेहरा पहचान) इस्तेमाल करिव।

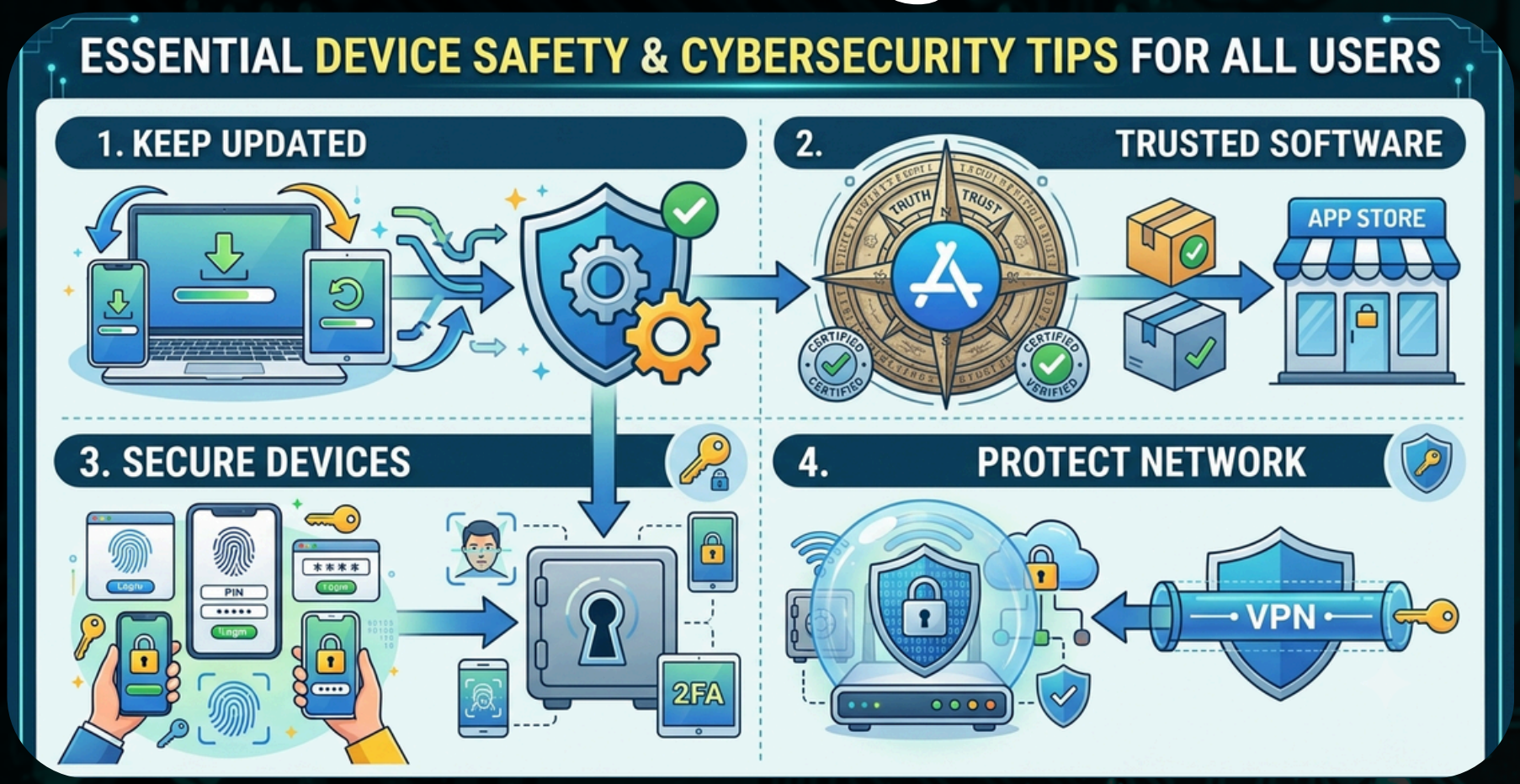
ईमेल तेह इंटरनेट इस्तेमाल करान वक़्त सुरक्षित रहिव

- संदिग्ध या असली-जेसे दिखन वाले ईमेल पते पहचाननस खातर भेजनहार (Sender) हुंद विवरण ध्यान सेत जांचिव।
- क्लिक करनस पेठे पहले लिंकन हंद तस्दीक करिव तेह गैर-मुतवक्के अटैचमेंट खोल्नस पेठ परहेज़ करिव।
- लॉगिन या वित्तीय जानकारी द्युनस पेठे पहले वेबसाइट हंद असलियत (Authenticity) ज़रूर जांचिव।
- अगर शक पैदा गछे, तोह पहले रुकिव तेह तस्दीक करिव, बे पथ कार्रवाई करिव।

मुसीबत आवनस पेठे पहले तैयार रहिव

- महत्वपूर्ण फाइलन हंद नियमित बैकअप तैयार रखिव, यिम ऑफलाइन या कुस सुरक्षित क्लाउड सेवा मंज़ संग्रहित आसिन।
- अकाउंट रिकवरी जानकारी (ईमेल/फ़ोन नंबर) हमेशा अद्यतन तेह सुरक्षित रखिव।

डिवाइस सुरक्षा



डिवाइसन अपडेट रखिव

1. ऑपरेटिंग सिस्टम, एप्लीकेशन, ब्राउज़र तेह सुरक्षा सॉफ्टवेयर नियमित तौर पेठ अपडेट करिव, ताकि मालूम कमज़ोरियन *(Vulnerabilities)* ठीक गछि सकन।
2. जत्थे मुमकिन आसि, तेत्ते ऑटोमैटिक अपडेट चालू करिव।

सिर्फ भरोसेमंद सॉफ्टवेयर इंस्टॉल करिव

1. असली *(Genuine)* सॉफ्टवेयर इस्तेमाल करिव तेह एप्लीकेशन सिर्फ आधिकारिक ऐप स्टोर या भरोसेमंद स्रोतस मंज़ सेत इंस्टॉल करिव।
2. भरोसेमंद एंटीवायरस या सुरक्षा समाधान इस्तेमाल करिव तेह तिम हमेशा अपडेट रखिव।

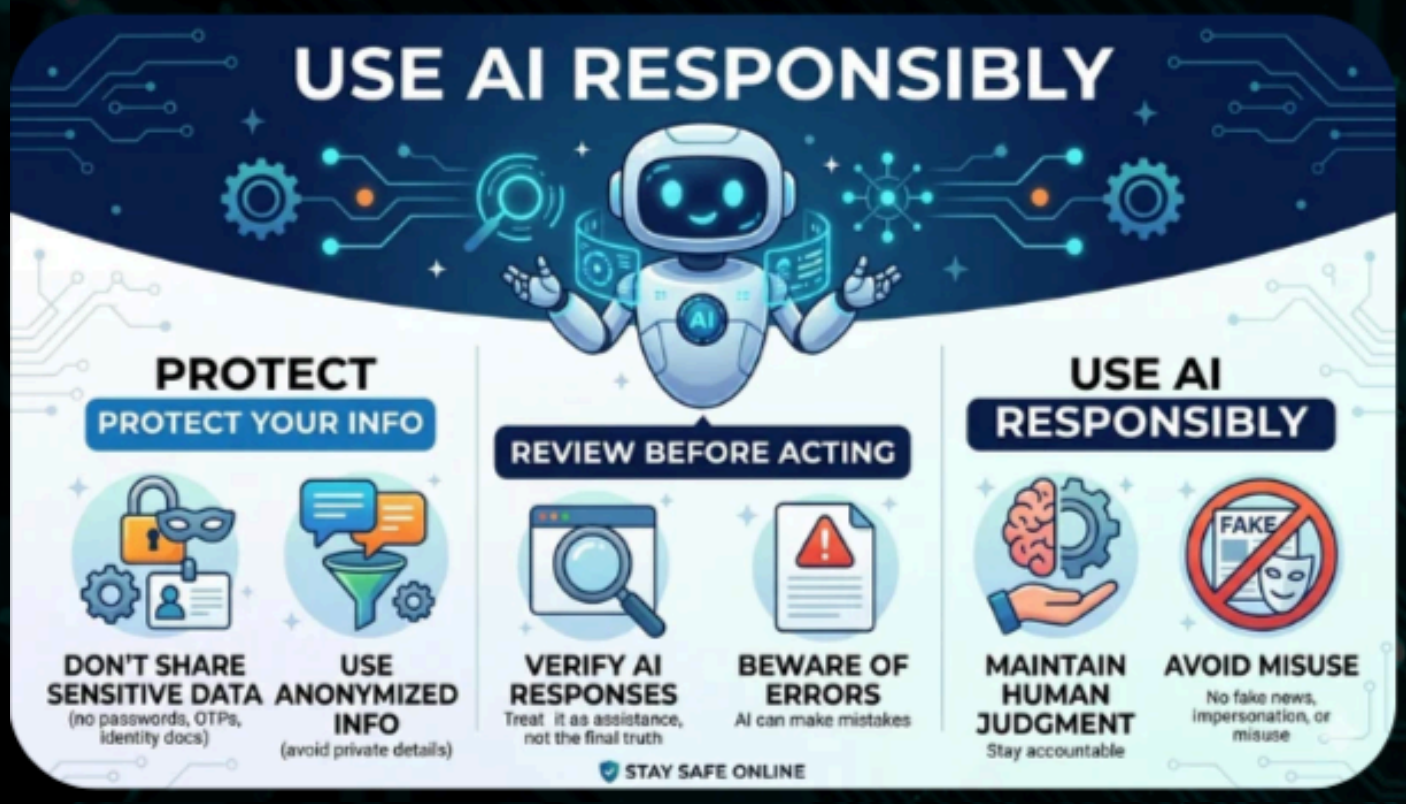
अपनॅ डिवाइस तेह अकाउंट सुरक्षित रखिव

1. तमाम डिवाइसन पेठ मज़बूत पासवर्ड या स्क्रीन लॉक इस्तेमाल करिव।
2. जत्थे उपलब्ध आसि, तेत्ते डिवाइस एन्क्रिप्शन तेह सुरक्षा विशेषताएँ *(Security Features)* सक्रिय करिव।
3. गैर-ज़रूरी एप्लीकेशन तेह अनुमति *(Permissions)* नियमित तौर पेठ जांचिव तेह हटाविव।

अपनॅ नेटवर्क कनेक्शन सुरक्षित रखिव

1. *Wi-Fi* खातर मज़बूत पासवर्ड इस्तेमाल करिव तेह राउटर हंद डिफ़ॉल्ट क्रेडेंशियल्स बदलिव।
2. अपडेटेड राउटर फर्मवेयर तेह सुरक्षित नेटवर्क सेटिंग्स इस्तेमाल करिव।
3. असुरक्षित *(Unsecured)* नेटवर्कन पेठ संवेदनशील अकाउंटन तक पहुँच या गोपनीय जानकारी साझा करनस पेठ परहेज़ करिव।

AI जिम्मेदारी सेत इस्तेमाल करिव



अपनी व्यक्तिगत जानकारी सुरक्षित रखिव

1. सार्वजनिक *AI* टूलन या गैर-मालूम ऑनलाइन सेवासन मंज़ निजी, वित्तीय, स्वास्थ्य संबंधी, आधिकारिक या गोपनीय जानकारी दाखिल न करिव।
2. पासवर्ड, *OTP,* अकाउंट नंबर, पहचान दस्तावेज़, ग्राहक डेटा या निजी बातचीत जैसे संवेदनशील विवरण साझा करनस पेठ परहेज़ करिव।
3. *AI* टूलन सेत मदद मांगन वक़्त अनाम *(Anonymized)* या सामान्य जानकारी इस्तेमाल करिव।

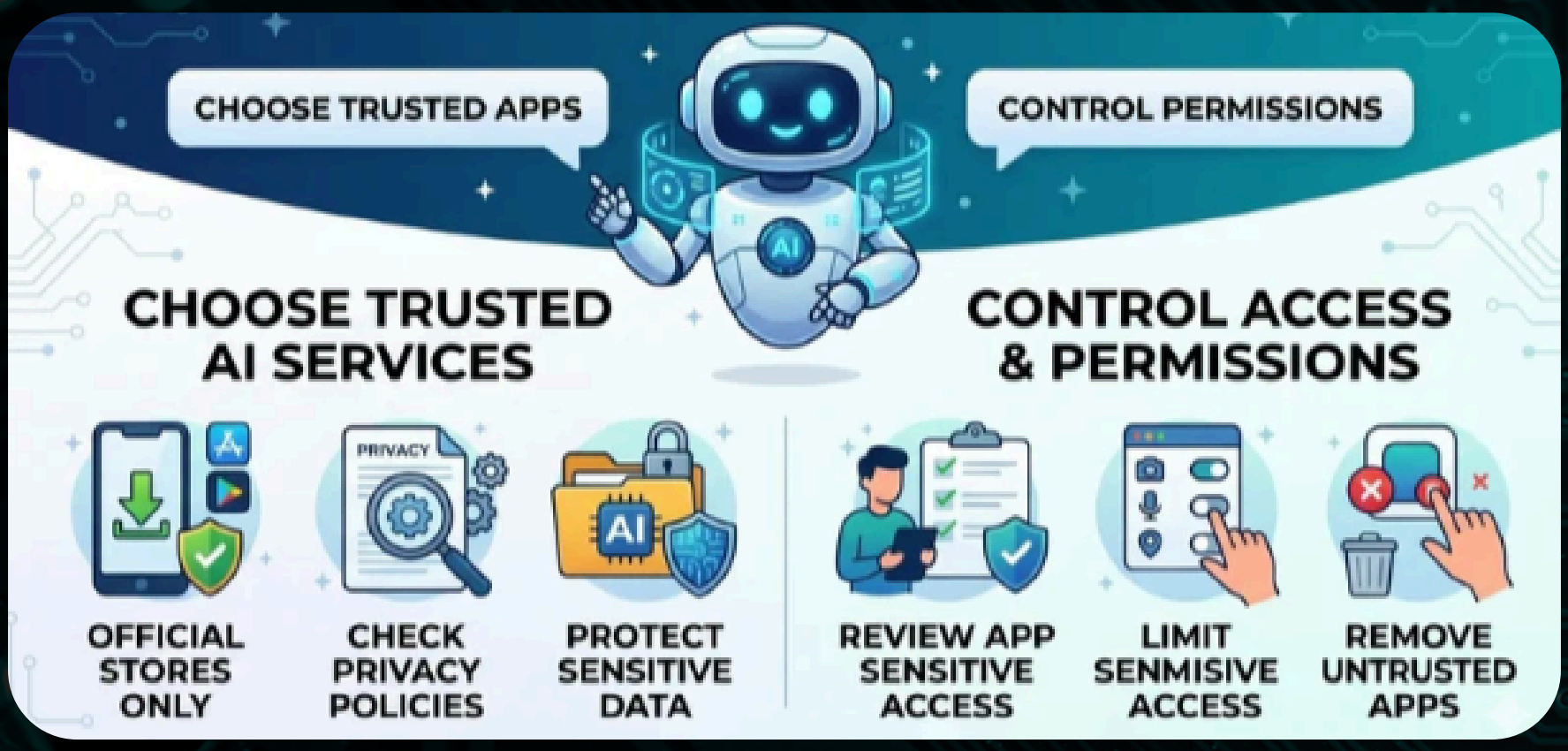
साझा करनस या कार्रवाई करनस पेठे पहले जांचिव

1. *AI* द्वारा तैयार जवाबन केवल मददगार जानकारी समझिव, अंतिम सच या अंतिम निर्णय न समझिव।
2. वित्तीय, कानूनी, पेशेवर या निजी फ़ैसलन खातर इस्तेमाल करनस पेठे पहले महत्वपूर्ण जानकारी ज़रूर तस्दीक करिव।
3. हमेशा याद रखिव कि *AI* टूल कभी-कभी गलत, अधूरी या गुमराह करन वाली जानकारी दे सकान।

AI टूलन हंद जिम्मेदारी सेत इस्तेमाल करिव

1. *AI* हंद इस्तेमाल अपने काम तेह सीखनस मंज़ मदद खातर करिव, मगर इंसानी सोच-विचार तेह जवाबदेही कायम रखिव।
2. *AI* हंद इस्तेमाल झूठी जानकारी तैयार करन, फैलावन, दुसरन हंद रूप धरन *(Impersonation),* या कुसुहिं हंद निजी डेटा हंद गलत इस्तेमाल करन खातर न करिव।

भरोसेमंद ऐप्स चुनिव



ऐप एक्सेस तेह अनुमति *(Permissions)* नियंत्रित करिव

1. *AI* एप्लीकेशन तेह डिजिटल असिस्टेंटन द्विमत अनुमति *(Permissions)* नियमित तौर पेठ जांचिव।
2. कैमरा, माइक्रोफोन, संपर्क *(Contacts)* या लोकेशन जेसन सुविधनस सिर्फ ज़रूरत पेठ एक्सेस द्विव।
3. गैर-ज़रूरी अनुमति हटाविव तेह गैर-भरोसेमंद स्रोतस मंज़ सेत इंस्टॉल करिमुत ऐप्स हटाविव।

भरोसेमंद *AI* सेवाएँ चुनिव

1. प्रतिष्ठित तेह भरोसेमंद सेवा-प्रदातन हंद *AI* एप्लीकेशन इस्तेमाल करिव तेह तिम सिर्फ आधिकारिक ऐप स्टोरस मंज़ सेत डाउनलोड करिव।
2. *AI* सेवा इस्तेमाल करनस पेठे पहले गोपनीयता सेटिंग्स, इस्तेमाल हंद शर्तन *(Terms of Use)* तेह डेटा संभालन्ये तरीक़न हंद जायज़ा ग्यिव।
3. संवेदनशील अकाउंटन या फाइलन सेत *AI* टूल तभी जोड़िव येलि तिमन हंद सुरक्षा नियंत्रण *(Security Controls)* ठीक तरह तस्दीक करिमुत आसि।

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