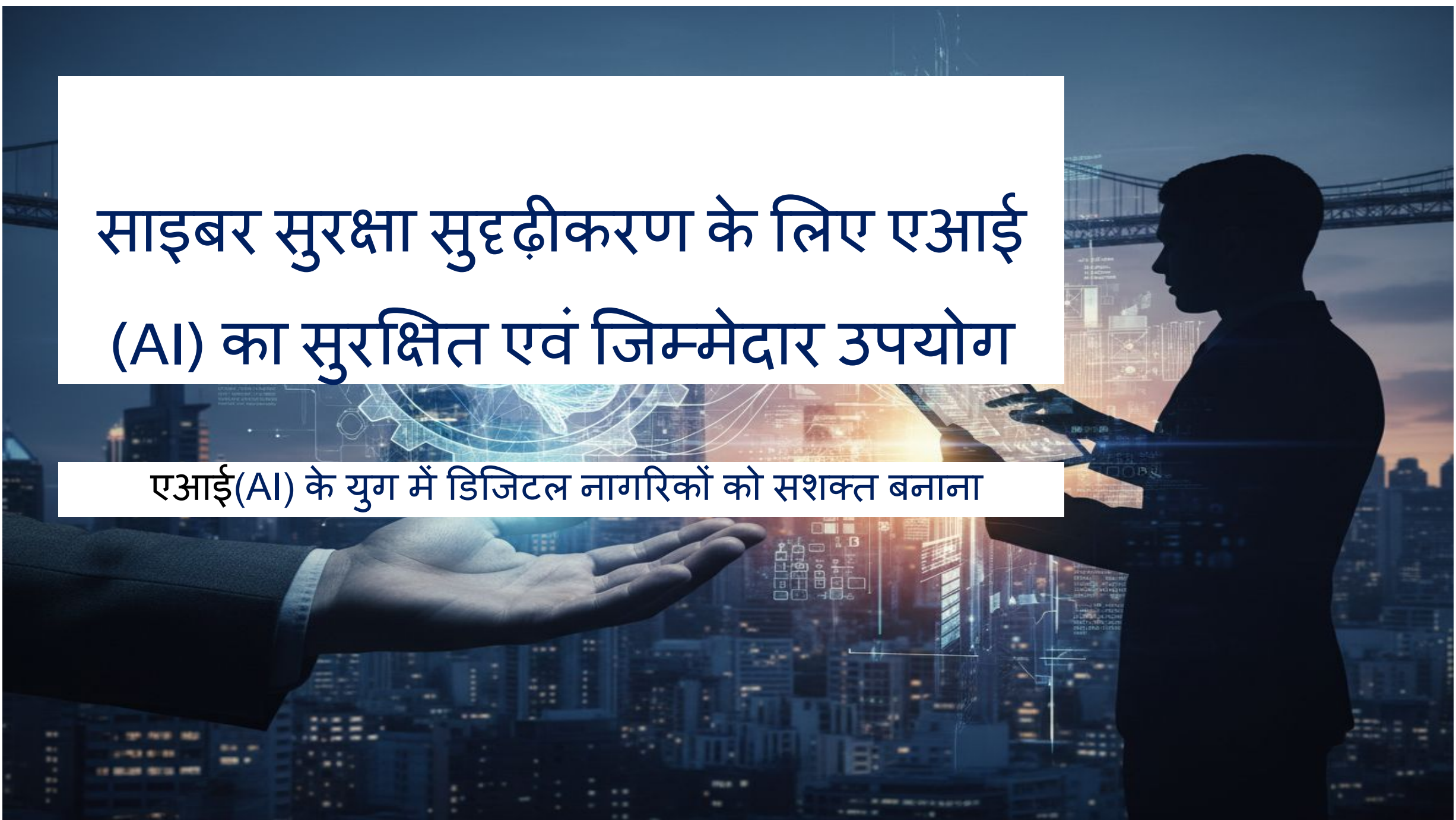


साइबर सुरक्षा सुदृढीकरण के लिए एआई (AI) का सुरक्षित एवं जिम्मेदार उपयोग

एआई(AI) के युग में डिजिटल नागरिकों को सशक्त बनाना



आज का एजेंडा

- सिंथेटिक मीडिया क्या है?
- साइबर सुदृढीकरण के मुख्य पहलू।
- AI (एआई) के युग में किस पर भरोसा करें?
- ट्रस्ट जोन के रोजमर्रा के उदाहरण।
- सुरक्षित AI उपयोग सुनिश्चित करें।
- रोजमर्रा की आदतों का पोषण।
- रिपोर्टिंग और सुरक्षा टूल।

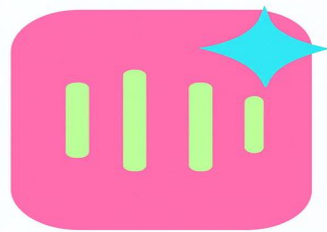


सिंथेटिक मीडिया क्या है?

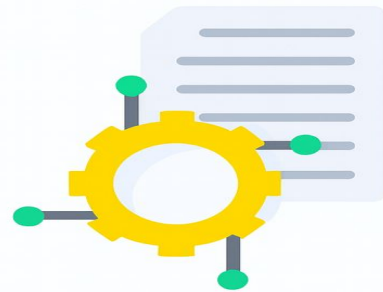
सिंथेटिक मीडिया कंप्यूटर से बनी तस्वीरें, वीडियो या आवाजें हैं जो वास्तविक लोगों की तरह दिखते हैं।



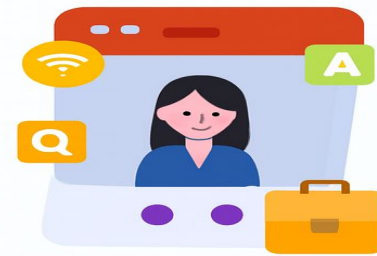
डीपफेक



AI द्वारा उत्पन्न
ऑडियो



सिंथेटिक पाठ



आभासी मानव
(Virtual Human)
और डिजिटल अवतार


सिंथेटिक मीडिया की नैतिक चिंताएं

- नकली को असली जैसा बना देता है।
- यह इस बात का फायदा उठाता है कि मनुष्य स्वाभाविक रूप से दृष्टि और ध्वनि पर भरोसा करते हैं।
- आलोचनात्मक सोच को प्रतिक्रियाशील स्वीकृति से बदल दिया जाता है।

साइबर सुदृढीकरण(रेज़िलिएंस) क्या है?

मुख्य पहलू	विवरण
Anticipate (अनुमान लगाना)	समझें कि AI घोटाले एक वास्तविकता हैं
Withstand (झेलना)	किसी भी प्रकार के साइबर हमले का सामना करने के लिए सुरक्षा उपाय सुनिश्चित करें
Recover (पुनर्प्राप्त करना)	बैकअप रखें ताकि आप जल्दी से सामान्य स्थिति में वापस आ सकें।
Adapt (अनुकूल बनाना)	सूचित रहें और अपनी और दूसरों की गलतियों से सीखें।

"सूचित विश्वास" मॉडल



रुकें	ब्लाइंड ट्रस्ट	स्कैमर्स ऐसे लोगों की तलाश करते हैं जो आंख मूंदकर भरोसा करते हैं।
परखें	सशर्त ट्रस्ट	सोचें कि क्या यह नकली हो सकता है? विश्वसनीयता स्थापित करने की दिशा में काम करें।
आगे बढ़ें	इन्फॉर्मड ट्रस्ट	दावों को सत्यापित करें और क्रॉस चेक करें

आवाज की क्लोनिंग/ लिप-सिंक एआई

👂 कान (श्रवण)



🧠 मन (अनुभूति और भावना)



आवाज की क्लोनिंग

👂 कान (श्रवण)



🧠 मन (अनुभूति और भावना)

पैसे, ओटीपी या बायोमेट्रिक डेटा के लिए कोई भी अवांछित अनुरोध

यदि आप बिना रुके क्लिक करते हैं, भुगतान करते हैं या साझा करते हैं, तो आप लाल क्षेत्र में हैं।

आप रुकते हैं, दोबारा जांच करते हैं, और जब यह बुनियादी जांचों में सफल हो जाता है तो कार्रवाई करते हैं।

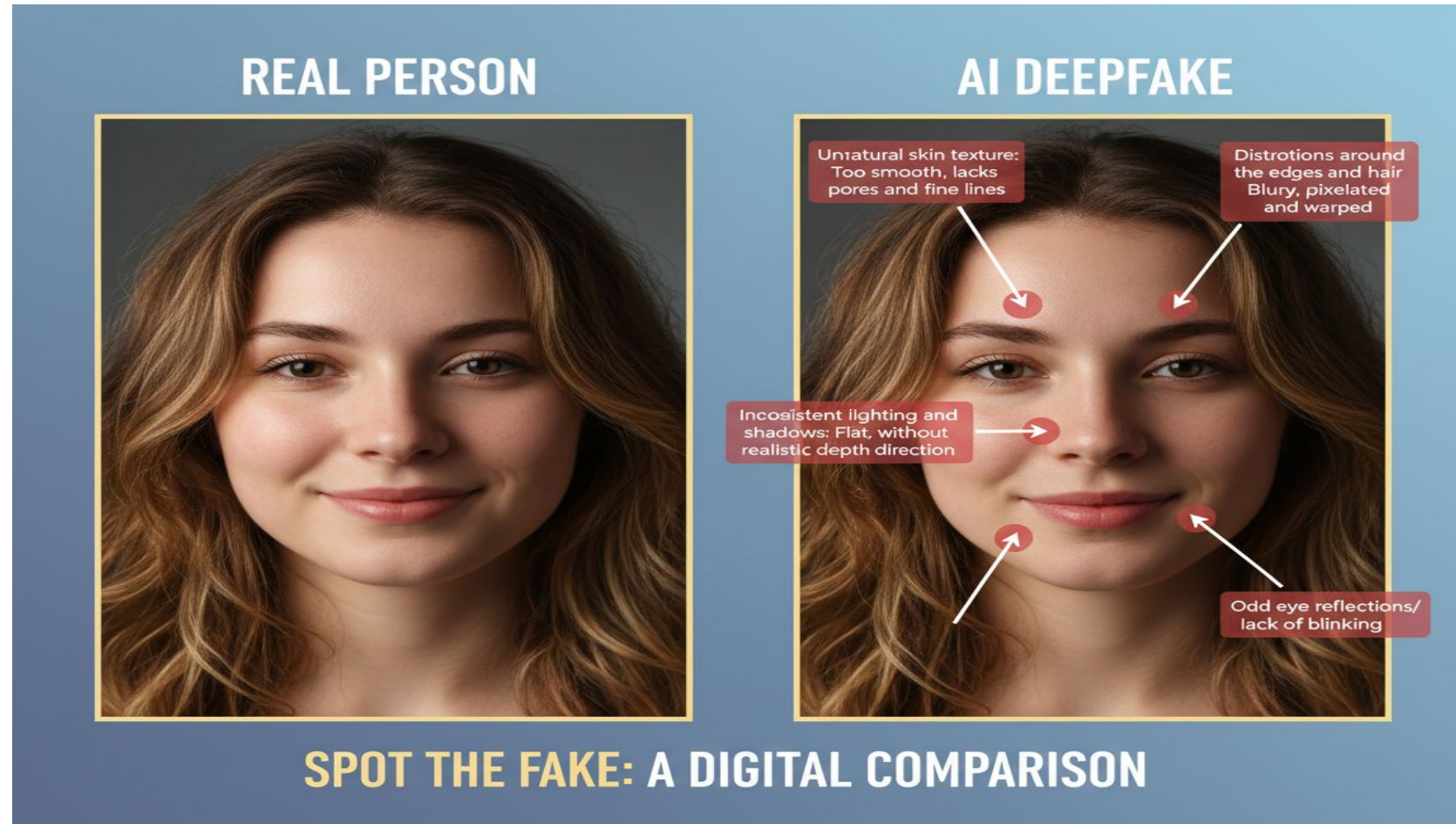
आप रुकते हैं, दोबारा जांच करते हैं, और जब यह बुनियादी जांचों में सफल हो जाता है तो कार्रवाई करते हैं।

👁️ आंखें (दृष्टि)



🧠 मन (अनुभूति और भावना)

लिप-सिंकिंग AI / डीपफेक वीडियो



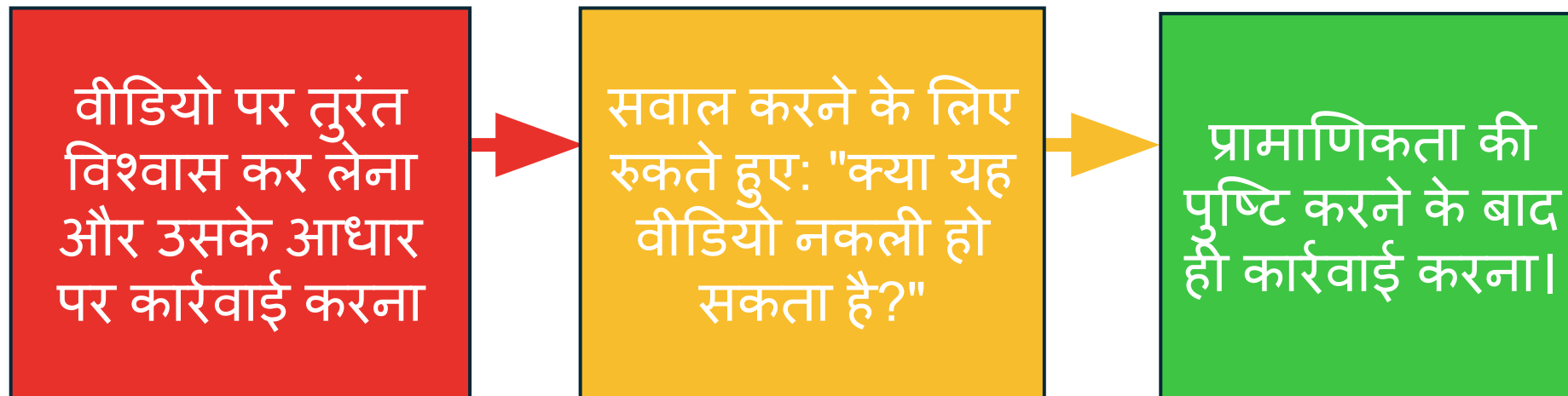
👁️ आंखें (दृष्टि)



🧠 मन (अनुभूति
और भावना)

रीयल-टाइम डीपफेक / डीपफेक वीडियो

कल्पना कीजिए कि आप एक प्रसिद्ध बिजनेस लीडर या यहां तक कि परिवार के किसी सदस्य का वीडियो प्राप्त कर रहे हैं जो आपसे तत्काल पैसे ट्रांसफर करने के लिए कह रहा है। चेहरा और आवाज असली दिखती है। आप क्या करेंगे?



संवादात्मक AI (व्यक्तित्व जाल)



संवादात्मक AI (व्यक्तित्व जाल)

कल्पना कीजिए कि कोई व्यक्ति तनाव भरे दिन के बाद देर रात किसी कृत्रिम बुद्धिमत्ता (एआई) से बात कर रहा है। एआई का व्यक्तित्व मित्रवत लगता है, धैर्यपूर्वक सुनता है और सलाह भी देता है। व्यक्ति सुरक्षित महसूस करता है।

व्यक्तिगत विवरण
साझा करना क्योंकि AI
व्यक्तित्व 'भरोसेमंद'
लगता है।

संवेदनशील या
भावनात्मक
प्रकटीकरण से बचें।

AI व्यक्तित्व को उपकरण के
रूप में मानें | किसी
विश्वसनीय मानव स्रोत से
सलाह सत्यापित करें

AI रुझान और छवि साझाकरण

किसी ट्रेंड को फॉलो करना मजेदार लगता है, आइए एक प्यारा कॉमिक-स्टाइल पोर्ट्रेट में बदलने के लिए अपनी फोटो अपलोड करें।



AI रुझान और छवि साझाकरण

हम अपनी तस्वीर को एक प्यारा कॉमिक-शैली के चित्र में बदलने के लिए अपलोड करते हैं, या पारिवारिक चित्रों को ऑनलाइन साझा करते हैं।

बिना किसी सावधानी के सार्वजनिक रूप से पहचान योग्य फ़ोटो पोस्ट करना या अपलोड करना।

अकेले फ़ोटो के बजाय समूह फ़ोटो साझा करना पसंद करें

AI टूल पर अपलोड करने से पहले रिज़ॉल्यूशन कम करें, जियोटैग के बिना, या छवियों को गुमनाम करें।

क्या आप एक sharent हैं?

बायोमेट्रिक्स और सेल्फी

कल्पना कीजिए कि कोई व्यक्ति 'वी' चिह्न दिखाते हुए एक सेल्फी पोस्ट कर रहा है। यह क्या नुकसान कर सकता है?



बायोमेट्रिक्स और सेल्फी

'वी' चिन्ह के साथ सेल्फी दिखाते हुए सेल्फी पोस्ट करना हानिरहित दिखता है - लेकिन AI उस तस्वीर से उंगलियों के निशान या चेहरे के डेटा का पुनर्निर्माण कर सकता है। जो आकस्मिक लगता है वह बायोमेट्रिक जोखिम बन सकता है।



कार्यस्थल/कक्षा में AI

सार्वजनिक एआई टूल में त्वरित सारांश प्राप्त करने के लिए गोपनीय स्कूल रिपोर्ट चिपकाने से क्या नुकसान हो सकता है?

गोपनीय रिपोर्ट, छात्र रिकॉर्ड या परीक्षा पत्रों को सीधे सार्वजनिक एआई टूल में कॉपी-पेस्ट करना।


नाम, पता आदि के रूप में संवेदनशील जानकारी को हटा दें।


सार्वजनिक एआई को सामान्य कार्यों के लिए सहायक के रूप में मानें, संवेदनशील डेटा के लिए नहीं।




AI का सुरक्षित उपयोग सुनिश्चित करें

साझा करने से पहले:




 **रुकें:** उच्च-रिज़ॉल्यूशन सेल्फी, गोपनीय दस्तावेज़ या संवेदनशील व्यक्तिगत विवरण अपलोड न करें।

 **परखें:** छवियों को क्रॉप करें, धुंधला करें या स्क्रीनशॉट लें; स्ट्रिप मेटाडेटा; पाठ को गुमनाम करें।

 **आगे बढ़ें:** केवल गैर-संवेदनशील, कम-रिज़ॉल्यूशन या अनाम सामग्री साझा करें।


AI का सुरक्षित उपयोग सुनिश्चित करें

पेस्ट करने से पहले:


-  **रुकें:** गोपनीय स्कूल/कार्य रिपोर्ट को सार्वजनिक AI टूल में पेस्ट न करें।
-  **परखें:** पहले नाम, आईडी या संवेदनशील विवरण हटाएं।
-  **आगे बढ़ें:** : संवेदनशील कार्य के लिए एंटरप्राइज़-अनुमोदित या सुरक्षित AI प्लेटफ़ॉर्म का उपयोग करें।

AI का सुरक्षित उपयोग सुनिश्चित करें

इससे पहले कि आप विश्वास करें :




 **रुकें:** पैसे, ओटीपी या बायोमेट्रिक डेटा के लिए अवांछित अनुरोधों पर कार्रवाई न करें, भले ही वे परिवार, प्राधिकरण या सेलिब्रिटी की तरह दिखें।

 **परखें:** किसी अन्य चैनल (कॉल, आधिकारिक साइट, तथ्य-जांच) के माध्यम से पुष्टि करें।

 **आगे बढ़ें:** विश्वसनीय स्रोतों के माध्यम से प्रामाणिकता की पुष्टि करने के बाद ही कार्रवाई करें।

AI का सुरक्षित उपयोग सुनिश्चित करें

इससे पहले कि आप विश्वास करें:

-  **रुकें:** ऑनलाइन वीडियो या छवियों पर आंख मूंदकर भरोसा न करें।
-  **परखें:** विसंगतियों की तलाश करें, तथ्य-जांच पोर्टल देखें।
-  **आगे बढ़ें:** केवल सत्यापित स्रोतों और आधिकारिक संचार पर भरोसा करें।

रोजमर्रा की आदतें

- सोशल मीडिया पर ओवरशेयरिंग सीमित करें।



ऐसे अवतार, चित्र या फ़िल्टर पसंद करें जो बायोमेट्रिक्स को अस्पष्ट करते हों।

गोपनीयता सेटिंग्स को अपडेट रखें।

AI व्यक्तित्व को उपकरण(टूल) के रूप में मानें, मानव मित्र के रूप में नहीं

|

रिपोर्टिंग और सुरक्षा टूल



चक्षु :

👉 संदिग्ध संचार की रिपोर्ट करना

साइबर अपराध पोर्टल (cybercrime.gov.in) :

👉 जब पैसा खो जाता है या पहचान चोरी हो जाती है

राष्ट्रीय हेल्पलाइन :

👉 डायल 1930.