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

ਏਆਈ ਜਾਗਰੂਕਤਾ ਗਾਈਡ

ਸਾਈਬਰ ਸਫਾਈ ਦਾ ਸੱਭਿਆਚਾਰ ਬਣਾਓ

#ਸਾਈਬਰ ਹਾਈਜੀਨ ਅਤੇ ਸੱਭਿਆਚਾਰ



ਰਾਸ਼ਟਰੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਜਾਗਰੂਕਤਾ ਮਹੀਨਾ (ਅਕਤੂਬਰ 2026)

ਪ੍ਰਕਾਸ਼ਕ

ਭਾਰਤੀ ਕੰਪਿਊਟਰ ਐਮਰਜੈਂਸੀ ਰਿਸਪਾਂਸ ਟੀਮ

ਸਾਨੂੰ ਫਾਲੋ ਕਰੋ :

@IndianCERT

@cert_india

ਵਿਸ਼ਾ - ਸੂਚੀ

ਮੁਖਬੰਧ 3

ਏਆਈ-ਵਧਾਇਆ ਫਿਸ਼ਿੰਗ ਅਤੇ ਸੋਸ਼ਲ ਇੰਜੀਨੀਅਰਿੰਗ 4

ਵੌਇਸ ਅਤੇ ਵੀਡੀਓ ਡੀਪਫੇਕ (ਵਿਸ਼ਿੰਗ) 5

ਏਆਈ-ਸਹਾਇਤਾ ਪ੍ਰਾਪਤ ਮਾਲਵੇਅਰ ਅਤੇ ਸਵੈਚਾਲਿਤ ਹਮਲੇ 6

ਨਕਲੀ ਵੈੱਬਸਾਈਟਾਂ ਅਤੇ ਪਛਾਣ ਦੀ ਚੋਰੀ 7

ਲਾਲ ਝੰਡੇ ਚੈੱਕਲਿਸਟ 8

ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ 9

ਡਿਵਾਈਸ ਸੁਰੱਖਿਆ 10

ਏਆਈ ਦੀ ਜ਼ਿੰਮੇਵਾਰੀ ਨਾਲ ਵਰਤੋਂ ਕਰੋ 11

ਭਰੋਸੇਯੋਗ ਐਪਸ ਚੁਣੋ 12

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਘਟਨਾਵਾਂ ਦੀ ਰਿਪੋਰਟ CERT-In ਨੂੰ ਕਰੋ 13

ਮੁਖਬੰਧ

ਆਰਟੀਫੀਸ਼ੀਅਲ ਇੰਟੈਲੀਜੈਂਸ (AI) ਸਾਡੇ ਰਹਿਣ-ਸਹਿਣ, ਕੰਮ ਕਰਨ ਅਤੇ ਸੰਚਾਰ ਕਰਨ ਦੇ ਤਰੀਕੇ ਨੂੰ ਬਦਲ ਰਹੀ ਹੈ। ਇਹ ਨਵੀਨਤਾ ਨੂੰ ਸਮਰੱਥ ਬਣਾਉਂਦੀ ਹੈ, ਉਤਪਾਦਕਤਾ ਨੂੰ ਬਿਹਤਰ ਬਣਾਉਂਦੀ ਹੈ, ਅਤੇ ਵੱਖ-ਵੱਖ ਖੇਤਰਾਂ ਵਿੱਚ ਗੁੰਝਲਦਾਰ ਸਮੱਸਿਆਵਾਂ ਨੂੰ ਹੱਲ ਕਰਨ ਵਿੱਚ ਮਦਦ ਕਰਦੀ ਹੈ। ਹਾਲਾਂਕਿ, ਉਸੇ ਤਕਨਾਲੋਜੀ ਦੀ ਦੁਰਵਰਤੋਂ ਖ਼ਤਰੇ ਦੇ ਕਾਰਕਾਂ ਦੁਆਰਾ ਵਧੇਰੇ ਉੱਨਤ ਅਤੇ ਭਰੋਸੇਮੰਦ ਸਾਈਬਰ ਖਤਰੇ ਪੈਦਾ ਕਰਨ ਲਈ ਵੀ ਕੀਤੀ ਜਾ ਰਹੀ ਹੈ।

ਏਆਈ ਡਿਜੀਟਲ ਖਤਰਿਆਂ ਦੀ ਪਛਾਣ ਕਰਨਾ ਵਧੇਰੇ ਮੁਸ਼ਕਲ ਬਣਾ ਰਿਹਾ ਹੈ ਕਿਉਂਕਿ ਹਮਲਾਵਰ ਹੁਣ ਬਹੁਤ ਹੀ ਯਥਾਰਥਵਾਦੀ ਈਮੇਲ, ਸੁਨੇਹੇ, ਆਡੀਓ, ਵੀਡੀਓ ਅਤੇ ਵੈੱਬਸਾਈਟਾਂ ਬਣਾ ਸਕਦੇ ਹਨ। ਰਵਾਇਤੀ ਚੇਤਾਵਨੀ ਚਿੰਨ੍ਹ, ਜਿਵੇਂ ਕਿ ਮਾੜੀ ਵਿਆਕਰਣ, ਅਸਾਧਾਰਨ ਫਾਰਮੈਟਿੰਗ, ਜਾਂ ਸਪੱਸ਼ਟ ਗਲਤੀਆਂ, ਹੁਣ ਭਰੋਸੇਯੋਗ ਸੰਕੇਤਕ ਨਹੀਂ ਹੋ ਸਕਦੇ। ਤਸਦੀਕ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਡਿਜੀਟਲ ਅਭਿਆਸ ਪਹਿਲਾਂ ਨਾਲੋਂ ਕਿਤੇ ਜ਼ਿਆਦਾ ਮਹੱਤਵਪੂਰਨ ਹੋ ਗਏ ਹਨ।

AI ਟੂਲ ਅਤੇ ਸਮਾਰਟ ਡਿਵਾਈਸ ਜੋ ਅਸੀਂ ਹਰ ਰੋਜ਼ ਵਰਤਦੇ ਹਾਂ, ਜੇਕਰ ਉਹਨਾਂ ਨੂੰ ਧਿਆਨ ਨਾਲ ਨਹੀਂ ਵਰਤਿਆ ਜਾਂਦਾ ਤਾਂ ਉਹ ਨਵੇਂ ਗੋਪਨੀਯਤਾ ਅਤੇ ਸੁਰੱਖਿਆ ਜੋਖਮ ਪੇਸ਼ ਕਰ ਸਕਦੇ ਹਨ। ਗੈਰ-ਭਰੋਸੇਯੋਗ AI ਐਪਲੀਕੇਸ਼ਨਾਂ ਨਾਲ ਨਿੱਜੀ ਜਾਂ ਗੁਪਤ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨਾ, ਬੇਲੋੜੀਆਂ ਇਜਾਜ਼ਤਾਂ ਦੇਣਾ, ਜਾਂ ਤਸਦੀਕ ਤੋਂ ਬਿਨਾਂ AI ਦੁਆਰਾ ਤਿਆਰ ਕੀਤੀ ਜਾਣਕਾਰੀ 'ਤੇ ਭਰੋਸਾ ਕਰਨਾ ਵਿਅਕਤੀਆਂ ਅਤੇ ਸੰਗਠਨਾਂ ਨੂੰ ਸੁਰੱਖਿਆ ਜੋਖਮਾਂ ਵਿੱਚ ਪਾ ਸਕਦਾ ਹੈ।

ਇੰਡੀਅਨ ਕੰਪਿਊਟਰ ਐਮਰਜੈਂਸੀ ਰਿਸਪਾਂਸ ਟੀਮ (CERT-In) ਦੁਆਰਾ "AI ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ" 'ਤੇ ਬਣਾਈ ਗਈ ਇਹ ਕਿਤਾਬਚਾ ਸਿਰਫ਼ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਪੇਸ਼ੇਵਰਾਂ ਲਈ ਹੀ ਨਹੀਂ, ਸਗੋਂ ਰੋਜ਼ਾਨਾ ਨਾਗਰਿਕਾਂ, ਕਰਮਚਾਰੀਆਂ ਅਤੇ ਡਿਜੀਟਲ ਉਪਭੋਗਤਾਵਾਂ ਲਈ ਤਿਆਰ ਕੀਤਾ ਗਿਆ ਹੈ। ਇਹ ਦੱਸਦਾ ਹੈ ਕਿ ਕਿਵੇਂ AI ਡਿਜੀਟਲ ਖਤਰੇ ਦੇ ਦ੍ਰਿਸ਼ ਨੂੰ ਬਦਲ ਰਿਹਾ ਹੈ ਅਤੇ ਸਧਾਰਨ, ਵਿਹਾਰਕ ਕਦਮ ਪ੍ਰਦਾਨ ਕਰਦਾ ਹੈ ਜਿਨ੍ਹਾਂ ਦੀ ਪਾਲਣਾ ਹਰ ਕੋਈ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਡਿਵਾਈਸਾਂ ਅਤੇ ਔਨਲਾਈਨ ਪਛਾਣ ਦੀ ਰੱਖਿਆ ਲਈ ਕਰ ਸਕਦਾ ਹੈ।

ਏਆਈ-ਇਨਹਾਂਸਡ ਫਿਸ਼ਿੰਗ ਅਤੇ ਸੋਸ਼ਲ ਇੰਜੀਨੀਅਰਿੰਗ



ਇਹ ਕਿਵੇਂ ਕੰਮ ਕਰਦਾ ਹੈ ?

ਧਮਕੀ ਦੇਣ ਵਾਲੇ ਹੁਣ ਈਮੇਲ ਅਤੇ ਟੈਕਸਟ ਭੇਜਦੇ ਹਨ ਜੋ ਅਸਲੀ ਅਤੇ ਗਲਤੀ-ਰਹਿਤ ਲੱਗਦੇ ਹਨ। ਉਹ ਤੁਹਾਡੇ ਬਾਰੇ ਵੇਰਵੇ ਵਰਤਦੇ ਹਨ, ਜਿਵੇਂ ਕਿ ਤੁਹਾਡੀ ਨੌਕਰੀ, ਤੁਹਾਡੇ ਦੁਆਰਾ ਵਰਤੀਆਂ ਜਾਂਦੀਆਂ ਸੇਵਾਵਾਂ, ਜਾਂ ਹਾਲੀਆ ਗਤੀਵਿਧੀਆਂ, ਤਾਂ ਜੋ ਸੁਨੇਹੇ ਨਿੱਜੀ ਮਹਿਸੂਸ ਹੋ ਸਕਣ। ਕਿਉਂਕਿ ਇਹ ਸੁਨੇਹੇ ਚੰਗੀ ਤਰ੍ਹਾਂ ਲਿਖੇ ਗਏ ਹਨ, ਇਸ ਲਈ ਉਹਨਾਂ ਨੂੰ ਲੱਭਣਾ ਬਹੁਤ ਮੁਸ਼ਕਲ ਹੋ ਸਕਦਾ ਹੈ।

ਕਿਵੇਂ ਪਛਾਣੀਏ?

- ਇਹ ਸੁਨੇਹਾ ਤੁਹਾਡੇ ਲਈ ਬਹੁਤ ਖਾਸ ਲੱਗਦਾ ਹੈ ਪਰ ਅਚਾਨਕ ਆ ਜਾਂਦਾ ਹੈ।
- ਇਹ ਇੱਕ ਜ਼ਰੂਰੀ ਜਾਂ ਧਮਕੀ ਭਰੇ ਸੁਰ ਦੀ ਵਰਤੋਂ ਕਰਦਾ ਹੈ ਅਤੇ ਤੁਰੰਤ ਕਾਰਵਾਈ ਦੀ ਮੰਗ ਕਰਦਾ ਹੈ।
- ਇਹ ਤੁਹਾਨੂੰ ਇੱਕ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਕਰਨ, ਇੱਕ ਖਾਤੇ ਦੀ ਪੁਸ਼ਟੀ ਕਰਨ, ਇੱਕ ਪਾਸਵਰਡ ਰੀਸੈਟ ਕਰਨ, ਜਾਂ ਭੁਗਤਾਨ ਕਰਨ ਲਈ ਕਹਿੰਦਾ ਹੈ।
- ਭੇਜਣ ਵਾਲੇ ਦਾ ਪਤਾ ਲਗਭਗ ਸਹੀ ਲੱਗਦਾ ਹੈ, ਪਰ ਬਿਲਕੁਲ ਨਹੀਂ।

ਸੁਰੱਖਿਅਤ ਕਿਵੇਂ ਰਹੀਏ?

- ਅਣਚਾਹੇ ਸੁਨੇਹਿਆਂ ਵਿੱਚ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ। ਇਸਦੀ ਬਜਾਏ ਸਿੱਧੇ ਅਧਿਕਾਰਤ ਵੈੱਬਸਾਈਟ ਜਾਂ ਐਪ 'ਤੇ ਜਾਓ।
- ਬੇਨਤੀਆਂ ਦੀ ਪੁਸ਼ਟੀ ਇੱਕ ਵੱਖਰੇ, ਭਰੋਸੇਯੋਗ ਸੰਪਰਕ ਚੈਨਲ, ਜਿਵੇਂ ਕਿ ਇੱਕ ਅਧਿਕਾਰਤ ਫ਼ੋਨ ਨੰਬਰ ਜਾਂ ਐਪ ਰਾਹੀਂ ਕਰੋ।
- ਕਿਸੇ ਸੁਨੇਹੇ ਦੇ ਲਿੰਕ ਰਾਹੀਂ ਪਹੁੰਚੇ ਪੰਨੇ 'ਤੇ ਕਦੇ ਵੀ ਪ੍ਰਮਾਣ ਪੱਤਰ ਜਾਂ OTP ਦਾਖਲ ਨਾ ਕਰੋ।
- ਸ਼ੱਕੀ ਸੁਨੇਹਿਆਂ ਦੀ ਰਿਪੋਰਟ ਕਰੋ ਅਤੇ ਉਹਨਾਂ ਨੂੰ ਮਿਟਾਓ, ਫਿਰ ਭੇਜਣ ਵਾਲੇ ਨੂੰ ਬਲੌਕ ਕਰੋ।

ਵੌਇਸ ਅਤੇ ਵੀਡੀਓ ਡੀਪਫੇਕਸ (ਵਿਸ਼ਿੰਗ)



ਇਹ ਕਿਵੇਂ ਕੰਮ ਕਰਦਾ ਹੈ ?

ਧਮਕੀ ਦੇਣ ਵਾਲੇ ਅਦਾਕਾਰ ਆਵਾਜ਼ਾਂ ਦਾ ਕਲੋਨ ਬਣਾ ਸਕਦੇ ਹਨ ਜਾਂ ਨਕਲੀ ਵੀਡੀਓ ਬਣਾ ਸਕਦੇ ਹਨ ਜੋ ਅਸਲੀ ਲੱਗਦੇ ਅਤੇ ਸੁਣਦੇ ਹਨ। ਉਹ ਤੁਹਾਡੇ 'ਤੇ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨ, ਪੈਸੇ ਭੇਜਣ ਜਾਂ ਜਲਦੀ ਕਾਰਵਾਈ ਕਰਨ ਲਈ ਦਬਾਅ ਪਾਉਣ ਲਈ ਪਰਿਵਾਰ, ਸਹਿਕਰਮੀਆਂ ਜਾਂ ਅਧਿਕਾਰੀਆਂ ਵਜੋਂ ਪੇਸ਼ ਆ ਸਕਦੇ ਹਨ।

ਕਿਵੇਂ ਪਛਾਣੀਏ?

- ਅਸਾਧਾਰਨ ਜਲਦਬਾਜ਼ੀ, ਘਬਰਾਹਟ, ਜਾਂ ਗੁਪਤਤਾ ਲਈ ਬੇਨਤੀਆਂ, ਜਿਵੇਂ ਕਿ ਕਿਸੇ ਨੂੰ ਨਾ ਦੱਸੋ।
- ਥੋੜ੍ਹਾ ਜਿਹਾ ਘਟੀਆ ਸੁਰ, ਰਫ਼ਤਾਰ, ਪਿਛੋਕੜ ਦਾ ਸ਼ੋਰ, ਜਾਂ ਆਡੀਓ ਗੁਣਵੱਤਾ।
- ਆਮ ਤਸਦੀਕ ਜਾਂ ਪ੍ਰਵਾਨਗੀ ਪ੍ਰਕਿਰਿਆਵਾਂ ਨੂੰ ਬਾਈਪਾਸ ਕਰਨ ਦੀਆਂ ਬੇਨਤੀਆਂ।
- ਗਿਫਟ ਕਾਰਡ, ਕ੍ਰਿਪਟੋਕਰੰਸੀ, ਜਾਂ ਵਾਇਰ ਟ੍ਰਾਂਸਫਰ ਰਾਹੀਂ ਭੁਗਤਾਨ ਲਈ ਬੇਨਤੀਆਂ।

ਸੁਰੱਖਿਅਤ ਕਿਵੇਂ ਰਹੀਏ?

- ਫ਼ੋਨ ਕੱਟੋ ਅਤੇ ਵਿਅਕਤੀ ਨੂੰ ਉਸਦੇ ਜਾਣੇ-ਪਛਾਣੇ, ਸੇਵ ਕੀਤੇ ਨੰਬਰ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਵਾਪਸ ਕਾਲ ਕਰੋ।
- ਐਮਰਜੈਂਸੀ ਵਿੱਚ ਪਛਾਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰਨ ਲਈ ਪਰਿਵਾਰ ਜਾਂ ਕੰਮ ਵਾਲੀ ਥਾਂ 'ਤੇ ਸੁਰੱਖਿਅਤ ਸ਼ਬਦ ਸੈੱਟ ਕਰੋ।
- ਕਦੇ ਵੀ ਸਿਰਫ਼ ਕਾਲ ਜਾਂ ਵੀਡੀਓ ਦੇ ਆਧਾਰ 'ਤੇ ਭੁਗਤਾਨਾਂ ਨੂੰ ਅਧਿਕਾਰਤ ਨਾ ਕਰੋ। ਇੱਕ ਵੱਖਰੇ ਚੈਨਲ ਰਾਹੀਂ ਲਿਖਤੀ ਰੂਪ ਵਿੱਚ ਪੁਸ਼ਟੀ ਕਰੋ।
- ਪ੍ਰਤੀਕਿਰਿਆ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਰੁਕੋ। ਧਮਕੀ ਦੇਣ ਵਾਲੇ ਤੁਹਾਡੇ ਫੈਸਲੇ ਨੂੰ ਧੁੰਦਲਾ ਕਰਨ ਲਈ ਘਬਰਾਹਟ 'ਤੇ ਨਿਰਭਰ ਕਰਦੇ ਹਨ।

ਏਆਈ-ਸਹਾਇਤਾ ਪ੍ਰਾਪਤ ਮਾਲਵੇਅਰ ਅਤੇ ਸਵੈਚਾਲਿਤ ਹਮਲੇ



ਇਹ ਕਿਵੇਂ ਕੰਮ ਕਰਦਾ ਹੈ ?

ਧਮਕੀ ਦੇਣ ਵਾਲੇ AI ਟੂਲਸ ਦੀ ਵਰਤੋਂ ਖਤਰਨਾਕ ਕੋਡ ਬਣਾਉਣ ਜਾਂ ਲੁਕਾਉਣ ਲਈ ਕਰਦੇ ਹਨ, ਕਈ ਸਾਈਟਾਂ 'ਤੇ ਚੋਰੀ ਹੋਏ ਪਾਸਵਰਡਾਂ ਦੀ ਜਾਂਚ ਕਰਦੇ ਹਨ, ਅਤੇ ਉਹਨਾਂ ਸਿਸਟਮਾਂ ਦੀ ਪਛਾਣ ਕਰਦੇ ਹਨ ਜਿਨ੍ਹਾਂ ਨੂੰ ਅੱਪਡੇਟ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ। ਇਹ ਹਮਲਿਆਂ ਨੂੰ ਤੇਜ਼ ਅਤੇ ਵਧੇਰੇ ਵਿਆਪਕ ਬਣਾਉਂਦਾ ਹੈ।

ਕਿਵੇਂ ਪਛਾਣੀਏ?

- ਅਣਕਿਆਸੇ ਲੌਗਇਨ ਅਲਰਟ, ਪਾਸਵਰਡ ਰੀਸੈਟ ਈਮੇਲ, ਜਾਂ MFA ਪ੍ਰੋਂਪਟ ਜੋ ਤੁਸੀਂ ਬੇਨਤੀ ਨਹੀਂ ਕੀਤੇ ਸਨ
- ਤੁਹਾਡੀ ਖਾਤਾ ਗਤੀਵਿਧੀ ਵਿੱਚ ਸੂਚੀਬੱਧ ਅਣਜਾਣ ਡਿਵਾਈਸਾਂ ਜਾਂ ਸੈਸ਼ਨ
- ਐਂਟੀਵਾਇਰਸ ਚੇਤਾਵਨੀਆਂ, ਪੌਪ-ਅੱਪ, ਜਾਂ ਡਿਵਾਈਸ ਦੀ ਅਸਧਾਰਨ ਤੌਰ 'ਤੇ ਹੌਲੀ ਕਾਰਗੁਜ਼ਾਰੀ
- ਫ਼ਾਈਲਾਂ, ਸੈਟਿੰਗਾਂ, ਜਾਂ ਬ੍ਰਾਊਜ਼ਰ ਐਕਸਟੈਂਸ਼ਨਾਂ ਜਿਨ੍ਹਾਂ ਨੂੰ ਤੁਸੀਂ ਨਹੀਂ ਪਛਾਣਦੇ

ਸੁਰੱਖਿਅਤ ਕਿਵੇਂ ਰਹੀਏ?

- ਹਰੇਕ ਖਾਤੇ ਲਈ ਇੱਕ ਵਿਲੱਖਣ, ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- ਸਾਰੇ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ 'ਤੇ ਮਲਟੀ ਫੈਕਟਰ ਪ੍ਰਮਾਣੀਕਰਨ (MFA) ਨੂੰ ਸਮਰੱਥ ਬਣਾਓ।
- ਐਂਟੀਵਾਇਰਸ ਸੌਫਟਵੇਅਰ, ਸਿਸਟਮ ਅਤੇ ਐਪਸ ਨੂੰ ਅੱਪ ਟੂ ਡੇਟ ਰੱਖੋ।
- ਅਚਾਨਕ ਲੌਗਇਨ ਜਾਂ MFA ਚੇਤਾਵਨੀਆਂ 'ਤੇ ਤੁਰੰਤ ਕਾਰਵਾਈ ਕਰੋ।

ਨਕਲੀ ਵੈੱਬਸਾਈਟਾਂ ਅਤੇ ਪਛਾਣ ਦੀ ਚੋਰੀ



ਇਹ ਕਿਵੇਂ ਕੰਮ ਕਰਦਾ ਹੈ ?

ਧਮਕੀ ਦੇਣ ਵਾਲੇ ਲੋਕ ਤੁਹਾਡੇ ਲੌਗਇਨ ਪ੍ਰਮਾਣ ਪੱਤਰ, OTP, ਜਾਂ ਭੁਗਤਾਨ ਵੇਰਵੇ ਚੋਰੀ ਕਰਨ ਲਈ ਇੱਕੋ ਜਿਹੀਆਂ ਦਿਖਾਈ ਦੇਣ ਵਾਲੀਆਂ ਵੈੱਬਸਾਈਟਾਂ ਅਤੇ ਚੈਟਬੋਟ ਬਣਾ ਸਕਦੇ ਹਨ, ਜਿਵੇਂ ਕਿ ਬੈਂਕਿੰਗ ਜਾਂ ਸ਼ਾਪਿੰਗ ਪੋਰਟਲ। ਉਹ ਝੂਠੀ ਪਛਾਣ ਬਣਾਉਣ ਲਈ ਨਕਲੀ ਫੋਟੋਆਂ ਜਾਂ ਦਸਤਾਵੇਜ਼ਾਂ ਦੀ ਵਰਤੋਂ ਵੀ ਕਰ ਸਕਦੇ ਹਨ।

ਕਿਵੇਂ ਪਛਾਣੀਏ?

- ਥੋੜ੍ਹਾ ਜਿਹਾ ਬਦਲਿਆ ਹੋਇਆ ਵੈੱਬਸਾਈਟ URL, ਜਿਵੇਂ ਕਿ ਵਾਧੂ ਅੱਖਰ, ਹਾਈਫਨ, ਜਾਂ ਇੱਕ ਵੱਖਰਾ ਡੋਮੇਨ ਅੰਤ।
- ਚੈਟਬੋਟ ਜਾਂ ਏਜੰਟ OTP, ਪਿੰਨ, ਜਾਂ ਪੂਰੇ ਕਾਰਡ ਨੰਬਰ ਮੰਗ ਰਹੇ ਹਨ।
- ਕਿਸੇ ਜਾਣੀ-ਪਛਾਣੀ ਸਾਈਟ 'ਤੇ HTTPS ਜਾਂ ਅਸਧਾਰਨ ਡਿਜ਼ਾਈਨ ਅਸੰਗਤੀਆਂ ਗੁੰਮ ਹਨ।

ਸੁਰੱਖਿਅਤ ਕਿਵੇਂ ਰਹੀਏ?

- ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਦੀ ਬਜਾਏ ਹਮੇਸ਼ਾ ਸਿੱਧੇ ਅਧਿਕਾਰਤ URL ਟਾਈਪ ਕਰੋ ਜਾਂ ਪ੍ਰਮਾਣਿਤ ਬੁੱਕਮਾਰਕਸ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- ਕਦੇ ਵੀ ਕਿਸੇ ਵੀ ਚੈਟਬੋਟ ਜਾਂ "ਸਹਾਇਤਾ ਏਜੰਟ" ਨਾਲ OTP, PIN, ਜਾਂ ਪੂਰੇ ਕਾਰਡ ਵੇਰਵੇ ਸਾਂਝੇ ਨਾ ਕਰੋ।
- ਕਿਤੇ ਵੀ ਲੌਗਇਨ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ HTTPS ਦੀ ਜਾਂਚ ਕਰੋ ਅਤੇ ਡੋਮੇਨ ਨਾਮ ਨੂੰ ਧਿਆਨ ਨਾਲ ਦੇਖੋ।
- ਅਣਜਾਣ ਗਤੀਵਿਧੀ ਲਈ ਆਪਣੇ ਬੈਂਕ ਸਟੇਟਮੈਂਟਾਂ ਅਤੇ ਕ੍ਰੈਡਿਟ ਰਿਪੋਰਟ ਦੀ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਨਿਗਰਾਨੀ ਕਰੋ।

ਲਾਲ ਝੰਡਿਆਂ ਦੀ ਸੂਚੀ

ਏਆਈ-ਸਮਰਥਿਤ ਹਮਲੇ ਦੇ ਇਹਨਾਂ ਸੰਕੇਤਾਂ 'ਤੇ ਨਜ਼ਰ ਰੱਖੋ:

- ਪੈਸੇ, ਪ੍ਰਮਾਣ ਪੱਤਰ, ਜਾਂ ਪ੍ਰਵਾਨਗੀ ਲਈ ਜ਼ਰੂਰੀ, ਦਬਾਅ ਹੇਠ ਬੇਨਤੀ
- ਕਿਸੇ "ਜਾਣ-ਪਛਾਣ ਵਾਲੇ" ਵਿਅਕਤੀ ਦੀ ਕਾਲ ਜਾਂ ਵੀਡੀਓ ਵਿੱਚ ਥੋੜ੍ਹੀਆਂ ਜਿਹੀਆਂ ਆਡੀਓ/ਵੀਡੀਓ ਅਸੰਗਤੀਆਂ।
- ਆਮ ਤਸਦੀਕ/ਮਨਜ਼ੂਰੀ ਪ੍ਰਕਿਰਿਆਵਾਂ ਨੂੰ ਬਾਈਪਾਸ ਕਰਨ ਦੀ ਬੇਨਤੀ
- ਅਣਜਾਣ ਭੇਜਣ ਵਾਲਾ ਡੋਮੇਨ ਜਾਂ ਥੋੜ੍ਹਾ ਜਿਹਾ ਬਦਲਿਆ ਹੋਇਆ URL
- ਅਣਕਿਆਸੇ MFA ਪ੍ਰੋਂਪਟ ਜਾਂ OTP ਜੋ ਤੁਸੀਂ ਬੇਨਤੀ ਨਹੀਂ ਕੀਤੇ ਸਨ
- ਸੁਰੱਖਿਆ ਸਾਫਟਵੇਅਰ ਨੂੰ ਅਯੋਗ ਕਰਨ ਜਾਂ ਅਣਅਧਿਕਾਰਤ ਲਿੰਕਾਂ ਰਾਹੀਂ "ਤਸਦੀਕ" ਕਰਨ ਦੀਆਂ ਬੇਨਤੀਆਂ।
- ਨੌਕਰੀ/ਨਿਵੇਸ਼ ਪੇਸ਼ਕਸ਼ਾਂ ਜਿਨ੍ਹਾਂ ਲਈ ਪਹਿਲਾਂ ਤੋਂ ਭੁਗਤਾਨ ਜਾਂ ਨਿੱਜੀ ਵਿੱਤੀ ਵੇਰਵਿਆਂ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ

ਜਦੋਂ ਸ਼ੱਕ ਹੋਵੇ — ਰੁਕੋ, ਸੁਤੰਤਰ ਤੌਰ 'ਤੇ ਪੁਸ਼ਟੀ ਕਰੋ, ਅਤੇ ਦਬਾਅ ਹੇਠ ਕੰਮ ਨਾ ਕਰੋ।

ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ



ਆਪਣੇ ਖਾਤਿਆਂ ਦੀ ਰੱਖਿਆ ਕਰੋ

- ਹਰੇਕ ਖਾਤੇ ਲਈ ਮਜ਼ਬੂਤ ਅਤੇ ਵਿਲੱਖਣ ਪਾਸਵਰਡ ਵਰਤੋ; ਉਹਨਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਸਟੋਰ ਕਰਨ ਲਈ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- ਜਿੱਥੇ ਵੀ ਉਪਲਬਧ ਹੋਵੇ, ਮਲਟੀ-ਫੈਕਟਰ ਪ੍ਰਮਾਣੀਕਰਨ (MFA) ਨੂੰ ਸਮਰੱਥ ਬਣਾਓ।
- ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ OTP, PIN, ਪਾਸਵਰਡ, ਜਾਂ ਸੁਰੱਖਿਆ ਕੋਡ ਸਾਂਝੇ ਨਾ ਕਰੋ।
- ਵਾਧੂ ਸੁਰੱਖਿਆ ਪਰਤ ਵਜੋਂ ਬਾਇਓਮੈਟ੍ਰਿਕ ਪ੍ਰਮਾਣੀਕਰਨ (ਫਿੰਗਰਪ੍ਰਿੰਟ/ਚਿਹਰੇ ਦੀ ਪਛਾਣ) ਦੀ ਵਰਤੋਂ ਕਰੋ।

ਈਮੇਲ ਅਤੇ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਸਮੇਂ ਸੁਰੱਖਿਅਤ ਰਹੋ

- ਸ਼ੱਕੀ ਜਾਂ ਇੱਕੋ ਜਿਹੇ ਦਿਖਾਈ ਦੇਣ ਵਾਲੇ ਈਮੇਲ ਪਤਿਆਂ ਲਈ ਭੇਜਣ ਵਾਲੇ ਦੇ ਵੇਰਵਿਆਂ ਦੀ ਧਿਆਨ ਨਾਲ ਜਾਂਚ ਕਰੋ।
- ਕਲਿੱਕ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਲਿੰਕਾਂ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ ਅਤੇ ਅਚਾਨਕ ਅਟੈਚਮੈਂਟਾਂ ਨੂੰ ਖੋਲ੍ਹਣ ਤੋਂ ਬਚੋ।
- ਲਾਗਇਨ ਜਾਂ ਵਿੱਤੀ ਵੇਰਵੇ ਦਰਜ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਵੈੱਬਸਾਈਟ ਦੀ ਪ੍ਰਮਾਣਿਕਤਾ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ।
- ਜਦੋਂ ਸ਼ੱਕ ਹੋਵੇ, ਤਾਂ ਕੁਝ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਰੁਕੋ ਅਤੇ ਪੁਸ਼ਟੀ ਕਰੋ।

ਕੁਝ ਗਲਤ ਹੋਣ ਤੋਂ ਪਹਿਲਾਂ ਤਿਆਰੀ ਕਰੋ

- ਔਫਲਾਈਨ ਜਾਂ ਸੁਰੱਖਿਅਤ ਕਲਾਉਡ ਸੇਵਾ ਵਿੱਚ ਸਟੋਰ ਕੀਤੀਆਂ ਮਹੱਤਵਪੂਰਨ ਫਾਈਲਾਂ ਦਾ ਨਿਯਮਤ ਬੈਕਅੱਪ ਰੱਖੋ।
- ਖਾਤਾ ਰਿਕਵਰੀ ਜਾਣਕਾਰੀ (ਈਮੇਲ/ਫ਼ੋਨ) ਨੂੰ ਅੱਪਡੇਟ ਅਤੇ ਸੁਰੱਖਿਅਤ ਰੱਖੋ

ਡਿਵਾਈਸ ਸੁਰੱਖਿਆ



ਡਿਵਾਈਸਾਂ ਨੂੰ ਅੱਪਡੇਟ ਰੱਖੋ

- **ਜਾਣੀਆਂ-ਪਛਾਣੀਆਂ ਕਮਜ਼ੋਰੀਆਂ ਨੂੰ ਠੀਕ ਕਰਨ ਲਈ ਓਪਰੇਟਿੰਗ ਸਿਸਟਮ, ਐਪਲੀਕੇਸ਼ਨ, ਬ੍ਰਾਊਜ਼ਰ ਅਤੇ ਸੁਰੱਖਿਆ ਸਾਫਟਵੇਅਰ ਨੂੰ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਅੱਪਡੇਟ ਕਰੋ।**
- ਜਿੱਥੇ ਵੀ ਸੰਭਵ ਹੋਵੇ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ ਚਾਲੂ ਕਰੋ।

ਸਿਰਫ਼ ਭਰੋਸੇਯੋਗ ਸਾਫਟਵੇਅਰ ਇੰਸਟਾਲ ਕਰੋ

- ਅਸਲੀ ਸਾਫਟਵੇਅਰ ਵਰਤੋ ਅਤੇ ਸਿਰਫ਼ ਅਧਿਕਾਰਤ ਐਪ ਸਟੋਰਾਂ ਜਾਂ ਭਰੋਸੇਯੋਗ ਸਰੋਤਾਂ ਤੋਂ ਹੀ ਐਪਲੀਕੇਸ਼ਨਾਂ ਇੰਸਟਾਲ ਕਰੋ।
- ਭਰੋਸੇਯੋਗ ਐਂਟੀਵਾਇਰਸ ਜਾਂ ਸੁਰੱਖਿਆ ਹੱਲ ਵਰਤੋ ਅਤੇ ਉਹਨਾਂ ਨੂੰ ਅੱਪਡੇਟ ਰੱਖੋ।

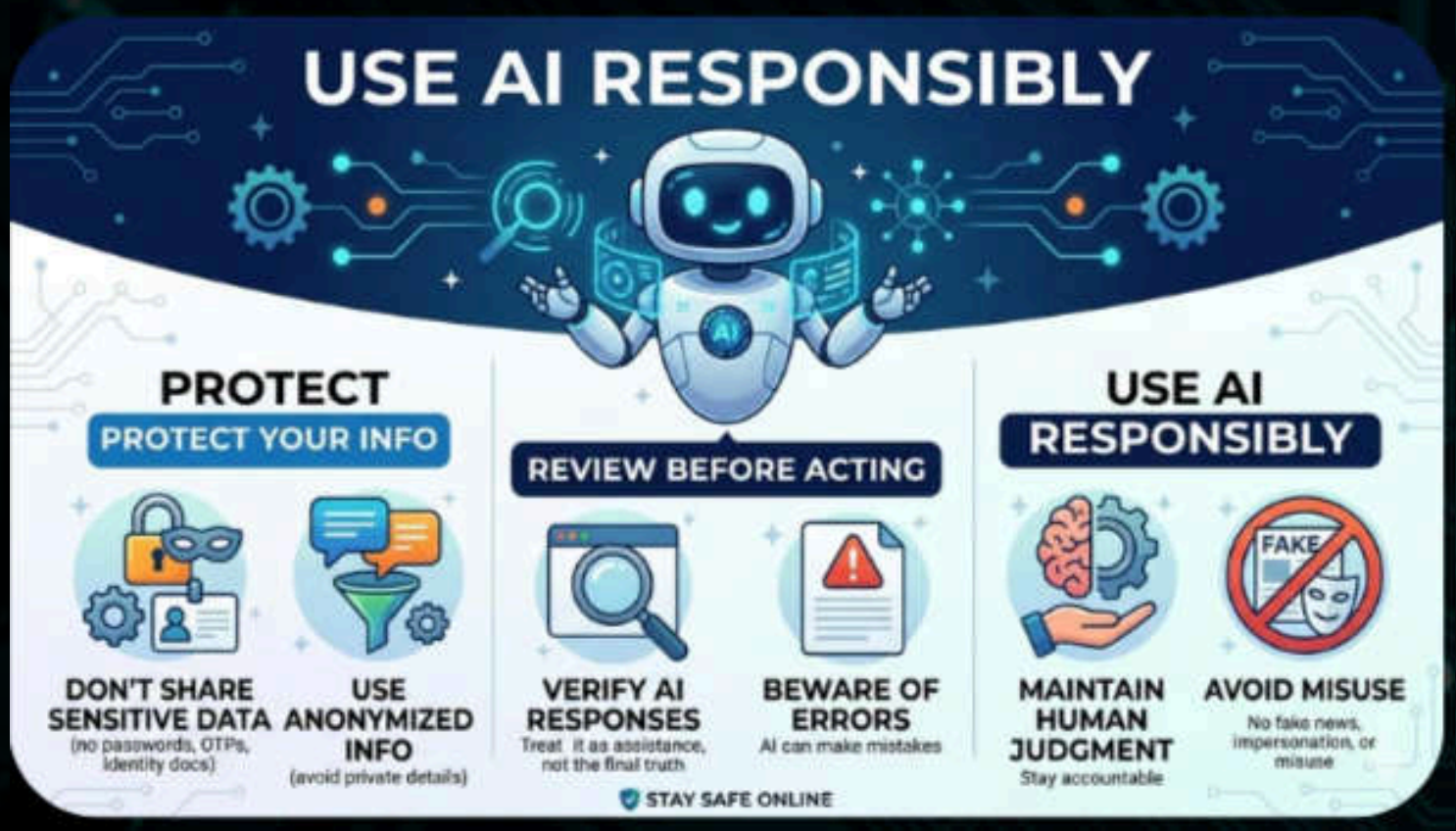
ਆਪਣੇ ਡਿਵਾਈਸਾਂ ਅਤੇ ਖਾਤਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ

- ਸਾਰੇ ਡਿਵਾਈਸਾਂ 'ਤੇ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਜਾਂ ਸਕ੍ਰੀਨ ਲਾਕ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- ਜਦੋਂ ਵੀ ਉਪਲਬਧ ਹੋਵੇ, ਡਿਵਾਈਸ ਇਨਕ੍ਰਿਪਸ਼ਨ ਅਤੇ ਸੁਰੱਖਿਆ ਵਿਸ਼ੇਸ਼ਤਾਵਾਂ ਨੂੰ ਸਮਰੱਥ ਬਣਾਓ।
- ਬੇਲੋੜੀਆਂ ਐਪਲੀਕੇਸ਼ਨਾਂ ਅਤੇ ਅਨੁਮਤੀਆਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ ਅਤੇ ਹਟਾਓ।

ਆਪਣੇ ਨੈੱਟਵਰਕ ਕਨੈਕਸ਼ਨ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ

- ਆਪਣੇ ਵਾਈ-ਫਾਈ ਨੂੰ ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਨਾਲ ਸੁਰੱਖਿਅਤ ਕਰੋ ਅਤੇ ਡਿਫੌਲਟ ਰਾਊਟਰ ਕ੍ਰੈਡੈਂਸ਼ੀਅਲ ਬਦਲੋ।
- ਅੱਪਡੇਟ ਕੀਤੇ ਰਾਊਟਰ ਫਰਮਵੇਅਰ ਅਤੇ ਸੁਰੱਖਿਅਤ ਨੈੱਟਵਰਕ ਸੈਟਿੰਗਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- ਸੰਵੇਦਨਸ਼ੀਲ ਖਾਤਿਆਂ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਜਾਂ ਅਸੁਰੱਖਿਅਤ ਨੈੱਟਵਰਕਾਂ 'ਤੇ ਗੁਪਤ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨ ਤੋਂ ਬਚੋ।

ਏਆਈ ਦੀ ਜ਼ਿੰਮੇਵਾਰੀ ਨਾਲ ਵਰਤੋਂ ਕਰੋ



ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਕਰੋ

- **ਜਨਤਕ *AI* ਟੂਲਸ ਜਾਂ ਅਣਜਾਣ ਔਨਲਾਈਨ ਸੇਵਾਵਾਂ ਵਿੱਚ ਨਿੱਜੀ, ਵਿੱਤੀ, ਸਿਹਤ, ਅਧਿਕਾਰਤ ਜਾਂ ਗੁਪਤ ਜਾਣਕਾਰੀ ਦਰਜ ਨਾ ਕਰੋ।**
- ਸੰਵੇਦਨਸ਼ੀਲ ਵੇਰਵਿਆਂ ਜਿਵੇਂ ਕਿ ਪਾਸਵਰਡ, OTP, ਖਾਤਾ ਨੰਬਰ, ਪਛਾਣ ਦਸਤਾਵੇਜ਼, ਗਾਹਕ ਡੇਟਾ, ਜਾਂ ਨਿੱਜੀ ਗੱਲਬਾਤਾਂ ਨੂੰ ਸਾਂਝਾ ਕਰਨ ਤੋਂ ਬਚੋ।
- AI ਟੂਲਸ ਤੋਂ ਸਹਾਇਤਾ ਮੰਗਦੇ ਸਮੇਂ ਗੁਮਨਾਮ ਜਾਂ ਆਮ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਕਰੋ।

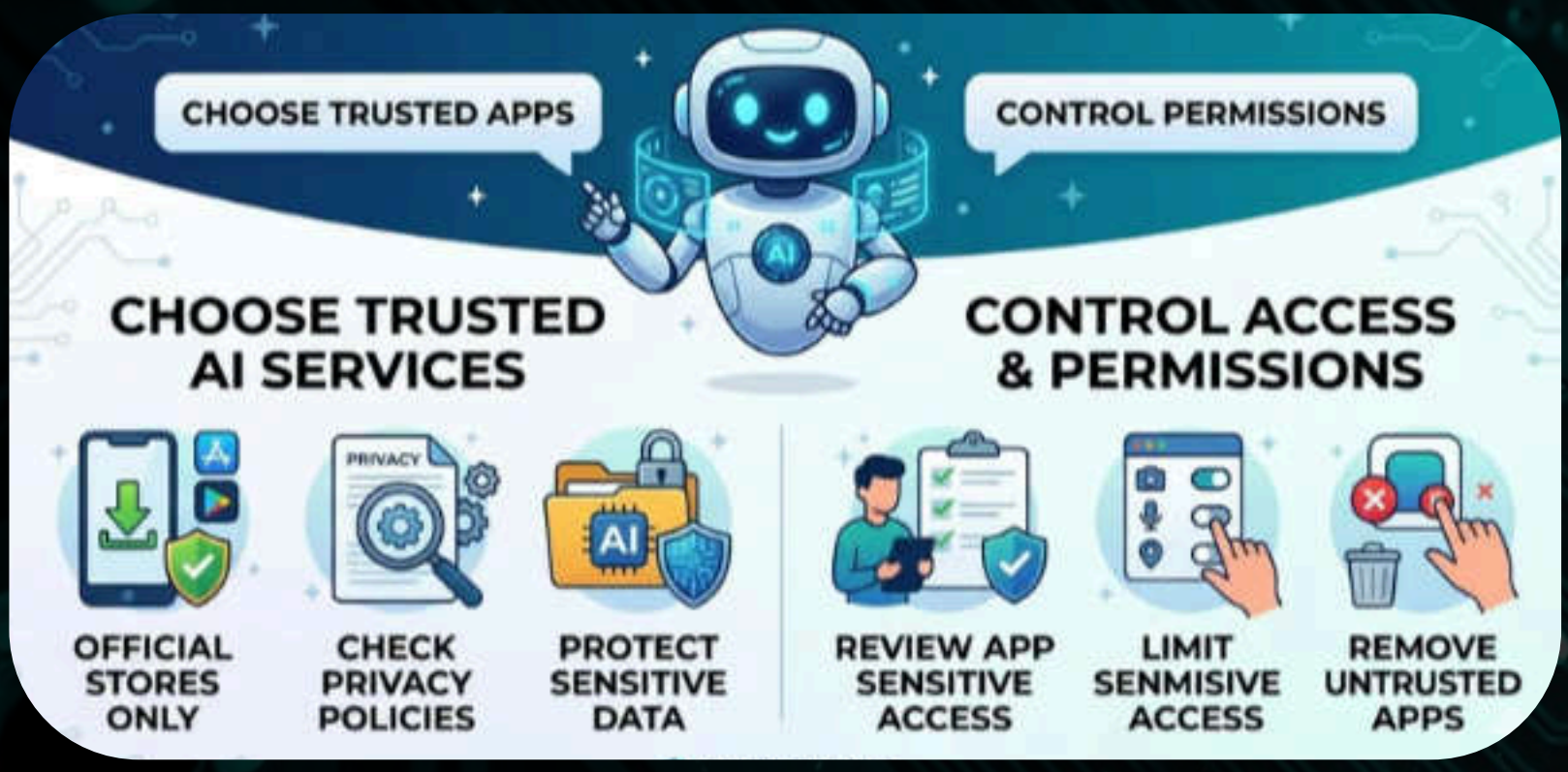
ਸਾਂਝਾ ਕਰਨ ਜਾਂ ਕੰਮ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸਮੀਖਿਆ ਕਰੋ

- ਏਆਈ-ਤਿਆਰ ਕੀਤੇ ਜਵਾਬਾਂ ਨੂੰ ਸਹਾਇਤਾ ਵਜੋਂ ਸਮਝੋ, ਸੱਚਾਈ ਦੇ ਅੰਤਿਮ ਸਰੋਤ ਵਜੋਂ ਨਹੀਂ।
- ਵਿੱਤੀ, ਕਾਨੂੰਨੀ, ਪੇਸ਼ੇਵਰ, ਜਾਂ ਨਿੱਜੀ ਫੈਸਲਿਆਂ ਲਈ ਮਹੱਤਵਪੂਰਨ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਇਸਦੀ ਪੁਸ਼ਟੀ ਕਰੋ।
- ਧਿਆਨ ਰੱਖੋ ਕਿ AI ਟੂਲ ਗਲਤ, ਅਧੂਰੀ, ਜਾਂ ਗੁੰਮਰਾਹਕੁੰਨ ਜਾਣਕਾਰੀ ਪੈਦਾ ਕਰ ਸਕਦੇ ਹਨ।

ਏਆਈ ਟੂਲਸ ਦੀ ਜ਼ਿੰਮੇਵਾਰੀ ਨਾਲ ਵਰਤੋਂ ਕਰੋ

- ਆਪਣੇ ਕੰਮ ਅਤੇ ਸਿੱਖਣ ਦਾ ਸਮਰਥਨ ਕਰਨ ਲਈ AI ਦੀ ਵਰਤੋਂ ਕਰੋ, ਪਰ ਮਨੁੱਖੀ ਨਿਰਣੇ ਅਤੇ ਜਵਾਬਦੇਹੀ ਨੂੰ ਬਣਾਈ ਰੱਖੋ।
- ਗਲਤ ਜਾਣਕਾਰੀ ਬਣਾਉਣ ਜਾਂ ਫੈਲਾਉਣ, ਦੂਜਿਆਂ ਦਾ ਰੂਪ ਧਾਰਨ ਕਰਨ, ਜਾਂ ਕਿਸੇ ਦੇ ਨਿੱਜੀ ਡੇਟਾ ਦੀ ਦੁਰਵਰਤੋਂ ਕਰਨ ਲਈ AI ਦੀ ਵਰਤੋਂ ਨਾ ਕਰੋ।

ਭਰੋਸੇਯੋਗ ਐਪਸ ਚੁਣੋ



ਐਪ ਪਹੁੰਚ ਅਤੇ ਅਨੁਮਤੀਆਂ ਨੂੰ ਕੰਟਰੋਲ ਕਰੋ

- ਏਆਈ ਐਪਲੀਕੇਸ਼ਨਾਂ ਅਤੇ ਡਿਜੀਟਲ ਸਹਾਇਕਾਂ ਨੂੰ ਦਿੱਤੀਆਂ ਗਈਆਂ ਇਜਾਜ਼ਤਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ।
- ਕੈਮਰਾ, ਮਾਈਕ੍ਰੋਫ਼ੋਨ, ਸੰਪਰਕ, ਜਾਂ ਸਥਾਨ ਵਰਗੀਆਂ ਵਿਸ਼ੇਸ਼ਤਾਵਾਂ ਲਈ ਸਿਰਫ਼ ਜ਼ਰੂਰੀ ਹੋਣ 'ਤੇ ਹੀ ਪਹੁੰਚ ਦੀ ਆਗਿਆ ਦਿਓ।
- ਬੇਲੋੜੀਆਂ ਇਜਾਜ਼ਤਾਂ ਹਟਾਓ ਅਤੇ ਗੈਰ-ਭਰੋਸੇਯੋਗ ਸਰੋਤਾਂ ਤੋਂ ਐਪਸ ਨੂੰ ਅਣਇੰਸਟੌਲ ਕਰੋ।

ਭਰੋਸੇਯੋਗ ਏਆਈ ਸੇਵਾਵਾਂ ਚੁਣੋ

- ਨਾਮਵਰ ਪ੍ਰਦਾਤਾਵਾਂ ਤੋਂ *AI* ਐਪਲੀਕੇਸ਼ਨਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ ਅਤੇ ਉਹਨਾਂ ਨੂੰ ਸਿਰਫ਼ ਅਧਿਕਾਰਤ ਐਪ ਸਟੋਰਾਂ ਤੋਂ ਹੀ ਡਾਊਨਲੋਡ ਕਰੋ।
- *AI* ਸੇਵਾਵਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਗੋਪਨੀਯਤਾ ਸੈਟਿੰਗਾਂ, ਵਰਤੋਂ ਦੀਆਂ ਸ਼ਰਤਾਂ ਅਤੇ ਡੇਟਾ ਹੈਂਡਲਿੰਗ ਅਭਿਆਸਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ।
- ਜਦੋਂ ਤੱਕ ਸੁਰੱਖਿਆ ਨਿਯੰਤਰਣਾਂ ਦੀ ਪੁਸ਼ਟੀ ਨਹੀਂ ਕੀਤੀ ਜਾਂਦੀ, *AI* ਟੂਲਸ ਨੂੰ ਸੰਵੇਦਨਸ਼ੀਲ ਖਾਤਿਆਂ ਜਾਂ ਫਾਈਲਾਂ ਨਾਲ ਜੋੜਨ ਤੋਂ ਬਚੋ।

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