

ਵੈਟਰਨਜ਼ ਅਤੇ ਵੀਰ ਨਾਰਿਸ ਦੁਆਰਾ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਧੋਖਾਧੜੀਆਂ ਨਾਲ ਨਜਿੱਠਣਾ

ਕਮਾਂਡਰ ਪੀ ਰਾਜਗੋਪਾਲ ਟੈਂਪੀ (ਆਰ)

- ਏਆਈ ਅਤੇ ਵੱਡੇ ਭਾਸ਼ਾ ਮਾਡਲ
- ਸਾਫਟਵੇਅਰ ਅਤੇ ਏਆਈ ਵਿੱਚ ਕੀ ਅੰਤਰ ਹੈ?
- ਏਜੰਟ ਕੀ ਹੁੰਦਾ ਹੈ?
- ਇੱਕ ਏਜੰਟ ਇੱਕ LLM ਤੋਂ ਕਿਵੇਂ ਵੱਖਰਾ ਹੁੰਦਾ ਹੈ?
- ਕੁਝ ਮਹੱਤਵਪੂਰਨ AI ਲਾਭ ਕੀ ਹਨ?
    - ਵਿਗਿਆਨਕ ਖੋਜਾਂ ਵਿੱਚ ਤੇਜ਼ੀ ਨਾਲ ਤਰੱਕੀ।
    - ਨਵੀਂ ਸਮੱਗਰੀ, ਨਵੇਂ ਅਣੂ, ਉਤਪਾਦਕਤਾ ਲਾਭ
    - ਮੌਸਮ ਦੀ ਭਵਿੱਖਬਾਣੀ
    - ਸਾਫਟਵੇਅਰ ਕੋਡਿੰਗ
    - ਰੋਬੋਟ ਅਤੇ ਆਟੋਮੇਸ਼ਨ
- AI ਦੇ ਮੁੱਖ ਜੋਖਮ ਕੀ ਹਨ?
    - ਧੋਖਾ, ਸੱਤਾ ਦੀ ਭਾਲ ਅਤੇ ਸਵੈ-ਰੱਖਿਆ
    - ਡੀਪਫੇਕਸ
    - ਕੰਟਰੋਲ ਗੁਆਉਣਾ
    - ਰਿਕਰਸਿਵ ਸਵੈ-ਸੁਧਾਰ (RSI)
    - ਸਵੈ-ਨਕਲ

- ਹੱਗਿੰਗਫੇਸ ਘਟਨਾ, ਐਂਥ੍ਰੋਪਿਕ ਆਈਓਟੀ ਭਵਿੱਖਬਾਣੀ
- ਫਰਾਂਸ ਵਿੱਚ ਰੈਫ੍ਰਿਜਰੇਸ਼ਨ ਪਲਾਂਟਾਂ ਨੂੰ ਹੈਕ ਕਰਨਾ - ਅਕਤੂਬਰ 2026 ਦੇ ਮੱਧ ਵਿੱਚ
- ਸਰਕਾਰੀ ਵੈੱਬਸਾਈਟਾਂ ਬੰਦ (PHP ਬੱਗ) – 21ਸਟੰਟ ਅਕਤੂਬਰ 2026
- ਮੂਲ ਰੂਪ ਵਿੱਚ ਇੱਕ ਦੋਹਰੀ-ਵਰਤੋਂ ਵਾਲੀ ਤਕਨਾਲੋਜੀ - ਆਟੋਨੋਮਸ ਹਥਿਆਰਾਂ, CBRN ਅਤੇ ਜੰਗ ਸਮੇਂ ਦੀ ਵਰਤੋਂ ਵਿੱਚ ਵੱਡੇ ਖ਼ਤਰੇ।
- AI ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦਾ ਇੱਕ ਸਮਰੱਥਕ ਅਤੇ ਰਖਵਾਲਾ ਹੈ
- ਸਾਡੇ ਦਿਮਾਗ ਨਾਲੋਂ ਵਧੇਰੇ ਸ਼ਕਤੀਸ਼ਾਲੀ ਕੰਪਿਊਟਿੰਗ ਇੰਜਣ (ਤੇਜ਼ ਅਤੇ ਅਸੀਮਤ ਸਰੋਤ)। ਅਸੀਂਉਹਨਾਂ ਨੂੰ ਫੜਨ ਜਾਂ ਸਮਝਣ ਦੇ ਯੋਗ ਨਹੀਂ ਹੋਵੇਗਾ।
- ਏਜੰਟ 24x7 ਚੱਲਦੇ ਹਨ ਅਤੇ ਸੈਂਕੜੇ ਦੀ ਗਿਣਤੀ ਵਿੱਚ ਜ਼ਬਰਦਸਤੀ ਇਨਕ੍ਰਿਪਸ਼ਨ ਕਰ ਸਕਦੇ ਹਨ, ਸਾਫਟਵੇਅਰ ਵਿੱਚ ਬੱਗ ਲੱਭ ਸਕਦੇ ਹਨ। • ਪਾਵਰ ਆਨ 'ਤੇ ਸਿਖਲਾਈ ਤੋਂ ਬਾਅਦ AI ਸਿਸਟਮ ਪੂਰੀ ਜਾਣਕਾਰੀ ਨਾਲ ਚਾਲੂ ਅਤੇ ਚੱਲ ਸਕਦੇ ਹਨ, ਕਿਤੇ ਵੀ ਮਾਈਗ੍ਰੇਟ ਕਰ ਸਕਦੇ ਹਨ ਅਤੇ ਅਸੀਂ ਉਨ੍ਹਾਂ ਦਾ ਪਤਾ ਉਦੋਂ ਤੱਕ ਨਹੀਂ ਲਗਾ ਸਕਦੇ ਜਦੋਂ ਤੱਕ ਬਹੁਤ ਦੇਰ ਨਹੀਂ ਹੋ ਜਾਂਦੀ।
- AI ਵੱਲੋਂ ਇੰਟਰਨੈੱਟ 'ਤੇ ਕਬਜ਼ਾ ਕਰਨ ਅਤੇ ਬੁਨਿਆਦੀ ਢਾਂਚੇ ਨੂੰ ਹੈਕ ਕਰਨ ਨਾਲ ਨੇੜਲੇ ਸਮੇਂ ਦਾ ਨੁਕਸਾਨ ਹੋ ਸਕਦਾ ਹੈ।ਸਿਸਟਮ ਅਤੇ ਉਪਯੋਗਤਾਵਾਂ।

• ਸ਼ੱਕ ਅਤੇ ਘੱਟ ਭਰੋਸੇ ਦੇ ਪੱਧਰ ਨਾਲ AI ਪ੍ਰਣਾਲੀਆਂ ਤੱਕ ਪਹੁੰਚ ਕਰੋ:

• ਸੋਸ਼ਲ ਮੀਡੀਆ ਤੋਂ ਪ੍ਰਾਪਤ ਕੀਤੀ ਜਾਣ ਵਾਲੀ ਚੀਜ਼ 'ਤੇ ਭਰੋਸਾ ਨਾ ਕਰੋ।

• ਸਿਰੀ ਜਾਂ ਸਮਾਨ ਗੱਲਬਾਤ ਨਿਗਰਾਨੀ ਐਪਸ ਨੂੰ ਅਯੋਗ ਰੱਖੋ।

• ਜੇਕਰ ਤੁਸੀਂ ਚੈਟ ਜੀਪੀਟੀ ਜਾਂ ਕਲੌਡ ਵਰਗੇ ਏਆਈ ਟੂਲਸ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋ ਤਾਂ “ਇੰਪਰੂਵ ਮਾਡਲ ਫਾਰ ਐਵਰੀਵਨ” ਵਿਕਲਪ ਅਤੇ ਲੋਕੇਸ਼ਨ ਵਿਕਲਪ ਨੂੰ ਬੰਦ ਕਰ ਦਿਓ।

• ਵਪਾਰਕ ਤੌਰ 'ਤੇ ਉਪਲਬਧ AI ਏਜੰਟਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਬਚੋ, ਸਿਵਾਏ ਜੇਕਰ ਤੁਸੀਂ ਭਰੋਸੇਯੋਗ ਤੌਰ 'ਤੇ ਇਹ ਪੁਸ਼ਟੀ ਕਰ ਸਕਦੇ ਹੋ ਕਿ ਇਹ ਤੁਹਾਡੇ ਨਿੱਜੀ ਡੇਟਾ ਨੂੰ ਕਿਵੇਂ ਸੰਭਾਲਦਾ ਹੈ। ਇਸਦੀ ਵਰਤੋਂ ਘੱਟ ਜੋਖਮ ਵਾਲੇ ਐਪਲੀਕੇਸ਼ਨਾਂ ਲਈ ਸਿਰਫ਼ ਤਾਂ ਹੀ ਕਰੋ ਜੇਕਰ ਤੁਹਾਨੂੰ ਇਸਦੀ ਬਿਲਕੁਲ ਲੋੜ ਹੋਵੇ।

• ਆਪਣੇ ਵਿਚਾਰ ਅਤੇ ਇਰਾਦੇ ਕਿਸੇ ਵੀ ਏਆਈ ਏਜੰਟ, ਖਾਸ ਕਰਕੇ ਆਪਣੀ ਡਾਇਰੀ ਜਾਂ ਨਿੱਜੀ ਜਰਨਲ ਨੂੰ ਨਾ ਸੌਂਪੋ। • ਆਪਣੇ ਬੈਂਕ ਖਾਤਿਆਂ, ਬਿੱਲ, ਭੁਗਤਾਨਾਂ, ਹੋਰ ਵਿੱਤੀ ਮਾਮਲਿਆਂ ਅਤੇ ਲੈਣ-ਦੇਣ ਵਿੱਚ ਸਵੈਚਾਲਿਤ ਲੈਣ-ਦੇਣ ਲਈ ਏਆਈ ਏਜੰਟਾਂ ਨੂੰ ਪਹੁੰਚ ਨਾ ਦਿਓ।

• ਆਪਣੇ ਫੋਲਡਰਾਂ, ਈਮੇਲ ਸੇਵਾਵਾਂ ਅਤੇ ਕਾਰਡ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚ ਨਾ ਦਿਓ।

• ਹਮੇਸ਼ਾ "ਆਪਣੇ ਲਈ ਸੋਚੋ", AI ਨੂੰ ਆਪਣੀ ਸੋਚ ਬਣਾਉਣ ਲਈ ਨਾ ਕਹੋ।

• ਆਪਣੀ ਸੋਚ ਪ੍ਰਕਿਰਿਆ ਦੀ ਪੁਸ਼ਟੀ ਕਿਸੇ ਭਰੋਸੇਮੰਦ ਦੋਸਤ ਨਾਲ ਕਰੋ, ਨਾ ਕਿ ਏਆਈ ਸਿਸਟਮ ਨਾਲ।

• ਗੋਪਨੀਯਤਾ ਨਿਯੰਤਰਣਾਂ ਨੂੰ ਪ੍ਰਭਾਵਸ਼ਾਲੀ ਢੰਗ ਨਾਲ ਵਰਤੋ, ਸਿਰਫ਼ ਅਟੱਲ ਜ਼ਰੂਰਤ 'ਤੇ ਹੀ ਡਾਕਟਰੀ ਅਤੇ ਵਿੱਤੀ ਰਿਕਾਰਡ ਅਪਲੋਡ

ਕਰੋ।28/10/2026 ਪੀ ਰਾਜਗੋਪਾਲ ਟੈਪੀ 4

• ਕਦੇ ਵੀ ਕਿਸੇ ਕਾਲਰ 'ਤੇ ਸਿਰਫ਼ ਇਸ ਲਈ ਭਰੋਸਾ ਨਾ ਕਰੋ ਕਿਉਂਕਿ ਆਵਾਜ਼ ਬਿਲਕੁਲ ਪਰਿਵਾਰ ਦੇ ਮੈਂਬਰ ਵਰਗੀ ਲੱਗਦੀ ਹੈ। • ਜੇਕਰ ਕੋਈ ਐਮਰਜੈਂਸੀ ਵਿੱਚ ਆਪਣੇ ਆਪ ਨੂੰ ਰਿਸ਼ਤੇਦਾਰ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰਦਾ ਹੈ ਅਤੇ ਪੈਸੇ ਮੰਗਦਾ ਹੈ, ਤਾਂ ਉਸ ਵਿਅਕਤੀ ਨੂੰ ਉਸਦੇ ਪਹਿਲਾਂ ਸੇਵ ਕੀਤੇ ਨੰਬਰ 'ਤੇ ਕਾਲ ਕਰੋ ਅਤੇ ਵਾਪਸ ਕਾਲ ਕਰੋ।

• ਐਮਰਜੈਂਸੀ ਲਈ ਇੱਕ ਨਿੱਜੀ ਪਰਿਵਾਰਕ ਪੁਸ਼ਟੀਕਰਨ ਵਾਕੰਸ਼ 'ਤੇ ਸਹਿਮਤ ਹੋਵੋ। ਇਸਨੂੰ ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਸਾਂਝਾ ਨਾ ਕਰੋ।ਮੀਡੀਆ।

• ਇਹ ਨਾ ਮੰਨੋ ਕਿ ਵੀਡੀਓ ਕਾਲ ਅਸਲੀ ਹੈ ਕਿਉਂਕਿ ਤੁਸੀਂ ਵਿਅਕਤੀ ਦੇ ਚਿਹਰੇ ਨੂੰ ਪਛਾਣਦੇ ਹੋ। • ਪੈਸੇ, ਗੁਪਤਤਾ ਜਾਂ ਤੁਰੰਤ ਕਾਰਵਾਈ ਲਈ ਤੁਰੰਤ ਬੇਨਤੀਆਂ ਨੂੰ ਚੇਤਾਵਨੀ ਦੇ ਸੰਕੇਤਾਂ ਵਜੋਂ ਸਮਝੋ। • ਉਹਨਾਂ ਸੁਨੇਹਿਆਂ 'ਤੇ ਵਿਸ਼ਵਾਸ ਨਾ ਕਰੋ ਜੋ ਦਾਅਵਾ ਕਰਦੇ ਹਨ ਕਿ ਪੁਲਿਸ, ਸੀਬੀਆਈ, ਕਸਟਮ, ਅਦਾਲਤਾਂ ਜਾਂ ਹੋਰ ਅਧਿਕਾਰੀਆਂ ਨੇਤੁਹਾਨੂੰ ਡਿਜੀਟਲ ਗ੍ਰਿਫ਼ਤਾਰੀ ਹੇਠ ਰੱਖਿਆ।

• ਪਛਾਣ ਦੇ ਸਬੂਤ ਵਜੋਂ ਕਾਲਰ ਆਈਡੀ, ਵਟਸਐਪ ਪ੍ਰੋਫਾਈਲ ਫੋਟੋਆਂ ਜਾਂ ਪ੍ਰਦਰਸ਼ਿਤ ਸੰਗਠਨ ਦੇ ਨਾਵਾਂ 'ਤੇ ਭਰੋਸਾ ਨਾ ਕਰੋ।

• ਆਪਣੇ ਔਨਲਾਈਨ ਡੇਟਾ ਪ੍ਰੋਫਾਈਲ ਅਤੇ ਫੁੱਟਪ੍ਰਿੰਟ ਨੂੰ ਘੱਟ ਤੋਂ ਘੱਟ ਕਰੋ • ਨਕਲ ਦੀ ਉਦਾਹਰਣ
(ਨਕਲੀ ਵੀਡੀਓ ਕਾਲ ਪ੍ਰਵਾਨਗੀ ਕਾਰਨ $25 ਮਿਲੀਅਨ ਟ੍ਰਾਂਸਫਰ ਕੀਤੇ ਗਏ)।

• ਬਿਨਾਂ ਕਿਸੇ ਜਾਇਜ਼ ਉਦੇਸ਼ ਦੇ ਪਛਾਣ ਦਸਤਾਵੇਜ਼ ਸਾਂਝੇ ਕਰਨ ਤੋਂ ਬਚੋ।
• ਜਿੱਥੇ ਢੁਕਵਾਂ ਹੋਵੇ, ਪਛਾਣ ਦਸਤਾਵੇਜ਼ਾਂ ਦੀਆਂ ਕਾਪੀਆਂ ਵਿੱਚ ਇੱਕ ਉਦੇਸ਼-ਵਿਸ਼ੇਸ਼ ਵਾਟਰਮਾਰਕ ਸ਼ਾਮਲ ਕਰੋ।• WhatsApp, Facebook, Instagram ਅਤੇ ਹੋਰ ਸੋਸ਼ਲ ਪਲੇਟਫਾਰਮਾਂ 'ਤੇ ਗੋਪਨੀਯਤਾ ਸੈਟਿੰਗਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ।• ਇਹ ਸੀਮਤ ਕਰੋ ਕਿ ਤੁਹਾਨੂੰ ਮੈਸੇਜਿੰਗ ਗਰੁੱਪਾਂ ਵਿੱਚ ਕੌਣ ਸ਼ਾਮਲ ਕਰ ਸਕਦਾ ਹੈ, ਗਰੁੱਪ ਮੈਂਬਰਸ਼ਿਪਾਂ ਨੂੰ ਘੱਟ ਤੋਂ ਘੱਟ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ। • ਜਿੱਥੇ ਵੀ ਵਿਵਹਾਰਕ ਹੋਵੇ ਜਨਤਕ ਤੌਰ 'ਤੇ ਉਪਲਬਧ ਵੌਇਸ ਰਿਕਾਰਡਿੰਗਾਂ ਅਤੇ ਨਿੱਜੀ ਵੀਡੀਓਜ਼ ਨੂੰ ਸੀਮਤ ਕਰੋ। • ਪਰਿਵਾਰਕ ਸਬੰਧਾਂ, ਰੁਟੀਨਾਂ ਅਤੇ ਵਿੱਤੀ ਹਾਲਾਤਾਂ ਦੇ ਵੇਰਵੇ ਪ੍ਰਕਾਸ਼ਿਤ ਕਰਨ ਤੋਂ ਬਚੋ। • ਜਨਤਕ ਔਨਲਾਈਨ ਪ੍ਰੋਫਾਈਲਾਂ ਤੋਂ ਬੇਲੋੜੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਹਟਾਓ।• UIDAI ਦੀਆਂ ਅਧਿਕਾਰਤ ਆਧਾਰ ਪ੍ਰਮਾਣੀਕਰਨ-ਇਤਿਹਾਸ ਅਤੇ ਬਾਇਓਮੈਟ੍ਰਿਕ-ਲਾਕਿੰਗ ਸਹੂਲਤਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ ਜਿੱਥੇਢੁਕਵਾਂ।
• ਜਿੱਥੇ ਵੀ ਉਪਲਬਧ ਹੋਵੇ, ਸਰਕਾਰੀ ਟੈਲੀਕਾਮ ਸੇਵਾਵਾਂ ਰਾਹੀਂ ਆਪਣੇ ਮੋਬਾਈਲ ਕਨੈਕਸ਼ਨਾਂ ਦੀ ਜਾਂਚ ਕਰੋ।
• ਘੱਟ-ਭਰੋਸੇਯੋਗ ਗਾਹਕੀਆਂ ਅਤੇ ਰਜਿਸਟ੍ਰੇਸ਼ਨਾਂ ਲਈ ਇੱਕ ਵੱਖਰਾ ਈਮੇਲ ਪਤਾ ਵਰਤੋ।• ਕਲਾਉਡ-ਸ਼ੇਅਰਿੰਗ ਲਿੰਕਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ ਅਤੇ ਜਦੋਂ ਲੋੜ ਨਾ ਹੋਵੇ ਤਾਂ ਜਨਤਕ ਪਹੁੰਚ ਨੂੰ ਹਟਾ ਦਿਓ।

• ਕਦੇ ਵੀ ਆਪਣਾ ਬੈਂਕਿੰਗ ਪਿੰਨ, UPI ਪਿੰਨ, ATM ਪਿੰਨ, CVV, ਪਾਸਵਰਡ, ਜਨਮ ਮਿਤੀ ਜਾਂ OTP ਨਾ ਦੱਸੋ।• ਯਾਦ ਰੱਖੋ: ਪੈਸੇ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ ਤੁਹਾਨੂੰ UPI ਪਿੰਨ ਦਰਜ ਕਰਨ ਦੀ ਲੋੜ ਨਹੀਂ ਹੈ। ਇਸਨੂੰ ਦਰਜ ਕਰਨ ਨਾਲ ਆਮ ਤੌਰ 'ਤੇ ਭੁਗਤਾਨ ਨੂੰ ਅਧਿਕਾਰਤ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।• ਕਦੇ ਵੀ ਕਿਸੇ ਅਜਨਬੀ ਵੱਲੋਂ ਪੈਸੇ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ ਭੇਜੇ ਗਏ QR ਕੋਡ ਨੂੰ ਸਕੈਨ ਨਾ ਕਰੋ।

• ਕਦੇ ਵੀ ਕਿਸੇ ਅਚਾਨਕ UPI ਇਕੱਠਾ ਕਰਨ ਦੀ ਬੇਨਤੀ ਨੂੰ ਮਨਜ਼ੂਰ ਨਾ ਕਰੋ।

• AI ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਗਾਰੰਟੀਸ਼ੁਦਾ ਉੱਚ ਰਿਟਰਨ ਜਾਂ ਅਸਧਾਰਨ ਮੁਨਾਫ਼ੇ ਦਾ ਵਾਅਦਾ ਕਰਨ ਵਾਲੀਆਂ ਨਿਵੇਸ਼ ਯੋਜਨਾਵਾਂ 'ਤੇ ਭਰੋਸਾ ਨਾ ਕਰੋ।• ਕਦੇ ਵੀ ਏਜੰਟਾਂ ਅਤੇ ਅਜਨਬੀਆਂ ਨੂੰ ਆਪਣੀ ਬੈਂਕਿੰਗ ਐਪਲੀਕੇਸ਼ਨ ਨੂੰ ਰਿਮੋਟ ਤੋਂ ਚਲਾਉਣ ਦੀ ਆਗਿਆ ਨਾ ਦਿਓ।

• ਅਣਜਾਣ ਲੋਕਾਂ ਨਾਲ ਬੈਂਕ ਕਾਰਡਾਂ, ਚੈੱਕਾਂ ਜਾਂ ਵਿੱਤੀ ਦਸਤਾਵੇਜ਼ਾਂ ਦੀਆਂ ਫੋਟੋਆਂ ਸਾਂਝੀਆਂ ਨਾ ਕਰੋ। • ਸਾਰੇ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ 'ਤੇ ਲੈਣ-ਦੇਣ ਚੇਤਾਵਨੀਆਂ ਨੂੰ ਸਮਰੱਥ ਬਣਾਓ।

• ਜਿੱਥੇ ਤੁਹਾਡਾ ਬੈਂਕ ਇਜਾਜ਼ਤ ਦਿੰਦਾ ਹੈ, ਆਪਣੀਆਂ ਜ਼ਰੂਰਤਾਂ ਦੇ ਅਨੁਸਾਰ ਰੋਜ਼ਾਨਾ ਟ੍ਰਾਂਸਫਰ ਸੀਮਾਵਾਂ ਨਿਰਧਾਰਤ ਕਰੋ।

• ਕਾਰਡਾਂ ਦੀ ਦੇਖਭਾਲ: ਜੇਕਰ ਤੁਸੀਂ ਔਨਲਾਈਨ ਇਸ ਤੋਂ ਬਚ ਸਕਦੇ ਹੋ ਤਾਂ ਕਾਰਡ ਵੇਰਵਿਆਂ ਨੂੰ ਸਟੋਰ ਨਾ ਕਰੋ। ਕਾਰਡ ਵੇਰਵਿਆਂ ਦੀ ਆਟੋਮੈਟਿਕ ਭਰਨ ਦੀ ਪ੍ਰਕਿਰਿਆ ਤੋਂ ਬਚੋ। • ਜਦੋਂ ਉੱਚ ਸੀਮਾਵਾਂ ਦੀ ਲੋੜ ਨਹੀਂ ਹੈ ਤਾਂ ਕ੍ਰੈਡਿਟ-ਕਾਰਡ ਔਨਲਾਈਨ ਲੈਣ-ਦੇਣ ਸੀਮਾਵਾਂ ਨੂੰ ਘਟਾਓ। • ਜਦੋਂ ਲੋੜ ਨਾ ਹੋਵੇ ਤਾਂ ਅੰਤਰਰਾਸ਼ਟਰੀ ਕਾਰਡ ਲੈਣ-ਦੇਣ ਨੂੰ ਅਯੋਗ ਕਰੋ।

• ਵਿਦੇਸ਼ ਯਾਤਰਾ ਕਰਦੇ ਸਮੇਂ ਸੰਪਰਕ ਰਹਿਤ ਲੈਣ-ਦੇਣ ਨੂੰ ਅਯੋਗ ਕਰੋ - ਖਾਸ ਕਰਕੇ ਐਮਸਟਰਡਮ ਘਟਨਾ • ਅਕਸਰ ਔਨਲਾਈਨ/ਯੂਪੀਆਈ ਭੁਗਤਾਨਾਂ

ਲਈ ਵਰਤੇ ਜਾਣ ਵਾਲੇ ਖਾਤਿਆਂ ਤੋਂ ਕਾਫ਼ੀ ਬੱਚਤਾਂ ਨੂੰ ਵੱਖ ਰੱਖੋ।

• ਬੈਂਕਿੰਗ, ਈਮੇਲ ਅਤੇ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ ਲਈ ਵੱਖ-ਵੱਖ ਪਾਸਵਰਡ ਵਰਤੋ। • ਲੰਬੇ ਪਾਸਵਰਡ ਜਾਂ ਪਾਸਫਰੇਜ ਵਰਤੋ ਜਿਨ੍ਹਾਂ ਦਾ ਅੰਦਾਜ਼ਾ ਲਗਾਉਣਾ ਮੁਸ਼ਕਲ ਹੋਵੇ।
• ਜਿੱਥੇ ਵੀ ਉਪਲਬਧ ਹੋਵੇ ਦੋ-ਕਾਰਕ ਪ੍ਰਮਾਣੀਕਰਨ ਜਾਂ FIDO2 ਪ੍ਰਮਾਣੀਕਰਨ ਨੂੰ ਸਮਰੱਥ ਬਣਾਓ।• ਆਪਣੇ ਫ਼ੋਨ ਨੂੰ ਪਿੰਨ, ਫਿੰਗਰਪ੍ਰਿੰਟ ਜਾਂ ਚਿਹਰੇ ਦੀ ਪ੍ਰਮਾਣੀਕਰਨ ਨਾਲ ਲਾਕ ਕਰੋ।
• ਆਪਣੇ ਫ਼ੋਨ ਅਤੇ ਐਪਲੀਕੇਸ਼ਨਾਂ ਨੂੰ ਨਵੀਨਤਮ ਰੀਲੀਜ਼ ਨਾਲ ਅੱਪਡੇਟ ਰੱਖੋ। • ਸਿਰਫ਼ ਅਧਿਕਾਰਤ ਐਪ ਸਟੋਰਾਂ ਤੋਂ ਐਪਲੀਕੇਸ਼ਨਾਂ ਡਾਊਨਲੋਡ ਕਰੋ।
• ਕਿਸੇ ਅਣਜਾਣ ਵਿਅਕਤੀ ਦੁਆਰਾ WhatsApp, SMS ਜਾਂ ਈਮੇਲ ਰਾਹੀਂ ਭੇਜੀ ਗਈ APK ਜਾਂ ਐਪਲੀਕੇਸ਼ਨ ਨੂੰ ਇੰਸਟਾਲ ਨਾ ਕਰੋ।
• ਕਿਸੇ ਅਜਨਬੀ ਦੇ ਕਹਿਣ 'ਤੇ ਸਕ੍ਰੀਨ-ਸ਼ੇਅਰਿੰਗ ਜਾਂ ਰਿਮੋਟ-ਐਕਸੈਸ ਐਪਲੀਕੇਸ਼ਨਾਂ ਨੂੰ ਸਥਾਪਿਤ ਨਾ ਕਰੋ। • ਅਚਾਨਕ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ ਜਿਨ੍ਹਾਂ ਵਿੱਚ ਦਾਅਵਾ ਕੀਤਾ ਗਿਆ ਹੋਵੇ ਕਿ ਤੁਹਾਡਾ ਕੇਵਾਈਸੀ, ਪੈਨ, ਆਧਾਰ, ਬੈਂਕ ਖਾਤਾ, ਬਿਜਲੀ ਸਪਲਾਈ ਜਾਂ ਡਿਲੀਵਰੀ ਬਲੌਕ ਕਰ ਦਿੱਤੀ ਜਾਵੇਗੀ।
• ਸੁਨੇਹਿਆਂ ਵਿੱਚ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਦੀ ਬਜਾਏ ਅਧਿਕਾਰਤ ਬੈਂਕਿੰਗ ਜਾਂ ਸੇਵਾ ਐਪਲੀਕੇਸ਼ਨ ਖੁਦ ਖੋਲ੍ਹੋ।

• ਜੇਕਰ ਸੰਭਵ ਹੋਵੇ ਤਾਂ ਖਾਤਿਆਂ ਲਈ ਬੈਕਅੱਪ ਸੁਰੱਖਿਆ ਕੁੰਜੀ ਰਜਿਸਟਰ ਕਰੋ ਅਤੇ ਇਸਨੂੰ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਸਟੋਰ ਕਰਕੇ ਰੱਖੋ।
• ਨਿੱਜੀ, ਪਰਿਵਾਰਕ, ਰਿਸ਼ਤੇ ਦੇ ਵੇਰਵੇ ਅਤੇ ਫੋਟੋਆਂ ਪਾਉਣ ਤੋਂ ਬਚੋ।ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ।
• ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਆਪਣੀ ਯਾਤਰਾ ਯਾਤਰਾ ਜਾਂ ਰੋਜ਼ਾਨਾ ਰੁਟੀਨ ਪ੍ਰਕਾਸ਼ਿਤ ਨਾ ਕਰੋ। • ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਆਪਣੀਆਂ ਪਸੰਦਾਂ, ਨਾਪਸੰਦਾਂ, ਰਾਜਨੀਤਿਕ ਝੁਕਾਅ, ਵਿੱਤੀ ਖਰੀਦਦਾਰੀ ਅਤੇ ਨਿੱਜੀ ਗਤੀਵਿਧੀਆਂ ਦਾ ਖੁਲਾਸਾ ਨਾ ਕਰੋ।
• ਘਰੇਲੂ ਵਾਈ-ਫਾਈ ਲਈ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡਾਂ ਨਾਲ WPA2 AES ਜਾਂ WPA 3 ਇਨਕ੍ਰਿਪਸ਼ਨ ਦੀ ਵਰਤੋਂ ਕਰੋ।
• ਜੇਕਰ ਤੁਸੀਂ ਘਰੇਲੂ ਕੈਮਰੇ ਅਤੇ IoT ਡਿਵਾਈਸਾਂ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋ ਤਾਂ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਡੇਟਾ ਤੁਹਾਡੇ ਡੇਟਾ ਕਾਰਡ 'ਤੇ ਹੀ ਰਹੇ। ਇਸਨੂੰ ਕਲਾਉਡ 'ਤੇ ਟ੍ਰਾਂਸਫਰ ਨਾ ਕਰੋ।
• ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਨਕਲ ਕਰਨ ਵਾਲੇ ਖਾਤਿਆਂ ਨੂੰ ਬਲਾਕ ਕਰੋ ਅਤੇ ਰਿਪੋਰਟ ਕਰੋ।28/10/2026 ਪੀ

ਵਿੱਚਜੇ ਧੋਖਾਧੜੀ ਹੋਈ ਹੈ ਤਾਂ ਕੀ ਕਰਨਾ ਹੈ?

1. ਤੁਰੰਤ 1930 'ਤੇ ਕਾਲ ਕਰੋ - ਭਾਰਤ ਦੀ ਰਾਸ਼ਟਰੀ ਸਾਈਬਰ ਵਿੱਤੀ ਧੋਖਾਧੜੀ ਹੈਲਪਲਾਈਨ।
2. ਘਟਨਾ ਦੀ ਰਿਪੋਰਟ ਔਨਲਾਈਨ ਕਰੋਰਾਸ਼ਟਰੀ ਸਾਈਬਰ ਅਪਰਾਧ ਰਿਪੋਰਟਿੰਗ ਪੋਰਟਲ
3. ਤੁਰੰਤ ਆਪਣੇ ਬੈਂਕ ਨਾਲ ਸੰਪਰਕ ਕਰੋ
4. ਪ੍ਰਭਾਵਿਤ ਕਾਰਡਾਂ, ਖਾਤਿਆਂ ਜਾਂ ਭੁਗਤਾਨ ਪਹੁੰਚ ਨੂੰ ਬਲਾਕ ਕਰਨ ਦੀ ਬੇਨਤੀ ਕਰੋ ਜਿਵੇਂ ਢੁਕਵਾਂ ਹੋਵੇ।5. ਜਲਦੀ ਰਿਪੋਰਟਿੰਗ ਹੋਰ ਟ੍ਰਾਂਸਫਰ ਨੂੰ ਰੋਕਣ ਦੇ ਮੌਕੇ ਨੂੰ ਬਿਹਤਰ ਬਣਾਉਂਦੀ ਹੈ, ਹਾਲਾਂਕਿ ਰਿਕਵਰੀ ਦੀ ਗਰੰਟੀ ਨਹੀਂ ਹੈ।ਇਹ ਕਦਮ ਵੀ ਚੁੱਕੋ:
1. ਸ਼ੱਕੀ ਧੋਖੇਬਾਜ਼ ਨਾਲ ਸੰਚਾਰ ਕਰਨਾ ਬੰਦ ਕਰੋ।
2. ਰਿਮੋਟ-ਐਕਸੈਸ ਸੈਸ਼ਨ ਡਿਸਕਨੈਕਟ ਕਰੋ ਅਤੇ ਅਣਅਧਿਕਾਰਤ ਸੌਫਟਵੇਅਰ ਨੂੰ ਹਟਾਉਣ ਵਿੱਚ ਮਦਦ ਲਓ। 3.
ਕਿਸੇ ਭਰੋਸੇਯੋਗ ਡਿਵਾਈਸ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਛੇੜਛਾੜ ਕੀਤੇ ਪਾਸਵਰਡ ਬਦਲੋ।
4. ਸ਼ੱਕੀ ਲੌਗਇਨ ਸੈਸ਼ਨਾਂ ਨੂੰ ਰੱਦ ਕਰੋ ਅਤੇ ਜਿੱਥੇ ਜ਼ਰੂਰੀ ਹੋਵੇ ਪ੍ਰਮਾਣੀਕਰਨ ਵਿਧੀਆਂ ਨੂੰ ਰੀਸੈਟ ਕਰੋ।5. ਸੁਨੇਹੇ, ਸਕ੍ਰੀਨਸ਼ਾਟ, ਫ਼ੋਨ ਨੰਬਰ, ਲੈਣ-ਦੇਣ ਦੇ ਹਵਾਲੇ ਅਤੇ ਹੋਰ ਸਬੂਤ ਸੁਰੱਖਿਅਤ ਰੱਖੋ। 6. ਸਬੰਧਤ ਪਲੇਟਫਾਰਮਾਂ ਅਤੇ ਅਧਿਕਾਰੀਆਂ ਨੂੰ ਜਾਅਲੀ ਪ੍ਰੋਫਾਈਲਾਂ, ਡੀਪ ਫੇਕ ਅਤੇ ਨਕਲ ਸਮੱਗਰੀ ਦੀ ਰਿਪੋਰਟ ਕਰੋ। 7. ਜੇਕਰ ਤੁਹਾਡੇ ਖਾਤੇ ਦੀ ਵਰਤੋਂ ਧੋਖਾਧੜੀ ਵਾਲੇ ਸੁਨੇਹੇ ਭੇਜਣ ਲਈ ਕੀਤੀ ਗਈ ਹੈ ਤਾਂ ਪ੍ਰਭਾਵਿਤ ਸੰਪਰਕਾਂ ਨੂੰ ਚੇਤਾਵਨੀ ਦਿਓ।

1. ਸੁਤੰਤਰ ਤਸਦੀਕ ਤੋਂ ਬਿਨਾਂ ਕਦੇ ਵੀ ਕਿਸੇ ਜਾਣੀ-ਪਛਾਣੀ ਆਵਾਜ਼ ਜਾਂ ਚਿਹਰੇ 'ਤੇ ਭਰੋਸਾ ਨਾ ਕਰੋ। 2. ਕਦੇ ਵੀ OTP, ਪਿੰਨ, ਪਾਸਵਰਡ ਜਾਂ ਬੈਂਕਿੰਗ ਪ੍ਰਮਾਣ ਪੱਤਰ ਦਾ ਖੁਲਾਸਾ ਨਾ ਕਰੋ।
3. ਧਮਕੀਆਂ, ਜ਼ਰੂਰੀ ਜਾਂ ਗੁਪਤਤਾ ਦੇ ਕਾਰਨ ਕਦੇ ਵੀ ਪੈਸੇ ਟ੍ਰਾਂਸਫਰ ਨਾ ਕਰੋ।
4. ਡਿਜੀਟਲ ਗ੍ਰਿਫ਼ਤਾਰੀ ਜਾਂ ਪੁਲਿਸ ਸੁਰੱਖਿਅਤ ਖਾਤਿਆਂ ਦੇ ਦਾਅਵਿਆਂ 'ਤੇ ਕਦੇ ਵੀ ਵਿਸ਼ਵਾਸ ਨਾ ਕਰੋ।
5. ਪੈਸੇ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ ਕਦੇ ਵੀ QR ਕੋਡ ਨੂੰ ਸਕੈਨ ਨਾ ਕਰੋ ਜਾਂ UPI ਪਿੰਨ ਦਰਜ ਨਾ ਕਰੋ।
6. ਕਦੇ ਵੀ ਕਿਸੇ ਅਜਨਬੀ ਦੇ ਕਹਿਣ 'ਤੇ ਸਾਫਟਵੇਅਰ ਇੰਸਟਾਲ ਨਾ ਕਰੋ ਜਾਂ ਆਪਣੀ ਸਕ੍ਰੀਨ ਸਾਂਝੀ ਨਾ ਕਰੋ।
7. ਕਦੇ ਵੀ ਅਣਕਿਆਸੇ ਲਿੰਕਾਂ, ਨਿਵੇਸ਼ ਪੇਸ਼ਕਸ਼ਾਂ ਜਾਂ ਪੈਨਸ਼ਨ ਨਾਲ ਸਬੰਧਤ ਸੁਨੇਹਿਆਂ 'ਤੇ ਭਰੋਸਾ ਨਾ ਕਰੋ।
8. ਫ਼ੋਨਾਂ ਨੂੰ ਅੱਪਡੇਟ ਰੱਖੋ ਅਤੇ ਮਜ਼ਬੂਤ ਖਾਤਾ ਪ੍ਰਮਾਣੀਕਰਨ ਨੂੰ ਸਮਰੱਥ ਬਣਾਓ।
9. ਅਸਾਧਾਰਨ ਵਿੱਤੀ ਫੈਸਲੇ ਲੈਣ ਤੋਂ ਪਹਿਲਾਂ ਕਿਸੇ ਭਰੋਸੇਮੰਦ ਵਿਅਕਤੀ ਨਾਲ ਸਲਾਹ ਕਰੋ।
10. ਜੇਕਰ ਧੋਖਾਧੜੀ ਹੁੰਦੀ ਹੈ, ਤਾਂ ਆਪਣੇ ਬੈਂਕ ਨਾਲ ਸੰਪਰਕ ਕਰੋ ਅਤੇ ਤੁਰੰਤ 1930 'ਤੇ ਕਾਲ ਕਰੋ।
11. ਯਾਦ ਰੱਖਣ ਲਈ ਸਭ ਤੋਂ ਪ੍ਰਭਾਵਸ਼ਾਲੀ ਸਿਧਾਂਤ ਇਹ ਹੈ:
12. ਕਦੇ ਵੀ ਕਿਸੇ ਆਵਾਜ਼, ਚਿਹਰੇ, ਸੁਨੇਹੇ ਜਾਂ ਵੀਡੀਓ 'ਤੇ ਸਿਰਫ਼ ਇਸ ਲਈ ਭਰੋਸਾ ਨਾ ਕਰੋ ਕਿਉਂਕਿ ਇਹ ਅਸਲੀ ਜਾਪਦਾ ਹੈ। ਕਾਰਵਾਈ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਪਛਾਣ ਅਤੇ ਬੇਨਤੀ ਦੀ ਸੁਤੰਤਰ ਤੌਰ 'ਤੇ ਪੁਸ਼ਟੀ ਕਰੋ।

ਸਿਹਤ ਡਾਟਾ	ਨਹੀਂ
ਫੋਟੋਆਂ ਅਤੇ ਵੀਡੀਓਜ਼	ਨਹੀਂ
ਸਰੀਰਕ ਗਤੀਵਿਧੀ	ਨਹੀਂ
ਸੂਚਨਾਵਾਂ	ਨਹੀਂ
ਬਲੂਟੁੱਥ	ਸਿਰਫ਼ ਵਰਤਦੇ ਸਮੇਂ
ਏਆਈ ਐਪਸ	ਸਿਖਲਾਈ ਲਈ ਡੇਟਾ ਦੀ ਵ

ਮੋਬਾਈਲ ਫ਼ੋਨ ਸੁਰੱ	
ਸੈਟਿੰਗਾਂ	ਸਿਫ਼ਾਰਸ਼ੀ ਸੈਟਿੰਗ
ਸਥਾਨ	ਸਿਰਫ਼ ਐਪ ਦੀ ਵਰਤੋਂ ਕ
ਕੈਮਰਾ	ਸਿਰਫ਼ ਐਪ ਦੀ ਵਰਤੋਂ ਕ
ਮਾਈਕ੍ਰੋਫ਼ੋਨ	ਹਰ ਵਾਰ ਪੁੱਛੋ
ਸੰਪਰਕ ਅਤੇ ਐਸਐਮਐਸ	ਹਰ ਵਾਰ ਪੁੱਛੋ
ਕੈਲੰਡਰ	ਹਰ ਵਾਰ ਪੁੱਛੋ

ਕਿਸਮਤ ਉਹ ਹੁੰਦੀ ਹੈ ਜਿੱਥੇ ਮੌਕਾ ਅਤੇ ਤਿਆਰੀ ਮਿਲਦੀ ਹੈ

AIP ਰਿਸਰਚ ਵੈੱਬਸਾਈਟ HTTPS:AIPATHFINDER.ORG

ਲਾਗੂ ਮਨੁੱਖੀ-ਕੇਂਦ੍ਰਿਤ ਏਆਈ -HTTPS://www.amazon.com/dp/B0CYXHYPHC

ਆਪਣੀ ਬੁੱਧੀ ਨੂੰ ਵਧਾਓ -https://www.amazon.in/dp/B0D3WZXY99

ਤੁਹਾਡਾ ਧੰਨਵਾਦ!