ਅੱਜ ਅਪਣਾਉ ਨੌਂ ਜ਼ਰੂਰੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਆਦਤਾਂ

1. ਕਲਿਕ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਰੁਕੋ !

ਲਿੰਕਾਂ ਅਟੈਚਮੈਂਟਾਂ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਦੋ ਵਾਰ ਸੋਚੋ, ਭਾਵੇਂ ਉਹ ਤੁਹਾਡੇ ਕਿਸੇ ਜਾਣਕਾਰ ਤੋਂ ਆਏ ਹੋਣ।

- • ਅਣਜਾਣ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਦੀ ਬਜਾਏ ਹਮੇਸ਼ਾਂ ਕਿਸੇ ਜਾਣੇ-ਪਛਾਣੇ, ਜਾਇਜ਼ ਸਰੋਤ (ਜਿਵੇਂ ਕਿ HTTPS) ਰਾਹੀਂ ਵੈਬ ਸਾਈਟਾਂ 'ਤੇ ਨੈਵੀਗੇਟ ਕਰੋ।
- ਜੇਕਰ ਕੋਈ ਅਟੈਚਮੈਂਟ ਅਚਾਨਕ ਜਾਪਦੀ ਹੈ, ਤਾਂ ਇੱਕ ਭਰੋਸੇਮੰਦ ਢੰਗ ਰਾਹੀਂ ਭੇਜਣ ਵਾਲੇ ਨਾਲ ਪੁਸ਼ਟੀ ਕਰੋ ਜਾਂ ਸੁਰੱਖਿਅਤ ਪਾਸੇ ਹੋਣ ਲਈ ਕਲਿੱਕ ਨਾ ਕਰਨ ਦੀ ਚੋਣ ਕਰੋ।

2. ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਲਈ ਬੇਨਤੀਆਂ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ

ਨਿੱਜੀ ਡੇਟਾ ਲਈ ਬੇਨਤੀਆਂ ਦੀ ਹਮੇਸ਼ਾਂ ਪੁਸ਼ਟੀ ਕਰੋ—ਭਾਵੇਂ ਇਹ ਤੁਹਾਡਾ ਹੋਵੇ ਜਾਂ ਕਿਸੇ ਹੋਰ ਦਾ।

- ਸਕੈਮਰ ਆਸਾਨੀ ਨਾਲ ਭਰੋਸੇਯੋਗ ਸੰਪਰਕਾਂ ਦੀ ਨਕਲ ਕਰਦਾ ਹੈ।
- ਵਿੱਤੀ ਸਟੇਟਮੈਂਟਾਂ ਅਤੇ ਕ੍ਰੈਡਿਟ ਰਿਪੋਰਟਾਂ ਦੀ ਅਸਾਧਾਰਨ ਗਤੀਵਿਧੀ ਲਈ ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਸਮੀਖਿਆ ਕਰੋ।
- ਬਹੁਤ ਸਾਰੇ ਫਿਸ਼ਿੰਗ ਸੁਨੇਹਿਆਂ ਵਿੱਚ ਸਪੈਲਿੰਗ ਅਤੇ ਵਿਆਕਰਣ ਦੀਆਂ ਗਲਤੀਆਂ ਹੁੰਦੀਆਂ ਹਨ।
- ਵਿਚਾਰ ਕਰੋ ਕਿ ਕੀ ਬੇਨਤੀ ਜਾਇਜ਼ ਹੈ। ਕੀ ਵਿਅਕਤੀ ਜਾਂ ਸੰਸਥਾ ਨੂੰ ਉਸ ਜਾਣਕਾਰੀ ਦੀ ਲੋੜ ਹੈ?

3. ਆਪਣੇ ਪਾਸਵਰਡ ਨੂੰ ਕੰਟਰੋਲ ਕਰੋ

ਆਪਣੇ ਖਾਤਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਮਜ਼ਬੂਤ, ਗੁੰਝਲਦਾਰ ਪਾਸਵਰਡ ਬਣਾਉਣਾ ਅਤੇ ਉਹਨਾਂ ਦਾ ਸਮਝਦਾਰੀ ਨਾਲ ਪ੍ਰਬੰਧਨ ਕਰਨਾ ਜ਼ਰੂਰੀ ਹੈ।.

- ਵੱਖ-ਵੱਖ ਖਾਤਿਆਂ ਲਈ ਵਿਲੱਖਣ ਪਾਸਵਰਡ ਵਰਤੋ।
- ਕੰਮ ਵਾਲੇ ਅਤੇ ਨਿੱਜੀ ਪਾਸਵਰਡ ਵੱਖਰੇ ਰੱਖੋ।
- ਕਦੇ ਵੀ ਪਾਸਵਰਡ ਸਾਂਝੇ ਨਾ ਕਰੋ।
- ਪਾਸਵਰਡ ਸਮੇ ਅਨੁਸਾਰ ਬਦਲਦੇ ਰਹੋ।
- ਬ੍ਰਾਊਜ਼ਰਾਂ ਵਿੱਚ ਪਾਸਵਰਡ ਸੁਰੱਖਿਅਤ ਕਰਨ ਤੋਂ ਗੁਰੇਜ਼ ਕੀਤਾ ਜਾਵੇ।
- ਵਾਧੂ ਸੁਰੱਖਿਆ ਲਈ ਮਲਟੀ-ਫੈਕਟਰ ਪ੍ਰਮਾਣੀਕਰਨ (MFA) ਨੂੰ ਅਪਣਾਓ।

Internal

4. ਆਪਣੀਆਂ ਉਪਕਰਣਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ

ਆਪਣੇ ਕੰਮ ਵਾਲੀ ਥਾਂ ਨੂੰ ਲੌਂਕ ਕਰੋ ਅਤੇ ਦੂਰ ਜਾਣ ਵੇਲੇ ਆਪਣੀਆਂ ਉਪਕਰਣਾਂ ਦੀ ਰੱਖਿਆ ਕਰੋ ।

- ਆਪਣੇ ਕੰਪਿਊਟਰ ਦੀ ਸਕਰੀਨ ਨੂੰ ਹਮੇਸ਼ਾ ਲੌਂਕ ਕਰੋ ।
- ਆਪਣੇ ਫ਼ੋਨ ਅਤੇ ਨਾਲ ਲੈਕੇ ਜਾਣ ਵਾਲੇ ਉਪਕਰਣਾਂ ਨੂੰ ਆਪਣੇ ਨਾਲ ਲੈ ਜਾਓ ਜਾਂ ਉਹਨਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਸਟੋਰ ਕਰੋ ।
- ਜਦੋਂ ਵੀ ਸੰਭਵ ਹੋਵੇ ਮਜ਼ਬੂਤ ਪ੍ਰਮਾਣਿਕਤਾ ਵਿਧੀਆਂ ਦੀ ਵਰਤੋਂ ਕਰੋ ।

5. ਮਹੱਤਵਪੂਰਨ ਫਾਈਲਾਂ ਦਾ ਬੈਕਅੱਪ ਲਓ

ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੇ ਮਹੱਤਵਪੂਰਨ ਡੇਟਾ ਦਾ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਬੈਕਅੱਪ ਲਿਆ ਜਾਂਦਾ ਹੈ ।

- ਬੈਕਅੱਪ ਨੂੰ ਮੂਲ ਜਗਹ ਤੋਂ ਵੱਖਰੀ ਜਗਹ 'ਤੇ ਸਟੋਰ ਕਰੋ ।
- ਸੰਗਠਨ ਦੁਆਰਾ ਪ੍ਰਵਾਨਿਤ ਸਟੋਰੇਜ ਸਰੋਤ ਵਰਤੋ ।
- ਇਹ ਯਕੀਨੀ ਬਣਾਉਣ ਲਈ ਕਿ ਉਹ ਸਹੀ ਢੰਗ ਨਾਲ ਕੰਮ ਕਰਦੇ ਹਨ, ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਬੈਕਅੱਪ ਦੀ ਜਾਂਚ ਕਰੋ ।

6. ਸ਼ੱਕੀ ਗਤੀਵਿਧੀ ਦੀ ਰਿਪੋਰਟ ਕਰੋ

ਜੇ ਕੋਈ ਚੀਜ਼ ਸ਼ੱਕੀ ਜਾਪਦੀ ਹੈ, ਤਾਂ ਆਪਣੀ ਸਮਝਦਾਰੀ 'ਤੇ ਭਰੋਸਾ ਕਰੋ- ਇਸਦੀ ਰਿਪੋਰਟ ਕਰੋ !

- ਆਪਣੇ ਸੁਪਰਵਾਈਜ਼ਰ ਨੂੰ ਸੁਚੇਤ ਕਰੋ ਅਤੇ ਸ਼ੱਕੀ ਘੁਟਾਲਿਆਂ ਜਾਂ ਸ਼ੱਕੀ ਗਤੀਵਿਧੀਆਂ ਲਈ ਆਪਣੀ ਸੰਸਥਾ ਦੇ ਰਿਪੋਰਟਿੰਗ ਪ੍ਰੋਟੋਕੋਲ ਦੀ ਪਾਲਣਾ ਕਰੋ ।

7. ਆਪਣੇ ਆਪ ਨੂੰ ਅਤੇ ਦੂਜਿਆਂ ਨੂੰ ਸਿੱਖਿਅਤ ਕਰੋ

ਨਵੀਨਤਮ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਖਤਰਿਆਂ ਅਤੇ ਰੁਝਾਨਾਂ ਬਾਰੇ ਜਾਣਕਾਰੀ ਰੱਖੋ ।

- ਜਦੋਂ ਵੀ ਤੁਹਾਨੂੰ ਮੌਕਾ ਮਿਲਦਾ ਹੈ ਸਿਖਲਾਈ ਸੈਸ਼ਨਾਂ ਵਿੱਚ ਸ਼ਾਮਲ ਹੋਵੋ ਅਤੇ ਸਹਿਕਰਮੀਆਂ ਨਾਲ ਗਿਆਨ ਸਾਂਝਾ ਕਰੋ।
- ਇੱਕ ਚੰਗੀ ਤਰ੍ਹਾਂ ਜਾਣੂ ਟੀਮ ਸਾਈਬਰ ਖਤਰਿਆਂ ਤੋਂ ਬਚਾਅ ਦੀ ਤੁਹਾਡੀ ਪਹਿਲੀ ਲਾਈਨ ਹੈ ।

8. ਸੁਰੱਖਿਅਤ ਨੈੱਟਵਰਕ ਵਰਤੋ

ਹਮੇਸ਼ਾ ਸੁਰੱਖਿਅਤ ਨੈੱਟਵਰਕਾਂ ਨਾਲ ਕਨੈਕਟ ਕਰੋ, ਖਾਸ ਕਰਕੇ ਜਦੋਂ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚ ਕੀਤੀ ਜਾ ਰਹੀ ਹੋਵੇ।

- ਵਿੱਤੀ ਲੈਣ-ਦੇਣ ਜਾਂ ਸੰਵੇਦਨਸ਼ੀਲ ਕੰਮ ਲਈ ਜਨਤਕ ਵਾਈ-ਫਾਈ ਦੀ ਵਰਤੋਂ ਨਾ ਕੀਤੀ ਜਾਵੇ।
- ਵਾਧੂ ਸੁਰੱਖਿਆ ਲਈ ਲੋੜ ਪੈਣ 'ਤੇ ਵਰਚੁਅਲ ਪ੍ਰਾਈਵੇਟ ਨੈੱਟਵਰਕ (VPN) ਦੀ ਵਰਤੋਂ ਕਰੋ।

9. ਸੋਸ਼ਲ ਮੀਡੀਆ ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ

ਤੁਹਾਡੇ ਦੁਆਰਾ ਔਨਲਾਈਨ ਸਾਂਝੀ ਕੀਤੀ ਜਾਣ ਵਾਲੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਮਾਤਰਾ ਨੂੰ ਸੀਮਤ ਕਰੋ। ਇਸ ਲਈ ਤੁਸੀਂ ਆਪਣੀ ਗੋਪਨੀਯਤਾ ਦੀ ਰੱਖਿਆ ਕਰ ਸਕਦੇ ਹੋ, ਆਪਣੀ ਸੁਰੱਖਿਆ ਨੂੰ ਵਧਾ ਸਕਦੇ ਹੋ, ਅਤੇ ਹੋਰ ਜਿਆਦਾ ਸਕਾਰਾਤਮਕ ਔਨਲਾਈਨ ਅਨੁਭਵ ਬਣਾ ਸਕਦੇ ਹੋ।

- ਸੋਸ਼ਲ ਮੀਡੀਆ ਪਲੇਟਫਾਰਮਾਂ 'ਤੇ ਗੋਪਨੀਯਤਾ ਸੈਟਿੰਗਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ।
- ਦੋਸਤ ਬੇਨਤੀਆਂ ਦਾ ਧਿਆਨ ਰੱਖੋ ਅਤੇ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਤੱਕ ਕਿਸ ਦੀ ਪਹੁੰਚ ਹੈ; ਲਾਕ ਕੀਤੇ ਪ੍ਰੋਫਾਈਲ ਤੋਂ ਬੇਨਤੀਆਂ ਨੂੰ ਸਵੀਕਾਰ ਨਾ ਕਰੋ।
- ਸੰਭਾਵੀ ਖਤਰਿਆਂ ਨੂੰ ਘੱਟ ਤੋਂ ਘੱਟ ਕਰਨ ਲਈ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਆਪਣੀ ਔਨਲਾਈਨ ਮੌਜੂਦਗੀ ਦਾ ਆਡਿਟ ਕਰੋ।

ਯਾਦ ਰੱਖੋ: ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਹਰ ਇੱਕ ਦੀ ਜ਼ਿੰਮੇਵਾਰੀ ਹੈ!