Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

ਨਿੱਜੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਮੁੱਢਲੇ ਕਦਮ

cyber.gov.au

ਨਿੱਜੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਲੜੀ

'ਨਿੱਜੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ: ਮੁੱਢਲੇ ਕਦਮ' ਨਾਮ ਦੀ ਗਾਈਡ ਤਿੰਨ ਗਾਈਡਾਂ ਦੀ ਇੱਕ ਲੜੀ ਵਿੱਚ ਪਹਿਲੀ ਹੈ ਜੋ ਆਮ ਆਸਟ੍ਰੇਲੀਆਈ ਲੋਕਾਂ ਨੂੰ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀਆਂ ਬੁਨਿਆਦੀ ਗੱਲਾਂ ਨੂੰ ਸਮਝਣ ਵਿੱਚ ਮੱਦਦ ਕਰਨ ਲਈ ਤਿਆਰ ਕੀਤੀ ਗਈ ਹੈ। ਜਾਣੋ ਕਿ ਤੁਸੀਂ ਆਪਣੇ-ਆਪ ਨੂੰ ਆਮ ਸਾਈਬਰ ਖ਼ਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਲਈ ਕਿਵੇਂ ਕਾਰਵਾਈ ਕਰ ਸਕਦੇ ਹੋ।

ਮੁੱਢਲੇ ਕਦਮ

ਅਗਲੇ ਕਦਮ

ਐਡਵਾਂਸਡ (ਤਕਨੀਕੀ) ਕਦਮ

ਵਿਸ਼ਾ-ਸੂਚੀ

ਜਾਣ-ਪਛਾਣ

ਨਿੱਜੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਕੀ ਹੈ?

ਲਗਾਤਾਰ ਵੱਧ ਰਹੀ ਤਕਨੀਕ-ਸੰਚਾਲਿਤ ਦੁਨੀਆਂ ਵਿੱਚ ਅਸੀਂ ਹਰ ਰੋਜ਼ ਉਨ੍ਹਾਂ ਯੰਤਰਾਂ ਅਤੇ ਖਾਤਿਆਂ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਾਂ ਜੋ ਸਾਈਬਰ ਖ਼ਤਰਿਆਂ ਲਈ ਜ਼ੋਖਮ-ਗ੍ਰਸਤ ਹਨ:

- ਤੁਹਾਡੇ ਯੰਤਰਾਂ ਵਿੱਚ ਕੰਪਿਊਟਰ, ਮੋਬਾਈਲ ਫ਼ੋਨ, ਟੈਬਲੇਟ ਅਤੇ ਹੋਰ ਇੰਟਰਨੈੱਟ ਨਾਲ ਜੁੜੇ ਯੰਤਰ ਸ਼ਾਮਲ ਹੋ ਸਕਦੇ ਹਨ।
- ਤੁਸੀਂ ਈਮੇਲ, ਬੈਂਕ ਨਾਲ ਲੈਣ-ਦੇਣ, ਖ਼ਰੀਦਦਾਰੀ, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਗੇਮਿੰਗ ਅਤੇ ਹੋਰ ਲਈ ਔਨਲਾਈਨ ਖਾਤਿਆਂ ਦੀ ਵਰਤੋਂ ਵੀ ਕਰ ਸਕਦੇ ਹੋ।

ਨਿੱਜੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਉਹ ਨਿਰੰਤਰ ਚੁੱਕਿਆ ਜਾਣ ਵਾਲਾ ਕਦਮ ਹੈ ਜੋ ਤੁਸੀਂ ਆਪਣੇ ਖਾਤਿਆਂ ਅਤੇ ਯੰਤਰਾਂ ਨੂੰ ਸਾਈਬਰ ਖ਼ਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਲਈ ਚੁੱਕ ਸਕਦੇ ਹੋ।

ਸਾਈਬਰ ਖ਼ਤਰੇ ਕੀ ਹੁੰਦੇ ਹਨ?

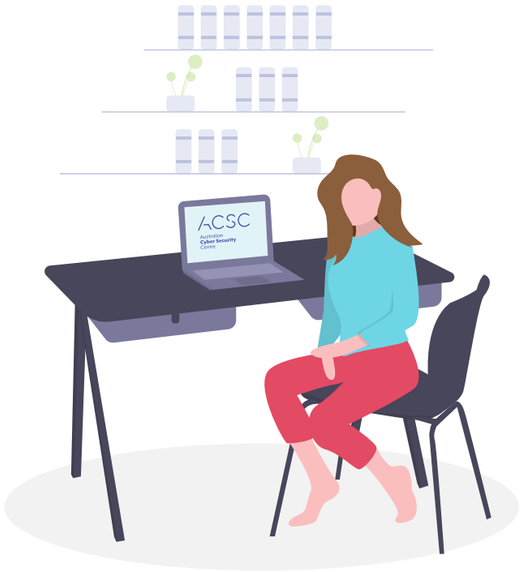
ਆਮ ਆਸਟ੍ਰੇਲੀਆਈ ਲੋਕਾਂ ਨੂੰ ਪ੍ਰਭਾਵਿਤ ਕਰਨ ਵਾਲੇ ਮੁੱਖ ਸਾਈਬਰ ਖ਼ਤਰੇ **ਘੁਟਾਲੇ (ਸਕੈਮ) ਅਤੇ ਮਾਲਵੇਅਰ** ਹਨ।

- **ਮਾਲਵੇਅਰ ਇੱਕ ਕੰਬਲਨੁਮਾ ਸ਼ਬਦ ਹੈ ਜੋ ਨੁਕਸਾਨ ਪਹੁੰਚਾਉਣ ਲਈ ਬਣਾਏ ਗਏ ਖ਼ਤਰਨਾਕ ਸਾਫ਼ਟਵੇਅਰਾਂ ਦਾ ਵਰਣਨ ਕਰਨ ਲਈ** ਵਰਤਿਆ ਜਾਂਦਾ ਹੈ। ਇਸ ਵਿੱਚ ਵਾਇਰਸ, ਵਰਮਜ਼, ਸਪਾਈਵੇਅਰ, ਟਰੋਜਨ ਅਤੇ ਰੈਨਸਮਵੇਅਰ ਸ਼ਾਮਲ ਹੋ ਸਕਦੇ ਹਨ।
  ਸਾਈਬਰ ਅਪਰਾਧੀ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਅਤੇ ਪੈਸੇ ਚੋਰੀ ਕਰਨ, ਅਤੇ ਤੁਹਾਡੇ ਯੰਤਰਾਂ ਅਤੇ ਖਾਤਿਆਂ ਨੂੰ ਕੰਟਰੋਲ ਕਰਨ ਲਈ ਮਾਲਵੇਅਰ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਨ।
- **ਘੁਟਾਲੇ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਦੁਆਰਾ ਭੇਜੇ ਗਏ ਸੁਨੇਹੇ ਹੁੰਦੇ ਹਨ** ਜੋ ਤੁਹਾਡੇ ਨਾਲ ਹੇਰਾਫੇਰੀ ਕਰਨ ਲਈ ਤੁਹਾਨੂੰ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਦੇਣ ਲਈ ਤਿਆਰ ਕਰਨ, ਜਾਂ ਤੁਹਾਡੇ ਯੰਤਰ 'ਤੇ ਮਾਲਵੇਅਰ ਨੂੰ ਸਰਗਰਮ ਕਰਨ ਲਈ ਤਿਆਰ ਕੀਤੇ ਗਏ ਹਨ।

ਇਹ ਹਮਲੇ ਪੀੜਤਾਂ 'ਤੇ ਕਾਫ਼ੀ ਜ਼ਿਆਦਾ ਨਿੱਜੀ ਅਤੇ ਵਿੱਤੀ ਪ੍ਰਭਾਵ ਪਾ ਸਕਦੇ ਹਨ। ਉਹ ਆਧੁਨਿਕ ਸੂਝਤਾ ਅਤੇ ਗਿਣਤੀ ਵਿੱਚ ਵੀ ਵਧ ਰਹੇ ਹਨ।

ਇਹ ਗਾਈਡ ਮੈਨੂੰ ਸਾਈਬਰ ਖ਼ਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਵਿੱਚ ਕਿਵੇਂ ਮੱਦਦ ਕਰ ਸਕਦੀ ਹੈ?

ਜੇਕਰ ਤੁਸੀਂ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਬਾਰੇ ਪਹਿਲੀ ਵਾਰ ਸਿੱਖ ਰਹੇ ਹੋ, ਜਾਂ ਆਪਣੇ-ਆਪ ਨੂੰ ਜਾਗਰੂਕ (ਅੱਪ-ਟੂ-ਡੇਟ) ਰੱਖ ਰਹੇ ਹੋ, ਤਾਂ ਇਹ ਗਾਈਡ ਸ਼ੁਰੂਆਤ ਕਰਨ ਲਈ ਇੱਕ ਬਹੁਤ ਹੀ ਵਧੀਆ ਸਥਾਨ ਹੈ। 'ਨਿੱਜੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ: ਮੁੱਢਲੇ ਕਦਮ' ਗਾਈਡ ਤਿੰਨ ਗਾਈਡਾਂ ਦੀ ਲੜੀ ਵਿੱਚੋਂ ਪਹਿਲੀ ਹੈ ਜੋ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀਆਂ ਮੂਲ ਗੱਲਾਂ ਨੂੰ ਸਮਝਣ ਵਿੱਚ ਤੁਹਾਡੀ ਮੱਦਦ ਕਰਨ ਲਈ ਤਿਆਰ ਕੀਤੀ ਗਈ ਹੈ।



ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਾਂ ਨੂੰ ਚਾਲੂ ਕਰੋ

ਅੱਪਡੇਟ ਕੀ ਹੁੰਦੇ ਹਨ?

ਅੱਪਡੇਟ ਉਸ ਸਾਫ਼ਟਵੇਅਰ (ਪ੍ਰੋਗਰਾਮਾਂ, ਐਪਾਂ ਅਤੇ ਓਪਰੇਟਿੰਗ ਸਿਸਟਮਾਂ) ਦਾ ਇੱਕ ਸੋਧਿਆ ਹੋਇਆ ਰੂਪ ਹੁੰਦਾ ਹੈ ਜੋ ਤੁਸੀਂ ਆਪਣੇ ਕੰਪਿਊਟਰ ਅਤੇ ਮੋਬਾਈਲ ਯੰਤਰਾਂ 'ਤੇ ਇੰਸਟਾਲ ਕੀਤਾ (ਪਾਇਆ) ਹੋਇਆ ਹੁੰਦਾ ਹੈ।

- **ਸਾਫ਼ਟਵੇਅਰ ਅੱਪਡੇਟ ਸਾਫ਼ਟਵੇਅਰ 'ਬੱਗਾਂ' (ਕੋਡਿੰਗ ਵਿਚਲੀਆਂ ਗਲਤੀਆਂ ਜਾਂ ਕਮਜ਼ੋਰੀਆਂ) ਨੂੰ ਠੀਕ ਕਰਕੇ** ਤੁਹਾਡੇ ਯੰਤਰਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਵਿੱਚ ਮੱਦਦ ਕਰਦੇ ਹਨ। ਸਾਈਬਰ ਅਪਰਾਧੀ ਅਤੇ ਮਾਲਵੇਅਰ ਇਹਨਾਂ 'ਬੱਗਾਂ' ਦੀ ਵਰਤੋਂ ਤੁਹਾਡੇ ਯੰਤਰ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਅਤੇ ਤੁਹਾਡੇ ਨਿੱਜੀ ਡੇਟਾ, ਖਾਤਿਆਂ, ਵਿੱਤੀ ਜਾਣਕਾਰੀ ਅਤੇ ਸ਼ਨਾਖ਼ਤ ਨੂੰ ਚੋਰੀ ਕਰਨ ਲਈ ਕਰ ਸਕਦੇ ਹਨ।
- **ਨਵੇਂ ਸਾਫ਼ਟਵੇਅਰ 'ਬੱਗ' ਲਗਾਤਾਰ ਲੱਭੇ ਜਾ ਰਹੇ ਹਨ** ਅਤੇ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਦੁਆਰਾ ਦੁਰਉਪਯੋਗ ਕੀਤਾ ਜਾ ਰਹੇ ਹਨ। ਆਪਣੇ ਯੰਤਰਾਂ 'ਤੇ ਸਾਫ਼ਟਵੇਅਰ ਅੱਪਡੇਟ ਕਰਨਾ ਤੁਹਾਨੂੰ ਸਾਈਬਰ-ਹਮਲਿਆਂ ਤੋਂ ਬਚਾਉਣ ਵਿੱਚ ਮੱਦਦ ਕਰਦਾ ਹੈ।

ਮੈਂ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ ਕਿਵੇਂ ਸੈੱਟ ਕਰਾਂ?

ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ ਇੱਕ ਪਹਿਲਾਂ-ਤੋਂ-ਲੱਗੀ ਹੋਈ ਜਾਂ 'ਸੈੱਟ ਕਰੋ ਅਤੇ ਭੁੱਲ ਜਾਓ' ਸੈਟਿੰਗ ਹੈ ਜੋ ਨਵੇਂ ਅੱਪਡੇਟਾਂ ਨੂੰ ਉਨ੍ਹਾਂ ਦੇ ਉਪਲਬਧ ਹੁੰਦੇ ਸਾਰ ਹੀ ਇੰਸਟਾਲ ਕਰਦੇ ਹਨ।

- ✓ ਸਾਰੇ ਸਾਫ਼ਟਵੇਅਰ ਅਤੇ ਯੰਤਰਾਂ 'ਤੇ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਾਂ ਨੂੰ ਚਾਲੂ ਕਰੋ ਅਤੇ ਪੁਸ਼ਟੀ ਕਰੋ।
- ✓ ਤੁਸੀਂ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਾਂ ਨੂੰ ਕਿਵੇਂ ਚਾਲੂ ਕਰ ਸਕਦੇ ਹੋ, ਇਹ ਸਾਫ਼ਟਵੇਅਰ ਅਤੇ ਯੰਤਰ ਦੇ ਆਧਾਰ 'ਤੇ ਵੱਖੋ-ਵੱਖਰਾ ਹੋ ਸਕਦਾ ਹੈ।
- ✓ ਜੇਕਰ ਸੰਭਵ ਹੋਵੇ ਤਾਂ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ ਹੋਣ ਲਈ ਕੋਈ ਸੁਵਿਧਾਜਨਕ ਸਮਾਂ ਸੈੱਟ ਕਰੋ, ਜਿਵੇਂ ਕਿ ਜਦੋਂ ਤੁਸੀਂ ਸੌਂ ਰਹੇ ਹੋਵੋ ਜਾਂ ਆਮ ਤੌਰ 'ਤੇ ਤੁਹਾਡੇ ਯੰਤਰ ਦੀ ਵਰਤੋਂ ਨਹੀਂ ਕਰ ਰਹੇ ਹੋਵੋ।

ਤੁਹਾਡਾ ਯੰਤਰ ਦੀ ਪਾਵਰ ਚਾਲੂ ਹੋਣੀ ਚਾਹੀਦੀ ਹੈ, ਬਿਜਲੀ ਲਈ ਪਲੱਗ ਲੱਗਿਆ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ ਅਤੇ ਅਣਵਰਤੀ ਸਟੋਰੇਜ ਸਪੇਸ ਹੋਣੀ ਚਾਹੀਦੀ ਹੈ।

ਸੁਝਾਅ: ਜੇਕਰ ਤੁਹਾਨੂੰ ਆਪਣੇ ਯੰਤਰ ਦੇ ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਅੱਪਡੇਟ ਕਰਨ ਲਈ ਕੋਈ ਸੁਨੇਹਾ (ਪ੍ਰੋਂਪਟ/ਨੋਟੀਫ਼ਿਕੇਸ਼ਨ) ਪ੍ਰਾਪਤ ਹੁੰਦਾ ਹੈ ਤਾਂ ਤੁਹਾਨੂੰ ਜਿੰਨੀ ਜਲਦੀ ਹੋ ਸਕੇ ਸਾਫ਼ਟਵੇਅਰ ਅੱਪਡੇਟ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ।

ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਾਂ ਦਾ ਹੋਣਾ ਕਿਵੇਂ ਚਾਲੂ ਕਰਨਾ ਹੈ ਇਸ ਬਾਰੇ ਵਧੇਰੇ ਵਿਸਥਾਰਪੂਰਵਕ ਜਾਣਕਾਰੀ cyber.gov.au 'ਤੇ 'ਅੱਪਡੇਟਸ' ਲੱਭ ਕੇ ਪ੍ਰਾਪਤ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ।

ਜੇਕਰ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ ਚਾਲੂ ਕਰਨ ਲਈ ਸੈਟਿੰਗ ਉਪਲਬਧ ਨਾ ਹੋਵੇ ਤਾਂ ਕੀ ਕਰਨਾ ਹੈ?

ਜੇਕਰ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ ਚਾਲੂ ਕਰਨ ਲਈ ਸੈਟਿੰਗ ਉਪਲਬਧ ਨਹੀਂ ਹੈ, ਤਾਂ ਤੁਹਾਨੂੰ ਬਾਕਾਇਦਾ ਤੌਰ 'ਤੇ ਆਪ ਆਪਣੇ ਸਾਫ਼ਟਵੇਅਰ ਜਾਂ ਯੰਤਰ ਦੇ ਸੈਟਿੰਗਜ਼ ਮੀਨੂ ਰਾਹੀਂ ਨਵੇਂ ਅੱਪਡੇਟਾਂ ਨੂੰ ਚੈੱਕ ਅਤੇ ਇੰਸਟਾਲ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ।

ਜੇ ਮੇਰੇ ਪੁਰਾਣੇ ਯੰਤਰ ਅਤੇ ਸਾਫ਼ਟਵੇਅਰ 'ਤੇ ਕੋਈ ਅੱਪਡੇਟ ਨਹੀਂ ਆਉਂਦੇ ਹਨ ਤਾਂ ਕੀ ਹੋਵੇਗਾ?

ਜੇਕਰ ਤੁਹਾਡਾ ਯੰਤਰ, ਓਪਰੇਟਿੰਗ ਸਿਸਟਮ ਜਾਂ ਸਾਫ਼ਟਵੇਅਰ ਬਹੁਤ ਪੁਰਾਣਾ ਹੈ, ਤਾਂ ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਇਹ ਹੁਣ ਨਿਰਮਾਤਾ ਜਾਂ ਡਿਵੈਲਪਰ (ਵਿਕਾਸਕਾਰ) ਦੁਆਰਾ ਸਮਰਥਿਤ ਨਾ ਹੋਵੇ।

ਜਦੋਂ ਉਤਪਾਦ ਇਸ 'ਸਮਰਥਨ ਦੇ ਅੰਤ' ਪੜਾਅ 'ਤੇ ਪਹੁੰਚ ਜਾਂਦੇ ਹਨ ਤਾਂ ਉਹ ਹੁਣ ਹੋਰ ਅੱਪਡੇਟ ਪ੍ਰਾਪਤ ਨਹੀਂ ਕਰਨਗੇ। ਇਹ ਤੁਹਾਨੂੰ ਸਾਈਬਰ-ਹਮਲੇ ਹੋਣ ਲਈ ਜ਼ੋਖਮ 'ਤੇ ਖੜ੍ਹਾ ਕਰ ਸਕਦਾ ਹੈ। ਉਹਨਾਂ ਉਤਪਾਦਾਂ ਦੀਆਂ ਉਦਾਹਰਨਾਂ ਵਿੱਚ Windows 7 ਓਪਰੇਟਿੰਗ ਸਿਸਟਮ ਅਤੇ iPhone 7 ਸ਼ਾਮਲ ਹਨ ਜੋ ਸਮਰਥਨ ਦੇ ਅੰਤਮ ਪੜਾਅ ਵਿੱਚ ਹਨ।

ਜੇਕਰ ਤੁਹਾਡਾ ਯੰਤਰ, ਓਪਰੇਟਿੰਗ ਸਿਸਟਮ ਜਾਂ ਸਾਫ਼ਟਵੇਅਰ ਸਮਰਥਨ ਦੇ ਅੰਤ 'ਤੇ ਪਹੁੰਚ ਗਿਆ ਹੈ, ਤਾਂ ACSC ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਜਿੰਨੀ ਜਲਦੀ ਹੋ ਸਕੇ ਅੱਪਗ੍ਰੇਡ ਕਰਨ (ਨਵਾਂ ਉਤਪਾਦ ਲੈਣ) ਦੀ ਸਿਫ਼ਾਰਸ਼ ਕਰਦਾ ਹੈ।

ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ, cyber.gov.au **'ਤੇ 'ਸਮਰਥਨ ਦਾ ਅੰਤ' (End of support) ਖੋਜੋ**

ਮਲਟੀ-ਫੈਕਟਰ (ਬੁਹ-ਤੱਥੀ) ਪੁਸ਼ਟੀਕਰਨ (MFA) ਨੂੰ ਚਾਲੂ ਕਰੋ

MFA ਕੀ ਹੈ?

ਤੁਸੀਂ ਆਪਣੇ ਸਭ ਤੋਂ ਵੱਧ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਨੂੰ ਬਿਹਤਰ ਬਣਾਉਣ ਲਈ ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ (MFA) ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦੇ ਹੋ। MFA ਤੁਹਾਨੂੰ ਕਿਸੇ ਖਾਤੇ ਤੱਕ ਪਹੁੰਚ ਦੇਣ ਤੋਂ ਪਹਿਲਾਂ ਤੁਹਾਡੇ ਵੱਲੋਂ ਦੋ ਜਾਂ ਦੋ ਤੋਂ ਵੱਧ ਪੁਸ਼ਟੀਕਰਨ ਕਿਸਮਾਂ ਦਾ ਸੁਮੇਲ ਤਿਆਰ ਕਰਕੇ ਦੇਣ ਦੀ ਮੰਗ ਕਰਦਾ ਹੈ।

- **ਅਜਿਹਾ ਕੁੱਝ ਜੋ ਤੁਸੀਂ ਜਾਣਦੇ ਹੋ** (ਉਦਾਹਰਨ ਲਈ, PIN, ਪਾਸਵਰਡ ਜਾਂ ਪਾਸਫਰੇਜ਼)
- **ਅਜਿਹੀ ਕੋਈ ਚੀਜ਼ ਹੈ ਜੋ ਤੁਹਾਡੇ ਕੋਲ ਹੈ** (ਜਿਵੇਂ ਕਿ ਸਮਾਰਟ ਕਾਰਡ, ਅਸਲੀ ਟੋਕਨ, ਪੁਸ਼ਟੀਕਰਨ ਐਪ, SMS ਜਾਂ ਈਮੇਲ)
- **ਅਜਿਹਾ ਕੋਈ ਚੀਜ਼ ਜੋ ਤੁਸੀਂ ਹੋ** (ਜਿਵੇਂ ਕਿ ਫਿੰਗਰਪ੍ਰਿੰਟ (ਉਂਗਲਾਂ ਦੇ ਨਿਸ਼ਾਨ), ਚਿਹਰੇ ਦੀ ਪਛਾਣ ਜਾਂ ਅੱਖਾਂ ਦੀ ਸਕੈਨ)

MFA ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਤੁਹਾਡੇ ਖਾਤੇ ਤੱਕ ਸ਼ੁਰੂਆਤੀ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰਨਾ ਔਖਾ ਬਣਾਉਂਦਾ ਹੈ। ਇਹ ਹੋਰ ਪ੍ਰਮਾਣਿਕਤਾ ਦੀਆਂ ਪਰਤਾਂ ਨੂੰ ਜੋੜਦਾ ਹੈ, ਜਿਸ ਨੂੰ ਤੋੜਨ ਲਈ ਵਾਧੂ ਸਮਾਂ, ਮਿਹਨਤ ਅਤੇ ਸਰੋਤਾਂ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ।

ਮੈਂ ਆਪਣੇ ਸਭ ਤੋਂ ਵੱਧ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਲਈ MFA ਨੂੰ ਕਿਵੇਂ ਚਾਲੂ ਕਰਾਂ?

ਖਾਤੇ, ਯੰਤਰ ਜਾਂ ਸਾਫ਼ਟਵੇਅਰ ਐਪਲੀਕੇਸ਼ਨ ਦੇ ਆਧਾਰ 'ਤੇ MFA ਨੂੰ ਚਾਲੂ (ਐਕਟੀਵੇਟ) ਕਰਨ ਦੇ ਪੜਾਅ ਵੱਖੋ-ਵੱਖਰੇ ਹਨ। ਤੁਹਾਨੂੰ ਹੁਣੇ ਆਪਣੇ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ ਤੋਂ ਸ਼ੁਰੂਆਤ ਕਰਦੇ ਹੋਏ, MFA ਨੂੰ ਚਾਲੂ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ:

- ਸਾਰੇ ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਅਤੇ ਵਿੱਤੀ ਖਾਤੇ (ਉਦਾਹਰਨ ਲਈ ਤੁਹਾਡਾ ਬੈਂਕ, ਪੇਅਪਾਲ (PayPal))
- ਸਾਰੇ ਈਮੇਲ ਖਾਤੇ (ਜਿਵੇਂ ਕਿ ਜੀਮੇਲ (Gmail), ਆਊਟਲੁੱਕ (Outlook), ਹਾਟਮੇਲ (Hotmail), ਯਾਹੂ! (Yahoo!))

ਜੇਕਰ ਤੁਹਾਡੇ ਕੋਲ ਬਹੁਤ ਸਾਰੇ ਈਮੇਲ ਖਾਤੇ ਹਨ, ਤਾਂ ਉਹਨਾਂ ਨੂੰ ਤਰਜੀਹ ਦਿਓ ਜੋ ਤੁਹਾਡੀ ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਜਾਂ ਹੋਰ ਮਹੱਤਵਪੂਰਨ ਸੇਵਾਵਾਂ ਨਾਲ ਜੁੜੇ ਹੋਏ ਹਨ।

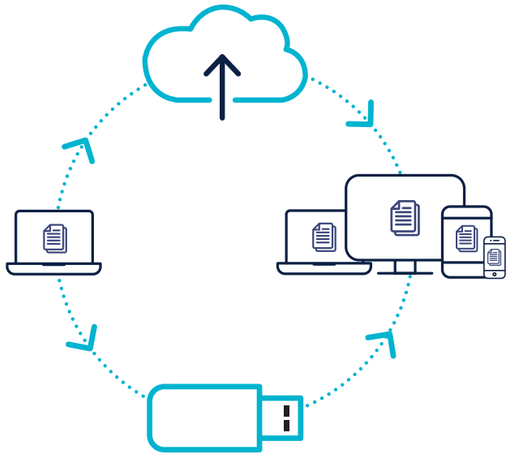
ਤੁਸੀਂ cyber.gov.au 'ਤੇ 'ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ' ਜਾਂ 'MFA' ਲੱਭ ਕੇ ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ ਨੂੰ ਕਿਵੇਂ ਚਾਲੂ ਕਰਨਾ ਹੈ ਇਸ ਬਾਰੇ ਹੋਰ ਪੜ੍ਹ ਸਕਦੇ ਹੋ।

ਬਾਕਾਇਦਾ ਤੌਰ ‘ਤੇ ਆਪਣੇ ਯੰਤਰਾਂ ਦਾ ਬੈਕਅੱਪ ਲਓ

ਬੈਕਅੱਪ ਕੀ ਹੁੰਦਾ ਹੈ?

ਬੈਕਅੱਪ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਦੀ ਇੱਕ ਡਿਜ਼ੀਟਲ ਨਕਲ ਹੁੰਦੀ ਹੈ। ਇਸ ਵਿੱਚ ਫ਼ੋਟੋਆਂ, ਵਿੱਤੀ ਜਾਣਕਾਰੀ ਜਾਂ ਰਿਕਾਰਡਾਂ ਵਰਗੀਆਂ ਚੀਜ਼ਾਂ ਸ਼ਾਮਲ ਹੋ ਸਕਦੀਆਂ ਹਨ ਜੋ ਤੁਸੀਂ ਕਿਸੇ ਬਾਹਰੀ ਸਟੋਰੇਜ ਯੰਤਰ, ਜਾਂ ਕਲਾਉਡ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਕੀਤੀਆਂ ਹਨ।

ਆਪਣੀ ਜਾਣਕਾਰੀ ਦਾ ਬੈਕਅੱਪ ਲੈਣਾ ਇੱਕ ਸਾਵਧਾਨੀ ਭਰਿਆ ਉਪਾਅ ਹੈ ਤਾਂ ਜੋ ਇਸਨੂੰ ਮੁੜ ਬਰਾਮਦ ਕੀਤਾ ਜਾ ਸਕੇ ਜੇਕਰ ਇਹ ਕਦੇ ਗੁੰਮ, ਚੋਰੀ ਜਾਂ ਖ਼ਰਾਬ ਹੋ ਜਾਂਦੀ ਹੈ।



ਮੈਂ ਆਪਣੇ ਯੰਤਰਾਂ ਅਤੇ ਫਾਈਲਾਂ ਦਾ ਬੈਕਅੱਪ ਕਿਵੇਂ ਲਵਾਂ?

ਤੁਹਾਨੂੰ ਆਪਣੀਆਂ ਫਾਈਲਾਂ ਅਤੇ ਯੰਤਰਾਂ ਦਾ ਬਾਕਾਇਦਾ ਤੌਰ ‘ਤੇ ਬੈਕਅੱਪ ਲੈਣਾ ਚਾਹੀਦਾ ਹੈ। ਇਹ ਕਿਹੋ ਜਿਹਾ ਲੱਗਦਾ ਹੈ, ਭਾਵੇਂ ਇਹ ਰੋਜ਼ਾਨਾ ਹੋਵੇ, ਹਫ਼ਤਾਵਾਰੀ ਹੋਵੇ ਜਾਂ ਮਹੀਨੇਵਾਰ ਵਾਰ, ਆਖ਼ਰ ਇਹ ਤੁਹਾਡੇ ‘ਤੇ ਨਿਰਭਰ ਕਰਦਾ ਹੈ।

ਤੁਸੀਂ ਕਿੰਨੀ ਵਾਰ ਬੈਕਅੱਪ ਲੈਂਦੇ ਹੋ ਉਹ ਇਨ੍ਹਾਂ ਦੀ ਗਿਣਤੀ ‘ਤੇ ਨਿਰਭਰ ਕਰਦਾ ਹੈ:

- ਨਵੀਆਂ ਫਾਈਲਾਂ ਜੋ ਤੁਸੀਂ ਆਪਣੇ ਯੰਤਰ ਉੱਤੇ ਲੋਡ ਕਰਦੇ ਹੋ,
- ਤੁਹਾਡੇ ਦੁਆਰਾ ਫਾਈਲਾਂ ਵਿੱਚ ਕੀਤੀਆਂ ਗਈਆਂ ਤਬਦੀਲੀਆਂ ‘ਤੇ।

ਸੁਝਾਅ: ਬਾਕਾਇਦਾ ਤੌਰ ‘ਤੇ ਆਪਣੇ ਬੈਕਅੱਪ ਦੀ ਜਾਂਚ ਕਰੋ ਤਾਂ ਜੋ ਤੁਸੀਂ ਵਾਪਸ ਪ੍ਰਾਪਤ ਕਰਨ ਦੀ (ਰਿਕਵਰੀ) ਪ੍ਰਕਿਰਿਆ ਤੋਂ ਜਾਣੂ ਹੋ ਜਾਵੋ। ਹਮੇਸ਼ਾ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੇ ਬੈਕਅੱਪ ਸਹੀ ਢੰਗ ਨਾਲ ਕੰਮ ਕਰ ਰਹੇ ਹਨ।

ਆਪਣੀ ਜਾਣਕਾਰੀ ਦਾ ਬੈਕਅੱਪ ਕਿਵੇਂ ਲੈਣਾ ਹੈ ਇਸ ਬਾਰੇ ਵਧੇਰੇ ਵਿਸਤ੍ਰਿਤ ਜਾਣਕਾਰੀ cyber.gov.au ‘ਤੇ ‘ਬੈਕਅੱਪ’ ਲੱਭ ਕੇ ਪ੍ਰਾਪਤ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ।

ਆਪਣੇ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਲਈ ਪਾਸਫਰੇਜ਼ ਦੀ ਵਰਤੋਂ ਕਰੋ

ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ (MFA) ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਨੂੰ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਤੋਂ ਬਚਾਉਣ ਦੇ ਸਭ ਤੋਂ ਪ੍ਰਭਾਵਸ਼ਾਲੀ ਤਰੀਕਿਆਂ ਵਿੱਚੋਂ ਇੱਕ ਹੈ। ਜੇਕਰ **MFA ਉਪਲਬਧ ਨਹੀਂ ਹੈ**, ਤਾਂ ਇੱਕ ਸਧਾਰਨ ਪਾਸਵਰਡ ਦੀ ਥਾਂ ਇੱਕ ਵਿਲੱਖਣ ਮਜ਼ਬੂਤ ਪਾਸਫਰੇਜ਼ ਤੁਹਾਡੇ ਖਾਤੇ ਦੀ ਬਿਹਤਰ ਸੁਰੱਖਿਆ ਕਰ ਸਕਦਾ ਹੈ।

ਪਾਸਫਰੇਜ਼ ਕੀ ਹੈ?

ਪਾਸਫਰੇਜ਼ ਤੁਹਾਡੇ ਪਾਸਵਰਡ ਵਜੋਂ ਚਾਰ ਜਾਂ ਵੱਧ ਬੇਤਰਤੀਬ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਕਰਦਾ ਹੈ।

ਉਦਾਹਰਨ ਲਈ: ‘ਕ੍ਰਿਸਟਲ ਪਿਆਜ਼ ਮਿੱਟੀ ਪ੍ਰੈਟਜ਼ਲ’।

- ਸਧਾਰਨ ਪਾਸਵਰਡਾਂ ਨਾਲੋਂ **ਪਾਸਫਰੇਜ਼ ਵਧੇਰੇ ਸੁਰੱਖਿਅਤ ਹਨ**।
- ਪਾਸਫਰੇਜ਼ ਨੂੰ ਤੋੜਨਾ **ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਔਖਾ ਹੈ**, ਪਰ **ਤੁਹਾਡੇ ਲਈ ਯਾਦ ਰੱਖਣਾ ਆਸਾਨ ਹੈ**।

ਮੈਂ ਪਾਸਫਰੇਜ਼ ਕਿਵੇਂ ਬਣਾਵਾਂ?

ਉਹ ਪਾਸਫਰੇਜ਼ ਬਣਾਓ ਜੋ:

- **ਲੰਬੇ ਹਨ:** ਘੱਟੋ-ਘੱਟ 14 ਅੱਖਰ ਲੰਬੇ, ਚਾਰ ਜਾਂ ਇਸਤੋਂ ਵੱਧ ਬੇਤਰਤੀਬੇ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਨ। ਤੁਹਾਡਾ ਪਾਸਫਰੇਜ਼ ਜਿੰਨ੍ਹਾਂ ਲੰਬਾ ਹੋਵੇਗਾ, ਇਹ ਓਨਾ ਹੀ ਸੁਰੱਖਿਅਤ ਹੋਵੇਗਾ।
- **ਗ਼ੈਰ-ਅਨੁਮਾਨਿਤ ਹਨ:** ਚਾਰ ਜਾਂ ਵੱਧ ਨਾ-ਸੰਬੰਧਿਤ ਸ਼ਬਦਾਂ ਦੇ ਬੇਤਰਤੀਬੇ ਮਿਸ਼ਰਣ ਦੀ ਵਰਤੋਂ ਕਰੋ। ਕੋਈ ਵੀ ਮਸ਼ਹੂਰ ਵਾਕਾਂਸ਼, ਅਨਮੋਲ ਬਚਨ ਜਾਂ ਗੀਤਾਂ ਦੇ ਬੋਲ ਨਾ ਵਰਤੋਂ।
- **ਵਿਲੱਖਣ ਹਨ:** ਕਈ ਖਾਤਿਆਂ ਵਿੱਚ ਬਾਰ-ਬਾਰ ਨਾ ਵਰਤੋਂ।

ਜੇਕਰ ਕਿਸੇ ਵੈੱਬਸਾਈਟ ਜਾਂ ਸੇਵਾ ਲਈ ਚਿੰਨ੍ਹਾਂ, ਵੱਡੇ ਅੱਖਰਾਂ ਜਾਂ ਸੰਖਿਆਵਾਂ ਸਮੇਤ ਗੁੰਝਲਦਾਰ ਪਾਸਵਰਡ ਦੀ ਲੋੜ ਹੈ, ਤਾਂ ਤੁਸੀਂ ਇਹਨਾਂ ਨੂੰ ਆਪਣੇ ਪਾਸਫਰੇਜ਼ ਵਿੱਚ ਸ਼ਾਮਲ ਕਰ ਸਕਦੇ ਹੋ। ਬੇਹਤਰੀਨ ਸੁਰੱਖਿਆ ਲਈ ਤੁਹਾਡਾ ਪਾਸਫਰੇਜ਼ ਅਜੇ ਵੀ ਲੰਮਾ, ਗ਼ੈਰ-ਅਨੁਮਾਨਿਤ ਅਤੇ ਵਿਲੱਖਣ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ।

ਮੈਨੂੰ ਪਾਸਫਰੇਜ਼ ਨਾਲ ਕਿਹੜੇ ਖਾਤਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ?

ਜੇਕਰ ਤੁਹਾਡੇ ਸਭ ਤੋਂ ਵੱਧ ਮਹੱਤਵਪੂਰਨ ਖਾਤੇ MFA ਨਾਲ ਸੁਰੱਖਿਅਤ ਨਹੀਂ ਹਨ, ਤਾਂ ਇਨ੍ਹਾਂ ਤੋਂ ਸ਼ੁਰੂ ਕਰਦੇ ਹੋਏ ਆਪਣੇ ਪਾਸਵਰਡਾਂ ਨੂੰ ਵਿਲੱਖਣ ਮਜ਼ਬੂਤ ਪਾਸਫਰੇਜਾਂ ਨਾਲ ਬਦਲੋ:

- ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਅਤੇ ਵਿੱਤੀ ਖਾਤੇ
- ਈਮੇਲ ਖਾਤੇ

ਜੇਕਰ ਤੁਹਾਡੇ ਕੋਲ ਬਹੁਤ ਸਾਰੇ ਈਮੇਲ ਖਾਤੇ ਹਨ, ਤਾਂ ਉਹਨਾਂ ਨੂੰ ਤਰਜੀਹ ਦਿਓ ਜੋ ਤੁਹਾਡੀ ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਜਾਂ ਹੋਰ ਮਹੱਤਵਪੂਰਨ ਸੇਵਾਵਾਂ ਨਾਲ ਜੁੜੇ ਹੋਏ ਹਨ।

ਤੁਸੀਂ ਆਮ ਤੌਰ ‘ਤੇ ਆਪਣੇ ਖਾਤਾ ਸੈਟਿੰਗ ਮੀਨੂ ਰਾਹੀਂ ਆਪਣੇ ਪਾਸਵਰਡ ਨੂੰ ਇੱਕ ਵਿਲੱਖਣ ਮਜ਼ਬੂਤ ਪਾਸਫਰੇਜ਼ ਵਿੱਚ ਬਦਲ ਸਕਦੇ ਹੋ।

ਸੁਝਾਅ: ਜੇਕਰ ਤੁਹਾਨੂੰ ਆਪਣੇ ਸਾਰੇ ਪਾਸਫਰੇਜਾਂ ਨੂੰ ਯਾਦ ਰੱਖਣ ਵਿੱਚ ਸਮੱਸਿਆ ਆਉਂਦੀ ਹੈ, ਤਾਂ ਕਿਸੇ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਦੀ ਵਰਤੋਂ ਕਰਨ ‘ਤੇ ਵਿਚਾਰ ਕਰੋ। ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਨਾਲ, ਤੁਹਾਨੂੰ ਸਿਰਫ਼ ਇੱਕ ਪਾਸਵਰਡ ਹੀ ਯਾਦ ਰੱਖਣ ਦੀ ਲੋੜ ਪੈਂਦੀ ਹੈ, ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਬਾਕੀ ਦੇ ਪਾਸਵਰਡਾਂ ਨੂੰ ਯਾਦ ਰੱਖਦਾ ਹੈ। ਹੋਰ ਸਲਾਹ ਲਈ cyber.gov.au ‘ਤੇ ‘ਪਾਸਵਰਡ ਮੈਨੇਜਰ’ ਖੋਜੋ।

ਸੁਰੱਖਿਅਤ ਪਾਸਫਰੇਜ਼ ਕਿਵੇਂ ਬਣਾਉਣੇ ਹਨ ਇਸ ਬਾਰੇ ਵਧੇਰੇ ਵਿਸਤ੍ਰਿਤ ਜਾਣਕਾਰੀ cyber.gov.au ‘ਤੇ ‘ਪਾਸਫਰੇਜ਼’ ਖੋਜ ਕੇ ਪ੍ਰਾਪਤ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ।

ਆਪਣੀ ਮੋਬਾਈਲ ਫ਼ੋਨ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ

ਅੱਜਕਲ੍ਹ ਸਮਾਰਟਫ਼ੋਨ ਅਤੇ ਟੈਬਲੇਟ ਰੋਜ਼ਮਰ੍ਹਾ ਜੀਵਨ ਵਿੱਚ ਵਰਤੇ ਜਾਂਦੇ ਹਨ। ਅਸੀਂ ਉਹਨਾਂ ਦੀ ਵਰਤੋਂ ਕਿਸੇ ਵੀ ਸਮੇਂ ਅਤੇ ਕਿਸੇ ਵੀ ਸਥਾਨ ਤੋਂ ਆਪਸ ਵਿੱਚ ਜੁੜਨ, ਖ਼ਰੀਦਦਾਰੀ ਕਰਨ, ਕੰਮ ਕਰਨ, ਬੈਂਕ ਦੇ ਕੰਮਕਾਜ ਕਰਨ, ਸਾਡੀ ਫਿਟਨੈੱਸ ਨੂੰ ਸਹੀ ਰੱਖਣ ਅਤੇ ਸੈਂਕੜੇ ਹੋਰ ਕੰਮ-ਕਾਰ ਨੂੰ ਕਰਨ ਲਈ ਕਰਦੇ ਹਾਂ।

ਜੇਕਰ ਮੇਰੇ ਮੋਬਾਈਲ ਯੰਤਰ ਨਾਲ ਛੇੜਛਾੜ ਹੁੰਦੀ ਹੈ, ਗੁੰਮ ਜਾਂ ਚੋਰੀ ਹੋ ਜਾਂਦਾ ਹੈ ਤਾਂ ਕੀ ਹੋ ਸਕਦਾ ਹੈ ?

- ਇਸਦੀ ਵਰਤੋਂ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਦੁਆਰਾ ਤੁਹਾਡੇ ਪੈਸੇ ਜਾਂ ਸ਼ਨਾਖ਼ਤ ਨੂੰ ਚੋਰੀ ਕਰਨ ਲਈ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ। ਉਹ ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਤੇ ਈਮੇਲ ਖਾਤਿਆਂ ਸਮੇਤ ਤੁਹਾਡੇ ਯੰਤਰ 'ਤੇ ਸਟੋਰ ਕੀਤੀ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਅਜਿਹਾ ਕਰਦੇ ਹਨ।
- ਤੁਸੀਂ ਫ਼ੋਟੋਆਂ, ਨੋਟਸ ਜਾਂ ਸੁਨੇਹਿਆਂ (ਜੇਕਰ ਇਸਦਾ ਬੈਕਅੱਪ ਨਹੀਂ ਲਿਆ ਗਿਆ ਹੈ) ਵਰਗਾ ਨਾ ਬਦਲਣਯੋਗ ਡਾਟਾ ਗੁਆ ਸਕਦੇ ਹੋ।
- ਸਾਈਬਰ ਅਪਰਾਧੀ ਦੂਜੇ ਲੋਕਾਂ ਨਾਲ ਧੋਖਾਧੜੀ ਕਰਨ ਲਈ ਤੁਹਾਡੇ ਫ਼ੋਨ ਨੰਬਰ ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦਾ ਹੈ।

ਮੈਂ ਆਪਣੇ ਮੋਬਾਈਲ ਯੰਤਰ ਨੂੰ ਕਿਵੇਂ ਸੁਰੱਖਿਅਤ ਕਰਾਂ?

ਯੰਤਰ ਸੁਰੱਖਿਆ:

- ਆਪਣੇ ਯੰਤਰ ਨੂੰ ਪਾਸਫਰੇਜ਼, ਪਾਸਵਰਡ, ਪਿੰਨ ਜਾਂ ਪਾਸਕੋਡ ਨਾਲ **ਲਾਕ (ਤਾਲਾ) ਲਗਾਓ**। ਇਨ੍ਹਾਂ ਦਾ ਅੰਦਾਜ਼ਾ ਲਗਾਉਣਾ ਮੁਸ਼ਕਲ ਬਣਾਓ - ਤੁਹਾਡੀ ਜਨਮ ਮਿਤੀ ਅਤੇ ਪੈਟਰਨ ਲਾਕ ਦਾ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਅੰਦਾਜ਼ਾ ਲਗਾਉਣਾ ਆਸਾਨ ਹੈ। ਬੇਹਤਰੀਨ ਸੁਰੱਖਿਆ ਲਈ ਪਾਸਫਰੇਜ਼ ਦੀ ਵਰਤੋਂ ਕਰੋ (ਪੰਨਾ 6 ਦੇਖੋ)। ਤੁਸੀਂ ਆਪਣੇ ਯੰਤਰ ਨੂੰ ਅਨਲੌਕ ਕਰਨ (ਖੋਲ੍ਹਣ) ਲਈ ਚਿਹਰੇ ਦੀ ਪਛਾਣ ਜਾਂ ਫ਼ਿੰਗਰਪ੍ਰਿੰਟ ਦੀ ਵਰਤੋਂ ਕਰਨ ਬਾਰੇ ਵੀ ਵਿਚਾਰ ਕਰ ਸਕਦੇ ਹੋ।
- **ਯਕੀਨੀ ਬਣਾਓ** ਕਿ ਤੁਹਾਡਾ ਯੰਤਰ ਨਾ-ਵਰਤਣ ਦੇ ਥੋੜ੍ਹੇ ਸਮੇਂ ਬਾਅਦ ਆਪਣੇ-ਆਪ ਬੰਦ ਹੋਣ ਲਈ ਸੈੱਟ ਕੀਤਾ ਗਿਆ ਹੈ।
- **ਕਿਸੇ** ਜਨਤਕ ਚਾਰਜਿੰਗ ਸਟੇਸ਼ਨ 'ਤੇ ਆਪਣੇ ਯੰਤਰ ਨੂੰ ਚਾਰਜ ਨਾ ਕਰੋ ਅਤੇ ਤੀਜੀ ਧਿਰ ਵੱਲੋਂ ਉਪਲਬਧ ਕਰਵਾਏ ਚਾਰਜਰਾਂ ਦੀ ਵਰਤੋਂ **ਕਰਨ ਤੋਂ ਬਚੋ।**
- ਆਪਣੇ ਫ਼ੋਨ ਨੂੰ ਆਪਣੇ ਬਟੂਏ **ਵਾਂਗ** ਵਰਤੋ। ਇਸਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖੋ ਅਤੇ ਹਰ ਸਮੇਂ ਆਪਣੇ ਨਾਲ ਰੱਖੋ।

ਸਾਫ਼ਟਵੇਅਰ ਅਤੇ ਐਪ ਸੁਰੱਖਿਆ:

- **ਵਰਤੋਂ:** ਨਵੀਂ ਐਪਲੀਕੇਸ਼ਨ ਅਤੇ ਓਪਰੇਟਿੰਗ ਸਿਸਟਮ ਅੱਪਡੇਟ ਉਪਲਬਧ ਹੁੰਦੇ ਹੀ ਉਹਨਾਂ ਨੂੰ ਇੰਸਟਾਲ ਕਰਨ ਲਈ ਆਪਣੇ ਯੰਤਰ ਦੀ ਆਟੋਮੈਟਿਕ ਅਪਡੇਟ ਕਰਨ ਦੀ ਸਹੂਲਤ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- **ਸੈੱਟ ਕਰੋ:** ਆਪਣੇ ਯੰਤਰ ਨੂੰ ਐਪਲੀਕੇਸ਼ਨਾਂ ਨੂੰ ਇੰਸਟਾਲ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਪਾਸਫਰੇਜ਼/ਪਾਸਵਰਡ ਮੰਗਣ ਲਈ ਸੈੱਟ ਕਰੋ। ਇਸ ਮਕਸਦ ਲਈ ਮਾਪਿਆਂ ਲਈ ਉਪਲਬਧ ਕੰਟਰੋਲ ਦੀ ਵਰਤੋਂ ਵੀ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ
- **ਜਾਂਚੋ:** ਆਪਣੇ ਯੰਤਰ 'ਤੇ ਨਵੇਂ ਐਪ ਇੰਸਟਾਲ ਕਰਦੇ ਸਮੇਂ ਗੁਪਤਤਾ ਅਗਿਆਵਾਂ ਨੂੰ ਧਿਆਨ ਨਾਲ ਜਾਂਚੋ, ਖ਼ਾਸ ਕਰਕੇ ਮੁਫ਼ਤ ਉਪਲਬਧ ਐਪਾਂ ਲਈ। ਸਿਰਫ਼ ਨਾਮਵਰ ਵਿਕਰੇਤਾਵਾਂ ਤੋਂ ਹੀ ਐਪਾਂ ਇੰਸਟਾਲ ਕਰੋ।

ਡਾਟਾ ਸੁਰੱਖਿਆ:

- **ਚਾਲੂ ਕਰੋ:** ਜੇਕਰ ਤੁਹਾਡਾ ਯੰਤਰ ਉਹਨਾਂ ਨੂੰ ਚਲਾਉਣ ਦੀ ਆਗਿਆ ਦਿੰਦਾ ਹੈ ਤਾਂ ਰਿਮੋਟ ਲਾਕਿੰਗ ਅਤੇ ਵਾਈਪਿੰਗ ਫੰਕਸ਼ਨਾਂ ਨੂੰ ਚਾਲੂ ਕਰੋ।
- **ਯਕੀਨੀ ਬਣਾਓ** ਕਿ ਤੁਸੀਂ ਆਪਣੇ ਯੰਤਰ ਨੂੰ ਵੇਚਣ ਜਾਂ ਨਿਪਟਾਉਣ ਤੋਂ ਪਹਿਲਾਂ ਇਸ ਵਿੱਚੋਂ ਨਿੱਜੀ ਡਾਟਾ ਨੂੰ ਚੰਗੀ ਤਰ੍ਹਾਂ ਹਟਾ ਦਿੱਤਾ ਹੈ।

ਕਨੈਕਟੀਵਿਟੀ ਸੁਰੱਖਿਆ:

- ਜਦੋਂ ਤੁਸੀਂ ਬਲਿਊਟੁੱਥ ਅਤੇ ਵਾਈ-ਫ਼ਾਈ ਦੀ ਵਰਤੋਂ ਨਹੀਂ ਕਰ ਰਹੇ ਹੋ ਤਾਂ **ਉਨ੍ਹਾਂ ਨੂੰ ਬੰਦ ਕਰਕੇ ਰੱਖੋ**।
- **ਯਕੀਨੀ ਬਣਾਓ** ਕਿ ਤੁਹਾਡੀ ਡਿਵਾਈਸ ਨਵੇਂ Wi-Fi ਨੈੱਟਵਰਕਾਂ ਨਾਲ ਆਪਣੇ-ਆਪ ਕਨੈਕਟ ਨਹੀਂ ਹੁੰਦੀ ਹੈ।

ਆਪਣੇ ਮੋਬਾਈਲ ਨੂੰ ਕਿਵੇਂ ਸੁਰੱਖਿਅਤ ਕਰਨਾ ਹੈ ਇਸ ਬਾਰੇ ਵਧੇਰੇ ਵਿਸਥਾਰ ਵਿੱਚ ਜਾਣਕਾਰੀ cyber.gov.au **'ਤੇ 'Secure your mobile phone' ਲੱਭ ਕੇ ਪ੍ਰਾਪਤ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ।**

ਆਪਣੀ ਸਾਈਬਰ ਸੁਰੱਖਿਅਤ ਸੋਚ ਦਾ ਵਿਕਾਸ ਕਰੋ

ਨਿੱਜੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਸਿਰਫ਼ ਸੈਟਿੰਗਾਂ ਨੂੰ ਬਦਲਣ ਬਾਰੇ ਨਹੀਂ ਹੈ, ਇਹ ਤੁਹਾਡੀ ਸੋਚ ਅਤੇ ਵਿਵਹਾਰ ਨੂੰ ਬਦਲਣ ਬਾਰੇ ਵੀ ਹੈ।

ਸਾਈਬਰ ਘੁਟਾਲਿਆਂ ਪ੍ਰਤੀ ਸਾਵਧਾਨ ਰਹੋ

ਸਾਈਬਰ ਅਪਰਾਧੀ ਆਸਟ੍ਰੇਲੀਆਈ ਲੋਕਾਂ ਨਾਲ ਧੋਖਾਧੜੀ ਕਰਨ ਲਈ ਈਮੇਲ, ਮੈਸਜ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਜਾਂ ਫ਼ੋਨ ਕਾਲਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਲਈ ਪ੍ਰਸਿੱਧ ਹਨ। ਉਹ ਕੋਈ ਵਿਅਕਤੀ ਜਾਂ ਸੰਸਥਾ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰ ਸਕਦੇ ਹਨ ਜੋ ਤੁਸੀਂ ਸੋਚਦੇ ਹੋ ਕਿ ਤੁਸੀਂ ਉਨ੍ਹਾਂ ਨੂੰ ਜਾਣਦੇ ਹੋ, ਜਾਂ ਸੋਚਦੇ ਹੋ ਕਿ ਤੁਹਾਨੂੰ ਭਰੋਸਾ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ।

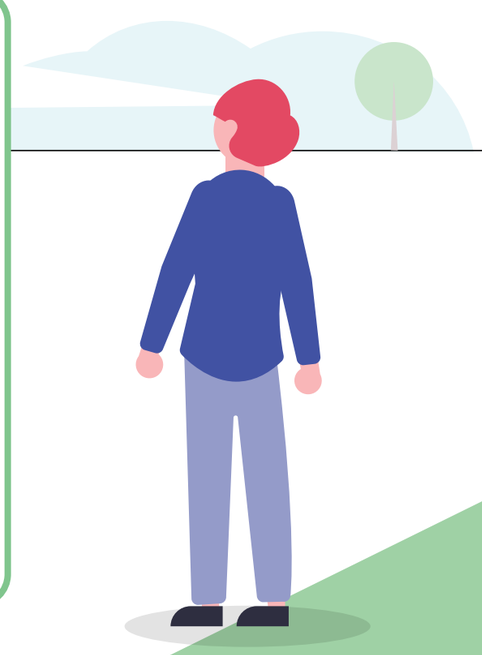
ਉਹਨਾਂ ਦੇ ਸੁਨੇਹੇ ਅਤੇ ਕਾਲਾਂ ਤੁਹਾਨੂੰ ਬੇਵਕੂਫ਼ ਬਣਾ ਕੇ ਕੁੱਝ ਖ਼ਾਸ ਚੀਜ਼ਾਂ ਕਰਵਾਉਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਦੀਆਂ ਹਨ, ਜਿਵੇਂ ਕਿ:

- ਬੈਂਕ ਖਾਤੇ ਦੇ ਵੇਰਵੇ, ਪਾਸਵਰਡ, ਅਤੇ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਨੰਬਰਾਂ ਦਾ ਖੁਲਾਸਾ ਕਰਵਾਉਣ ਦੀ,
- ਤੁਹਾਡੇ ਕੰਪਿਊਟਰ ਨੂੰ ਰਿਮੋਟ ਪਹੁੰਚ ਦੇਣ ਦੀ,
- ਕੋਈ ਅਟੈਚਮੈਂਟ ਖੋਲ੍ਹਣ ਦੀ, ਜਿਸ ਵਿੱਚ ਮਾਲਵੇਅਰ ਹੋ ਸਕਦਾ ਹੈ,
- ਪੈਸੇ ਜਾਂ ਤੋਹਫ਼ੇ ਕਾਰਡ ਭੇਜਣ ਦੀ।

ਮੈਂ ਧੋਖਾਧੜੀ ਕਰਨ ਵਾਲੇ ਸੁਨੇਹਿਆਂ ਦੀ ਪਛਾਣ ਕਿਵੇਂ ਕਰਾਂ?

ਧੋਖਾਧੜੀ ਕਰਨ ਵਾਲੇ ਸੁਨੇਹਿਆਂ ਨੂੰ ਪਛਾਣਨਾ ਮੁਸ਼ਕਲ ਹੋ ਸਕਦਾ ਹੈ। ਸਾਈਬਰ ਅਪਰਾਧੀ ਅਕਸਰ ਤੁਹਾਨੂੰ ਬੇਵਕੂਫ਼ ਬਣਾਉਣ ਲਈ ਕੁੱਝ ਖ਼ਾਸ ਤਰੀਕਿਆਂ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਨ। ਉਹਨਾਂ ਦੇ ਸੁਨੇਹਿਆਂ ਵਿੱਚ ਸ਼ਾਮਲ ਹੋ ਸਕਦੇ ਹਨ:

- **ਅਥਾਰਟੀ:** ਕੀ ਉਹ ਸੁਨੇਹਾ ਕਿਸੇ ਅਧਿਕਾਰੀ ਵੱਲੋਂ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰ ਰਿਹਾ ਹੈ, ਜਿਵੇਂ ਕਿ ਤੁਹਾਡੇ ਬੈਂਕ ਵੱਲੋਂ?
- **ਜ਼ਰੂਰੀ:** ਕੀ ਤੁਹਾਨੂੰ ਕੋਈ ਸਮੱਸਿਆ ਹੋਣ ਬਾਰੇ ਦੱਸਿਆ ਗਿਆ ਹੈ, ਜਾਂ ਇਹ ਕਿ ਤੁਹਾਡੇ ਕੋਲ ਜਵਾਬ ਦੇਣ ਜਾਂ ਭੁਗਤਾਨ ਕਰਨ ਲਈ ਸੀਮਤ ਸਮਾਂ ਬਚਿਆ ਹੈ?
- **ਭਾਵੁਕਤਾ:** ਕੀ ਉਹ ਸੁਨੇਹਾ ਤੁਹਾਨੂੰ ਘਬਰਾਹਟ ਵਿੱਚ ਪਾਉਂਦਾ, ਆਸ਼ਾਵਾਦੀ ਜਾਂ ਉਤਸੁਕ ਬਣਾਉਂਦਾ ਹੈ?
- **ਕਮੀ:** ਕੀ ਉਹ ਸੁਨੇਹਾ ਕੁੱਝ ਅਜਿਹਾ ਪੇਸ਼ ਕਰ ਰਿਹਾ ਹੈ ਜੋ ਘੱਟ ਸਪਲਾਈ ਵਿੱਚ ਹੈ, ਜਾਂ ਵਧੀਆ ਸੌਦਾ ਲੱਗ ਰਿਹਾ ਹੈ?
- ਮੌਜੂਦਾ ਘਟਨਾਵਾਂ: ਕੀ ਉਹ ਸੁਨੇਹਾ ਕਿਸੇ ਮੌਜੂਦਾ ਸਮਾਚਾਰ ਕਹਾਣੀ ਜਾਂ ਵੱਡੀ ਘਟਨਾ ਬਾਰੇ ਹੈ?



ਫਿਸ਼ਿੰਗ ਜਾਂ ਧੋਖਾਧੜੀ ਦੇਣ ਦੇ ਸੁਨੇਹਿਆਂ ਨੂੰ ਕਿਵੇਂ ਲੱਭਿਆ ਜਾਵੇ ਇਸ ਬਾਰੇ cyber.gov.au **'ਤੇ 'ਬੁਨਿਆਦੀ ਗੱਲਾਂ ਸਿੱਖੋ' (Learn the basics) 'ਤੇ ਜਾ ਕੇ ਸਿੱਖੋ।**

ਜੇਕਰ ਮੈਨੂੰ ਕੋਈ ਧੋਖਾਧੜੀ ਕਰਨ ਸੰਬੰਧੀ ਸੁਨੇਹਾ ਮਿਲਦਾ ਹੈ ਤਾਂ ਮੈਨੂੰ ਕੀ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ?

ਜੇਕਰ ਤੁਹਾਨੂੰ ਕੋਈ ਧੋਖਾਧੜੀ ਕਰਨ ਸੰਬੰਧੀ ਸੁਨੇਹਾ ਜਾਂ ਫ਼ੋਨ ਕਾਲ ਪ੍ਰਾਪਤ ਹੁੰਦੀ ਹੈ, ਤਾਂ ਤੁਹਾਨੂੰ ਇਸ ਨੂੰ ਅਣਡਿੱਠ ਕਰਨਾ, ਮਿਟਾਉਣਾ ਜਾਂ ਇਸਦੀ ਰਿਪੋਰਟ scamwatch.gov.au 'ਤੇ ਜਾਂ ਕੇ ACCC ਦੀ Scamwatch ਨੂੰ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ।

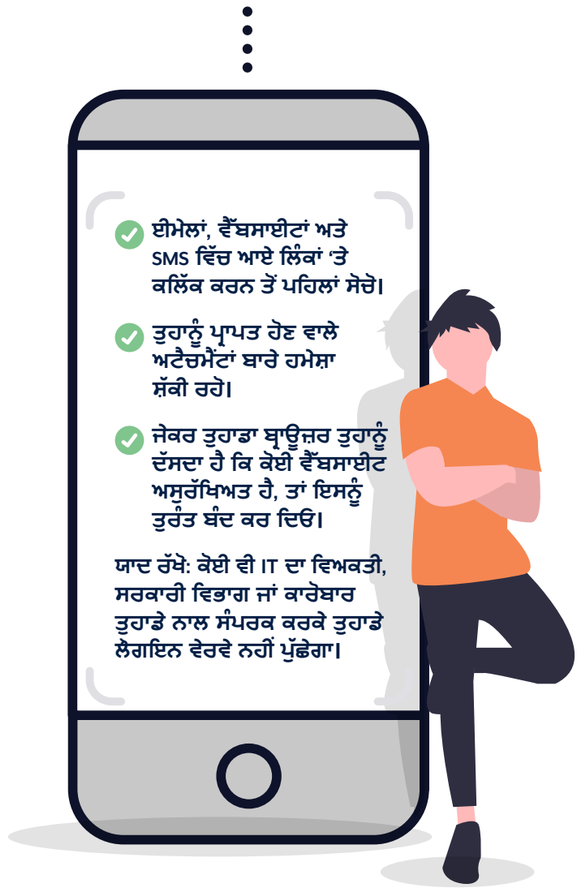
ਜੇਕਰ ਤੁਸੀਂ ਆਪਣੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਬਾਰੇ ਚਿੰਤਤ ਹੋ ਤਾਂ ਤੁਸੀਂ ACSC ਦੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਹੈਲਪਲਾਈਨ ਨਾਲ **1300 CYBER1** (1300 292 371) 'ਤੇ ਵੀ ਸੰਪਰਕ ਕਰ ਸਕਦੇ ਹੋ।

ਜੇਕਰ ਤੁਹਾਡੇ ਨਾਲ ਕੋਈ ਧੋਖਾਧੜੀ ਹੋ ਗਈ ਹੈ ਅਤੇ ਸੋਚਦੇ ਹੋ ਕਿ ਤੁਹਾਡੇ ਬੈਂਕ ਖਾਤੇ, ਕ੍ਰੈਡਿਟ ਜਾਂ ਡੈਬਿਟ ਕਾਰਡ ਖ਼ਤਰੇ ਵਿੱਚ ਹੋ ਸਕਦੇ ਹਨ, ਤਾਂ ਤੁਸੀਂ ਤੁਰੰਤ ਆਪਣੀ ਵਿੱਤੀ ਸੰਸਥਾ ਨਾਲ ਸੰਪਰਕ ਕਰੋ। ਉਹ ਤੁਹਾਡੇ ਖਾਤੇ ਨੂੰ ਬੰਦ ਕਰਨ ਜਾਂ ਲੈਣ-ਦੇਣ ਨੂੰ ਰੋਕਣ ਦੇ ਯੋਗ ਹੋ ਸਕਦੇ ਹਨ।

ਜੇ ਮੈਨੂੰ ਪੱਕਾ ਪਤਾ ਨਹੀਂ ਹੈ ਕਿ ਕੋਈ ਸੁਨੇਹਾ ਧੋਖਾਧੜੀ ਹੈ ਜਾਂ ਨਹੀਂ ਤਾਂ ਕੀ ਕਰਨਾ ਹੈ?

ਜੇਕਰ ਤੁਹਾਨੂੰ ਲੱਗਦਾ ਹੈ ਕਿ ਕੋਈ ਸੁਨੇਹਾ ਜਾਂ ਫ਼ੋਨ ਸੱਚਮੁੱਚ ਕਿਸੇ ਅਜਿਹੀ ਸੰਸਥਾ ਤੋਂ ਆਇਆ ਹੋ ਸਕਦੀ ਹੈ ਜਿਸ 'ਤੇ ਤੁਸੀਂ ਭਰੋਸਾ ਕਰਦੇ ਹੋ (ਜਿਵੇਂ ਕਿ ਤੁਹਾਡਾ ਬੈਂਕ) ਤਾਂ ਕੋਈ ਅਜਿਹਾ ਸੰਪਰਕ ਕਰਨ ਦਾ ਤਰੀਕਾ ਲੱਭੋ ਜਿਸ 'ਤੇ ਤੁਸੀਂ ਭਰੋਸਾ ਕਰ ਸਕਦੇ ਹੋ। ਉਨ੍ਹਾਂ ਦੀ ਅਧਿਕਾਰਤ ਵੈੱਬਸਾਈਟ ਲੱਭੋ, ਉਹਨਾਂ ਦੇ ਉੱਥੇ ਦਿੱਤੇ ਫ਼ੋਨ ਨੰਬਰ 'ਤੇ ਫ਼ੋਨ ਕਰੋ, ਜਾਂ ਕਿਸੇ ਸਟੋਰ ਜਾਂ ਸ਼ਾਖਾ 'ਤੇ ਵਿਅਕਤੀਗਤ ਰੂਪ ਵਿੱਚ ਜਾਓ। ਤੁਹਾਨੂੰ ਫ਼ੋਨ 'ਤੇ ਭੇਜੇ ਜਾਂ ਦਿੱਤੇ ਗਏ ਸੁਨੇਹੇ ਵਿੱਚ ਲਿੰਕ ਜਾਂ ਸੰਪਰਕ ਵੇਰਵਿਆਂ ਦੀ ਵਰਤੋਂ ਨਾ ਕਰੋ ਕਿਉਂਕਿ ਇਹ ਧੋਖਾਧੜੀ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਹੋ ਸਕਦੀ ਹੈ।

ਸੁਝਾਅ:
ਕਲਿੱਕ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸੋਚੋ



- **ਈਮੇਲਾਂ, ਵੈੱਬਸਾਈਟਾਂ ਅਤੇ SMS ਵਿੱਚ ਆਏ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸੋਚੋ।**
- **ਤੁਹਾਨੂੰ ਪ੍ਰਾਪਤ ਹੋਣ ਵਾਲੇ ਅਟੈਚਮੈਂਟਾਂ ਬਾਰੇ ਹਮੇਸ਼ਾ ਸ਼ੱਕੀ ਰਹੋ।**
- **ਜੇਕਰ ਤੁਹਾਡਾ ਬ੍ਰਾਊਜ਼ਰ ਤੁਹਾਨੂੰ ਦੱਸਦਾ ਹੈ ਕਿ ਕੋਈ ਵੈੱਬਸਾਈਟ ਅਸੁਰੱਖਿਅਤ ਹੈ, ਤਾਂ ਇਸਨੂੰ ਤੁਰੰਤ ਬੰਦ ਕਰ ਦਿਓ।**

ਯਾਦ ਰੱਖੋ: ਕੋਈ ਵੀ IT ਦਾ ਵਿਅਕਤੀ, ਸਰਕਾਰੀ ਵਿਭਾਗ ਜਾਂ ਕਾਰੋਬਾਰ ਤੁਹਾਡੇ ਨਾਲ ਸੰਪਰਕ ਕਰਕੇ ਤੁਹਾਡੇ ਲੈਗਇਨ ਵੇਰਵੇ ਨਹੀਂ ਪੁੱਛੇਗਾ।

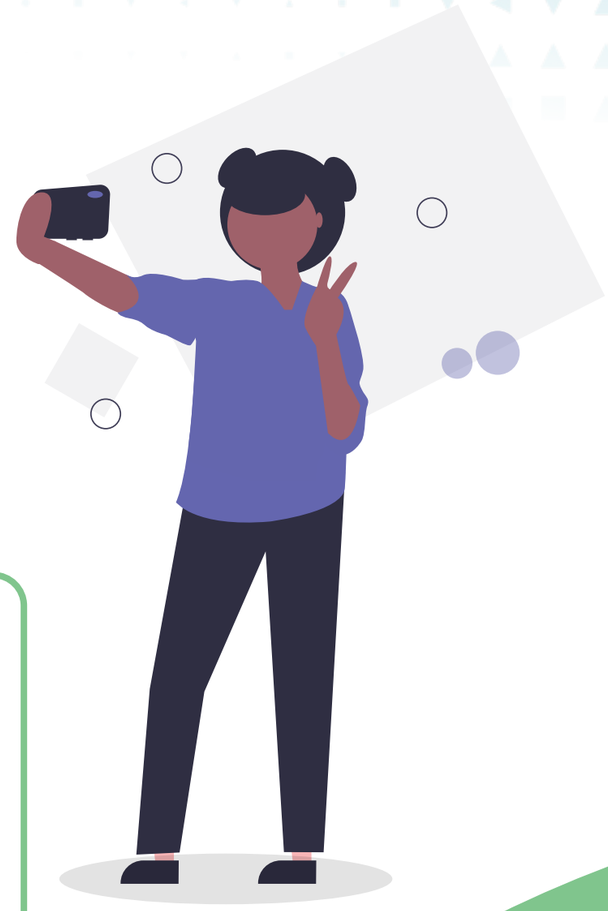
ਜੇਕਰ ਤੁਸੀਂ ਸੋਚਦੇ ਹੋ ਕਿ ਤੁਸੀਂ ਸਾਈਬਰ ਅਪਰਾਧ ਦੇ ਸ਼ਿਕਾਰ ਹੋ ਗਏ ਹੋ ਤਾਂ ਇਸਦੀ ਰਿਪੋਰਟ ACSC ਦੇ ReportCyber ਰਾਹੀਂ cyber.gov.au/report 'ਤੇ ਕਰੋ ਜਾਂ ਸਾਡੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਹੈਲਪਲਾਈਨ ਨੂੰ 1300 CYBER1 (1300 292 371) 'ਤੇ ਫ਼ੋਨ ਕਰੋ।

ਤੁਸੀਂ ACSC ਦੀ ਮੁਫ਼ਤ ਚੇਤਾਵਨੀ ਸੇਵਾ ਨਾਲ ਜੁੜ ਕੇ (ਸਬਸਕ੍ਰਾਈਬ ਕਰਕੇ) ਨਵੀਨਤਮ ਖ਼ਤਰਿਆਂ ਬਾਰੇ ਵੀ ਤਾਜ਼ਾ ਜਾਣਕਾਰੀ ਰੱਖ ਸਕਦੇ ਹੋ। cyber.gov.au
'ਤੇ 'ACSC ਚੇਤਾਵਨੀ ਸੇਵਾ ਲਈ ਸਬਸਕ੍ਰਾਈਬ ਕਰੋ' ਖੋਜੋ ਜਦੋਂ ਅਸੀਂ ਕਿਸੇ ਨਵੇਂ ਸਾਈਬਰ ਖ਼ਤਰੇ ਦੀ ਪਛਾਣ ਕਰਦੇ ਹਾਂ ਤਾਂ ਅਸੀਂ ਤੁਹਾਨੂੰ ਇੱਕ ਚੇਤਾਵਨੀ ਭੇਜਾਂਗੇ।

ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਕੁੱਝ ਵੀ ਸਾਂਝਾ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਰੁਕੋ ਅਤੇ ਸੋਚੋ

ਸਾਈਬਰ ਅਪਰਾਧੀ ਤੁਹਾਡੇ ਦੁਆਰਾ ਜਨਤਕ ਤੌਰ 'ਤੇ ਤੁਹਾਡੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤਿਆਂ 'ਤੇ ਪੋਸਟ ਕੀਤੀ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਆਪਣੀ ਧੋਖਾਧੜੀ ਅਤੇ ਸਾਈਬਰ-ਹਮਲਿਆਂ ਵਿੱਚ ਕਰ ਸਕਦੇ ਹਨ।

ਯਾਦ ਰੱਖੋ ਕਿ ਇੰਟਰਨੈੱਟ 'ਤੇ ਜਾਣਕਾਰੀ ਹਮੇਸ਼ਾ ਲਈ ਹੁੰਦੀ ਹੈ ਅਤੇ ਤੁਸੀਂ ਜੋ ਪੋਸਟ ਕੀਤਾ ਗਿਆ ਹੈ ਉਸ ਨੂੰ ਤੁਸੀਂ ਕਦੇ ਵੀ ਪੂਰੀ ਤਰ੍ਹਾਂ ਹਟਾ ਨਹੀਂ ਸਕਦੇ ਹੋ।



ਮੈਂ ਪੋਸਟ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਕਿਵੇਂ ਰੁਕਾਂ ਅਤੇ ਸੋਚਾਂ?

- **ਸੋਚੋ:** ਕਿ ਕੋਈ ਸਾਈਬਰ ਅਪਰਾਧੀ ਮੈਨੂੰ ਜਾਂ ਮੇਰੇ ਖਾਤਿਆਂ ਨੂੰ ਨਿਸ਼ਾਨਾ ਬਣਾਉਣ ਲਈ ਇਸ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਕਿਵੇਂ ਕਰ ਸਕਦਾ ਹੈ?
- **ਸੋਚੋ:** ਕੀ ਮੈਂ ਬਿਲਕੁਲ ਅਜਨਬੀ ਵਿਅਕਤੀ ਨੂੰ ਇਹ ਜਾਣਕਾਰੀ ਜਾਂ ਚਿੱਤਰ ਔਫਲਾਈਨ ਦਿਖਾਉਣ ਵਿੱਚ ਸਹਿਜ ਹਾਂ?

ਮੈਨੂੰ ਕਿਹੜੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨ ਤੋਂ ਬਚਣਾ ਚਾਹੀਦਾ ਹੈ?

(ਫ਼ੋਟੋਆਂ ਸਮੇਤ) ਜਾਣਕਾਰੀ ਨੂੰ ਔਨਲਾਈਨ ਸਾਂਝਾ ਕਰਨ ਤੋਂ ਬਚੋ ਜਿਸਦੀ ਵਰਤੋਂ ਸਾਈਬਰ ਅਪਰਾਧੀ ਤੁਹਾਡੀ ਪਛਾਣ ਕਰਨ, ਕਿਸੇ ਧੋਖਾਧੜੀ ਰਾਹੀਂ ਤੁਹਾਡੇ ਨਾਲ ਹੇਰਾਫੇਰੀ ਕਰਨ ਜਾਂ ਤੁਹਾਡੇ ਖਾਤੇ ਨੂੰ ਬਰਾਮਦ ਕਰਨ ਵਾਲੇ (ਰਿਕਵਰੀ) ਸਵਾਲਾਂ ਦਾ ਅੰਦਾਜ਼ਾ ਲਗਾਉਣ ਲਈ ਕਰ ਸਕਦੇ ਹਨ। ਇਸ ਵਿੱਚ ਤੁਹਾਡੀ ਇਹ ਜਾਣਕਾਰੀ ਸ਼ਾਮਲ ਹੋ ਸਕਦੀ ਹੈ:

- ਜਨਮ ਸਥਾਨ ਅਤੇ ਜਨਮ ਮਿਤੀ।
- ਪਤਾ ਅਤੇ ਫ਼ੋਨ ਨੰਬਰ।
- ਰੁਜ਼ਗਾਰਦਾਤਾ ਅਤੇ ਨੌਕਰੀ ਸੰਬੰਧੀ ਪੁਰਾਣੀ ਜਾਣਕਰੀ।
- ਜਿੱਥੇ ਤੁਸੀਂ ਸਕੂਲ ਗਏ ਸੀ।
- ਕੋਈ ਹੋਰ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਜੋ ਤੁਹਾਨੂੰ ਨਿਸ਼ਾਨਾ ਬਣਾਉਣ ਲਈ ਵਰਤੀ ਜਾ ਸਕਦੀ ਹੈ।

ਸੰਖੇਪ ਚੈੱਕ-ਲਿਸਟ

ਕੀ ਤੁਸੀਂ ਇਸ ਗਾਈਡ ਵਿੱਚ ਦੱਸਿਆ ਸਭ ਕੁੱਝ ਕਰ ਲਿਆ ਹੈ?

ਅਜਿਹਾ ਕਰਨ ਵਿੱਚ ਆਪਣੀ ਪ੍ਰਗਤੀ ਦਾ ਪਤਾ ਰੱਖਣ ਲਈ ਇਸ ਸੌਖੀ ਚੈੱਕਲਿਸਟ ਦੀ ਵਰਤੋਂ ਕਰੋ:

- **ਮੈਂ ਆਪਣੇ ਸਾਰੇ ਯੰਤਰਾਂ ਲਈ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ ਚਾਲੂ ਕਰ ਦਿੱਤੇ ਹਨ:**
  - ਕੰਪਿਊਟਰ (ਡੈਸਕਟਾਪ ਅਤੇ ਲੈਪਟਾਪ),
  - ਮੋਬਾਇਲ ਫ਼ੋਨ,
  - ਟੈਬਲੇਟ।
- **ਮੈਂ ਆਪਣੇ ਸਭ ਤੋਂ ਵੱਧ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ 'ਤੇ ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ ਨੂੰ ਚਾਲੂ ਕਰ ਦਿੱਤਾ ਹੈ:**
  - ਮੇਰੇ ਸਾਰੇ ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਅਤੇ ਵਿੱਤੀ ਖਾਤਿਆਂ 'ਤੇ (ਜਿਵੇਂ ਕਿ ਬੈਂਕ, PayPal)
  - ਮੇਰੇ ਸਾਰੇ ਈਮੇਲ ਖਾਤਿਆਂ 'ਤੇ (ਜਿਵੇਂ ਕਿ Gmail, Outlook, Hotmail, Yahoo!)
- **ਮੈਂ ਬਾਕਾਇਦਾ ਤੌਰ 'ਤੇ ਆਪਣੇ ਯੰਤਰਾਂ ਦਾ ਬੈਕਅੱਪ ਲੈਂਦਾ/ਦੀ ਹਾਂ:**
  - ਕੰਪਿਊਟਰ (ਡੈਸਕਟਾਪ ਅਤੇ ਲੈਪਟਾਪ),
  - ਮੋਬਾਇਲ ਫ਼ੋਨ,
  - ਟੈਬਲੇਟ।
- **ਮੈਂ ਆਪਣੇ ਸਭ ਤੋਂ ਵੱਧ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ 'ਤੇ ਵਿਲੱਖਣ ਮਜ਼ਬੂਤ ਪਾਸਫਰੇਜ਼ ਦੀ ਵਰਤੋਂ ਕਰਦਾ/ਦੀ ਹਾਂ ਜੋ MFA ਦੁਆਰਾ ਸੁਰੱਖਿਅਤ ਨਹੀਂ ਹਨ:**
  - ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਅਤੇ ਵਿੱਤੀ ਖਾਤੇ।
  - ਈਮੇਲ ਖਾਤੇ।
- **ਮੈਂ ਆਪਣੇ ਮੋਬਾਈਲ ਯੰਤਰਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰ ਲਿਆ ਹੈ:**
  - ਲੈਪਟਾਪ,
  - ਮੋਬਾਇਲ ਫ਼ੋਨ,
  - ਟੈਬਲੇਟ।
- **ਮੈਂ ਰੋਜ਼ਾਨਾ ਸਾਈਬਰ ਸੁਰੱਖਿਅਤ ਸੋਚ ਦੀ ਵਰਤੋਂ ਕਰਦਾ/ਦੀ ਹਾਂ:**
  - ਮੈਂ ਧੋਖਾਧੜੀ ਵਾਲੇ ਸੁਨੇਹਿਆਂ ਨੂੰ ਪਛਾਣ ਸਕਦਾ/ਦੀ ਹਾਂ।
  - ਮੈਨੂੰ ਪਤਾ ਹੈ ਕਿ ਜੇਕਰ ਮੈਨੂੰ ਕੋਈ ਧੋਖਾਧੜੀ ਕਰਨ ਵਾਲਾ ਸੁਨੇਹਾ ਮਿਲਦਾ ਹੈ ਤਾਂ ਕੀ ਕਰਨਾ ਹੈ।
  - ਜੇਕਰ ਮੈਨੂੰ ਪੂਰਾ ਯਕੀਨ ਨਹੀਂ ਹੈ ਤਾਂ ਮੈਨੂੰ ਪਤਾ ਹੈ ਕਿ ਇਹ ਕਿਵੇਂ ਚੈੱਕ ਕਰਨਾ ਹੈ ਕਿ ਕੀ ਕੋਈ ਸੁਨੇਹਾ ਧੋਖਾਧੜੀ ਹੈ
  - ਮੈਂ ਲਿੰਕਾਂ ਅਤੇ ਅਟੈਚਮੈਂਟਾਂ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸੋਚਦਾ/ਦੀ ਹਾਂ।
  - ਮੈਂ ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਕੁੱਝ ਵੀ ਸਾਂਝਾ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸੋਚਦਾ/ਦੀ ਹਾਂ।
- **ਮੈਨੂੰ ਪਤਾ ਹੈ ਕਿ ਜੇਕਰ ਮੈਂ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਜਾਂ ਧੋਖਾਧੜੀ ਦਾ ਸ਼ਿਕਾਰ ਹੋ ਗਿਆ/ਗਈ ਹਾਂ ਤਾਂ ਸਹਾਇਤਾ ਕਿੱਥੋਂ ਪ੍ਰਾਪਤ ਕਰਨੀ ਹੈ।**

ਸ਼ਬਦਾਵਲੀ

ਖਾਤਾ ਰਿਕਵਰੀ।
ਇੱਕ ਅਜਿਹੀ ਪ੍ਰਕਿਰਿਆ ਜਿਸ ਵਿੱਚ ਸਵਾਲਾਂ ਦੀ ਇੱਕ ਲੜੀ ਜਾਂ ਹੋਰ ਤਸਦੀਕ ਵਿਧੀਆਂ ਦੀ ਵਰਤੋਂ ਕਿਸੇ ਖਾਤੇ ਤੱਕ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰਨ ਜਾਂ ਮੁੜ ਬਰਾਮਦ ਕਰਨ ਲਈ ਜਾਂ ਖਾਤਾ ਪਾਸਫਰੇਜ਼/ਪਾਸਵਰਡ ਬਦਲਣ ਲਈ ਕੀਤੀ ਜਾਂਦੀ ਹੈ।

ਮਾਲਵੇਅਰ।
ਕਿਸੇ ਉਪਭੋਗਤਾ ਦੇ ਕੰਪਿਊਟਰ ਤੱਕ ਅਣਅਧਿਕਾਰਤ ਪਹੁੰਚ ਅਤੇ ਕੰਟਰੋਲ ਪ੍ਰਾਪਤ ਕਰਨ, ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰਨ ਅਤੇ ਨੈੱਟਵਰਕਾਂ ਨੂੰ ਵਿਗਾੜਨ ਜਾਂ ਚੱਲਣ ਤੋਂ ਅਸਮਰੱਥ ਬਣਾਉਣ ਲਈ ਵਰਤਿਆ ਜਾਣ ਵਾਲਾ ਖ਼ਤਰਨਾਕ ਸਾਫ਼ਟਵੇਅਰ ਹੁੰਦਾ ਹੈ।

ਐਪ।
ਇੱਕ ਮੋਬਾਈਲ ਐਪਲੀਕੇਸ਼ਨ ਵਜੋਂ ਵੀ ਜਾਣਿਆ ਜਾਂਦਾ ਹੈ, ਐਪ ਅਜਿਹੇ ਸਾਫ਼ਟਵੇਅਰ ਲਈ ਇੱਕ ਸ਼ਬਦ ਹੈ ਜੋ ਆਮ ਤੌਰ 'ਤੇ ਸਮਾਰਟਫ਼ੋਨ ਜਾਂ ਟੈਬਲੇਟ ਲਈ ਵਰਤਿਆ ਜਾਂਦਾ ਹੈ।

ਅਟੈਚਮੈਂਟ।
ਈਮੇਲ ਸੁਨੇਹੇ ਨਾਲ ਭੇਜੀ ਗਈ ਕੋਈ ਫਾਈਲ ਹੁੰਦੀ ਹੈ।

ਆਪਰੇਟਿੰਗ ਸਿਸਟਮ।
ਕੰਪਿਊਟਰ ਦੀ ਹਾਰਡ ਡਰਾਈਵ 'ਤੇ ਇੰਸਟਾਲ ਕੀਤਾ ਗਿਆ ਸਾਫ਼ਟਵੇਅਰ ਜੋ ਕੰਪਿਊਟਰ ਹਾਰਡਵੇਅਰ ਨੂੰ ਕੰਪਿਊਟਰ ਪ੍ਰੋਗਰਾਮਾਂ ਨਾਲ ਸੰਚਾਰ ਕਰਨ ਅਤੇ ਚੱਲਣ ਯੋਗ ਬਣਾਉਂਦਾ ਹੈ। ਉਦਾਹਰਨਾਂ: Microsoft Windows, Apple macOS, iOS, Android।

ਭੌਤਿਕ ਟੋਕਨ।
ਇੱਕ ਭੌਤਿਕ ਯੰਤਰ ਹੁੰਦਾ ਹੈ ਜੋ ਆਮ ਤੌਰ 'ਤੇ ਕਿਸੇ ਚਾਬੀ ਵਾਲੇ ਛੱਲੇ ਵਿੱਚ ਫਿੱਟ ਹੋ ਸਕਦਾ ਹੈ, ਜੋ MFA ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋਏ ਕੰਪਿਊਟਰ ਉਪਭੋਗਤਾ ਦੀ ਪਛਾਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰਨ ਲਈ ਵਰਤਿਆ ਜਾਣ ਵਾਲਾ ਸੁਰੱਖਿਆ ਕੋਡ ਤਿਆਰ ਕਰਦਾ ਹੈ।

ਪੁਸ਼ਟੀਕਰਨ ਐਪ।
ਇੱਕ ਅਜਿਹਾ ਐਪ ਜੋ ਮਲਟੀ-ਫੈਕਟਰ ਪ੍ਰਮਾਣਿਕਤਾ (MFA) ਦੁਆਰਾ ਪਹੁੰਚ ਦੀ ਆਗਿਆ ਦੇਣ ਲਈ ਕੰਪਿਊਟਰ ਉਪਭੋਗਤਾ ਦੀ ਪਛਾਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰਨ ਲਈ ਵਰਤਿਆ ਜਾਂਦਾ ਹੈ।

ਕਲਾਉਡ।
ਰਿਮੋਟ ਸਰਵਰਾਂ ਦਾ ਇੱਕ ਨੈੱਟਵਰਕ ਹੁੰਦਾ ਹੈ ਜੋ ਵਿਸ਼ਾਲ, ਕਈ ਹਿੱਸਿਆਂ ਵਿੱਚ ਵੰਡੀ ਗਈ ਸਟੋਰੇਜ ਅਤੇ ਪ੍ਰੋਸੈਸਿੰਗ ਪਾਵਰ ਪ੍ਰਦਾਨ ਕਰਦਾ ਹੈ।

ਰਿਮੋਟ ਪਹੁੰਚ।
ਅੰਫ਼ਸਾਈਟ ਟਿਕਾਣੇ ਤੋਂ ਯੰਤਰਾਂ ਅਤੇ ਨੈੱਟਵਰਕਾਂ 'ਤੱਕ ਪਹੁੰਚ ਅਤੇ ਕੰਟਰੋਲ ਦਿੰਦਾ ਹੈ।

ਸਾਈਬਰ ਅਪਰਾਧੀ।
ਕੋਈ ਵੀ ਵਿਅਕਤੀ ਜੋ ਜਾਣਕਾਰੀ ਨੂੰ ਨੁਕਸਾਨ ਪਹੁੰਚਾਉਣ ਜਾਂ ਚੋਰੀ ਕਰਨ ਲਈ ਗੈਰ-ਕਾਨੂੰਨੀ ਤੌਰ 'ਤੇ ਕੰਪਿਊਟਰ ਸਿਸਟਮ ਜਾਂ ਖਾਤੇ ਤੱਕ ਪਹੁੰਚ ਕਰਦਾ ਹੈ।

ਯੰਤਰ।
ਕੋਈ ਵੀ ਕੰਪਿਊਟਿੰਗ ਜਾਂ ਸੰਚਾਰ ਯੰਤਰ। ਉਦਾਹਰਨ ਲਈ, ਕੰਪਿਊਟਰ, ਲੈਪਟਾਪ, ਮੋਬਾਈਲ ਫ਼ੋਨ ਜਾਂ ਟੈਬਲੇਟ।

ਸਾਫ਼ਟਵੇਅਰ।
ਇਸ ਨੂੰ ਆਮ ਤੌਰ 'ਤੇ ਪ੍ਰੋਗਰਾਮਾਂ ਵਜੋਂ ਜਾਣਿਆ ਜਾਂਦਾ ਹੈ,ਜੋ ਹਦਾਇਤਾਂ ਦਾ ਸੰਗ੍ਰਹਿ ਹੁੰਦਾ ਹੈ ਜੋ ਉਪਭੋਗਤਾ ਨੂੰ ਕੰਪਿਊਟਰ, ਇਸਦੇ ਹਾਰਡਵੇਅਰ ਜਾਂ ਇਸ ਉੱਪਰ ਕੰਮ ਕਰਨ ਦੇ ਯੋਗ ਬਣਾਉਂਦਾ ਹੈ।

ਸਮਰਥਨ ਦਾ ਅੰਤ
ਸਮਰਥਨ ਦਾ ਅੰਤ ਇੱਕ ਅਜਿਹੀ ਸਥਿਤੀ ਨੂੰ ਦਰਸਾਉਂਦਾ ਹੈ ਜਿਸ ਵਿੱਚ ਕੋਈ ਕੰਪਨੀ ਕਿਸੇ ਉਤਪਾਦ ਜਾਂ ਸੇਵਾ ਦਾ ਸਮਰਥਨ ਕਰਨਾ ਬੰਦ ਕਰ ਦਿੰਦੀ ਹੈ। ਇਹ ਆਮ ਤੌਰ 'ਤੇ ਹਾਰਡਵੇਅਰ ਅਤੇ ਸਾਫ਼ਟਵੇਅਰ ਉਤਪਾਦਾਂ 'ਤੇ ਲਾਗੂ ਹੁੰਦਾ ਹੈ ਜਦੋਂ ਕੋਈ ਕੰਪਨੀ ਨਵਾਂ ਰੂਪ ਜਾਰੀ ਕਰਦੀ ਹੈ ਅਤੇ ਪਿਛਲੇ ਰੂਪਾਂ ਲਈ ਸਮਰਥਨ ਖ਼ਤਮ ਕਰਦੀ ਹੈ।

ਬੇਦਾਅਵਾ

ਇਸ ਗਾਈਡ ਵਿਚਲੀ ਸਮੱਗਰੀ ਆਮ ਜਾਣਕਾਰੀ ਲਈ ਹੈ ਅਤੇ ਇਸਨੂੰ ਕਾਨੂੰਨੀ ਸਲਾਹ ਨਹੀਂ ਮੰਨਿਆ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ ਜਾਂ ਇਸ ਉੱਪਰ ਕਿਸੇ ਖ਼ਾਸ ਸਥਿਤੀ ਜਾਂ ਐਮਰਜੈਂਸੀ ਦੀ ਸਥਿਤੀ ਵਿੱਚ ਸਹਾਇਤਾ ਲਈ ਨਿਰਭਰ ਨਹੀਂ ਰਿਹਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ। ਕਿਸੇ ਵੀ ਮਹੱਤਵਪੂਰਨ ਮਾਮਲੇ ਵਿੱਚ, ਤੁਹਾਨੂੰ ਆਪਣੇ ਹਾਲਾਤਾਂ ਦੇ ਸੰਬੰਧ ਵਿੱਚ ਢੁੱਕਵੀਂ ਆਤਮ-ਨਿਰਭਰ ਪੇਸ਼ੇਵਰ ਸਲਾਹ ਲੈਣੀ ਚਾਹੀਦੀ ਹੈ।

ਇਸ ਗਾਈਡ ਵਿੱਚ ਸ਼ਾਮਲ ਜਾਣਕਾਰੀ 'ਤੇ ਨਿਰਭਰਤਾ ਦੇ ਨਤੀਜੇ ਵਜੋਂ ਹੋਏ ਕਿਸੇ ਵੀ ਨੁਕਸਾਨ, ਘਾਟੇ ਜਾਂ ਖ਼ਰਚੇ ਲਈ ਕਾਮਨਵੈਲਥ ਕੋਈ ਵੀ ਜ਼ਿੰਮੇਵਾਰੀ ਜਾਂ ਦੇਣਦਾਰੀ ਸਵੀਕਾਰ ਨਹੀਂ ਕਰਦਾ ਹੈ।

ਵਧੇਰੇ ਜਾਣਕਾਰੀ ਲਈ, ਜਾਂ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਘਟਨਾ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਲਈ, ਸਾਡੇ ਨਾਲ ਸੰਪਰਕ ਕਰੋ:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ਇਹ ਨੰਬਰ ਸਿਰਫ਼ ਆਸਟ੍ਰੇਲੀਆ ਵਿੱਚ ਵਰਤੋਂ ਲਈ ਉਪਲਬਧ ਹੈ।

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre