ਆਸਟ੍ਰੇਲੀਆ ਦੀ ਸੁਰੱਖਿਆ ਨੂੰ ਕਾਇਮ ਰੱਖਣ ਲਈ ਸਾਈਬਰ-ਹਮਲੇ ਅਤੇ ਘਟਨਾਵਾਂ ਦੀ ਰਿਪੋਰਟ ਕਰੋ।

ਸਾਇਨ ਅੱਪ ਕਰੋ

ਸਾਡੀ ਮੁਫਤ ਚੇਤਾਵਨੀ ਸੇਵਾ ਲਈ

cyber.gov.au

ਰਿਪੋਰਟ ਕਰੋ

ਸਾਈਬਰ ਅਪਰਾਧ ਨੂੰ ਰਿਪੋਰਟਸਾਈਬਰ 'ਤੇ:

cyber.gov.au/report

ਸੰਪਰਕ ਕਰੋ

1300 CYBER1 'ਤੇ ਫੋਨ ਕਰੋ ਜਾਂ

cyber.gov.au 'ਤੇ ਜਾਉ

ਇਹ ਨੰਬਰ ਸਿਰਫ਼ ਆਸਟ੍ਰੇਲੀਆ ਵਿੱਚ ਵਰਤੋਂ ਲਈ ਉਪਲਬਧ ਹੈ।

ਸਾਨੂੰ ਫਾਲੋ ਕਰੋ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. ਘੁਟਾਲਿਆਂ 'ਤੇ ਧਿਆਨ ਰੱਖੋ

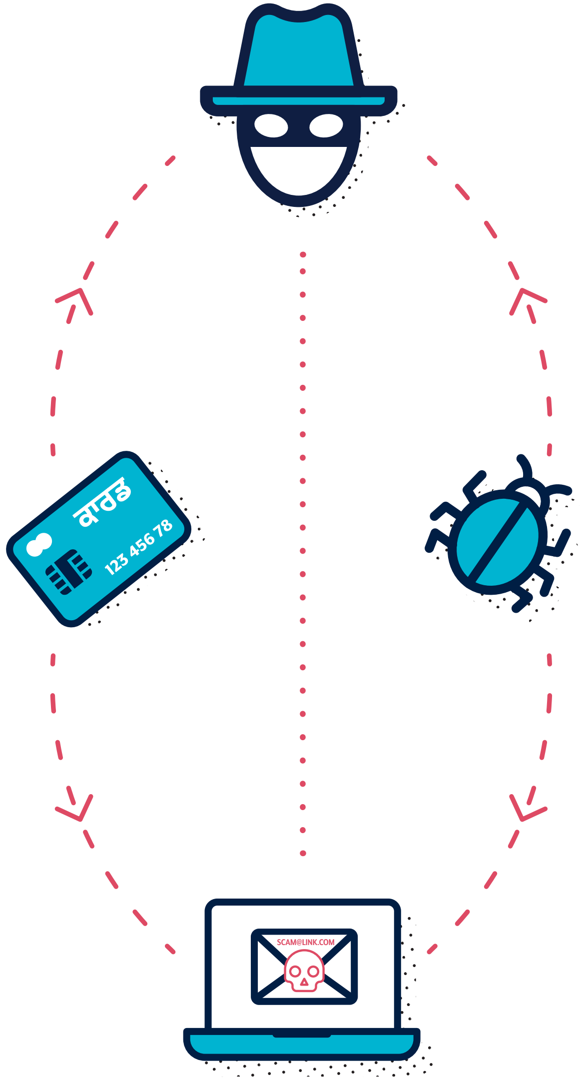
ਸਾਈਬਰ ਅਪਰਾਧੀ ਈਮੇਲ, ਐਸ ਐਮ ਐਸ, ਫ਼ੋਨ ਕਾਲਾਂ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਦੀ ਵਰਤੋਂ ਤੁਹਾਨੂੰ ਅਟੈਚਮੈਂਟ ਖੋਲ੍ਹਣ, ਵੈਬਸਾਈਟ 'ਤੇ ਜਾਣ, ਖਾਤੇ ਦੇ ਲੌਗ-ਇਨ ਵੇਰਵਿਆਂ ਦਾ ਖੁਲਾਸਾ ਕਰਨ, ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਦਾ ਖੁਲਾਸਾ ਕਰਨ ਜਾਂ ਪੈਸੇ ਜਾਂ ਗਿਫਟ ਕਾਰਡਾਂ ਨੂੰ

ਘੁਟਾਲੇ ਵਾਲੇ ਸੰਦੇਸ਼ਾਂ ਦੀ ਪਛਾਣ ਕਰਨ ਲਈ, ਰੁਕੋ ਅਤੇ ਸੋਚੋ:

- **ਅਥਾਰਟੀ:** ਕੀ ਸੁਨੇਹਾ ਕਿਸੇ ਅਧਿਕਾਰੀ ਵੱਲੋਂ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰ ਰਿਹਾ ਹੈ?
- **ਜ਼ਰੂਰੀ:** ਕੀ ਤੁਹਾਨੂੰ ਦੱਸਿਆ ਗਿਆ ਹੈ ਕਿ ਤੁਹਾਡੇ ਕੋਲ ਜਵਾਬ ਦੇਣ ਲਈ ਸੀਮਤ ਸਮਾਂ ਹੈ?
- **ਭਾਵਨਾ:** ਕੀ ਸੁਨੇਹਾ ਤੁਹਾਨੂੰ ਦਹਿਸ਼ਤ ਦੇਂਦਾ ਹੈ, ਡਰਾਉਂਦਾ ਹੈ, ਆਸ਼ਾਵਾਦੀ ਜਾਂ ਉਤਸੁਕ ਬਣਾਉਂਦਾ ਹੈ?
- **ਕਮੀ:** ਕੀ ਸੁਨੇਹਾ ਘੱਟ ਪੂਰਤੀ ਵਾਲੀ ਕਿਸੇ ਚੀਜ਼ ਦੀ ਪੇਸ਼ਕਸ਼ ਕਰ ਰਿਹਾ ਹੈ?
- **ਮੌਜੂਦਾ ਘਟਨਾਵਾਂ:** ਕੀ ਉਹ ਸੁਨੇਹਾ ਮੌਜੂਦਾ ਖ਼ਬਰਾਂ, ਵੱਡੀਆਂ ਘਟਨਾਵਾਂ ਜਾਂ ਸਾਲ ਦੇ ਖ਼ਾਸ ਸਮੇਂ (ਜਿਵੇਂ ਕਿ ਟੈਕਸ ਰਿਪੋਰਟ ਕਰਨ ਦੇ ਸਮੇਂ) ਨਾਲ ਸੰਬੰਧਿਤ ਹੈ?

ਇਹ ਦੇਖਣ ਲਈ ਕਿ, ਕੀ ਸੁਨੇਹਾ ਜਾਇਜ਼ ਹੈ:

- ਉਸ ਚੀਜ਼ 'ਤੇ ਵਾਪਸ ਜਾਓ ਜਿਸ ਤੇ ਤੁਸੀਂ ਭਰੋਸਾ ਕਰ ਸਕਦੇ ਹੋ। ਅਧਿਕਾਰਤ ਵੈਬਸਾਈਟ ਤੇ ਜਾਉ, ਆਪਣੇ ਖਾਤੇ ਵਿੱਚ ਲੌਗ-ਇਨ ਕਰੋ, ਜਾਂ ਉਨ੍ਹਾਂ ਦੇ ਇਸ਼ਤਿਹਾਰਿਤ ਫ਼ੋਨ ਨੰਬਰ 'ਤੇ ਫ਼ੋਨ ਕਰੋ। ਤੁਹਾਨੂੰ ਭੇਜੇ ਗਏ ਸੰਦੇਸ਼ ਵਿੱਚਲੇ ਲਿੰਕਾਂ ਜਾਂ ਸੰਪਰਕ ਵੇਰਵਿਆਂ ਜਾਂ ਫੋਨ ਤੇ ਦਿੱਤੇ ਗਏ ਵੇਰਵਿਆਂ ਦੀ ਵਰਤੋਂ ਨਾ ਕਰੋ।
- ਇਹ ਵੇਖਣ ਲਈ ਜਾਂਚ ਕਰੋ ਕੀ ਜੇ ਅਧਿਕਾਰਤ ਸਰੋਤ ਨੇ ਤੁਹਾਨੂੰ ਪਹਿਲਾਂ ਹੀ ਦੱਸ ਦਿੱਤਾ ਹੈ ਕਿ ਉਹ ਤੁਹਾਨੂੰ ਕਿਸ ਬਾਰੇ ਕਦੇ ਨਹੀਂ ਪੁੱਛਣਗੇ। ਉਦਾਹਰਣ ਦੇ ਲਈ, ਸ਼ਾਇਦ ਤੁਹਾਡੇ ਬੈਂਕ ਨੇ ਤੁਹਾਨੂੰ ਦੱਸਿਆ ਹੋਵੇ ਕਿ ਉਹ ਕਦੇ ਵੀ ਤੁਹਾਡਾ ਪਾਸਵਰਡ ਨਹੀਂ ਮੰਗਣਗੇ।



ਘੁਟਾਲੇ ਦੇ ਸੰਦੇਸ਼ਾਂ ਨੂੰ ਪਛਾਣਨ ਬਾਰੇ ਵਧੇਰੇ ਜਾਣਕਾਰੀ ਲਈ, ਆਸਟ੍ਰੇਲੀਅਨ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਕੇਂਦਰ (ਏ ਸੀ ਐਸ ਸੀ) ਦਾ ਸੋਸ਼ਲੀ ਇੰਜੀਨੀਅਰਡ ਸੰਦੇਸ਼ਾਂ ਬਾਰੇ ਪਤਾ ਲਗਾਉਣ ਉੱਪਰ ਪ੍ਰਕਾਸ਼ਨ ਵੇਖੋ, ਅਤੇ **cyber.gov.au** 'ਤੇ ਏ ਸੀ ਐਸ ਸੀ ਦੀ ਚੇਤਾਵਨੀ ਸੇਵਾ 'ਤੇ ਸਾਈਨ ਅੱਪ ਕਰਕੇ ਸੂਚਿਤ ਰਹੋ।

ਅਸਾਨ ਕਦਮ

ਆਪਣੇ ਉਪਕਰਣਾਂ ਅਤੇ ਖਾਤਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਲਈ

ਇਨ੍ਹਾਂ ਕਦਮਾਂ ਦੀ ਪਾਲਣਾ ਕਰਦਿਆਂ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਦੁਆਰਾ ਨਿਸ਼ਾਨਾ ਬਣਨ ਦੇ ਜੋਖਮ ਨੂੰ ਘਟਾਓ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. ਆਪਣੇ ਉਪਕਰਣਾਂ ਨੂੰ ਅੱਪਡੇਟ ਕਰੋ

ਸਾਈਬਰ ਅਪਰਾਧੀ ਸਿਸਟਮ ਜਾਂ ਐਪਸ ਵਿੱਚ ਜਾਣੂ ਕਮਜ਼ੋਰੀਆਂ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋਏ ਉਪਕਰਣਾਂ ਨੂੰ ਹੈਕ ਕਰਦੇ ਹਨ। ਇਨ੍ਹਾਂ ਕਮਜ਼ੋਰੀਆਂ ਨੂੰ ਠੀਕ ਕਰਨ ਲਈ ਅੱਪਡੇਟਾਂ ਵਿੱਚ ਸੁਰੱਖਿਆ ਅੱਪਗ੍ਰੇਡ ਹੁੰਦੇ ਹਨ। ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਾਂ ਨੂੰ ਚਾਲੂ ਕਰੋ ਤਾਂ ਜੋ ਇਹ ਤੁਹਾਡੇ ਵੱਲੋਂ ਬਿਨ੍ਹਾਂ ਕੁੱਝ ਕੀਤੇ ਹੋ ਜਾਵੇ।

ਆਪਣੇ ਸਾਰੇ ਉਪਕਰਨਾਂ ਤੇ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਸ ਚਾਲੂ ਕਰੋ:

- ਮੋਬਾਇਲ ਫੋਨ
- ਲੈਪਟਾਪ
- ਡੈਸਕਟਾਪ

ਅੱਪਡੇਟਾਂ ਲਈ ਨਿਯਮਤ ਤੌਰ ‘ਤੇ ਜਾਂਚ ਕਰੋ, ਆਪਣੇ:

- ਐਪਸ
- ਪ੍ਰੋਗਰਾਮਾਂ
- ਸਮਾਰਟ ਉਪਕਰਣਾਂ ਲਈ

2. ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ (MFA) ਨੂੰ ਚਾਲੂ ਕਰੋ

ਐਮ ਐਫ ਏ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਤੁਹਾਡੀਆਂ ਫਾਈਲਾਂ ਜਾਂ ਖਾਤੇ ਤੱਕ ਪਹੁੰਚਣ ਵਿੱਚ ਮੁਸ਼ਕਲ ਵਧਾ ਕੇ ਤੁਹਾਡੀ ਸੁਰੱਖਿਆ ਵਿੱਚ ਸੁਧਾਰ ਕਰਦਾ ਹੈ

ਐਮ ਐਫ ਏ ਨੂੰ ਚਾਲੂ ਕਰੋ, ਆਪਣੇ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ ਨਾਲ ਇਸਦਾ ਅਰੰਭ ਕਰੋ:

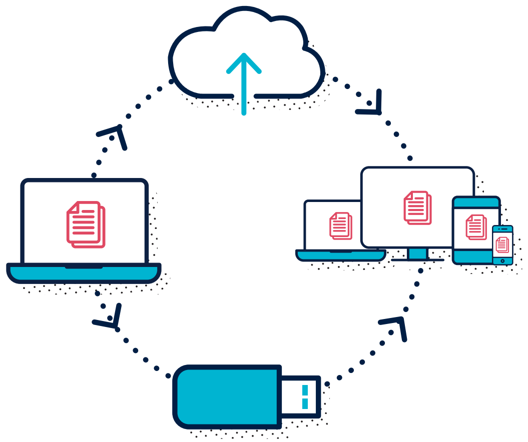
- ਈਮੇਲ ਖਾਤੇ
- ਆਨਲਾਈਨ ਬੈਂਕਿੰਗ ਅਤੇ ਉਹ ਖਾਤੇ ਜਿਸ ਵਿੱਚ ਭੁਗਤਾਨ ਦੇ ਵੇਰਵੇ ਰੱਖੇ ਹਨ
- ਸੋਸ਼ਲ ਮੀਡੀਆ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ

3. ਆਪਣੇ ਉਪਕਰਣਾਂ ਦਾ ਬੈਕਅੱਪ ਲਓ

ਬੈਕਅੱਪ ਤੁਹਾਡੇ ਉਪਕਰਣ ਤੇ ਸਟੋਰ ਕੀਤੀ ਜਾਣਕਾਰੀ ਦੀ ਇੱਕ ਡਿਜ਼ਿਟਲ ਕਾਪੀ ਹੈ, ਜਿਵੇਂ ਕਿ ਫੋਟੋਆਂ, ਦਸਤਾਵੇਜ਼, ਵਿਡੀਓ ਅਤੇ ਐਪਲੀਕੇਸ਼ਨਾਂ ਤੋਂ ਡੈਟਾ। ਇਸਨੂੰ ਬਾਹਰੀ ਸਟੋਰੇਜ ਉਪਕਰਣਾਂ ਜਾਂ ਕਲਾਉਡ ‘ਤੇ ਸੁਰੱਖਿਅਤ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ। ਬੈਕਅੱਪ ਲੈਣ ਦਾ ਮਤਲਬ ਹੈ ਕਿ ਜੇ ਤੁਹਾਡਾ ਉਪਕਰਣ ਕਦੇ ਗੁੰਮ, ਚੋਰੀ ਜਾਂ ਖਰਾਬ ਹੋ ਜਾਂਦਾ ਹੈ ਤਾਂ ਤੁਸੀਂ ਆਪਣੀਆਂ ਫਾਈਲਾਂ ਨੂੰ ਮੁੜ-ਪ੍ਰਾਪਤ ਕਰ ਸਕਦੇ ਹੋ।

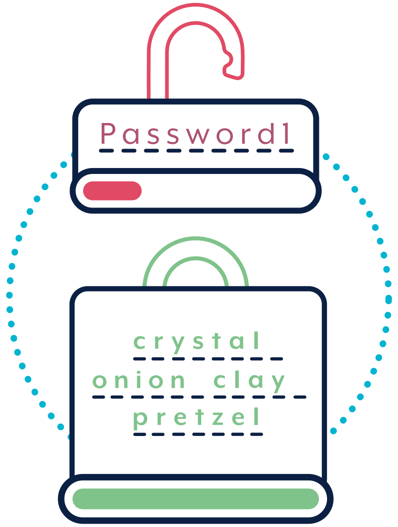
ਆਪਣੇ ਉਪਕਰਣਾਂ ਦਾ ਨਿਯਮਤ ਤੌਰ ਤੇ ਬੈਕਅੱਪ ਲਓ:

- ਮੋਬਾਇਲ ਫੋਨ
- ਲੈਪਟਾਪ
- ਡੈਸਕਟਾਪ
- ਟੈਬਲੇਟ



4. ਸੁਰੱਖਿਅਤ ਪਾਸਫਰੇਜ਼ (ਛੋਟੇ ਵਾਕ) ਸੈਟ ਕਰੋ

ਅਜਿਹੇ ਮਾਮਲਿਆਂ ਵਿੱਚ ਜਿੱਥੇ ਐਮ ਐਫ ਏ ਉਪਲਬਧ ਨਹੀਂ ਹੈ, ਇੱਕ ਸੁਰੱਖਿਅਤ ਪਾਸਫਰੇਜ਼ ਅਕਸਰ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਅਤੇ ਖਾਤਿਆਂ ਨੂੰ ਅਪਰਾਧੀਆਂ ਤੋਂ ਬਚਾਉਣ ਵਾਲੀ ਇਕੋ ਇੱਕ ਚੀਜ਼ ਹੋ ਸਕਦੀ ਹੈ।

ਇੱਕ ਪਾਸਫਰੇਜ਼ ਤੁਹਾਡੇ ਪਾਸਵਰਡ ਦੇ ਰੂਪ ਵਿੱਚ ਚਾਰ ਜਾਂ ਵਧੇਰੇ ਬੇਤਰਤੀਬੇ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਕਰਦਾ ਹੈ। ਆਪਣੇ ਪਾਸਵਰਡ ਨੂੰ ਪਾਸਫਰੇਜ਼ ਵਿੱਚ ਬਦਲੋ, ਇਹ ਸੁਨਿਸ਼ਚਿਤ ਕਰਦੇ ਹੋਏ ਕਿ ਉਹ:

- ਲੰਮਾ: ਤੁਹਾਡਾ ਪਾਸਫਰੇਜ਼ ਜਿੰਨਾ ਲੰਬਾ ਹੋਵੇਗਾ, ਉੱਨਾ ਹੀ ਵਧੀਆ ਹੋਵੇਗਾ। ਇਸਨੂੰ ਘੱਟੋ ਘੱਟ 14 ਅੱਖਰਾਂ ਦੀ ਲੰਬਾਈ ਵਿੱਚ ਬਣਾਉ।
- ਨਾ ਬੁੱਝਣ ਯੋਗ: ਗੈਰ ਸੰਬੰਧਤ ਸ਼ਬਦਾਂ ਦੇ ਬੇਤਰਤੀਬੇ ਮਿਸ਼ਰਣ ਦੀ ਵਰਤੋਂ ਕਰੋ
- ਵਿਲੱਖਣ: ਬਹੁਤੇ ਖਾਤਿਆਂ ‘ਤੇ ਪਾਸਫਰੇਜ਼ਾਂ ਦੀ ਦੁਬਾਰਾ ਵਰਤੋਂ ਨਾ ਕਰੋ