Australian Government

ਐਕਟ ਨਾਓ। ਸਟੇਅ ਸਿਕਓਰ।

ਆਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਕਿਵੇਂ ਰਹਿਣਾ ਹੈ

ਸੌਖੀ ਪੜ੍ਹਾਈ (ਅਸਾਨੀ ਨਾਲ ਪੜ੍ਹਿਆ ਜਾਣ) ਯੋਗ ਸੰਸਕਰਣ

Easy Read®

ਇਹ ਗਾਈਡ ਕਿਵੇਂ ਵਰਤਣੀ ਹੈ

ਅਸੀਂ ਆਸਟ੍ਰੇਲੀਆਈ ਸਰਕਾਰ ਹਾਂ।

ਅਸੀਂ ਇਹ ਗਾਈਡ ਲਿਖੀ ਹੈ।

ਅਸੀਂ ਕੁਝ ਸ਼ਬਦ **ਮੋਟੇ** ਅੱਖਰਾਂ ਵਿੱਚ ਲਿਖੇ ਹਨ।

ਅਸੀਂ ਦੱਸਦੇ ਹਾਂ ਕਿ ਇਹ ਸ਼ਬਦ ਕੀ ਮਤਲਬ ਰੱਖਦੇ ਹਨ।

ਪੰਨਾ 28 ‘ਤੇ ਇਹਨਾਂ ਸ਼ਬਦਾਂ ਦੀ ਇੱਕ ਸੂਚੀ ਵੀ ਹੈ।

ਤੁਸੀਂ ਕਿਸੇ ਭਰੋਸੇਯੋਗ ਵਿਅਕਤੀ ਤੋਂ ਮਦਦ ਮੰਗ ਸਕਦੇ ਹੋ ਤਾਂ ਜੋ ਉਹ:

- ਇਹ ਗਾਈਡ ਪੜ੍ਹੇ
- ਹੋਰ ਜਾਣਕਾਰੀ ਲੱਭੇ।

ਇਹ ਕਿਸੇ ਹੋਰ ਗਾਈਡ ਦਾ ਇੱਕ ਆਸਾਨ ਪੜ੍ਹਿਆ ਜਾਣ ਯੋਗ ਵਾਲਾ ਸਾਰ ਹੈ।

ਇਸ ਵਿੱਚ ਸਿਰਫ਼ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਨ ਹੀ ਸ਼ਾਮਲ ਕੀਤੇ ਗਏ ਹਨ।

ਤੁਸੀਂ ਸਾਡੀ ਵੈਬਸਾਈਟ ‘ਤੇ ਹੋਰ ਗਾਈਡ ਲੱਭ ਸਕਦੇ ਹੋ।

www.actnowstaysecure.gov.au

ਇਸ ਗਾਈਡ ਵਿੱਚ ਕੀ ਹੈ?

ਇਸ ਗਾਈਡ ਬਾਰੇ 4

ਆਪਣੇ ਖਾਤਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖੋ 6

ਆਪਣੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਲਈ ਆਪਣੀਆਂ ਸੈਟਿੰਗਾਂ ਦੀ ਜਾਂਚ ਕਰੋ 10

ਆਪਣੇ ਡਿਵਾਈਸਾਂ ਦੀ ਸੁਰੱਖਿਆ ਕਰੋ 16

ਧੋਖਾਧੜੀਆਂ (Scams) 20

ਆਵਾਜ਼ ਉਠਾਓ 25

ਸ਼ਬਦ ਸੂਚੀ 28

ਸਾਡੇ ਨਾਲ ਸੰਪਰਕ ਕਰੋ 30

ਇਸ ਗਾਈਡ ਬਾਰੇ

ਸਾਨੂੰ ਸਭ ਨੂੰ ਸੋਚਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਅਸੀਂ ਆਨਲਾਈਨ ਕਿਵੇਂ ਸੁਰੱਖਿਅਤ ਰਹਿ ਸਕਦੇ ਹਾਂ।

ਅਸੀਂ ਇਸਨੂੰ **ਸਾਈਬਰ** ਸੁਰੱਖਿਆ ਕਹਿੰਦੇ ਹਾਂ।

ਸਾਈਬਰ ਦਾ ਮਤਲਬ ਹੁੰਦਾ ਹੈ ਇੰਟਰਨੈੱਟ ਨਾਲ ਸੰਬੰਧਿਤ ਕੁਝ।

ਇਹ ਗਾਈਡ ਕੁਝ ਚੀਜ਼ਾਂ ਬਾਰੇ ਸਮਝਾਉਂਦੀ ਹੈ ਜੋ ਤੁਸੀਂ ਆਪਣੇ ਆਪ ਨੂੰ ਆਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਕਰ ਸਕਦੇ ਹੋ।

ਉਦਾਹਰਨ ਲਈ, **ਸਾਈਬਰ ਅਪਰਾਧ** ਤੋਂ ਬਚਾਅ ਲਈ।

ਸਾਈਬਰ ਅਪਰਾਧ ਉਹ ਹੁੰਦਾ ਹੈ ਜਦੋਂ ਅਪਰਾਧੀ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਜੁਰਮ ਕਰਦੇ ਹਨ।

ਉਦਾਹਰਨ ਲਈ, ਉਹ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦੇ ਹਨ:

- ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰਨ ਲਈ
- ਤੁਹਾਡੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਜਾਂ ਪ੍ਰੋਫ਼ਾਈਲਾਂ 'ਤੇ ਕਬਜ਼ਾ ਕਰਨ ਲਈ।

ਸਾਈਬਰ ਅਪਰਾਧ ਕਿਸੇ ਵੀ ਡਿਵਾਈਸ ‘ਤੇ ਹੋ ਸਕਦਾ ਹੈ।

ਇਸ ਵਿੱਚ ਸ਼ਾਮਲ ਹਨ ਤੁਹਾਡੇ:

- ਕੰਪਿਊਟਰ
- ਸਮਾਰਟਫੋਨ
- ਸਮਾਰਟ ਵਾਚ।

ਕੁਝ ਚੀਜ਼ਾਂ ਹਨ ਜੋ ਤੁਸੀਂ ਸਾਈਬਰ ਅਪਰਾਧ ਤੋਂ ਬਚਣ ਲਈ ਕਰ ਸਕਦੇ ਹੋ।

ਅਸੀਂ ਅਗਲੇ ਸਫ਼ਿਆਂ ‘ਤੇ ਸਮਝਾਉਂਦੇ ਹਾਂ ਕਿ ਤੁਸੀਂ ਕੀ ਕਰ ਸਕਦੇ ਹੋ।

ਆਪਣੇ ਖਾਤਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖੋ

ਤੁਹਾਨੂੰ ਸੋਚਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਤੁਸੀਂ ਆਪਣੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਨੂੰ ਕਿਵੇਂ ਸੁਰੱਖਿਅਤ ਰੱਖ ਸਕਦੇ ਹੋ।

ਮਜ਼ਬੂਤ ਅਤੇ ਵੱਖ-ਵੱਖ ਪਾਸਫ੍ਰੇਜ਼ ਵਰਤੋ

ਪਾਸਫ੍ਰੇਜ਼ ਪਾਸਵਰਡ ਦੀ ਇੱਕ ਹੋਰ ਮਜ਼ਬੂਤ ਕਿਸਮ ਹੁੰਦੀ ਹੈ।

ਇਸਦੇ ਬਾਰੇ ਹੋਰ ਲੋਕਾਂ ਵੱਲੋਂ ਅਨੁਮਾਨ ਲਗਾਉਣਾ ਬਹੁਤ ਔਖਾ ਹੁੰਦਾ ਹੈ।

ਮਜ਼ਬੂਤ ਅਤੇ ਵੱਖ-ਵੱਖ ਪਾਸਫ੍ਰੇਜ਼ ਵਰਤਣਾ ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਸਭ ਤੋਂ ਵਧੀਆ ਤਰੀਕਿਆਂ ਵਿੱਚੋਂ ਇੱਕ ਹੈ।

ਤੁਹਾਨੂੰ ਆਪਣੇ ਹਰ ਆਨਲਾਈਨ ਖਾਤੇ ਲਈ ਵੱਖਰਾ ਪਾਸਫ੍ਰੇਜ਼ ਵਰਤਣਾ ਚਾਹੀਦਾ ਹੈ।

ਮਜ਼ਬੂਤ ਪਾਸਫ੍ਰੇਜ਼ ਵਿੱਚ ਸ਼ਾਮਲ ਹੁੰਦੇ ਹਨ:

- 4 ਜਾਂ ਇਸ ਤੋਂ ਵੱਧ ਅਣਯੋਜਿਤ ਸ਼ਬਦ
- 15 ਜਾਂ ਇਸ ਤੋਂ ਵੱਧ ਅੱਖਰ ਅਤੇ ਅੰਕ।

ਤੁਸੀਂ ਕੁਝ ਵੱਡੇ ਅੱਖਰ (ਕੈਪਿਟਲ ਲੇਟਰ) ਵੀ ਸ਼ਾਮਲ ਕਰ ਸਕਦੇ ਹੋ।

ਤੁਸੀਂ ਚਿੰਨ੍ਹ ਵੀ ਵਰਤ ਸਕਦੇ ਹੋ, ਜਿਵੇਂ ਕਿ:

- ਡੈਸ਼ (-)
- ਡਾਲਰ ਨਿਸ਼ਾਨ ($)
- ਈਮੇਲ ਵਾਲਾ @ ਨਿਸ਼ਾਨ।

ਤੁਹਾਨੂੰ ਆਪਣੇ ਪਾਸਫ੍ਰੇਜ਼ ਵਿੱਚ ਕੋਈ ਵੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨਹੀਂ ਵਰਤਣੀ ਚਾਹੀਦੀ।

ਉਦਾਹਰਨ ਲਈ:

- ਤੁਹਾਡਾ ਜਨਮਦਿਨ
- ਤੁਹਾਡੇ ਪਰਿਵਾਰ ਦੇ ਮੈਂਬਰਾਂ ਜਾਂ ਪਾਲਤੂ ਜਾਨਵਰਾਂ ਦੇ ਨਾਮ।

ਆਪਣੇ ਖਾਤਿਆਂ ਵਿੱਚ ਲਾਗਇਨ ਕਰਨ ਲਈ ਵਾਧੂ ਕਦਮ ਸ਼ਾਮਲ ਕਰੋ

ਤੁਸੀਂ ਆਪਣੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਨੂੰ **ਮਲਟੀ-ਫੈਕਟਰ ਆਥੈਂਟੀਕੇਸ਼ਨ (MFA)** ਨਾਲ ਸੁਰੱਖਿਅਤ ਕਰ ਸਕਦੇ ਹੋ।

MFA ਦਾ ਮਤਲਬ ਹੈ ਕਿ ਤੁਸੀਂ ਹਰ ਵਾਰ ਆਪਣੇ ਖਾਤੇ ਵਿੱਚ ਲਾਗਇਨ ਕਰਨ ਲਈ 2 ਜਾਂ ਇਸ ਤੋਂ ਵੱਧ ਵੱਖ-ਵੱਖ ਤਰੀਕੇ ਵਰਤਦੇ ਹੋ|

ਉਦਾਹਰਨ ਲਈ, ਤੁਸੀਂ ਪਹਿਲਾਂ ਆਪਣਾ ਪਾਸਫ੍ਰੇਜ਼ ਭਰ ਕਰ ਸਕਦੇ ਹੋ|

ਫਿਰ ਤੁਸੀਂ ਆਪਣੇ ਫੋਨ 'ਤੇ ਆਉਣ ਵਾਲਾ ਕੋਡ ਭਰਦੇ ਹੋ।

ਤੁਹਾਡੇ ਕੋਲ ਇਹ ਚੋਣਾਂ ਹੋ ਸਕਦੀਆਂ ਹਨ:

- ਆਪਣੇ ਫੋਨ ‘ਤੇ ਇੱਕ ਐਪ ਪਾਉਣੀ ਜੋ ਤੁਹਾਨੂੰ ਕੋਡ ਦੇਵੇ

- ਕੋਡ ਈਮੇਲ ਵਿੱਚ ਪ੍ਰਾਪਤ ਕਰਨਾ

- ਕੋਡ ਟੈਕਸਟ ਮੈਸੇਜ ਵਿੱਚ ਪ੍ਰਾਪਤ ਕਰਨਾ।

MFA ਹੋਰ ਲੋਕਾਂ ਲਈ ਤੁਹਾਡੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਵਿੱਚ ਦਾਖਲ

ਹੋਣਾ ਔਖਾ ਬਣਾ ਦਿੰਦਾ ਹੈ,

ਭਾਵੇਂ ਉਹ ਤੁਹਾਡਾ ਪਾਸਫ੍ਰੇਜ਼ ਪਤਾ ਕਰ ਲੈਣ।

ਆਪਣੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਲਈ ਆਪਣੀਆਂ ਸੈਟਿੰਗਾਂ ਦੀ ਜਾਂਚ ਕਰੋ

ਤੁਸੀਂ ਇਹ ਜਾਂਚ ਸਕਦੇ ਹੋ ਕਿ ਤੁਹਾਡੀਆਂ ਸੈਟਿੰਗਾਂ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਨੂੰ ਆਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰੱਖ ਰਹੀਆਂ ਹਨ।

ਇਸ ਵਿੱਚ ਤੁਹਾਡੀਆਂ ਹੇਠ ਲਿਖੀਆਂ ਸੈਟਿੰਗਾਂ ਸ਼ਾਮਲ ਹਨ:

- ਆਨਲਾਈਨ ਖਾਤੇ
- ਡਿਵਾਈਸਾਂ
- ਐਪਸ।

ਤੁਸੀਂ ਇਹ ਕਰ ਸਕਦੇ ਹੋ:

- ਆਪਣੀਆਂ ਸੈਟਿੰਗਾਂ ਬਦਲੋ
- ਇਹ ਚੁਣੋ ਕਿ ਕਿਹੜੀਆਂ ਐਪਸ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਵਰਤ ਸਕਦੀਆਂ ਹਨ।

ਤੁਸੀਂ ਆਪਣੇ ਡਿਵਾਈਸ ‘ਤੇ ਸੈਟਿੰਗਾਂ ਇਸ ਤਰ੍ਹਾਂ ਲੱਭ ਸਕਦੇ ਹੋ:

- ਗੀਅਰ ਆਈਕਨ (⚙)ਨੂੰ ਵੇਖ ਕੇ ਲੱਭੋ

  ਜਾਂ

- ਆਪਣੇ ਡਿਵਾਈਸ ਦੀ ਖੋਜ ਪੱਟੀ ਵਿੱਚ ‘settings’ ਟਾਈਪ ਕਰਕੇ।

ਤੁਸੀਂ ਕਿਸੇ ਐਪ ਜਾਂ ਆਨਲਾਈਨ ਖਾਤੇ ਵਿੱਚ ਸੈਟਿੰਗਾਂ ਮੈਨੂ ਖੋਲ੍ਹ ਕੇ ਲੱਭ ਸਕਦੇ ਹੋ।

ਮੈਨੂ ਅਕਸਰ 3 ਸਿੱਧੀਆਂ ਲਾਈਨਾਂ ਵਰਗਾ ਦਿਖਾਈ ਦਿੰਦਾ ਹੈ।

ਇਨ੍ਹਾਂ ਵਿੱਚੋਂ ਕੁਝ ਸੈਟਿੰਗਾਂ ਇਹ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰ ਸਕਦੀਆਂ ਹਨ:

- ਤੁਸੀਂ ਕੌਣ ਹੋ
- ਤੁਸੀਂ ਕਿੱਥੇ ਹੋ
- ਤੁਸੀਂ ਕਿੱਥੇ ਰਹਿੰਦੇ ਹੋ।

ਇਹ ਜਾਣਕਾਰੀ ਆਨਲਾਈਨ ਸਾਂਝੀ ਕਰਨ ਨਾਲ ਤੁਹਾਨੂੰ ਸਾਈਬਰ ਅਪਰਾਧ ਦਾ ਖਤਰਾ ਹੋ ਸਕਦਾ ਹੈ।

ਸਾਈਬਰ ਅਪਰਾਧੀ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਦਾ ਇਸਤੇਮਾਲ ਕਰਕੇ ਤੁਹਾਡੇ ਵਾਂਗ ਹੋਣ ਦਾ ਨਾਟਕ ਕਰ ਸਕਦੇ ਹਨ।

ਉਦਾਹਰਨ ਲਈ, ਉਹ ਇਸ ਤਰ੍ਹਾਂ ਦੀ ਜਾਣਕਾਰੀ ਵਰਤ ਸਕਦੇ ਹਨ:

- ਤੁਸੀਂ ਕਿੱਥੇ ਰਹਿੰਦੇ ਹੋ

- ਤੁਹਾਡੇ ਪਰਿਵਾਰ ਦੇ ਮੈਂਬਰਾਂ ਦੇ ਨਾਮ

- ਤੁਹਾਡੇ ਪਾਲਤੂ ਜਾਨਵਰਾਂ ਦੇ ਨਾਮ।

ਤੁਸੀਂ ਆਪਣੇ ਖਾਤਿਆਂ ਨੂੰ ਇਸ ਤਰ੍ਹਾਂ ਸੈਟ ਕਰ ਸਕਦੇ ਹੋ ਕਿ ਸਿਰਫ਼ ਉਹੀ ਲੋਕ ਤੁਹਾਡੀਆਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪ੍ਰੋਫ਼ਾਈਲਾਂ ਵੇਖ ਸਕਣ ਜਿਨ੍ਹਾਂ ਨੂੰ ਤੁਸੀਂ ਜਾਣਦੇ ਹੋ।

ਉਦਾਹਰਨ ਲਈ, ਤੁਹਾਡੀ ਫੇਸਬੁੱਕ ਪ੍ਰੋਫ਼ਾਈਲ।

ਇਹ ਸੈਟਿੰਗਾਂ ਨੂੰ ਆਮ ਤੌਰ ‘ਤੇ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਕਿਹਾ ਜਾਂਦਾ ਹੈ।

ਤੁਸੀਂ ਆਪਣੀਆਂ **ਲੋਕੇਸ਼ਨ (ਸਥਾਨ) ਸੈਟਿੰਗਾਂ** ਨੂੰ ਵੀ ਨਿਯੰਤਰਿਤ ਕਰ ਸਕਦੇ ਹੋ।

ਲੋਕੇਸ਼ਨ (ਸਥਾਨ) ਸੈਟਿੰਗਾਂ ਦਿਖਾਉਂਦੀਆਂ ਹਨ ਕਿ ਤੁਹਾਡਾ ਡਿਵਾਈਸ ਕਿੱਥੇ ਹੈ।

ਤੁਸੀਂ ਟਿਕਾਣਾ ਸੈਟਿੰਗਾਂ ਨੂੰ ਚਾਲੂ ਜਾਂ ਬੰਦ ਕਰ ਸਕਦੇ ਹੋ।

ਤੁਸੀਂ ਇਹ ਵੀ ਚੁਣ ਸਕਦੇ ਹੋ ਕਿ ਕਿਹੜੀਆਂ ਐਪਸ ਤੁਹਾਡੇ ਟਿਕਾਣੇ ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦੀਆਂ ਹਨ।

ਤੁਸੀਂ ਇਹ ਆਪਣੇ ਇਹਨਾਂ ਲਈ ਕਰ ਸਕਦੇ ਹੋ:

- ਆਨਲਾਈਨ ਖਾਤੇ
- ਡਿਵਾਈਸਾਂ
- ਐਪਸ।

ਕੁਝ ਐਪਸ ਤੁਹਾਨੂੰ ਇਹ ਵੀ ਪੁੱਛ ਸਕਦੀਆਂ ਹਨ ਕਿ ਕੀ ਉਹ:

- ਤੁਹਾਡਾ ਕੈਮਰਾ ਵਰਤ ਸਕਦੀਆਂ ਹਨ

- ਤੁਹਾਡੀਆਂ ਤਸਵੀਰਾਂ ਵੇਖ ਸਕਦੀਆਂ ਹਨ।

ਤੁਹਾਨੂੰ ਸਿਰਫ਼ ਉਹਨਾਂ ਐਪਸ ਨੂੰ ਹੀ ਆਪਣੇ ਕੈਮਰੇ ਅਤੇ ਤਸਵੀਰਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਦੀ ਇਜਾਜ਼ਤ ਦੇਣੀ ਚਾਹੀਦੀ ਹੈ ਜਿਨ੍ਹਾਂ ਨਾਲ ਤੁਸੀਂ ਜਾਣੂ ਹੋ।

ਆਪਣੇ ਡਿਵਾਈਸਾਂ ਦੀ ਸੁਰੱਖਿਆ ਕਰੋ

ਤੁਹਾਨੂੰ ਸੋਚਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਤੁਸੀਂ ਆਪਣੇ ਡਿਵਾਈਸਾਂ ਦੀ ਸੁਰੱਖਿਆ ਕਿਵੇਂ ਕਰ ਸਕਦੇ ਹੋ ਤਾਂ ਜੋ ਤੁਸੀਂ ਆਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿ ਸਕੋ।

ਉਦਾਹਰਨ ਲਈ, ਤੁਹਾਡਾ ਫੋਨ ਜਾਂ ਸਮਾਰਟ ਵਾਚ|

ਇਹ ਉਹਨਾਂ ਡਿਵਾਈਸਾਂ ਲਈ ਮਹੱਤਵਪੂਰਨ ਹੈ ਜੋ ਇੰਟਰਨੈੱਟ ਨਾਲ ਜੁੜਦੇ ਹਨ।

ਆਪਣੇ ਡਿਵਾਈਸਾਂ ਨੂੰ ਅਪਡੇਟ ਕਰੋ

ਤੁਸੀਂ ਆਪਣੇ ਡਿਵਾਈਸਾਂ ਨੂੰ ਆਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਅਪਡੇਟ ਕਰ ਸਕਦੇ ਹੋ।

ਉਦਾਹਰਨ ਲਈ, ਤੁਹਾਡਾ ਫੋਨ ਅਤੇ ਲੈਪਟਾਪ|

ਤੁਹਾਡਾ ਡਿਵਾਈਸ ਇਸਨੂੰ ਸਾਫਟਵੇਅਰ ਅਪਡੇਟ ਕਹਿ ਸਕਦਾ ਹੈ।

ਅਪਡੇਟ ਕਿਸੇ ਡਿਵਾਈਸ ਨੂੰ ਸਾਈਬਰ ਅਪਰਾਧ ਤੋਂ ਆਪਣੇ ਆਪ ਦੀ ਰੱਖਿਆ ਕਰਨ ਵਿੱਚ ਮਦਦ ਕਰਦੇ ਹਨ।

ਤੁਸੀਂ ਆਪਣੇ ਡਿਵਾਈਸ ਨੂੰ ਆਪਣੇ ਆਪ ਅਪਡੇਟ ਹੋਣ ਲਈ ਸੈਟ ਕਰ ਸਕਦੇ ਹੋ।

ਤੁਸੀਂ ਸਾਡੇ ਵੈਬਸਾਈਟ ‘ਤੇ ਜਾ ਕੇ ਆਪਣੇ ਡਿਵਾਈਸਾਂ ਨੂੰ ਅਪਡੇਟ ਕਰਨ ਬਾਰੇ ਹੋਰ ਜਾਣਕਾਰੀ ਲੈ ਸਕਦੇ ਹੋ:

www.actnowstaysecure.gov.au/cyber-safe-actions

ਪਬਲਿਕ Wi-Fi ਨੈੱਟਵਰਕ

ਜਦੋਂ **ਤੁਸੀਂ ਪਬਲਿਕ Wi-Fi** ਵਰਤਦੇ ਹੋ, ਤਾਂ ਤੁਹਾਨੂੰ ਸਾਵਧਾਨ ਰਹਿਣਾ ਚਾਹੀਦਾ ਹੈ।

ਪਬਲਿਕ Wi-Fi ਮੁਫ਼ਤ ਵਾਇਰਲੈੱਸ ਇੰਟਰਨੈੱਟ ਹੁੰਦਾ ਹੈ ਜੋ ਤੁਸੀਂ ਸਰਵਜਨਿਕ ਸਥਾਨਾਂ ‘ਤੇ ਵਰਤ ਸਕਦੇ ਹੋ।

ਉਦਾਹਰਨ ਲਈ:

- ਕੈਫੇ
- ਏਅਰਪੋਰਟ
- ਹੋਟਲ।

ਜਦੋਂ ਤੁਸੀਂ ਪਬਲਿਕ Wi-Fi ਵਰਤਦੇ ਹੋ, ਤਾਂ ਤੁਹਾਨੂੰ ਇਹ ਧਿਆਨ ਰੱਖਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਤੁਸੀਂ ਕਿਸੇ ਵੈਬਸਾਈਟ 'ਤੇ ਕਿਹੜੀ ਜਾਣਕਾਰੀ ਦਰਜ ਕਰ ਰਹੇ ਹੋ।

ਉਦਾਹਰਨ ਲਈ, ਤੁਹਾਡੇ:

- ਬੈਂਕ ਦੀ ਜਾਣਕਾਰੀ
- ਈਮੇਲ ਖਾਤੇ
- ਸੋਸ਼ਲ ਮੀਡੀਆ ਪ੍ਰੋਫ਼ਾਈਲਾਂ।

ਕੁਝ ਸਾਈਬਰ ਅਪਰਾਧੀ ਪਬਲਿਕ Wi-Fi ਦੀ ਵਰਤੋਂ ਕਰਕੇ:

- ਦੇਖ ਸਕਦੇ ਹਨ ਕਿ ਤੁਸੀਂ ਆਨਲਾਈਨ ਕੀ ਕਰ ਰਹੇ ਹੋ
- ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰ ਸਕਦੇ ਹਨ।

ਇਸ ਦਾ ਕਾਰਨ ਇਹ ਹੈ ਕਿ:

- ਕੋਈ ਵੀ ਇਸਨੂੰ ਵਰਤ ਸਕਦਾ ਹੈ

- ਤੁਹਾਡੇ ਡਿਵਾਈਸਾਂ ਦੀ ਰੱਖਿਆ ਕਰਨਾ ਹੋਰ ਔਖਾ ਹੁੰਦਾ ਹੈ।

ਤੁਸੀਂ ਸਾਡੇ ਵੈਬਸਾਈਟ 'ਤੇ ਪਬਲਿਕ Wi-Fi ਵਰਤਦੇ ਸਮੇਂ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਬਾਰੇ ਹੋਰ ਜਾਣ ਸਕਦੇ ਹੋ:

www.actnowstaysecure.gov.au/cyber-safe-actions

ਧੋਖਾਧੜੀਆਂ (Scams)

ਅਸੀਂ ਇਸਨੂੰ **ਧੋਖਾਧੜੀ** ਕਹਿੰਦੇ ਹਾਂ ਜਦੋਂ ਕੋਈ ਤੁਹਾਨੂੰ:

- ਠੱਗਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਦਾ ਹੈ
- ਤੁਹਾਡੇ ਪੈਸੇ ਲੈਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਦਾ ਹੈ।

ਧੋਖੇਬਾਜ਼ ਉਹ ਵਿਅਕਤੀ ਹੁੰਦਾ ਹੈ ਜੋ ਧੋਖਾਧੜੀਆਂ ਕਰਦਾ ਹੈ।

ਧੋਖੇਬਾਜ਼ ਤੁਹਾਨੂੰ ਠੱਗਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰ ਸਕਦੇ ਹਨ:

- ਟੈਕਸਟ ਮੈਸੇਜ ਜਾਂ ਫੋਨ ਕਾਲ ਰਾਹੀਂ
- ਈਮੇਲ ਰਾਹੀਂ
- ਸੋਸ਼ਲ ਮੀਡੀਆ ਰਾਹੀਂ
- ਵੈਬਸਾਈਟ ਰਾਹੀਂ।

ਉਹ ਦੋਸਤਾਨਾ ਲੱਗ ਸਕਦੇ ਹਨ,

ਪਰ ਉਹ ਧੋਖੇ ਨਾਲ ਤੁਹਾਡੇ ਤੋਂ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਕਢਾ ਸਕਦੇ ਹਨ।

ਉਹ ਇਸ ਜਾਣਕਾਰੀ ਦਾ ਇਸਤੇਮਾਲ ਕਰ ਸਕਦੇ ਹਨ:

- ਤੁਹਾਡੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਵਿੱਚ ਦਾਖਲ ਹੋਣ ਲਈ

- ਤੁਸੀਂ ਹੋਣ ਦਾ ਨਾਟਕ ਕਰਣ ਲਈ

- ਤੁਹਾਡੇ ਪੈਸੇ ਚੋਰੀ ਕਰਨ ਲਈ।

ਧੋਖੇਬਾਜ਼ ਇਹ ਵੀ ਕਰ ਸਕਦੇ ਹਨ:

- ਤੁਹਾਨੂੰ ਠੱਗਣ ਲਈ ਨਕਲੀ ਖਾਤੇ ਬਣਾਉਣਾ

- ਤੁਹਾਨੂੰ ਕਲਿੱਕ ਕਰਨ ਲਈ ਲਿੰਕ ਅਤੇ ਇਸ਼ਤਿਹਾਰ ਸਾਂਝੇ ਕਰਨਾ।

ਧੋਖਾਧੜੀ ਨੂੰ ਕਿਵੇਂ ਪਛਾਣਨਾ ਹੈ

ਇਹ ਧੋਖਾਧੜੀ ਹੋ ਸਕਦੀ ਹੈ ਜੇ ਇਹ:

- ਤੁਹਾਨੂੰ ਕੁਝ ਜਲਦੀ ਕਰਨ ਲਈ ਕਹਿੰਦੀ ਹੈ

- ਤੁਹਾਨੂੰ ਬਹੁਤ ਜ਼ਿਆਦਾ ਪੈਸੇ ਦੀ ਪੇਸ਼ਕਸ਼ ਕਰਦੀ ਹੈ

- ਤੁਹਾਡੇ ਤੋਂ ਪੈਸੇ ਮੰਗਦੀ ਹੈ

- ਤੁਹਾਨੂੰ ਕਿਸੇ ਲਿੰਕ ‘ਤੇ ਕਲਿੱਕ ਕਰਨ ਲਈ ਕਹਿੰਦੀ ਹੈ।

ਧੋਖੇਬਾਜ਼ (Scammers) ਕਈ ਵਾਰ ਕਿਸੇ ਅਜਿਹੀ ਸੰਸਥਾ ਬਣ ਕੇ ਵੀ ਆ ਸਕਦੇ ਹਨ ਜਿਸਨੂੰ ਤੁਸੀਂ ਜਾਣਦੇ ਅਤੇ ਭਰੋਸਾ ਕਰਦੇ ਹੋ।

ਉਦਾਹਰਨ ਲਈ, ਤੁਹਾਡਾ ਬੈਂਕ।

ਉਹ ਇਹ ਇਸ ਲਈ ਕਰਦੇ ਹਨ ਤਾਂ ਜੋ ਤੁਸੀਂ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਉਨ੍ਹਾਂ ਨਾਲ ਸਾਂਝੀ ਕਰੋ।

ਜੇ ਤੁਹਾਨੂੰ ਲੱਗੇ ਕਿ ਕੋਈ ਵਿਅਕਤੀ ਧੋਖੇਬਾਜ਼ ਹੈ, ਤਾਂ ਤੁਹਾਨੂੰ ਉਸ ਨਾਲ ਗੱਲ ਕਰਨੀ ਬੰਦ ਕਰ ਦੇਣੀ ਚਾਹੀਦੀ ਹੈ।

ਤੁਹਾਨੂੰ ਇਹ ਪੱਕਾ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਉਹ ਵਿਅਕਤੀ ਵਾਕਈ ਉਹੀ ਹੈ ਜੋ ਉਹ ਕਹਿੰਦਾ ਹੈ।

ਤੁਸੀਂ ਉਸ ਵਿਅਕਤੀ ਜਾਂ ਸੰਸਥਾ ਨਾਲ ਉਹਨਾਂ ਜਾਣਕਾਰੀਆਂ ਰਾਹੀਂ ਸੰਪਰਕ ਕਰ ਸਕਦੇ ਹੋ ਜਿਨ੍ਹਾਂ 'ਤੇ ਤੁਸੀਂ ਭਰੋਸਾ ਕਰਦੇ ਹੋ ਅਤੇ ਜੋ ਤੁਸੀਂ ਖੁਦ ਲੱਭੀਆਂ ਹਨ।

ਜੇ ਤੁਹਾਨੂੰ ਕੁਝ ਗਲਤ ਲੱਗਦਾ ਹੈ, ਤਾਂ ਆਪਣੇ ਆਪ ਦੀ ਰੱਖਿਆ ਲਈ ਤੁਰੰਤ ਕਾਰਵਾਈ ਕਰੋ।

ਧੋਖਾਧੜੀ ਦੀ ਰਿਪੋਰਟ ਕਰੋ

Scamwatch ਆਸਟ੍ਰੇਲੀਆਈ ਲੋਕਾਂ ਦੀ ਮਦਦ ਕਰਦਾ ਹੈ:

- ਧੋਖਾਧੜੀਆਂ ਨੂੰ ਸਮਝਣ ਵਿੱਚ
- ਧੋਖਾਧੜੀਆਂ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਵਿੱਚ।

Scamwatch ਉਹਨਾਂ ਲੋਕਾਂ ਦੀ ਵੀ ਮਦਦ ਕਰਦਾ ਹੈ ਜਿਨ੍ਹਾਂ ਨੇ ਧੋਖਾਧੜੀ ਦਾ ਤਜਰਬਾ ਕੀਤਾ ਹੈ।

ਤੁਸੀਂ Scamwatch ਵੈਬਸਾਈਟ ‘ਤੇ ਧੋਖਾਧੜੀ ਦੀ ਰਿਪੋਰਟ ਕਰ ਸਕਦੇ ਹੋ:

www.scamwatch.gov.au/report-a-scam

ਆਵਾਜ਼ ਉਠਾਓ

ਤੁਹਾਨੂੰ ਇਸ ਬਾਰੇ ਗੱਲ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ ਕਿ ਹੋਰ ਲੋਕ ਆਪਣੇ ਆਪ ਨੂੰ ਆਨਲਾਈਨ ਕਿਵੇਂ ਸੁਰੱਖਿਅਤ ਰੱਖ ਸਕਦੇ ਹਨ।

ਇਸ ਵਿੱਚ ਸ਼ਾਮਲ ਹੈ:

- ਸਾਈਬਰ ਅਪਰਾਧ ਦੀ ਰਿਪੋਰਟ ਕਰਨਾ

- ਆਪਣੇ ਪਰਿਵਾਰ ਅਤੇ ਦੋਸਤਾਂ ਨਾਲ ਆਪਣੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨਾ।

ਅਸੀਂ ਅਗਲੇ ਸਫ਼ਿਆਂ ‘ਤੇ ਸਮਝਾਵਾਂਗੇ ਕਿ ਤੁਸੀਂ ਕਿਵੇਂ ਆਵਾਜ਼ ਉਠਾ ਸਕਦੇ ਹੋ।

ਸਾਈਬਰ ਅਪਰਾਧ ਦੀ ਰਿਪੋਰਟ ਕਰੋ

ਸਾਈਬਰ ਅਪਰਾਧ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਨਾਲ ਸਰਕਾਰ ਨੂੰ ਮਦਦ ਮਿਲਦੀ ਹੈ:

- ਇਹ ਜਾਣਣ ਵਿੱਚ ਕਿ ਸਾਈਬਰ ਅਪਰਾਧੀ ਲੋਕਾਂ 'ਤੇ ਹਮਲਾ ਕਰਨ ਲਈ ਕਿਵੇਂ ਕੋਸ਼ਿਸ਼ ਕਰਦੇ ਹਨ

- ਹੋਰ ਲੋਕਾਂ ਦੀ ਰੱਖਿਆ ਕਰਨ ਵਿੱਚ।

ਤੁਸੀਂ ਸਾਈਬਰ ਅਪਰਾਧ ਦੀ ਰਿਪੋਰਟ ReportCyber ਵੈਬਸਾਈਟ 'ਤੇ ਕਰ ਸਕਦੇ ਹੋ:

www.cyber.gov.au/report

ਆਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਬਾਰੇ ਆਪਣੇ ਪਰਿਵਾਰ ਅਤੇ ਦੋਸਤਾਂ ਨਾਲ ਗੱਲ ਕਰੋ

ਤੁਹਾਨੂੰ ਆਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਬਾਰੇ ਆਪਣੇ ਸੁਝਾਅ ਆਪਣੇ ਪਰਿਵਾਰ ਅਤੇ ਦੋਸਤਾਂ ਨਾਲ ਸਾਂਝੇ ਕਰਨੇ ਚਾਹੀਦੇ ਹਨ।

ਤੁਸੀਂ ਉਨ੍ਹਾਂ ਤੋਂ ਵੀ ਸਿੱਖ ਸਕਦੇ ਹੋ।

ਤੁਸੀਂ ਆਪਣੇ ਅਤੇ ਆਪਣੇ ਆਲੇ-ਦੁਆਲੇ ਦੇ ਲੋਕਾਂ ਦੀ ਰੱਖਿਆ ਕਰ ਸਕਦੇ ਹੋ, ਜੇ ਤੁਸੀਂ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਬਾਰੇ ਆਪਣੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਦੇ ਹੋ।

ਇਹ ਤਾਂ ਵੀ ਮਹੱਤਵਪੂਰਨ ਹੈ ਜੇ ਤੁਸੀਂ ਹੋਰ ਲੋਕਾਂ ਨਾਲ ਡਿਵਾਈਸ ਸਾਂਝੇ ਕਰਦੇ ਹੋ।

ਸ਼ਬਦ ਸੂਚੀ

ਇਹ ਸੂਚੀ ਸਮਝਾਉਂਦੀ ਹੈ ਕਿ ਇਸ ਗਾਈਡ ਵਿੱਚ **ਮੋਟੇ ਅੱਖਰਾਂ (bold)** ਵਿੱਚ ਲਿਖੇ ਸ਼ਬਦਾਂ ਦਾ ਕੀ ਮਤਲਬ ਹੈ|

ਸਾਈਬਰ (Cyber)

ਸਾਈਬਰ ਦਾ ਮਤਲਬ ਹੁੰਦਾ ਹੈ ਇੰਟਰਨੈੱਟ ਨਾਲ ਸੰਬੰਧਿਤ ਕੁਝ।.

ਸਾਈਬਰ ਅਪਰਾਧ (Cyber crime)

ਸਾਈਬਰ ਅਪਰਾਧ ਉਹ ਹੁੰਦਾ ਹੈ ਜਦੋਂ ਅਪਰਾਧੀ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਜੁਰਮ ਕਰਦੇ ਹਨ|

ਉਦਾਹਰਨ ਲਈ, ਉਹ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦੇ ਹਨ:

- ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰਨ ਲਈ
- ਤੁਹਾਡੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ 'ਤੇ ਕਬਜ਼ਾ ਕਰਨ ਲਈ|

ਲੋਕੇਸ਼ਨ (ਟਿਕਾਣਾ)ਸੈਟਿੰਗਾਂ (Location settings)

ਟਿਕਾਣਾ ਸੈਟਿੰਗਾਂ ਦਿਖਾਉਂਦੀਆਂ ਹਨ ਕਿ ਤੁਹਾਡਾ ਡਿਵਾਈਸ ਕਿੱਥੇ ਹੈ|

ਮਲਟੀ-ਫੈਕਟਰ ਪ੍ਰਮਾਣਿਕਤਾ (MFA)

MFA ਉਹ ਹੁੰਦੀ ਹੈ ਜਦੋਂ ਤੁਸੀਂ ਹਰ ਵਾਰ ਆਪਣੇ ਅਕਾਊਂਟ ਵਿੱਚ ਲਾਗਇਨ ਕਰਨ ਲਈ 2 ਜਾਂ ਇਸ ਤੋਂ ਵੱਧ ਵੱਖ-ਵੱਖ ਤਰੀਕੇ ਵਰਤਦੇ ਹੋ।

ਪਾਸਫ੍ਰੇਜ਼

ਪਾਸਫ੍ਰੇਜ਼ ਪਾਸਵਰਡ ਦੀ ਇੱਕ ਹੋਰ ਮਜ਼ਬੂਤ ਕਿਸਮ ਹੁੰਦੀ ਹੈ।

ਦੂਸਰਿਆਂ ਲਈ ਅੰਦਾਜ਼ਾ ਲਗਾਉਣਾ ਬਹੁਤ ਮੁਸ਼ਕਲ ਹੁੰਦਾ ਹੈ।

ਪਬਲਿਕ

ਪਬਲਿਕ Wi-Fi ਮੁਫ਼ਤ ਵਾਇਰਲੈਸ ਇੰਟਰਨੈਟ ਹੁੰਦਾ ਹੈ ਜੋ ਤੁਸੀਂ ਜਨਤਕ ਥਾਵਾਂ ‘ਤੇ ਵਰਤ ਸਕਦੇ ਹੋ।

ਠੱਗੀਆਂ

ਅਸੀਂ ਇਸਨੂੰ ਠੱਗੀ ਕਹਿੰਦੇ ਹਾਂ ਜਦੋਂ ਕੋਈ ਵਿਅਕਤੀ ਕੋਸ਼ਿਸ਼ ਕਰਦਾ ਹੈ ਕਿ:

- ਤੁਹਾਨੂੰ ਧੋਖਾ ਦੇਵੇ
- ਤੁਹਾਡੇ ਪੈਸੇ ਲੈ ਲਵੇ।

ਠੱਗ

ਠੱਗ ਉਹ ਵਿਅਕਤੀ ਹੁੰਦਾ ਹੈ ਜੋ ਠੱਗੀਆਂ ਕਰਦਾ ਹੈ।

ਸਾਡੇ ਨਾਲ ਸੰਪਰਕ ਕਰੋ

ਤੁਸੀਂ ਆਸਟ੍ਰੇਲੀਆਈ ਸਾਇਬਰ ਸੁਰੱਖਿਆ ਹੈਲਪਲਾਈਨ ‘ਤੇ ਫ਼ੋਨ ਕਰ ਸਕਦੇ ਹੋ।

1300 292 371

ਤੁਸੀਂ ਸਾਡੀ ਵੈਬਸਾਈਟ ‘ਤੇ ਜਾ ਸਕਦੇ ਹੋ।

www.actnowstaysecure.gov.au

ਤੁਸੀਂ ReportCyber ਵੈਬਸਾਈਟ ‘ਤੇ ਸਾਇਬਰ ਅਪਰਾਧ ਦੀ ਰਿਪੋਰਟ ਕਰ ਸਕਦੇ ਹੋ।

www.cyber.gov.au/report

ਇਨਫਰਮੇਸ਼ਨ ਐਕਸੈੱਸ ਗਰੁੱਪ ਨੇ ਇਹ ਆਸਾਨੀ ਨਾਲ ਪੜ੍ਹਿਆ ਜਾਣ ਯੋਗ ਦਸਤਾਵੇਜ਼ ਸਟਾਕ ਤਸਵੀਰਾਂ ਅਤੇ ਖਾਸ ਤਸਵੀਰਾਂ ਦੀ ਵਰਤੋਂ ਨਾਲ ਬਣਾਇਆ ਹੈ। ਇਹ ਤਸਵੀਰਾਂ ਬਿਨਾਂ ਇਜਾਜ਼ਤ ਦੁਬਾਰਾ ਵਰਤੀਆਂ ਨਹੀਂ ਜਾ ਸਕਦੀਆਂ। ਤਸਵੀਰਾਂ ਬਾਰੇ ਕਿਸੇ ਵੀ ਪੁੱਛਗਿੱਛ ਲਈ, ਕਿਰਪਾ ਕਰਕੇ www.informationaccessgroup.com ‘ਤੇ ਜਾਓ। ਜੌਬ ਨੰਬਰ 6342 ਦਾ ਹਵਾਲਾ ਦਿਓ।