Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

ਇੰਟਰਨੈੱਟ ਦੀ ਸੁਰੱਖਿਅਤ ਵਰਤੋਂ ਕਿਵੇਂ ਕਰੀਏ

ਬਜ਼ੁਰਗਾਂ ਲਈ ਇੱਕ ਗਾਈਡ

cyber.gov.au

ਜਾਣ-ਪਛਾਣ

ਔਨਲਾਈਨ ਜਾਣਾ ਤੁਹਾਨੂੰ ਦੋਸਤਾਂ ਅਤੇ ਪਰਿਵਾਰ ਨਾਲ ਸੰਪਰਕ ਵਿੱਚ ਰਹਿਣ, ਕਈ ਵਿਸ਼ਿਆਂ ਬਾਰੇ ਸਿੱਖਣ ਅਤੇ ਇੱਥੋਂ ਤੱਕ ਕਿ ਗੇਮਾਂ ਵੀ ਖੇਡਣ ਦਿੰਦਾ ਹੈ।

ਠੀਕ ਉਸੇ ਤਰ੍ਹਾਂ ਜਿਵੇਂ ਗੱਡੀ ਚਲਾਉਣ ਤੋਂ ਪਹਿਲਾਂ ਆਪਣੀ ਸੀਟਬੈਲਟ ਬੰਨ੍ਹਣੀ ਜ਼ਰੂਰੀ ਹੈ, ਤੁਹਾਨੂੰ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਵਧੇਰੇ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਕੁੱਝ ਕਦਮ ਚੁੱਕਣੇ ਚਾਹੀਦੇ ਹਨ।

ਆਸਟ੍ਰੇਲੀਅਨ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਕੇਂਦਰ (ACSC) ਇਹ ਯਕੀਨੀ ਬਣਾਉਣਾ ਚਾਹੁੰਦਾ ਹੈ ਕਿ ਹਰ ਕੋਈ ਔਨਲਾਈਨ ਹੋਣ ਸਮੇਂ ਸੁਰੱਖਿਅਤ ਹੋਵੇ। ਇਹ ਦਸਤਾਵੇਜ਼ ਕੁੱਝ ਬੁਨਿਆਦੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਆਦਤਾਂ ਬਾਰੇ ਦੱਸਦਾ ਹੈ ਜਿੰਨ੍ਹਾਂ ਦੀ ਵਰਤੋਂ ਤੁਸੀਂ ਇੰਟਰਨੈੱਟ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਵੇਲੇ ਆਪਣੇ-ਆਪ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਕਰ ਸਕਦੇ ਹੋ।

ਆਸਟ੍ਰੇਲੀਅਨ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਕੇਂਦਰ (ACSC), ਆਸਟ੍ਰੇਲੀਅਨ ਸਿਗਨਲ ਡਾਇਰੈਕਟੋਰੇਟ (ASD) ਦੇ ਇੱਕ ਹਿੱਸੇ ਵਜੋਂ, ਆਸਟ੍ਰੇਲੀਆ ਲਈ ਸਾਈਬਰ ਖ਼ਤਰਿਆਂ ਨੂੰ ਰੋਕਣ, ਪਤਾ ਲਗਾਉਣ ਅਤੇ ਹੱਲ ਕਰਨ ਲਈ ਸਲਾਹ, ਸਹਾਇਤਾ ਅਤੇ ਕਾਰਜਸ਼ੀਲ ਹੱਲ ਪ੍ਰਦਾਨ ਕਰਦਾ ਹੈ। ACSC ਆਸਟ੍ਰੇਲੀਆ ਨੂੰ ਔਨਲਾਈਨ ਜੁੜਨ ਲਈ ਸਭ ਤੋਂ ਸੁਰੱਖਿਅਤ ਸਥਾਨ ਬਣਾਉਣ ਵਿੱਚ ਮੱਦਦ ਕਰਨ ਲਈ ਇੱਥੇ ਮੌਜੂਦ ਹੈ।
ਹੋਰ ਵਧੇਰੇ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਜਾਣਕਾਰੀ, ਗਾਈਡਾਂ ਅਤੇ ਸਲਾਹ ਲਈ cyber.gov.au 'ਤੇ ਜਾਓ

ਬਜ਼ੁਰਗਾਂ ਲਈ ਸਾਈਬਰ ਸੁਰੱਖਿਆ।

ਸੁਝਾਅ 1: ਆਪਣੇ ਯੰਤਰ ਨੂੰ ਅੱਪਡੇਟ ਕਰੋ।

ਆਪਣੇ ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਅੱਪਡੇਟ ਕਰਨਾ ਆਪਣੀ ਕਾਰ ਦੀ ਸਰਵਿਸ ਕਰਵਾਉਣ ਵਰਗਾ ਹੈ। ਇਹ ਤੁਹਾਡੇ ਯੰਤਰ ਦੀ ਕਾਰਗੁਜ਼ਾਰੀ ਨੂੰ ਬਿਹਤਰ ਬਣਾਉਂਦਾ ਹੈ ਅਤੇ ਇਸਨੂੰ ਹੋਰ ਸੁਰੱਖਿਅਤ ਬਣਾਉਂਦਾ ਹੈ।

ਸਾਈਬਰ ਅਪਰਾਧੀ ਹਮੇਸ਼ਾ ਯੰਤਰਾਂ ਨੂੰ ਹੈਕ ਕਰਨ ਦੇ ਨਵੇਂ ਤਰੀਕੇ ਲੱਭਦੇ ਰਹਿੰਦੇ ਹਨ। ਆਪਣੇ ਯੰਤਰ ਨੂੰ ਅੱਪਡੇਟਾਂ ਨੂੰ ਆਪਣੇ-ਆਪ ਇੰਸਟਾਲ ਕਰਨ ਲਈ ਸੈੱਟ ਕਰਨਾ ਤੁਹਾਡੇ ਸਾਫ਼ਟਵੇਅਰ ਵਿੱਚ ਮੌਜੂਦ ਕਿਸੇ ਵੀ ਕਮਜ਼ੋਰੀ ਨੂੰ ਠੀਕ ਕਰ ਸਕਦਾ ਹੈ ਅਤੇ ਹੈਕਰਾਂ ਨੂੰ ਦੂਰ ਰੱਖ ਸਕਦਾ ਹੈ।

ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ, cyber.gov.au 'ਤੇ 'ਅੱਪਡੇਟਸ' ਲਿਖਕੇ ਖੋਜ ਕਰੋ

ਕੀ ਤੁਸੀ ਜਾਣਦੇ ਹੋ:

ਅੱਪਡੇਟ ਤੁਹਾਡੇ ਯੰਤਰ ਵਿੱਚ ਨਵੀਆਂ ਸੁਵਿਧਾਵਾਂ ਵੀ ਜੋੜ ਸਕਦੇ ਹਨ ਅਤੇ ਇਸਨੂੰ ਤੇਜ਼ੀ ਨਾਲ ਚੱਲਣ ਯੋਗ ਬਣਾ ਸਕਦੇ ਹਨ।

ਸੁਝਾਅ 2: ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ ਨੂੰ ਚਾਲੂ ਕਰੋ।

ਤੁਹਾਡੇ ਖਾਤੇ 'ਤੇ ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ ਲੱਗਿਆ ਹੋਣਾ ਤੁਹਾਡੇ ਘਰ ਲਈ ਲੱਗੀ ਸੁਰੱਖਿਆ ਜਾਲੀ (ਸਕਿਊਰਿਟੀ ਸਕ੍ਰੀਨ) ਵਾਂਗ ਹੈ। ਇਹ ਤੁਹਾਨੂੰ ਅਪਰਾਧੀਆਂ ਤੋਂ ਬਚਾਉਂਦਾ ਹੈ ਜੋ ਅੰਦਰ ਵੜ੍ਹਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰ ਰਹੇ ਹੁੰਦੇ ਹਨ।

ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ ਚਾਲੂ ਕਰਨ ਨਾਲ, ਤੁਹਾਨੂੰ ਆਪਣੇ ਖਾਤੇ ਤੱਕ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ ਇੱਕ ਤੋਂ ਵੱਧ ਜਾਣਕਾਰੀ ਦੇਣ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ। ਉਦਾਹਰਨ ਲਈ, ਤੁਹਾਨੂੰ ਆਪਣੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤੇ ਵਿੱਚ ਲੌਗ-ਇਨ ਕਰਨ ਲਈ ਆਪਣਾ ਪਾਸਵਰਡ ਅਤੇ ਟੈਕਸਟ ਮੈਸਜ਼ ਵਿੱਚ ਆਏ ਕੋਡ ਨੂੰ ਭਰਨ ਦੀ ਲੋੜ ਹੋ ਸਕਦੀ ਹੈ।

ਇਹ ਕਈ ਸੁਰੱਖਿਆ-ਪਰਤਾਂ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਹੈਕ ਕਰਨ ਨੂੰ ਔਖਾ ਬਣਾਉਂਦੀਆਂ ਹਨ। ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਉਹ ਇਸਦੇ ਇੱਕ ਹਿੱਸੇ ਨੂੰ ਪਤਾ ਕਰਨ ਵਿੱਚ ਸਫ਼ਲ ਹੋਣ ਜਾਣ, ਜਿਵੇਂ ਕਿ ਤੁਹਾਡਾ ਪਾਸਵਰਡ, ਪਰ ਉਹਨਾਂ ਨੂੰ ਤੁਹਾਡੇ ਖਾਤੇ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਲਈ ਅਜੇ ਵੀ ਇਸ ਬੁਝਾਰਤ ਦੇ ਹੋਰ ਹਿੱਸੇ ਲੱਭਣ ਦੀ ਲੋੜ ਹੋਵੇਗੀ।

ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ, cyber.gov.au 'ਤੇ 'ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ' ਜਾਂ 'MFA' ਲਿਖ ਕੇ ਖੋਜ ਕਰੋ।

ਯਾਦ ਰੱਖੋ:

ਜੇਕਰ ਤੁਹਾਨੂੰ ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ ਨੂੰ ਚਾਲੂ ਕਰਨ ਵਿੱਚ ਮੱਦਦ ਦੀ ਲੋੜ ਹੈ, ਤਾਂ ਸਹਾਇਤਾ ਲਈ ਕਿਸੇ ਦੋਸਤ ਜਾਂ ਪਰਿਵਾਰਕ ਮੈਂਬਰ ਨੂੰ ਪੁੱਛੋ।

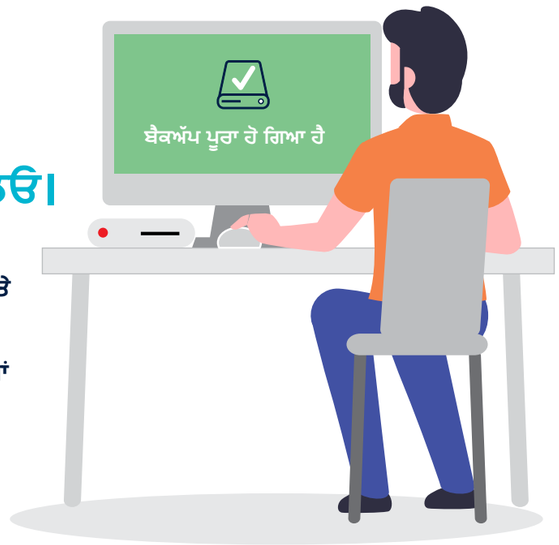
ਸੁਝਾਅ 3: ਆਪਣੇ ਯੰਤਰ ਦਾ ਬੈਕਅੱਪ ਲਓ।

'ਬੈਕਅੱਪ' ਲੈਣਾ ਉਦੋਂ ਹੁੰਦਾ ਹੈ ਜਦੋਂ ਤੁਸੀਂ ਆਪਣੀਆਂ ਮਹੱਤਵਪੂਰਨ ਫ਼ਾਈਲਾਂ ਦੀ ਇੱਕ ਨਕਲ ਬਣਾਉਂਦੇ ਹੋ ਅਤੇ ਉਹਨਾਂ ਨੂੰ ਕਿਤੇ ਸੁਰੱਖਿਅਤ ਰੱਖਦੇ ਹੋ। ਇਹ ਕੀਮਤੀ ਫ਼ੋਟੋਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਫ਼ੋਟੋਕਾਪੀ ਕਰਨ ਵਰਗਾ ਹੈ ਉਸ ਸਥਿਤੀ ਲਈ ਜੇਕਰ ਤੁਸੀਂ ਅਸਲ ਫ਼ੋਟੋਆਂ ਗੁਆ ਲੈਂਦੇ ਹੋ।

ਜਦੋਂ ਤੁਸੀਂ ਆਪਣੇ ਕੰਪਿਊਟਰ, ਫ਼ੋਨ ਜਾਂ ਟੈਬਲੈੱਟ ਦਾ ਬੈਕਅੱਪ ਲੈਂਦੇ ਹੋ, ਤਾਂ ਤੁਹਾਡੀਆਂ ਫ਼ਾਈਲਾਂ ਦੀਆਂ ਨਕਲਾਂ ਔਨਲਾਈਨ ਜਾਂ ਕਿਸੇ ਵੱਖਰੇ ਯੰਤਰ 'ਤੇ ਸੁਰੱਖਿਅਤ ਕੀਤੀਆਂ ਜਾਂਦੀਆਂ ਹਨ। ਆਪਣੀਆਂ ਮਹੱਤਵਪੂਰਨ ਫ਼ਾਈਲਾਂ ਅਤੇ ਪਿਆਰੀਆਂ ਫ਼ੋਟੋਆਂ ਦਾ ਬੈਕਅੱਪ ਲੈਣਾ ਤੁਹਾਨੂੰ ਮਨ ਦੀ ਸ਼ਾਂਤੀ ਦੇਵੇਗਾ।

ਜੇਕਰ ਤੁਹਾਡੇ ਯੰਤਰ ਵਿੱਚ ਕੁੱਝ ਗਲਤ ਹੋ ਜਾਂਦਾ ਹੈ ਜਾਂ ਤੁਸੀਂ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਦੁਆਰਾ ਹੈਕ ਹੋ ਜਾਂਦੇ ਹੋ, ਤਾਂ ਤੁਸੀਂ ਆਸਾਨੀ ਨਾਲ ਆਪਣੇ ਬੈਕਅੱਪ ਤੋਂ ਆਪਣੀਆਂ ਫ਼ਾਈਲਾਂ ਨੂੰ ਰੀਸਟੋਰ (ਦੋਬਾਰਾ ਪ੍ਰਾਪਤ) ਕਰ ਸਕਦੇ ਹੋ।

ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ, cyber.gov.au 'ਤੇ 'ਬੈਕਅੱਪ' ਲਿਖਕੇ ਖੋਜੋ

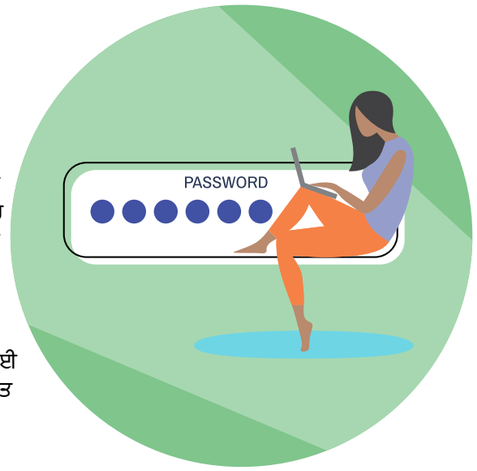


ਕੀ ਤੁਸੀ ਜਾਣਦੇ ਹੋ:

ਆਪਣੇ ਯੰਤਰ ਦਾ ਬਾਕਾਇਦਾ ਤੌਰ 'ਤੇ ਬੈਕਅੱਪ ਲੈਣ ਦਾ ਮਤਲਬ ਹੈ ਕਿ ਤੁਹਾਡੇ ਕੋਲ ਹਮੇਸ਼ਾ ਆਪਣੀਆਂ ਸਭ ਤੋਂ ਤਾਜ਼ਾ (ਅੱਪ-ਟੂ-ਡੇਟ) ਫ਼ਾਈਲਾਂ ਤੱਕ ਪਹੁੰਚ ਹੋਵੇਗੀ।

ਸੁਝਾਅ 4: ਇੱਕ ਪਾਸਫਰੇਜ਼ ਦੀ ਵਰਤੋਂ ਕਰੋ।

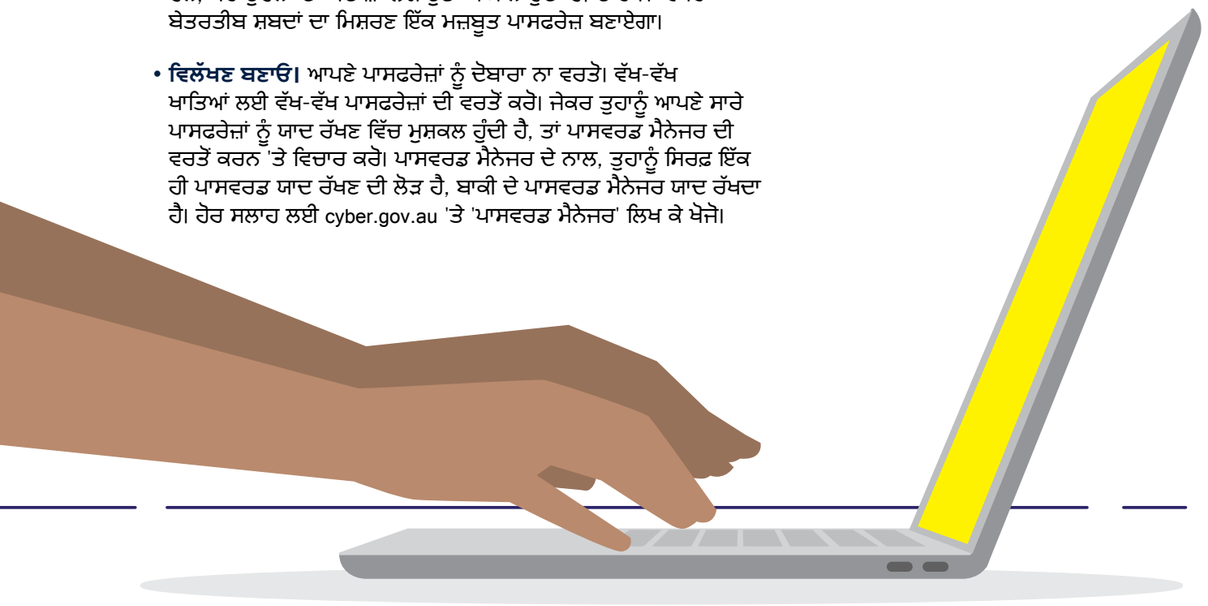
ਜੇਕਰ ਪਾਸਵਰਡ ਤੁਹਾਡੇ ਖਾਤੇ 'ਤੇ ਤਾਲਾ ਲਗਾਉਂਦਾ ਹੈ, ਤਾਂ ਇੱਕ ਪਾਸਫਰੇਜ਼ ਆਪਣੀ ਸੁਰੱਖਿਆ ਪ੍ਰਣਾਲੀ ਦਿੰਦਾ ਹੈ! ਉਹ ਪਾਸਵਰਡਾਂ ਦੇ ਮਜ਼ਬੂਤ ਅਤੇ ਵਧੇਰੇ ਸੁਰੱਖਿਅਤ ਰੂਪ ਹਨ।



ਜਦੋਂ ਤੁਸੀਂ MFA ਨੂੰ ਚਾਲੂ ਨਹੀਂ ਕਰ ਸਕਦੇ ਹੋ, ਤਾਂ ਆਪਣੇ ਖਾਤੇ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਲਈ ਪਾਸਫਰੇਜ਼ ਦੀ ਵਰਤੋਂ ਕਰੋ। ਪਾਸਫਰੇਜ਼ ਤੁਹਾਡੇ ਪਾਸਵਰਡ ਵਜੋਂ ਚਾਰ ਜਾਂ ਵੱਧ ਬੇਤਰਤੀਬੇ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਨ। ਇਹ ਪਾਸਫਰੇਜ਼ਾਂ ਨੂੰ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਅੰਦਾਜ਼ਾ ਲਗਾਉਣਾ ਔਖਾ ਬਣਾਉਂਦਾ ਹੈ ਪਰ ਤੁਹਾਡੇ ਲਈ ਯਾਦ ਰੱਖਣਾ ਆਸਾਨ ਬਣਾਉਂਦਾ ਹੈ।

ਜਦੋਂ ਤੁਸੀਂ ਪਾਸਫਰੇਜ਼ ਬਣਾਉਂਦੇ ਹੋ, ਤਾਂ ਇਸਨੂੰ:

- **ਲੰਬਾ ਬਣਾਓ।** ਜਿੰਨ੍ਹਾਂ ਲੰਬਾ, ਓਨ੍ਹਾਂ ਹੀ ਵਧੀਆ। ਘੱਟੋ-ਘੱਟ 14 ਅੱਖਰਾਂ ਦੀ ਲੰਬਾਈ ਦਾ ਟੀਚਾ ਰੱਖੋ। ਚਾਰ ਜਾਂ ਵੱਧ ਬੇਤਰਤੀਬੇ ਸ਼ਬਦ ਜੋ ਤੁਹਾਨੂੰ ਯਾਦ ਰਹਿਣ ਬਹੁਤ ਵਧੀਆ ਪਾਸਫਰੇਜ਼ ਹੁੰਦੇ ਹਨ।
  ਉਦਾਹਰਨ ਲਈ, 'ਜਾਮਨੀ ਬੱਤਖ਼ ਆਲੂ ਕਿਸ਼ਤੀ'।
- **ਗ਼ੈਰ-ਅਨੁਮਾਨਿਤ ਰੱਖੋ।** ਤੁਹਾਡੇ ਪਾਸਫਰੇਜ਼ ਦਾ ਜਿੰਨ੍ਹਾਂ ਘੱਟ ਅਨੁਮਾਨ ਲਗਾਇਆ ਜਾ ਸਕਦਾ ਹੋਵੇ, ਓਨ੍ਹਾਂ ਹੀ ਇਹ ਵਧੀਆ ਹੈ। ਵਾਕ ਵਧੀਆ ਪਾਸਫਰੇਜ਼ ਬਣਾ ਸਕਦੇ ਹਨ, ਪਰ ਉਹਨਾਂ ਦਾ ਅੰਦਾਜ਼ਾ ਲਗਾਉਣਾ ਆਸਾਨ ਹੁੰਦਾ ਹੈ। ਚਾਰ ਜਾਂ ਵਧੇਰੇ ਬੇਤਰਤੀਬ ਸ਼ਬਦਾਂ ਦਾ ਮਿਸ਼ਰਣ ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਫਰੇਜ਼ ਬਣਾਏਗਾ।
- **ਵਿਲੱਖਣ ਬਣਾਓ।** ਆਪਣੇ ਪਾਸਫਰੇਜ਼ਾਂ ਨੂੰ ਦੋਬਾਰਾ ਨਾ ਵਰਤੋ। ਵੱਖ-ਵੱਖ ਖਾਤਿਆਂ ਲਈ ਵੱਖ-ਵੱਖ ਪਾਸਫਰੇਜ਼ਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਆਪਣੇ ਸਾਰੇ ਪਾਸਫਰੇਜ਼ਾਂ ਨੂੰ ਯਾਦ ਰੱਖਣ ਵਿੱਚ ਮੁਸ਼ਕਲ ਹੁੰਦੀ ਹੈ, ਤਾਂ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਦੀ ਵਰਤੋਂ ਕਰਨ 'ਤੇ ਵਿਚਾਰ ਕਰੋ। ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਦੇ ਨਾਲ, ਤੁਹਾਨੂੰ ਸਿਰਫ਼ ਇੱਕ ਹੀ ਪਾਸਵਰਡ ਯਾਦ ਰੱਖਣ ਦੀ ਲੋੜ ਹੈ, ਬਾਕੀ ਦੇ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਯਾਦ ਰੱਖਦਾ ਹੈ। ਹੋਰ ਸਲਾਹ ਲਈ cyber.gov.au 'ਤੇ 'ਪਾਸਵਰਡ ਮੈਨੇਜਰ' ਲਿਖ ਕੇ ਖੋਜੋ।



cyber.gov.au 'ਤੇ ' Passphrases' ਖੋਜ ਕੇ ਸੁਰੱਖਿਅਤ ਪਾਸਫਰੇਜ਼ ਬਣਾਉਣ ਬਾਰੇ ਹੋਰ ਜਾਣੋ।

ਸੁਝਾਅ 5: ਧੋਖਾਧੜੀ ਨੂੰ ਪਛਾਣੋ ਅਤੇ ਰਿਪੋਰਟ ਕਰੋ।

ਜਿੰਨ੍ਹੀ ਜਲਦੀ ਤੁਸੀਂ ਕਿਸੇ ਧੋਖਾਧੜੀ ਦੀ ਰਿਪੋਰਟ ਕਰੋਗੇ, ਅਸੀਂ ਓਨ੍ਹੀ ਹੀ ਜਲਦੀ ਕਾਰਵਾਈ ਕਰ ਸਕਦੇ ਹਾਂ।

ਜੇਕਰ ਤੁਸੀਂ ਮੰਨਦੇ ਹੋ ਕਿ ਕੋਈ ਤੁਹਾਡੇ ਨਾਲ ਧੋਖਾਧੜੀ ਕਰਨ ਲਈ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰ ਰਿਹਾ ਹੈ, ਤਾਂ ਇਸ ਦਾ ਫ਼ਾਇਦਾ ਉਠਾਉਣ ਦੇ ਜ਼ੋਖਮ ਨਾਲੋਂ ਸਰਗਰਮ ਅਤੇ ਸਾਵਧਾਨ ਰਹਿਣਾ ਬਿਹਤਰ ਹੈ।

ਜੇ ਇਹ ਸੌਦਾ ਬਹੁਤ ਵਧੀਆ ਲੱਗ ਰਿਹਾ ਹੈ, ਤਾਂ ਇਹ ਸ਼ਾਇਦ ਧੋਖਾਧੜੀ ਹੈ। ਜਦੋਂ ਕੋਈ ਸੁਨੇਹਾ ਇਹ ਕਹਿੰਦਾ ਹੋਵੇ ਕਿ ਤੁਸੀਂ ਕੋਈ ਇਨਾਮ ਜਿੱਤ ਲਿਆ ਹੈ ਜਾਂ ਤੁਹਾਡੇ ਕੰਪਿਊਟਰ ਵਿੱਚ ਵਾਇਰਸ ਹੈ, ਉਹ ਸੁਨੇਹਾ ਤੁਹਾਡੇ ਲਈ ਵਿਲੱਖਣ ਨਹੀਂ ਹੈ।

ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਇਹ ਕਿਸੇ ਘੁਟਾਲੇਬਾਜ਼ ਵੱਲੋਂ ਆ ਰਿਹਾ ਹੋਵੇ ਅਤੇ ਉਹ ਤੁਹਾਡਾ ਫ਼ਾਇਦਾ ਉਠਾਉਣਾ ਚਾਹੁੰਦੇ ਹਨ।

ਯਾਦ ਰੱਖੋ, ਘੁਟਾਲੇਬਾਜ਼ ਅਕਸਰ ਕੋਈ ਅਜਿਹਾ ਵਿਅਕਤੀ ਜਾਂ ਸੰਸਥਾ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰਨਗੇ ਜਿਸ 'ਤੇ ਤੁਸੀਂ ਭਰੋਸਾ ਕਰਦੇ ਹੋ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਕੋਈ ਅਜਿਹਾ ਸੁਨੇਹਾ ਮਿਲਦਾ ਹੈ ਜੋ ਲੱਗਦਾ ਹੈ ਕਿ ਇਹ ਕਿਸੇ ਅਜਿਹੇ ਵਿਅਕਤੀ ਵੱਲੋਂ ਆਇਆ ਹੈ ਜਿਸ 'ਤੇ ਤੁਸੀਂ ਭਰੋਸਾ ਕਰਦੇ ਹੋ ਪਰ ਉਹ ਕਿਸੇ ਨਵੇਂ ਫ਼ੋਨ ਨੰਬਰ, ਈਮੇਲ ਪਤੇ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪ੍ਰੋਫ਼ਾਈਲ ਦੀ ਵਰਤੋਂ ਕਰ ਰਹੇ ਹਨ ਤਾਂ ਸ਼ੱਕੀ ਬਣੋ। ਜਵਾਬ ਦੇਣ ਤੋਂ ਪਹਿਲਾਂ, ਕਿਸੇ ਅਜਿਹੇ ਚੈਨਲ ਦੁਆਰਾ ਜਿਸ 'ਤੇ ਤੁਸੀਂ ਭਰੋਸਾ ਕਰ ਸਕਦੇ ਹੋ ਉਹਨਾਂ ਨਾਲ ਸੰਪਰਕ ਕਰਕੇ ਇਸ ਗੱਲ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ ਕਿ ਤੁਹਾਨੂੰ ਸੁਨੇਹਾ ਭੇਜਣ ਵਾਲਾ ਵਿਅਕਤੀ ਜਾਂ ਸੰਸਥਾ ਅਸਲ ਵਿੱਚ ਉਹ ਵਿਅਕਤੀ ਜਾਂ ਸੰਸਥਾ ਹੈ ਜੋ ਉਹ ਕਹਿ ਰਹੇ ਹਨ ਕਿ ਉਹ ਹਨ। ਉਦਾਹਰਨ ਲਈ, ਜੇਕਰ ਤੁਹਾਨੂੰ ਕੋਈ ਟੈਕਸਟ ਸੁਨੇਹਾ ਮਿਲਦਾ ਹੈ ਜੋ ਲੱਗਦਾ ਹੈ ਕਿ ਇਹ ਤੁਹਾਡੇ ਬੱਚਿਆਂ ਵਿੱਚੋਂ ਕਿਸੇ ਦਾ ਹੈ, ਪਰ ਇਹ ਇੱਕ ਨਵੇਂ ਨੰਬਰ ਤੋਂ ਆਉਂਦਾ ਹੈ, ਤਾਂ ਜਵਾਬ ਨਾ ਦਿਓ। ਉਨ੍ਹਾਂ ਨੂੰ ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਸੁਨੇਹਾ ਭੇਜੋ ਤਾਂ ਜੋ ਪਹਿਲਾਂ ਇਹ ਪਤਾ ਲਗਾਇਆ ਜਾ ਸਕੇ ਕਿ ਉਨ੍ਹਾਂ ਨੇ ਸੱਚਮੁੱਚ ਆਪਣਾ ਫ਼ੋਨ ਨੰਬਰ ਬਦਲਿਆ ਹੈ।

ਕੀ ਤੁਸੀ ਜਾਣਦੇ ਹੋ:

ਸਾਈਬਰ ਅਪਰਾਧੀ ਬਹੁਤ ਚਲਾਕ ਹੁੰਦੇ ਹਨ ਅਤੇ ਉਹ ਕਿਸੇ ਜਾਣੇ-ਪਛਾਣੇ ਨਾਮ ਅਤੇ ਈਮੇਲ ਪਤੇ ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦੇ ਹਨ।

ਸਾਵਧਾਨ ਰਹੋ ਜੇਕਰ:

- ਤੁਹਾਨੂੰ ਤੁਰੰਤ ਕਿਸੇ ਬਿੱਲ ਦਾ ਭੁਗਤਾਨ ਕਰਨ ਲਈ ਕਿਹਾ ਜਾਂਦਾ ਹੈ।
- ਤੁਹਾਨੂੰ ਆਪਣੇ ਵੇਰਵੇ ਜਾਂ ਪਾਸਵਰਡ ਬਦਲਣ ਲਈ ਕਿਹਾ ਜਾਂਦਾ ਹੈ।
- ਤੁਹਾਨੂੰ ਕਿਸੇ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਜਾਂ ਅਟੈਚਮੈਂਟ ਖੋਲ੍ਹਣ ਲਈ ਕਿਹਾ ਜਾਂਦਾ ਹੈ।

ਸਿੱਟਾ

ਹੁਣ ਜਦੋਂ ਤੁਸੀਂ ਇੰਟਰਨੈੱਟ ਨੂੰ ਵਧੇਰੇ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਵਰਤਣ ਲਈ ਗਿਆਨ ਨਾਲ ਲੈਸ ਹੋ ਗਏ ਹੋ, ਤਾਂ ਤੁਸੀਂ ਭਰੋਸੇ ਨਾਲ ਬ੍ਰਾਊਜ਼ ਕਰ (ਇੰਟਰਨੈੱਟ ਵਰਤ) ਸਕਦੇ ਹੋ ਅਤੇ ਆਪਣੇ ਸਮੇਂ ਦਾ ਔਨਲਾਈਨ ਆਨੰਦ ਲੈਣਾ ਜਾਰੀ ਰੱਖ ਸਕਦੇ ਹੋ।

ਬੱਸ ਯਾਦ ਰੱਖੋ, ਸਾਈਬਰ ਅਪਰਾਧੀ ਹਮੇਸ਼ਾ ਲੋਕਾਂ ਨੂੰ ਨਿਸ਼ਾਨਾ ਬਣਾਉਣ ਦੇ ਨਵੇਂ ਤਰੀਕਿਆਂ ਨਾਲ ਆ ਰਹੇ ਹਨ।

ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਤੁਹਾਡੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀ ਜਾਣਕਾਰੀ ਨੂੰ ਵਧਾਉਣਾ ਅਤੇ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਦੇ ਨਵੇਂ ਤਰੀਕੇ ਸਿੱਖਣਾ ਕਦੇ ਵੀ ਘਾਟੇ ਦਾ ਸੌਦਾ ਨਹੀਂ ਹੁੰਦਾ ਹੈ।

ਬੋਨਸ ਸੁਝਾਅ।

ਕੀ ਤੁਸੀਂ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਦੇ ਹੋਰ ਤਰੀਕੇ ਸਿੱਖਣਾ ਚਾਹੁੰਦੇ ਹੋ? ਹੇਠਾਂ ਦਿੱਤੇ ਸੁਝਾਅ ਦੇਖੋ।

ਤੁਸੀਂ ਜੋ ਪੋਸਟ ਕਰਨ ਜਾ ਰਹੇ ਹੋ ਉਸ ਬਾਰੇ ਸੋਚੋ।

ਤੁਹਾਡੇ ਦੁਆਰਾ ਔਨਲਾਈਨ ਸਾਂਝੀ ਕੀਤੀ ਜਾਣ ਵਾਲੀ ਜਾਣਕਾਰੀ ਬਾਰੇ ਧਿਆਨ ਨਾਲ ਸੋਚੋ ਅਤੇ ਇਹ ਵੀ ਕਿ ਇਸਨੂੰ ਕੌਣ ਦੇਖੇਗਾ। ਸਿਰਫ਼ ਉਨ੍ਹਾਂ ਲੋਕਾਂ ਤੋਂ ਦੋਸਤੀ ਦੀਆਂ ਬੇਨਤੀਆਂ ਸਵੀਕਾਰ ਕਰੋ ਜਿੰਨ੍ਹਾਂ ਨੂੰ ਤੁਸੀਂ ਅਸਲ ਜ਼ਿੰਦਗੀ ਵਿੱਚ ਜਾਣਦੇ ਹੋ।

ਨਵੇਂ ਖ਼ਤਰਿਆਂ ਬਾਰੇ ਚੇਤਾਵਨੀਆਂ ਪ੍ਰਾਪਤ ਕਰੋ।

ਸਾਡੀ ਮੁਫ਼ਤ ਚੇਤਾਵਨੀ ਸੇਵਾ ਲਈ ਸਾਈਨ ਅੱਪ ਕਰੋ। ਜਦੋਂ ਵੀ ਸਾਨੂੰ ਕੋਈ ਨਵਾਂ ਸਾਈਬਰ ਖ਼ਤਰਾ ਮਿਲਦਾ ਹੈ ਤਾਂ ਇਹ ਤੁਹਾਨੂੰ ਇਸ ਬਾਰੇ ਸੂਚਿਤ ਕਰੇਗਾ।

ਇਹ ਤੁਹਾਨੂੰ ਇਹ ਸਲਾਹ ਵੀ ਦੇਵੇਗਾ ਕਿ ਜੇਕਰ ਕੋਈ ਹਮਲਾ ਹੁੰਦਾ ਹੈ ਤਾਂ ਕੀ ਕਰਨਾ ਹੈ।

ਪਰਿਵਾਰ ਅਤੇ ਦੋਸਤਾਂ ਨਾਲ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਬਾਰੇ ਗੱਲ ਕਰੋ।

ਹੁਣ ਜਦੋਂ ਤੁਸੀਂ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਵਿੱਚ ਨਿਪੁੰਨ ਹੋ ਗਏ ਹੋ, ਤਾਂ ਜੋ ਤੁਸੀਂ ਸਿੱਖਿਆ ਹੈ ਆਪਣੇ ਪਰਿਵਾਰ ਅਤੇ ਦੋਸਤਾਂ ਨਾਲ ਸਾਂਝਾ ਕਰੋ। ਤੁਹਾਡਾ ਗਿਆਨ ਉਹਨਾਂ ਨੂੰ ਕਿਸੇ ਮੁਸ਼ਕਲ ਸਥਿਤੀ ਵਿੱਚੋਂ ਬਾਹਰ ਨਿੱਕਲਣ ਵਿੱਚ ਮੱਦਦ ਕਰ ਸਕਦਾ ਹੈ!

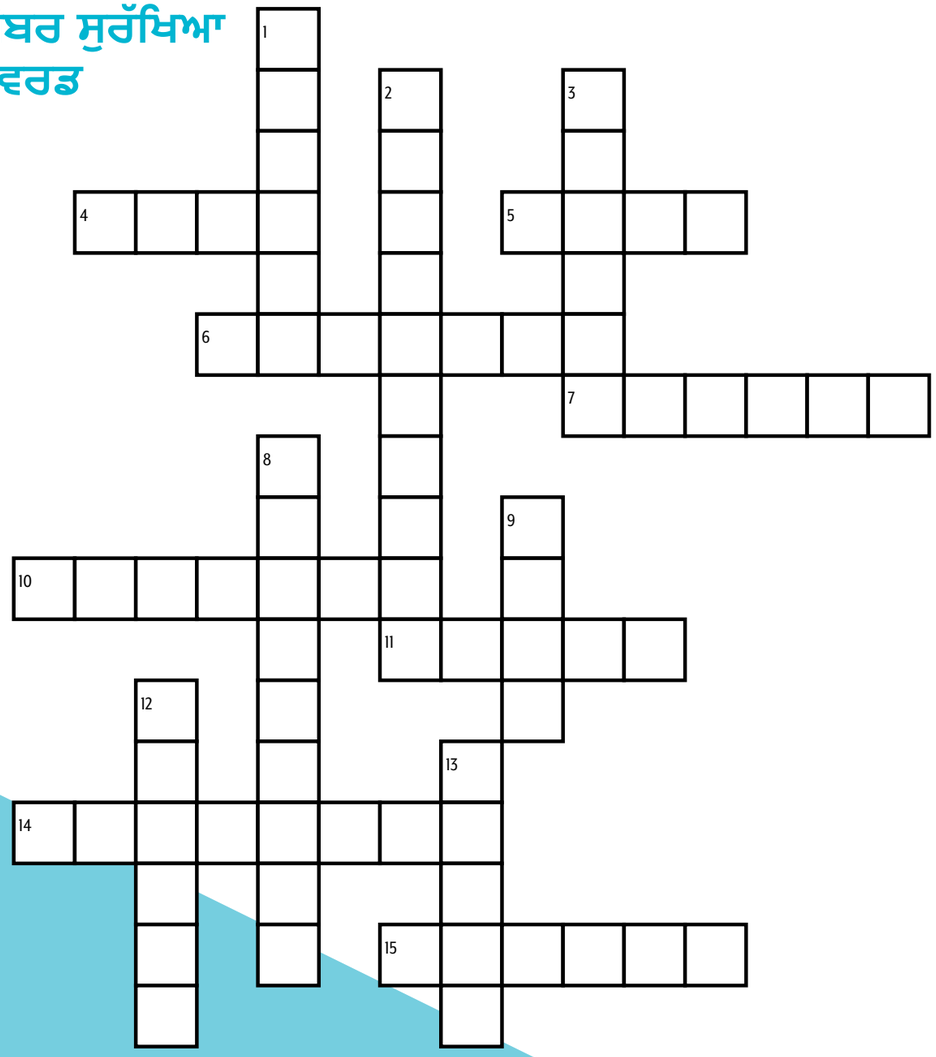
ਜਦੋਂ ਤੁਸੀਂ ਬੈਂਕ ਸੰਬੰਧੀ ਚੀਜ਼ਾਂ ਜਾਂ ਔਨਲਾਈਨ ਖ਼ਰੀਦਦਾਰੀ ਕਰ ਰਹੇ ਹੋਵੋ ਤਾਂ ਜਨਤਕ Wi-Fi ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਬਚੋ।

ਜਨਤਕ Wi-Fi ਵੀਡੀਓ ਦੇਖਣ ਜਾਂ ਵੈੱਬਸਾਈਟਾਂ 'ਤੇ ਕੁੱਝ ਪੜ੍ਹਨ ਲਈ ਬਹੁਤ ਵਧੀਆ ਹਨ ਪਰ ਪੈਸੇ ਵਾਲੀ ਕੋਈ ਵੀ ਔਨਲਾਈਨ ਗਤੀਵਿਧੀ ਨੂੰ ਆਪਣੇ ਘਰ ਦੇ ਇੰਟਰਨੈਟ ਕਨੈਕਸ਼ਨ ਲਈ ਹੀ ਸੀਮਤ ਰੱਖੋ। ਜਨਤਕ Wi-Fi ਦੀ ਵਰਤੋਂ ਖ਼ਤਰੇ ਭਰੀ ਹੋ ਸਕਦੀ ਹੈ।

ਆਸਟ੍ਰੇਲੀਆ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਸਾਈਬਰ ਅਪਰਾਧਾਂ ਅਤੇ ਘਟਨਾਵਾਂ ਦੀ ਰਿਪੋਰਟ ਕਰੋ।

ਜੇਕਰ ਤੁਸੀਂ ਸੋਚਦੇ ਹੋ ਕਿ ਤੁਸੀਂ ਸਾਈਬਰ ਅਪਰਾਧ ਦੇ ਸ਼ਿਕਾਰ ਹੋਏ ਹੋ, ਤਾਂ ਜਲਦੀ ਕਾਰਵਾਈ ਕਰੋ। ਹੋਰ ਸਲਾਹ cyber.gov.au 'ਤੇ ਉਪਲਬਧ ਹੈ।

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਕ੍ਰਾਸਵਰਡ



ਹੇਠਾਂ ਵੱਲ ਨੂੰ

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

ਆਰ-ਪਾਰ

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

ਪੂਰਕ ਗਾਈਡਾਂ।

ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ ਕਿਰਪਾ ਕਰਕੇ ਸਾਡੀ ਨਿੱਜੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਲੜੀ ਨੂੰ ਦੇਖੋ: ਇਸ ਲੜੀ ਵਿਚਲੀਆਂ ਤਿੰਨ ਗਾਈਡਾਂ ਆਮ ਆਸਟ੍ਰੇਲੀਅਨ ਲੋਕਾਂ ਨੂੰ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀਆਂ ਬੁਨਿਆਦੀ ਗੱਲਾਂ ਨੂੰ ਸਮਝਣ ਵਿੱਚ ਅਤੇ ਤੁਸੀਂ ਆਪਣੇ-ਆਪ ਨੂੰ ਆਮ ਸਾਈਬਰ ਖਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਲਈ ਕਿਵੇਂ ਕਾਰਵਾਈ ਕਰ ਸਕਦੇ ਹੋ, ਬਾਰੇ ਮੱਦਦ ਕਰਨ ਲਈ ਤਿਆਰ ਕੀਤੀਆਂ ਗਈਆਂ ਹਨ।

ਤੁਸੀਂ **cyber.gov.au** 'ਤੇ ਤਿੰਨੇਂ ਗਾਈਡਾਂ ਤੱਕ ਪਹੁੰਚ ਕਰ ਸਕਦੇ ਹੋ

ਕ੍ਰਾਸਵਰਡ ਦੇ ਜਵਾਬ:

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

ਟਿੱਪਣੀਆਂ।

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

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

ਇਹ ਨੰ ਬਰ ਸਿ ਰਫ਼ ਆਸਟ੍ਰਰੇਲੀਆ ਵਿ ੱਚ ਵਰਤੋ ਲਈ ਉਪਲਬਧ ਹੈ।.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre