Community Resilience
to Foreign Interference

National Cyber Security Centre

ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰੱਖਣਾ

ਮੇਰੇ ਲਈ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਮਹੱਤਵਪੂਰਨ ਕਿਉਂ ਹੈ?

ਇੰਟਰਨੈੱਟ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਦਭੁਤ ਪਲੇਟਫਾਰਮ ਹਨ ਜੋ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨ ਅਤੇ ਦੋਸਤਾਂ ਅਤੇ ਪਰਿਵਾਰ ਨਾਲ ਸੰਪਰਕ ਵਿੱਚ ਰਹਿਣ ਵਿੱਚ ਸਾਡੀ ਮਦਦ ਕਰਦੇ ਹਨ।

ਹਾਲਾਂਕਿ, ਅਪਰਾਧੀ ਅਤੇ ਹੋਰ ਗ਼ੈਰ-ਕਾਨੂੰਨੀ ਸੰਗਠਨ ਵੀ ਇਹਨਾਂ ਦੀ ਵਰਤੋਂ ਤੁਹਾਡੇ ਪੈਸੇ, ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਪ੍ਰਾਪਤ ਕਰਨ ਜਾਂ ਤੁਹਾਨੂੰ ਡਰਾਉਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨ ਲਈ ਕਰਦੇ ਹਨ।

ਉਹ ਦੁਨੀਆ ਵਿੱਚ ਕਿਸੇ ਵੀ ਥਾਂ ਤੋਂ ਕੰਮ ਕਰ ਸਕਦੇ ਹਨ, ਜ਼ਿਆਦਾਤਰ ਭਾਸ਼ਾਵਾਂ ਚੰਗੀ ਤਰ੍ਹਾਂ ਬੋਲ ਸਕਦੇ ਹਨ ਅਤੇ ਯਕੀਨਨ ਜਾਅਲੀ ਵੈੱਬਸਾਈਟਾਂ ਬਣਾ ਸਕਦੇ ਹਨ। ਉਹ ਈਮੇਲ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਤੇ ਟੈਕਸਟ ਮੈਸੇਜ਼ ਰਾਹੀਂ ਤੁਹਾਡੇ ਨਾਲ ਸੰਪਰਕ ਕਰਨਗੇ ਅਤੇ ਉਹ ਤੁਹਾਨੂੰ ਡਰ ਜਾਂ ਚਿੰਤਾ ਮਹਿਸੂਸ ਕਰਵਾਉਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨਗੇ, ਇਸ ਲਈ ਤੁਸੀਂ ਸਪੱਸ਼ਟ ਤੌਰ ਉੱਤੇ ਨਹੀਂ ਸੋਚ ਰਹੇ ਹੋ।

ਇਸ ਸਭ ਦਾ ਮਤਲਬ ਹੈ ਕਿ ਤੁਹਾਨੂੰ ਤਿਆਰ ਰਹਿਣ ਦੀ ਲੋੜ ਹੈ ਅਤੇ ਉਹਨਾਂ ਦੁਆਰਾ ਵਰਤੀਆਂ ਜਾਣ ਵਾਲੀਆਂ ਚਾਲਾਂ ਤੋਂ ਹਮੇਸ਼ਾ ਜਾਣੂ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ।

ਕੁਝ ਆਮ ਸਮੱਸਿਆਵਾਂ ਕੀ ਹਨ ਜੋ ਮੈਨੂੰ ਔਨਲਾਈਨ ਪੇਸ਼ ਆ ਸਕਦੀਆਂ ਹਨ?

ਇਹ ਕੁਝ ਸਭ ਤੋਂ ਆਮ ਸਥਿਤੀਆਂ ਹਨ ਜੋਕਿ ਅਸੀਂ ਦੇਖਦੇ ਹਾਂ।

- **ਤੁਹਾਨੂੰ ਇੱਕ ਸ਼ੱਕੀ ਈਮੇਲ ਜਾਂ ਟੈਕਸਟ ਮੈਸੇਜ਼ ਮਿਲਦਾ ਹੈ ਜੋ ਤੁਹਾਨੂੰ ਇੱਕ ਲਿੰਕ ਉੱਤੇ ਕਲਿੱਕ ਕਰਨ ਲਈ ਕਹਿੰਦਾ ਹੈ।**
  ਇਹ ਲਿੰਕ ਅਕਸਰ ਜਾਅਲੀ ਵੈੱਬਸਾਈਟਾਂ ਵੱਲ ਲੈ ਜਾਂਦੇ ਹਨ ਜੋਕਿ ਤੁਹਾਡੇ ਲੌਗਿਨ ਜਾਂ ਵਿੱਤੀ ਵੇਰਵਿਆਂ ਨੂੰ ਚੋਰੀ ਕਰਨ ਲਈ ਤਿਆਰ ਕੀਤੀਆਂ ਗਈਆਂ ਹਨ।

- **ਤੁਹਾਨੂੰ ਇੱਕ ਸ਼ੱਕੀ ਕਾਲ ਆਉਂਦੀ ਹੈ ਜੋਕਿ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਮੰਗਦੀ ਹੈ।**
  ਜਿਵੇਂਕਿ ਉਪਰੋਕਤ ਕਾਲ ਕਰਨ ਵਾਲਾ ਤੁਹਾਡੇ ਬੈਂਕ ਤੋਂ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰੇਗਾ ਅਤੇ ਜਾਣਕਾਰੀ ਮੰਗੇਗਾ।

- **ਤੁਸੀਂ ਕਿਸੇ ਵਿਅਕਤੀ ਤੋਂ ਸੰਚਾਰ ਪ੍ਰਾਪਤ ਕਰਦੇ ਹੋ ਜੋਕਿ ਇੱਕ ਅਧਿਕਾਰਤ ਵਿਅਕਤੀ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰ ਰਿਹਾ ਹੈ, ਤੁਹਾਡੇ ਤੋਂ ਕੁਝ ਕਰਵਾਉਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰ ਰਿਹਾ ਹੈ।**
  ਅਕਸਰ ਵਿਅਕਤੀ ਕਿਸੇ ਨਾ ਕਿਸੇ ਤਰ੍ਹਾਂ ਦੀ ਧਮਕੀ ਦਿੰਦਾ ਹੈ।

- **ਕੋਈ ਵਿਅਕਤੀ ਤੁਹਾਡੇ ਇੱਕ ਜਾਂ ਵੱਧ ਔਨਲਾਈਨ ਖਾਤਿਆਂ ਵਿੱਚ ਦਾਖਲ ਹੋ ਜਾਂਦਾ ਹੈ (ਉਦਾਹਰਨ ਲਈ: ਈਮੇਲ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ)।**
  ਜੇਕਰ ਕੋਈ ਤੁਹਾਡੇ ਔਨਲਾਈਨ ਖਾਤੇ ਵਿੱਚ ਦਾਖਲ ਹੁੰਦਾ ਹੈ ਤਾਂ ਉਹ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰ ਸਕਦਾ ਹੈ, ਭੁਗਤਾਨਾਂ ਨੂੰ ਕਿਤੇ ਹੋਰ ਮੋੜ ਸਕਦਾ ਹੈ, ਅਤੇ ਸੰਭਾਵੀ ਤੌਰ ਉੱਤੇ ਤੁਹਾਡੇ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰਕੇ ਤੁਹਾਡੇ ਦੋਸਤਾਂ ਜਾਂ ਪਰਿਵਾਰ ਨੂੰ ਨਿਸ਼ਾਨਾ ਬਣਾ ਸਕਦਾ ਹੈ।

- **ਤੁਹਾਡੇ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਦੇ ਵੇਰਵੇ ਚੋਰੀ ਹੋ ਗਏ ਹਨ, ਜਾਂ ਤੁਹਾਡੇ ਨਾਲ ਜਾਅਲੀ ਵਿਕਰੀ ਜਾਂ ਨਿਵੇਸ਼ ਵਿੱਚ ਪੈਸੇ ਦੀ ਧੋਖਾਧੜੀ ਕੀਤੀ ਹੈ।**
  ਘੁਟਾਲੇਬਾਜ਼ ਉਮੀਦ ਕਰ ਰਹੇ ਹਨ ਕਿ ਤੁਸੀਂ ਇੱਕ ਚੰਗਾ ਸੌਦਾ ਦੇਖੋਗੇ ਅਤੇ ਬਿਨਾਂ ਸੋਚੇ-ਸਮਝੇ ਭੁਗਤਾਨ ਕਰਨਾ ਚਾਹੋਗੇ। ਜਾਂ ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਇੱਕ ਅਸਲ ਵੈਬਸਾਈਟ ਇੱਕ ਡੇਟਾ ਉਲੰਘਣਾ ਵਿੱਚ ਫਸ ਗਈ ਹੋਵੇ ਅਤੇ ਤੁਹਾਡੇ ਵੇਰਵੇ ਔਨਲਾਈਨ ਲੀਕ ਹੋ ਗਏ ਹੋਣ।

ਇੱਥੇ ਹੋਰ ਪਰਿਸਥਿਤੀਆਂ ਹਨ: ਹੁਣੇ ਮਦਦ ਪ੍ਰਾਪਤ ਕਰੋ - ਆਪਣੇ ਔਨਲਾਈਨ ਮਾਲਕ ਆਪ ਬਣੋ

ਮੈਂ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਕਿਵੇਂ ਰਹਿ ਸਕਦਾ/ਸਕਦੀ ਹਾਂ?

ਲੰਬੇ ਅਤੇ ਅਨੋਖੇ ਪਾਸਵਰਡ।

- ਪਾਸਵਰਡ ਜਿੰਨਾ ਲੰਬਾ ਹੁੰਦਾ ਹੈ, ਇਹ ਓਨਾ ਹੀ ਮਜ਼ਬੂਤ ਹੁੰਦਾ ਹੈ।

- ਚਾਰ ਬੇਤਰਤੀਬੇ ਸ਼ਬਦਾਂ ਨੂੰ ਇਕੱਠੇ ਜੋੜ ਕੇ (ਉਦਾਹਰਨ ਲਈ: TriangleRhinoOperationShoes) ਅਤੇ ਲੋੜ ਪੈਣ 'ਤੇ ਨੰਬਰ, ਵੱਡੇ ਅੱਖਰ ਅਤੇ ਚਿੰਨ੍ਹ ਜੋੜ ਕੇ 16 ਤੋਂ ਵੱਧ ਅੱਖਰਾਂ ਦਾ ਇੱਕ ਯਾਦਗਾਰੀ ਪਾਸਵਰਡ ਬਣਾਓ (ਉਦਾਹਰਨ ਲਈ: Triangle&"Rhino"Operation2Shoes)।

- ਮਹੱਤਵਪੂਰਨ ਤੌਰ ਉੱਤੇ, ਆਪਣੇ ਪਾਸਵਰਡ ਨਾ ਦੁਹਰਾਓ। ਜੇਕਰ ਕਿਸੇ ਅਪਰਾਧੀ ਨੂੰ ਤੁਹਾਡਾ ਪਾਸਵਰਡ ਮਿਲਦਾ ਹੈ ਤਾਂ ਉਹ ਦੂਜੇ ਖਾਤਿਆਂ ਉੱਤੇ ਵੀ ਇਸ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨਗੇ।

- ਤੁਹਾਡੇ ਲਈ ਤੁਹਾਡੇ ਪਾਸਵਰਡ ਯਾਦ ਰੱਖਣ ਅਤੇ ਨਵੇਂ ਪਾਸਵਰਡ ਬਣਾਉਣ ਲਈ ਇੱਕ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- ਚੰਗੇ ਪਾਸਵਰਡ ਬਣਾਓ - ਆਪਣੇ ਔਨਲਾਈਨ ਮਾਲਕ ਆਪ ਬਣੋ

ਦੋ-ਕਾਰਕ ਪ੍ਰਮਾਣਿਕਤਾ ਨੂੰ ਚਾਲੂ ਕਰੋ।

- ਇਹ ਜਾਣਕਾਰੀ ਦਾ ਇੱਕ ਵਾਧੂ ਟੁਕੜਾ ਹੈ – ਆਮ ਤੌਰ ਉੱਤੇ ਤੁਹਾਡੇ ਫ਼ੋਨ ਉੱਤੇ ਇੱਕ ਕੋਡ – ਜਿਸ ਦੀ ਤੁਹਾਨੂੰ ਕਿਸੇ ਵੈੱਬਸਾਈਟ ਵਿੱਚ ਲੌਗਿਨ ਕਰਨ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ।
- ਇਹ ਤਕਨੀਕ ਅਵਿਸ਼ਵਾਸੀ ਤੌਰ ਉੱਤੇ ਮਜ਼ਬੂਤ ਹੈ ਅਤੇ ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਵਿੱਚ ਦਾਖਲ ਹੋਣ ਦੀਆਂ ਜ਼ਿਆਦਾਤਰ ਕੋਸ਼ਿਸ਼ਾਂ ਨੂੰ ਰੋਕ ਸਕਦੀ ਹੈ।
- ਅਸੀਂ ਇੱਕ 'ਪ੍ਰਮਾਣਿਕ ਐਪ' ਵਰਤਣ ਦੀ ਸਿਫ਼ਾਰਿਸ਼ ਕਰਦੇ ਹਾਂ, ਜਿੱਥੇ ਇਹ ਸਮਰਥਿਤ ਹੈ।
- ਦੋ ਕਾਰਕ ਪ੍ਰਮਾਣਿਕਤਾ ਸਥਾਪਤ ਕਰੋ (2FA) - ਆਪਣੇ ਔਨਲਾਈਨ ਮਾਲਕ ਆਪ ਬਣੋ

ਔਨਲਾਈਨ ਨਿਜੀ ਬਣੇ ਰਹੋ।

- ਸੋਸ਼ਲ ਮੀਡੀਆ ਉੱਤੇ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਦਾ ਸਭ ਤੋਂ ਵਧੀਆ ਵਿਕਲਪ ਤੁਹਾਡੀ ਗੋਪਨੀਯਤਾ ਸੈਟਿੰਗਾਂ ਨੂੰ ਚਾਲੂ ਕਰਨਾ ਹੈ।
- ਇਹ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਸਮੇਤ ਬੇਤਰਤੀਬੇ ਲੋਕਾਂ ਨੂੰ ਤੁਹਾਡੀਆਂ ਪੋਸਟਾਂ ਦੇਖਣ ਜਾਂ ਤੁਹਾਨੂੰ ਮੈਸੇਜ਼ ਭੇਜਣ ਦੇ ਯੋਗ ਹੋਣ ਤੋਂ ਰੋਕ ਦੇਵੇਗਾ।
- ਫਿਰ ਵੀ ਆਪਣੇ, ਆਪਣੇ ਪਰਿਵਾਰ ਜਾਂ ਆਪਣੇ ਦੋਸਤਾਂ ਬਾਰੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਪੋਸਟ ਕਰਨ ਵਿੱਚ ਸਾਵਧਾਨ ਰਹੋ।
- ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਸੰਪਰਕ ਓਹੀ ਹਨ ਜੋ ਉਹ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰਦੇ ਹਨ।
- ਨਕਲੀ ਦੋਸਤ ਬੇਨਤੀਆਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ। ਉਨ੍ਹਾਂ ਲੋਕਾਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ ਜੋ ਪੱਤਰਕਾਰ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰਦੇ ਹਨ ਜਾਂ ਹੋਰ ਜਿਨ੍ਹਾਂ ਨੂੰ ਤੁਸੀਂ ਚੰਗੀ ਤਰ੍ਹਾਂ ਨਹੀਂ ਜਾਣਦੇ ਹੋ।
- ਆਪਣੀ ਗੋਪਨੀਯਤਾ ਨੂੰ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਕਰੋ - ਆਪਣੇ ਔਨਲਾਈਨ ਮਾਲਕ ਆਪ ਬਣੋ

ਹਰ ਚੀਜ਼ ਨੂੰ ਅੱਪਡੇਟ ਰੱਖੋ।

- ਜਦੋਂ ਤੁਸੀਂ ਆਪਣੇ ਫ਼ੋਨ, ਕੰਪਿਊਟਰ ਜਾਂ ਸੌਫਟਵੇਅਰ ਨੂੰ ਅੱਪਡੇਟ ਕਰਦੇ ਹੋ, ਤਾਂ ਇਹ ਸੁਰੱਖਿਆ ਵਿੱਚ ਹੋਣ ਵਾਲੇ ਕਿਸੇ ਵੀ ਛੇਕਾਂ ਨੂੰ ਰੋਕਦੇ ਹਨ।
- ਅਪਰਾਧੀ ਹਮੇਸ਼ਾ ਅੰਦਰ ਦਾਖਲ ਹੋਣ ਦੇ ਤਰੀਕੇ ਲੱਭਦੇ ਰਹਿੰਦੇ ਹਨ ਅਤੇ ਅੱਪਡੇਟ ਕਮਜ਼ੋਰੀਆਂ ਨੂੰ ਠੀਕ ਕਰਦੇ ਹਨ।
- ਆਪਣੀਆਂ ਡਿਵਾਈਸਾਂ ਨੂੰ ਨਿਯਮਿਤ ਤੌਰ ਉੱਤੇ ਰੀਸਟਾਰਟ ਕਰੋ।
- ਆਪਣੇ ਅੱਪਡੇਟ ਨਾਲ ਜੁੜੇ ਰਹੋ - ਆਪਣੇ ਔਨਲਾਈਨ ਮਾਲਕ ਆਪ ਬਣੋ

ਘੁਟਾਲਿਆਂ ਤੋਂ ਸੁਚੇਤ ਰਹੋ।

- ਸਭ ਤੋਂ ਵਧੀਆ ਸਲਾਹ ਇਹ ਹੈ ਕਿ ਇਹਨਾਂ ਘੁਟਾਲਿਆਂ ਤੋਂ ਸੁਚੇਤ ਰਹੋ ਅਤੇ ਉਹਨਾਂ ਉੱਤੇ ਨਜ਼ਰ ਬਣਾਏ ਰੱਖੋ।
- ਜੇਕਰ ਕੁਝ ਗਲਤ ਲੱਗਦਾ ਹੈ, ਤਾਂ ਉਸ ਵਿਅਕਤੀ ਨਾਲ ਸੰਪਰਕ ਨਾ ਕਰੋ ਜਿਸ ਨੇ ਤੁਹਾਨੂੰ ਸੰਪਰਕ ਕੀਤਾ ਹੈ। ਖਾਸ ਤੌਰ ਉੱਤੇ ਸਾਵਧਾਨ ਰਹੋ ਜੇਕਰ ਉਹ ਪੈਸੇ ਦੀ ਮੰਗ ਕਰਦੇ ਹਨ, ਭਾਵੇਂ ਉਹ ਦੋਸਤਾਨਾ ਲੱਗਦੇ ਹੋਣ।
- ਅਜੀਬ ਲਿੰਕ ਅਤੇ ਈਮੇਲ ਪਤੇ ਦੇਖੋ) ਤੁਹਾਡਾ ਬੈਂਕ ਤੁਹਾਨੂੰ ਜੀਮੇਲ :ਉਦਾਹਰਨ ਲਈ)Gmail) ਖਾਤੇ ਤੋਂ ਈਮੇਲ ਨਹੀਂ ਭੇਜੇਗਾ ।(
- ਟੈਕਸਟ ਮੈਸੇਜ਼ਾਂ ਵਿੱਚ ਆਏ ਲਿੰਕਾਂ ਉੱਤੇ ਕਦੇ ਵੀ ਕਲਿੱਕ *ਨਾ* ਕਰੋ।
- ਸਿਰਫ਼ ਅਧਿਕਾਰਤ ਐਪ ਸਟੋਰਾਂ ਤੋਂ ਆਪਣੀ ਡਿਵਾਈਸ ਉੱਤੇ ਐਪਸ ਡਾਊਨਲੋਡ ਕਰੋ।
- ਜੇਕਰ ਸ਼ੱਕ ਹੈ, ਤਾਂ ਉਸ ਸੰਗਠਨ ਨਾਲ ਸੰਪਰਕ ਕਰੋ ਜਿਸ ਨੇ ਤੁਹਾਡੇ ਨਾਲ ਸਿੱਧਾ ਸੰਪਰਕ ਕੀਤਾ ਹੈ ਅਤੇ ਤੁਹਾਨੂੰ ਭੇਜੇ ਗਏ ਕਿਸੇ ਵੀ ਲਿੰਕ ਜਾਂ ਫ਼ੋਨ ਨੰਬਰ ਦੀ ਪਾਲਣਾ ਨਾ ਕਰੋ।
- ਤੁਹਾਡੇ ਲਈ, ਤੁਹਾਡੇ ਭਾਈਚਾਰੇ ਲਈ, ਅਤੇ ਤੁਹਾਡੇ ਨਾਲ ਸਬੰਧਤ ਕਿਸੇ ਵੀ ਸਮੂਹ ਲਈ ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ ਖਤਰਿਆਂ ਤੋਂ ਸੁਚੇਤ ਰਹਿਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ।

ਆਪਣੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਕਰੋ।

- ਇਨਕ੍ਰਿਪਟਡ ਮੈਸੇਜਿੰਗ ਐਪਸ ਦੀ ਵਰਤੋਂ ਕਰੋ, ਜਿਵੇਂਕਿ ਸਿਗਨਲ। ਇਹ ਕਿਸੇ ਨੂੰ ਵੀ ਤੁਹਾਡੇ ਮੈਸੇਜ਼ਾਂ ਨੂੰ ਪੜ੍ਹਨ ਦੇ ਯੋਗ ਹੋਣ ਤੋਂ ਰੋਕ ਦੇਵੇਗਾ।

- ਸਿਰਫ਼ ਉਸੇ ਵੈੱਬਸਾਈਟ ਨਾਲ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰੋ ਜੇਕਰ ਪਤਾ HTTPS ਨਾਲ ਸ਼ੁਰੂ ਹੁੰਦਾ ਹੈ। S ਦਾ ਮਤਲਬ ਹੈ "secure" (ਸੁਰੱਖਿਅਤ) ਅਤੇ ਇਸਦਾ ਮਤਲਬ ਹੈ ਕਿ ਤੁਹਾਡੇ ਅਤੇ ਵੈੱਬਸਾਈਟ ਵਿਚਕਾਰ ਭੇਜੀ ਗਈ ਕੋਈ ਵੀ ਜਾਣਕਾਰੀ ਐਨਕ੍ਰਿਪਟ ਕੀਤੀ ਗਈ ਹੈ।
- ਇੱਕ ਵਰਚੁਅਲ ਪ੍ਰਾਈਵੇਟ ਨੈੱਟਵਰਕ (VPN) ਦੀ ਵਰਤੋਂ ਕਰਨ ਉੱਤੇ ਵਿਚਾਰ ਕਰੋ ਜੋ ਤੁਹਾਡੇ ਡੇਟਾ ਦੀ ਸੁਰੱਖਿਆ ਕਰ ਸਕਦਾ ਹੈ ਅਤੇ ਤੁਹਾਡੇ ਟਿਕਾਣੇ ਨੂੰ ਲੁਕਾ ਸਕਦਾ ਹੈ।
- ਜਾਂਚ ਕਰੋ ਕਿ ਤੁਹਾਡੀਆਂ ਐਪਸ ਨੂੰ ਕਿਹੜੇ ਡੇਟਾ ਅਤੇ ਅਨੁਮਤੀਆਂ ਤੱਕ ਪਹੁੰਚ ਹੈ। ਉਦਾਹਰਨ ਲਈ, ਇੱਕ ਫਿਟਨੈਸ ਐਪ ਨੂੰ ਤੁਹਾਡੇ ਸੰਪਰਕਾਂ ਤੱਕ ਪਹੁੰਚ ਦੀ ਲੋੜ ਨਹੀਂ ਹੈ।

ਜੇਕਰ ਮੇਰੇ ਨਾਲ ਘੁਟਾਲਾ ਜਾਂ ਉਸ ਤੋਂ ਵੀ ਜ਼ਿਆਦਾ ਗਲਤ ਕੰਮ ਹੋ ਜਾਂਦਾ ਹੈ ਤਾਂ ਮੈਂ ਕੀ ਕਰਾਂ?

ਇੱਥੇ ਬਹੁਤ ਸਾਰੀਆਂ ਥਾਵਾਂ ਹਨ ਜਿੱਥੇ ਤੁਸੀਂ ਮਦਦ ਲਈ ਜਾ ਸਕਦੇ ਹੋ। ਇਹ ਸੰਗਠਨ ਤੁਹਾਡੇ ਵੇਰਵੇ ਕਿਸੇ ਹੋਰ ਨਾਲ ਸਾਂਝੇ ਨਹੀਂ ਕਰਨਗੇ, ਜਦੋਂ ਤੱਕ ਤੁਸੀਂ ਆਪਣੀ ਸਹਿਮਤੀ ਨਹੀਂ ਦਿੰਦੇ।

ਤੁਸੀਂ CERT NZ ਪੋਰਟਲ ਰਾਹੀਂ NCSC ਨੂੰ ਸਾਈਬਰ ਘਟਨਾਵਾਂ ਦੀ ਰਿਪੋਰਟ ਕਰ ਸਕਦੇ ਹੋ ਅਤੇ ਅਸੀਂ ਤੁਹਾਡੀ ਮਦਦ ਕਰ ਸਕਦੇ ਹਾਂ ਜਾਂ ਕਿਸੇ ਹੋਰ ਏਜੰਸੀ ਨਾਲ ਸੰਪਰਕ ਕਰਵਾ ਸਕਦੇ ਹਾਂ: ਘਟਨਾ ਦੀ ਰਿਪੋਰਟ ਕਰੋ | CERT NZ

ਜੇਕਰ ਤੁਸੀਂ ਪੈਸਾ ਗੁਆ ਚੁਕੇ ਹੋ, ਤਾਂ ਤੁਹਾਨੂੰ ਤੁਰੰਤ ਆਪਣੇ ਬੈਂਕ ਨਾਲ ਸੰਪਰਕ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ।

ਘੁਟਾਲੇ ਦੇ ਟੈਕਸਟ ਮੈਸੇਜ਼ਾਂ ਨੂੰ, ਅੰਦਰੂਨੀ ਮਾਮਲਿਆਂ ਦੇ ਵਿਭਾਗ ਦੁਆਰਾ ਚਲਾਈ ਜਾਂਦੀ ਸੇਵਾ, 7726 ਉੱਤੇ, ਮੁਫ਼ਤ, ਅੱਗੇ ਭੇਜਿਆ ਜਾ ਸਕਦਾ ਹੈ।