Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਲਈ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਗਾਈਡ

ਸਮੱਗਰੀ ਦੀ ਗੁੰਝਲਤਾ
ਸਰਲ ● ○ ○

cyber.gov.au

ਜਾਣ-ਪਛਾਣ

ਇੱਕ ਛੋਟੇ ਕਾਰੋਬਾਰ ਲਈ, ਮਾਮੂਲੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਘਟਨਾ ਦੇ ਵੀ ਵਿਨਾਸ਼ਕਾਰੀ ਪ੍ਰਭਾਵ ਹੋ ਸਕਦੇ ਹਨ। ਇਸ ਗਾਈਡ ਵਿੱਚ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਨੂੰ ਆਮ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਖ਼ਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਵਿੱਚ ਮੱਦਦ ਲਈ ਬੁਨਿਆਦੀ ਸੁਰੱਖਿਆ ਉਪਾਅ ਸ਼ਾਮਲ ਹਨ। ਸ਼ੁਰੂਆਤ ਕਰਨ ਲਈ, ਅਸੀਂ ਹੇਠਾਂ ਦਿੱਤੇ ਤਿੰਨ ਉਪਾਵਾਂ ਦੀ ਸਿਫ਼ਾਰਿਸ਼ ਕਰਦੇ ਹਾਂ:

- ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ (MFA) ਨੂੰ ਚਾਲੂ ਕਰੋ
- ਆਪਣੇ ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਅੱਪਡੇਟ ਕਰੋ
- ਆਪਣੀ ਜਾਣਕਾਰੀ ਦਾ ਬੈਕਅੱਪ ਲਓ

ਇਸ ਗਾਈਡ ਵਿੱਚ ਉਹ ਉਪਾਅ ਵੀ ਸ਼ਾਮਲ ਹੋ ਸਕਦੇ ਹਨ ਜੋ ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਲਈ ਢੁੱਕਵੇਂ ਨਾ ਹੋਣ, ਜਾਂ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਦੀਆਂ ਲੋੜਾਂ ਵਧੇਰੇ ਗੁੰਝਲਦਾਰ ਹੋ ਸਕਦੀਆਂ ਹਨ। ਇਸ ਗਾਈਡ ਵਿਚਲੇ ਉਪਾਵਾਂ ਨੂੰ ਪੂਰਾ ਕਰਨ ਤੋਂ ਬਾਅਦ, ਅਸੀਂ ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਨੂੰ ਜ਼ਰੂਰੀ ਅੱਠ ਕਾਰਕਾਂ (Essential Eight) ਵਿੱਚੋਂ ਮੈਚਿਓਰਿਟੀ ਲੈਵਲ ਵੰਨ (Maturity Level One) ਨੂੰ ਲਾਗੂ ਕਰਨ ਦੀ ਸਿਫ਼ਾਰਸ਼ ਕਰਦੇ ਹਾਂ। ਜੇਕਰ ਤੁਹਾਡੇ ਕੋਲ ਇਸ ਸਲਾਹ ਜਾਂ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਬਾਰੇ ਵਧੇਰੇ ਵਿਆਪਕ ਸਵਾਲ ਹਨ, ਤਾਂ ਅਸੀਂ ਤੁਹਾਨੂੰ ਕਿਸੇ IT ਪੇਸ਼ੇਵਰ ਜਾਂ ਭਰੋਸੇਯੋਗ ਸਲਾਹਕਾਰ ਨਾਲ ਗੱਲ ਕਰਨ ਦੀ ਸਿਫ਼ਾਰਸ਼ ਕਰਦੇ ਹਾਂ।

ਸਾਡੀ ਪੂਰੀ ਗਾਈਡ ਪੜ੍ਹਨ ਲਈ cyber.gov.au 'ਤੇ ਜਾਓ, ਜਿਸ ਵਿੱਚ ਇਸ ਬਾਰੇ ਸਲਾਹ ਵੀ ਸ਼ਾਮਲ ਹੈ ਕਿ ਹਰੇਕ ਉਪਾਅ ਨੂੰ ਕਿਵੇਂ ਕਰਨਾ ਹੈ।

ਵਿਸ਼ਾ-ਸੂਚੀ

ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਲਈ ਖ਼ਤਰੇ

ਧੋਖਾਧੜੀ ਕਰਨ ਲਈ ਭੇਜੇ ਜਾਂਦੇ ਸੁਨੇਹੇ

ਧੋਖਾਧੜੀ ਇੱਕ ਆਮ ਤਰੀਕਾ ਹੈ ਜਿਸ ਰਾਹੀਂ ਸਾਈਬਰ ਅਪਰਾਧੀ ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਨੂੰ ਆਪਣਾ ਨਿਸ਼ਾਨਾ ਬਣਾਉਂਦੇ ਹਨ। ਉਹਨਾਂ ਦਾ ਟੀਚਾ ਤੁਹਾਨੂੰ ਜਾਂ ਤੁਹਾਡੇ ਕਰਮਚਾਰੀਆਂ ਨੂੰ ਇਨ੍ਹਾਂ ਚੀਜ਼ਾਂ ਵਿੱਚ ਧੋਖਾ ਦੇਣਾ ਹੈ:

- ਪੈਸੇ ਜਾਂ ਗਿਫ਼ਟ ਕਾਰਡ ਭੇਜਣ ਵਿੱਚ
- ਖ਼ਤਰਨਾਕ ਲਿੰਕਾਂ ਜਾਂ ਅਟੈਚਮੈਂਟਾਂ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਲਈ
- ਪਾਸਵਰਡ ਵਰਗੀ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਦੇਣ ਲਈ।

ਸਾਈਬਰ ਅਪਰਾਧੀ ਈਮੇਲ, ਟੈਕਸਟ ਸੁਨੇਹਿਆਂ, ਫ਼ੋਨ ਕਾਲਾਂ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਰਾਹੀਂ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਨੂੰ ਧੋਖਾ ਦੇ ਸਕਦੇ ਹਨ। ਉਹ ਅਕਸਰ ਕੋਈ ਅਜਿਹਾ ਵਿਅਕਤੀ ਜਾਂ ਸੰਸਥਾ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰਨਗੇ ਜਿਸ 'ਤੇ ਤੁਸੀਂ ਭਰੋਸਾ ਕਰਦੇ ਹੋ।

ਫਿਸ਼ਿੰਗ ਹਮਲੇ

ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਲਈ ਖ਼ਾਸ ਚਿੰਤਾ ਦਾ ਕਾਰਨ **ਫਿਸ਼ਿੰਗ ਹਮਲੇ** ਹਨ। ਇਨ੍ਹਾਂ ਧੋਖਾਧੜੀਆਂ ਵਿੱਚ ਅਕਸਰ ਇੱਕ ਜਾਅਲੀ ਵੈੱਬਸਾਈਟ ਦਾ ਲਿੰਕ ਹੁੰਦਾ ਹੈ ਜਿੱਥੇ ਤੁਹਾਨੂੰ ਕਿਸੇ ਖਾਤੇ ਵਿੱਚ ਲੈਗਇਨ ਕਰਨ ਜਾਂ ਗੁਪਤ ਵੇਰਵੇ ਦਾਖਲ ਕਰਨ ਲਈ ਉਤਸ਼ਾਹਿਤ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।

ਫਿਸ਼ਿੰਗ ਹਮਲੇ ਆਮ ਤੌਰ 'ਤੇ ਤੁਹਾਡੇ ਖਾਤੇ ਦੇ ਪਾਸਵਰਡ ਚੋਰੀ ਕਰਦੇ ਹਨ। ਸਾਈਬਰ ਅਪਰਾਧੀ ਅਕਸਰ ਇਸ ਵਿਧੀ ਦੀ ਵਰਤੋਂ ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਦੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤਿਆਂ 'ਤੇ "ਕਬਜ਼ਾ ਕਰਨ" ਅਤੇ ਉਨ੍ਹਾਂ ਤੋਂ ਫਿਰੌਤੀ ਮੰਗਣ ਲਈ ਕਰਦੇ ਹਨ।

ਖ਼ਤਰੇ ਨੂੰ ਘਟਾਉਣ ਦੇ ਤਰੀਕੇ

ਜੇਕਰ ਕੋਈ ਸੁਨੇਹਾ ਕਿਸੇ ਜਾਣੀ-ਪਛਾਣੀ ਸੰਸਥਾ ਤੋਂ ਹੈ ਅਤੇ ਸ਼ੱਕੀ ਲੱਗਦਾ ਹੈ, ਤਾਂ ਸਾਵਧਾਨੀ ਵਰਤੋ। ਇਹ ਦੇਖਣ ਲਈ ਕਿ ਕੀ ਉਹ ਸੁਨੇਹਾ ਜਾਇਜ਼ ਹੈ, ਭੇਜਣ ਵਾਲੇ ਵਿਅਕਤੀ ਜਾਂ ਕਾਰੋਬਾਰ ਨਾਲ ਵੱਖਰੇ ਤੌਰ 'ਤੇ ਸੰਪਰਕ ਕਰੋ। ਉਨ੍ਹਾਂ ਸੰਪਰਕ ਵੇਰਵਿਆਂ ਦੀ ਵਰਤੋਂ ਕਰੋ ਜੋ ਤੁਸੀਂ ਕਿਸੇ ਜਾਇਜ਼ ਸਰੋਤ ਦੀ ਵਰਤੋਂ ਕਰਨ ਰਾਹੀਂ ਲੱਭਦੇ ਹੋ, ਉਦਾਹਰਨ ਲਈ ਕਾਰੋਬਾਰ ਦੀ ਅਧਿਕਾਰਤ ਵੈੱਬਸਾਈਟ 'ਤੇ ਜਾ ਕੇ, ਨਾ ਕਿ ਸ਼ੱਕੀ ਸੁਨੇਹੇ ਵਿੱਚ ਦਿੱਤੇ ਗਏ ਸੰਪਰਕ ਵੇਰਵਿਆਂ ਦੀ।

ਅੱਗੇ ਦਿੱਤੇ ਸਰੋਤਾਂ ਨਾਲ ਧੋਖਾਧੜੀ ਅਤੇ ਫਿਸ਼ਿੰਗ ਹਮਲਿਆਂ ਦੀ ਪਛਾਣ ਕਰਨ ਬਾਰੇ ਹੋਰ ਜਾਣੋ:

- ਧੋਖਾਧੜੀ ਨੂੰ ਪਛਾਣੋ ਅਤੇ ਰਿਪੋਰਟ ਕਰੋ।
- ਫਿਸ਼ਿੰਗ ਧੋਖਾਧੜੀ ਦਾ ਪਤਾ ਲਗਾਉਣ ਦਾ ਤਰੀਕਾ ਸਿੱਖੋ
- ਸਮਾਜਿਕ ਤੌਰ 'ਤੇ ਇੰਜੀਨੀਅਰਡ ਸੁਨੇਹਿਆਂ ਦਾ ਪਤਾ ਲਗਾਉਣਾ।

ਮਾਮਲੇ ਦਾ ਅਧਿਐਨ (ਕੇਸ ਸਟੱਡੀ):

ਇੱਕ ਕੋਰੀਅਰ ਕੰਪਨੀ ਦੇ ਕਰਮਚਾਰੀ ਨੂੰ ਉਹਨਾਂ ਦੇ ਪ੍ਰਬੰਧਕੀ (ਐਗਜ਼ੀਕਿਊਟਿਵ) ਸਟਾਫ਼ ਤੋਂ ਇੱਕ ਈਮੇਲ ਪ੍ਰਾਪਤ ਹੁੰਦੀ ਹੈ, ਜਿਸ ਵਿੱਚ ਉਸ ਕਰਮਚਾਰੀ ਨੂੰ 6 x $500 ਮਾਸਟਰਕਾਰਡ ਪ੍ਰੀਪੇਡ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਖ਼ਰੀਦਣ ਲਈ ਕਿਹਾ ਗਿਆ ਹੈ। ਐਗਜ਼ੀਕਿਊਟਿਵ ਨੇ ਉਸ ਕਰਮਚਾਰੀ ਨੂੰ ਇਸ ਗੱਲ ਨੂੰ ਗੁਪਤ ਰੱਖਣ ਲਈ ਕਿਹਾ ਕਿਉਂਕਿ ਕਾਰਡ ਸਟਾਫ਼ ਮੈਂਬਰਾਂ ਲਈ ਗਿਫ਼ਟ ਵਾਊਚਰ ਹੋਣਗੇ। ਐਗਜ਼ੀਕਿਊਟਿਵ ਨੇ ਉਸ ਕਰਮਚਾਰੀ ਨੂੰ ਕਾਰਡ ਖ਼ਰੀਦਣ ਤੋਂ ਬਾਅਦ, ਉਨ੍ਹਾਂ ਕਾਰਡਾਂ ਦੇ ਦੋਵਾਂ ਪਾਸਿਆਂ ਦੀ ਫ਼ੋਟੋ ਖਿੱਚਣ ਅਤੇ ਖ਼ਰੀਦ ਦੇ ਸਬੂਤ ਵਜੋਂ ਉਸਨੂੰ ਭੇਜਣ ਲਈ ਕਿਹਾ ਸੀ।

ਹਿਦਾਇਤ ਅਨੁਸਾਰ, ਕਰਮਚਾਰੀ ਡਾਕਘਰ ਗਈ ਅਤੇ ਗਿਫ਼ਟ ਕਾਰਡ ਖਰੀਦਣ ਲਈ ਆਪਣੇ ਨਿੱਜੀ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਦੀ ਵਰਤੋਂ ਕੀਤੀ। ਉਸਨੇ ਐਗਜ਼ੀਕਿਊਟਿਵ ਦੀ ਈਮੇਲ ਦਾ ਜਵਾਬ ਦਿੱਤਾ ਅਤੇ ਸਬੂਤ ਵਜੋਂ ਗਿਫ਼ਟ ਕਾਰਡਾਂ ਦੀਆਂ ਫ਼ੋਟੋਆਂ ਭੇਜੀਆ।

ਡਾਕਖਾਨੇ ਤੋਂ ਵਾਪਸ ਆਉਣ ਤੋਂ ਬਾਅਦ, ਕਰਮਚਾਰੀ ਨੇ ਐਗਜ਼ੀਕਿਊਟਿਵ ਨੂੰ ਉਹ ਕਾਰਡ ਸੌਂਪ ਦਿੱਤੇ - ਜਿਸਨੂੰ ਉਨ੍ਹਾਂ ਕਾਰਡਾਂ ਬਾਰੇ ਕੋਈ ਜਾਣਕਾਰੀ ਨਹੀਂ ਸੀ। ਸਮੀਖਿਆ ਕਰਨ 'ਤੇ ਪਤਾ ਲੱਗਾ ਕਿ, **ਗਿਫ਼ਟ ਕਾਰਡਾਂ ਬਾਰੇ ਸਾਰੀਆਂ ਈਮੇਲਾਂ ਅਣਜਾਣ ਈਮੇਲ ਪਤੇ ਤੋਂ ਆਈਆਂ ਸਨ ਅਤੇ ਐਗਜ਼ੀਕਿਊਟਿਵ ਦੇ ਜਾਇਜ਼ ਈਮੇਲ ਖਾਤੇ ਤੋਂ ਨਹੀਂ ਆਈਆਂ ਸਨ। ਇਹ ਇੱਕ ਧੋਖਾਧੜੀ ਸੀ।**

ਈਮੇਲ ਰਾਹੀਂ ਹਮਲੇ

ਫਿਸ਼ਿੰਗ ਵਰਗੀਆਂ ਧੋਖਾਧੜੀਆਂ ਤੋਂ ਇਲਾਵਾ, ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਵਿਰੁੱਧ ਹੋਣ ਵਾਲਾ ਆਮ ਈਮੇਲ ਹਮਲਾ **ਕਾਰੋਬਾਰੀ ਈਮੇਲ ਚੁਰਾਉਣਾ** (BEC) ਹੈ। ਅਪਰਾਧੀ ਚੋਰੀ ਕੀਤੇ ਗਏ ਈਮੇਲ ਖਾਤਿਆਂ ਦੀ ਵਰਤੋਂ ਕਰਕੇ, ਜਾਂ ਹੋਰ ਸਾਧਨਾਂ ਰਾਹੀਂ ਕਾਰੋਬਾਰ ਦੇ ਨੁਮਾਇੰਦਿਆਂ ਦੀ ਨਕਲ ਕਰ ਸਕਦੇ ਹਨ - ਜਿਵੇਂ ਕਿ ਡੋਮੇਨ ਨਾਮ ਦੀ ਵਰਤੋਂ ਕਰਨਾ ਜੋ ਅਸਲ ਕਾਰੋਬਾਰ ਵਰਗਾ ਦਿਖਾਈ ਦਿੰਦਾ ਹੈ। ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰਨ ਤੋਂ ਇਲਾਵਾ, ਇਨ੍ਹਾਂ ਹਮਲਿਆਂ ਦਾ ਟੀਚਾ ਆਮ ਤੌਰ 'ਤੇ ਧੋਖਾਧੜੀ ਦੇ ਸ਼ਿਕਾਰ ਲੋਕਾਂ ਤੋਂ ਧੋਖੇਬਾਜ਼ ਦੁਆਰਾ ਸੰਚਾਲਿਤ ਬੈਂਕ ਖਾਤੇ ਵਿੱਚ ਫ਼ੰਡ ਭਿਜਵਾਉਣਾ ਹੁੰਦਾ ਹੈ।

ਖ਼ਤਰੇ ਨੂੰ ਘਟਾਉਣ ਦੇ ਤਰੀਕੇ

ਤੁਹਾਡੇ ਕਰਮਚਾਰੀਆਂ ਲਈ ਈ-ਮੇਲ ਹਮਲਿਆਂ ਦੇ ਵਿਰੁੱਧ ਸਭ ਤੋਂ ਵਧੀਆ ਬਚਾਅ ਸਿਖਲਾਈ ਅਤੇ ਜਾਗਰੂਕਤਾ ਹੈ। ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡਾ ਸਟਾਫ਼ ਹਮੇਸ਼ਾ ਹੇਠ ਲਿਖੀਆਂ ਈਮੇਲਾਂ ਤੋਂ ਸਾਵਧਾਨੀ ਵਰਤਣ ਲਈ ਜਾਣਕਾਰੀ ਰੱਖਦਾ ਹੈ:

- ਭੁਗਤਾਨਾਂ ਲਈ ਬੇਨਤੀਆਂ ਬਾਰੇ, ਖ਼ਾਸ ਕਰਕੇ ਜੇ ਫੈਰੀ ਜਾਂ ਬਕਾਇਆ ਹੋਣ
- ਬੈਂਕ ਵੇਰਵਿਆਂ ਵਿੱਚ ਤਬਦੀਲੀ ਬਾਰੇ
- ਅਜਿਹੇ ਈਮੇਲ ਪਤਾ ਬਾਰੇ ਜੋ ਪੂਰੀ ਤਰ੍ਹਾਂ ਸਹੀ ਨਹੀਂ ਲੱਗ ਰਿਹਾ ਹੈ, ਜਿਵੇਂ ਕਿ ਈ-ਮੇਲ ਦਾ ਡੋਮੇਨ ਨਾਮ ਸਪਲਾਇਰ ਦੀ ਕੰਪਨੀ ਦੇ ਨਾਮ ਨਾਲ ਬਿਲਕੁਲ ਮੇਲ ਨਹੀਂ ਖਾਂਦਾ ਹੈ।

ਹਾਲਾਂਕਿ ਇਹ ਹਮਲੇ ਵਿਨਾਸ਼ਕਾਰੀ ਹੋ ਸਕਦੇ ਹਨ, ਪਰ ਇਸ ਨੂੰ ਘਟਾਉਣ ਦੇ ਉਪਾਅ ਆਸਾਨ ਹਨ ਅਤੇ ਇਸਦੀ ਲਾਗਤ ਲਗਭਗ ਕੁੱਝ ਵੀ ਨਹੀਂ ਹੈ। **ਜਦੋਂ ਸਟਾਫ਼ ਨੂੰ ਇਸ ਤਰ੍ਹਾਂ ਦੀਆਂ ਈਮੇਲਾਂ ਮਿਲਣ, ਤਾਂ ਸਭ ਤੋਂ ਪ੍ਰਭਾਵੀ ਹੱਲ ਈਮੇਲ ਭੇਜਣ ਵਾਲੇ ਨੂੰ ਫ਼ੋਨ ਕਰਕੇ ਪੁਸ਼ਟੀ ਕੀਤੀ ਜਾਵੇ ਕਿ ਉਹ ਈਮੇਲਾਂ ਜਾਇਜ਼ ਹਨ।** ਤੁਹਾਨੂੰ ਭੇਜੇ ਗਏ ਸੰਪਰਕ ਵੇਰਵਿਆਂ ਦੀ ਵਰਤੋਂ ਨਾ ਕਰੋ ਕਿਉਂਕਿ ਇਹ ਧੋਖਾਧੜੀ ਵਾਲੇ ਹੋ ਸਕਦੇ ਹਨ। ਜਦੋਂ ਭੁਗਤਾਨ ਲਈ ਬੇਨਤੀਆਂ ਪ੍ਰਾਪਤ ਹੁੰਦੀਆਂ ਹਨ ਜਾਂ ਬੈਂਕ ਵੇਰਵਿਆਂ ਨੂੰ ਬਦਲਿਆ ਜਾਂਦਾ ਹੈ ਤਾਂ ਸਟਾਫ਼ ਵਲੋਂ ਪਾਲਣਾ ਕਰਨ ਲਈ ਇੱਕ ਰਸਮੀ ਪ੍ਰਕਿਰਿਆ ਸ਼ੁਰੂ ਕਰੋ।

ਹੇਠਾਂ ਦਿੱਤੇ ਸਰੋਤਾਂ ਨਾਲ ਆਪਣੇ ਕਾਰੋਬਾਰ ਨੂੰ BEC ਧੋਖਾਧੜੀਆਂ ਅਤੇ ਈ-ਮੇਲ ਚੋਰੀ ਹੋਣ ਤੋਂ ਬਚਾਉਣਾ ਸਿੱਖੋ:

- ਕਾਰੋਬਾਰੀ ਈਮੇਲ ਚੋਰੀ ਹੋਣਾ
- ਆਪਣੇ ਕਾਰੋਬਾਰ ਨੂੰ ਈ-ਮੇਲ ਬਾਰੇ ਧੋਖਾਧੜੀ ਅਤੇ ਚੋਰੀ ਹੋਣ ਤੋਂ ਬਚਾਓ
- ਜੇਕਰ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਨੂੰ ਈ-ਮੇਲ ਬਾਰੇ ਧੋਖਾਧੜੀ ਜਾਂ ਚੋਰੀ ਕੀਤੇ ਜਾਣ ਦੁਆਰਾ ਨਿਸ਼ਾਨਾ ਬਣਾਇਆ ਗਿਆ ਹੈ ਤਾਂ ਕੀ ਕਰਨਾ ਹੈ।

ਮਾਮਲੇ ਦਾ ਅਧਿਐਨ (ਕੇਸ ਸਟੱਡੀ):

ਇੱਕ ਛੋਟੇ ਨਿਰਮਾਣ ਕਾਰੋਬਾਰ ਨੂੰ ਉਹਨਾਂ ਦੇ ਸਪਲਾਇਰ ਤੋਂ ਇੱਕ ਈਮੇਲ ਮਿਲੀ ਜਿਸ ਵਿੱਚ ਕਿਹਾ ਗਿਆ ਸੀ ਕਿ ਉਹਨਾਂ ਨੇ ਆਪਣਾ ਬੈਂਕ ਬਦਲ ਲਿਆ ਹੈ। ਇਸ ਸਪਲਾਇਰ ਨੇ ਇਨਵੌਇਸ ਭੁਗਤਾਨਾਂ ਲਈ ਨਵੇਂ ਖਾਤੇ ਦੇ ਵੇਰਵੇ ਪ੍ਰਦਾਨ ਕੀਤੇ। ਕਿਉਂਕਿ ਈਮੇਲ ਜਾਇਜ਼ ਲੱਗ ਰਹੀ ਸੀ, **ਨਿਰਮਾਣ ਕਾਰੋਬਾਰ ਨੇ ਬੈਂਕ ਖਾਤੇ ਦੇ ਵੇਰਵਿਆਂ ਵਿੱਚ ਤਬਦੀਲੀ ਦੀ ਪੁਸ਼ਟੀ ਕਰਨ ਲਈ ਸਪਲਾਇਰ ਨੂੰ ਫ਼ੋਨ ਨਹੀਂ ਕੀਤਾ।**

ਉਸ ਕਾਰੋਬਾਰ ਨੇ ਸਪਲਾਇਰ ਤੋਂ ਮਿਲੀ ਇੱਕ $70,000 ਤੋਂ ਵੱਧ ਦੀ ਇਨਵੌਇਸ ਦਾ ਭੁਗਤਾਨ ਕੀਤਾ। ਅਗਲੇ ਹੀ ਦਿਨ, ਇੱਕ ਹੋਰ ਕਰਮਚਾਰੀ ਨੇ ਗਲਤੀ ਨਾਲ $70,000 ਤੋਂ ਵੱਧ ਦੀ ਵਧੀਕ ਰਕਮ ਲਈ ਉਹੀ ਇਨਵੌਇਸ ਦੁਬਾਰਾ ਅਦਾ ਕਰ ਦਿੱਤੀ। ਕੁੱਲ ਮਿਲਾ ਕੇ, ਨਵੇਂ ਬੈਂਕ ਖਾਤੇ ਵਿੱਚ $150,000 ਤੋਂ ਵੱਧ ਦਾ ਭੁਗਤਾਨ ਕੀਤਾ ਗਿਆ।

ਜਦੋਂ ਕਾਰੋਬਾਰ ਨੇ ਆਪਣੇ ਸਪਲਾਇਰ ਨੂੰ ਇਹ ਪੁੱਛਣ ਲਈ ਫ਼ੋਨ ਕੀਤਾ ਕਿ ਕੀ ਉਹ ਡੁਪਲੀਕੇਟ ਭੁਗਤਾਨ ਵਾਪਸ ਕਰ ਸਕਦੇ ਹਨ, ਤਾਂ ਉਸ ਸਪਲਾਇਰ ਨੇ ਦੱਸਿਆ ਕਿ ਬੈਂਕ ਦੇ ਉਹ ਵੇਰਵੇ ਗਲਤ ਸਨ। ਤੁਰੰਤ ਇੱਕ ਜਾਂਚ-ਪੜਤਾਲ ਸ਼ੁਰੂ ਕੀਤੀ ਗਈ, ਅਤੇ ਉਸ ਸਪਲਾਇਰ ਨੂੰ ਪਤਾ ਲੱਗਾ ਕਿ ਉਹਨਾਂ ਦਾ ਇੱਕ ਈਮੇਲ ਖਾਤਾ ਹੈਕ ਕੀਤਾ ਗਿਆ ਸੀ ਅਤੇ ਉਹ ਧੋਖਾਧੜੀ ਵਾਲੇ ਬੈਂਕ ਖਾਤੇ ਦੇ ਵੇਰਵੇ ਭੇਜ ਰਿਹਾ ਸੀ। **ਕੋਈ ਵੀ ਪੈਸੇ ਮੁੜ ਪ੍ਰਾਪਤ ਨਹੀਂ ਕੀਤਾ ਜਾ ਸਕਿਆ।**

ਹਾਨੀਕਾਰਕ ਸਾਫ਼ਟਵੇਅਰ

ਮੈੱਲਵੇਅਰ ਨੁਕਸਾਨ ਪਹੁੰਚਾਉਣ ਲਈ ਬਣਾਏ ਗਏ ਖ਼ਤਰਨਾਕ ਸਾਫ਼ਟਵੇਅਰ ਲਈ ਇੱਕ ਕੰਬਲਨੁਮਾ ਸ਼ਬਦ ਹੈ, ਜਿਵੇਂ ਕਿ ਰੈਨਸਮਵੇਅਰ, ਵਾਇਰਸ, ਸਪਾਈਵੇਅਰ ਅਤੇ ਟ੍ਰੋਜਨ। ਮੈੱਲਵੇਅਰ:

- ਤੁਹਾਡੇ ਉਪਕਰਨ 'ਤੇ ਫਾਈਲਾਂ ਨੂੰ ਚੋਰੀ ਜਾਂ ਲੌਕ ਕਰ ਸਕਦਾ ਹੈ
- ਤੁਹਾਡੇ ਬੈਂਕ ਜਾਂ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਨੰਬਰਾਂ ਨੂੰ ਚੋਰੀ ਕਰ ਸਕਦਾ ਹੈ
- ਤੁਹਾਡੇ ਯੂਜ਼ਰਨੇਮ ਅਤੇ ਪਾਸਵਰਡ ਚੋਰੀ ਕਰ ਸਕਦਾ ਹੈ
- ਤੁਹਾਡੇ ਕੰਪਿਊਟਰ 'ਤੇ ਕੰਟਰੋਲ ਜਾਂ ਜਾਸੂਸੀ ਕਰ ਸਕਦਾ ਹੈ।

ਮੈੱਲਵੇਅਰ ਤੁਹਾਡੀ ਡਿਵਾਈਸ ਨੂੰ ਸਹੀ ਢੰਗ ਨਾਲ ਕੰਮ ਕਰਨ ਤੋਂ ਰੋਕ ਸਕਦਾ ਹੈ, ਤੁਹਾਡੀਆਂ ਫਾਈਲਾਂ ਨੂੰ ਮਿਟਾ ਸਕਦਾ ਹੈ ਜਾਂ ਖ਼ਰਾਬ ਕਰ ਸਕਦਾ ਹੈ, ਜਾਂ ਦੂਜਿਆਂ ਨੂੰ ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਂ ਕਾਰੋਬਾਰੀ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਦੀ ਆਗਿਆ ਦੇ ਸਕਦਾ ਹੈ। ਜੇਕਰ ਤੁਹਾਡੇ ਉਪਕਰਨ ਮੈੱਲਵੇਅਰ ਨਾਲ ਪ੍ਰਭਾਵਿਤ ਹਨ, ਤਾਂ ਤੁਸੀਂ ਹੋਰ ਹਮਲਿਆਂ ਲਈ ਕਮਜ਼ੋਰ ਹੋ ਸਕਦੇ ਹੋ। ਇਹ ਮੈੱਲਵੇਅਰ ਤੁਹਾਡੇ ਨੈੱਟਵਰਕ 'ਤੇ ਮੌਜੂਦ ਹੋਰ ਉਪਕਰਨਾਂ 'ਤੇ ਵੀ ਫ਼ੈਲ ਸਕਦਾ ਹੈ।

ਤੁਹਾਡੇ ਉਪਕਰਨ ਮੈੱਲਵੇਅਰ ਦੁਆਰਾ ਕਈ ਤਰੀਕਿਆਂ ਨਾਲ ਪ੍ਰਭਾਵਿਤ ਹੋ ਸਕਦੇ ਹਨ, ਜਿਸ ਵਿੱਚ ਸ਼ਾਮਲ ਹਨ:

- ਮੈੱਲਵੇਅਰ ਦੁਆਰਾ ਪ੍ਰਭਾਵਿਤ ਵੈੱਬਸਾਈਟਾਂ 'ਤੇ ਜਾਣ ਨਾਲ
- ਇੰਟਰਨੈੱਟ ਤੋਂ ਪ੍ਰਭਾਵਿਤ ਫਾਈਲਾਂ ਜਾਂ ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਡਾਊਨਲੋਡ ਕਰਨ ਨਾਲ
- ਪ੍ਰਭਾਵਿਤ ਈਮੇਲ ਅਟੈਚਮੈਂਟਾਂ ਨੂੰ ਖੋਲ੍ਹਣ ਨਾਲ।

ਰੈਨਸਮਵੇਅਰ

ਰੈਨਸਮਵੇਅਰ ਮੈੱਲਵੇਅਰ ਦੀ ਇੱਕ ਆਮ ਅਤੇ ਖ਼ਤਰਨਾਕ ਕਿਸਮ ਹੈ। ਇਹ ਤੁਹਾਡੀਆਂ ਫ਼ਾਈਲਾਂ ਨੂੰ ਲੈਕ ਜਾਂ ਇਨਕ੍ਰਿਪਟ ਕਰਕੇ ਕੰਮ ਕਰਦਾ ਹੈ ਤਾਂ ਜੋ ਤੁਸੀਂ ਹੁਣ ਉਨ੍ਹਾਂ ਤੱਕ ਪਹੁੰਚ ਨਾ ਕਰ ਸਕੋ। ਫਾਈਲਾਂ ਤੱਕ ਪਹੁੰਚ ਨੂੰ ਬਹਾਲ ਕਰਨ ਲਈ ਫਿਰੌਤੀ ਦੀ ਮੰਗ ਕੀਤੀ ਜਾਂਦੀ ਹੈ ਜੋ ਕਿ ਆਮ ਤੌਰ 'ਤੇ ਕ੍ਰਿਪਟੋਕਰੰਸੀ ਦੇ ਰੂਪ ਵਿੱਚ ਹੁੰਦੀ ਹੈ। ਸਾਈਬਰ ਅਪਰਾਧੀ ਡੈਟੇ ਨੂੰ ਔਨਲਾਈਨ ਪ੍ਰਕਾਸ਼ਿਤ ਕਰਨ ਜਾਂ ਵੇਚਣ ਦੀ ਧਮਕੀ ਵੀ ਦੇ ਸਕਦੇ ਹਨ, ਜਦੋਂ ਤੱਕ ਫਿਰੌਤੀ ਦਾ ਭੁਗਤਾਨ ਨਹੀਂ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।

ਖ਼ਤਰੇ ਨੂੰ ਘਟਾਉਣ ਦੇ ਤਰੀਕੇ

ਹਾਲਾਂਕਿ ਐਂਟੀ-ਵਾਇਰਸ ਜਾਂ ਸੁਰੱਖਿਆ ਸਾਫ਼ਟਵੇਅਰ ਤੁਹਾਨੂੰ ਮੈੱਲਵੇਅਰ ਤੋਂ ਬਚਾਉਣ ਵਿੱਚ ਮੱਦਦ ਕਰ ਸਕਦੇ ਹਨ, ਕੋਈ ਵੀ ਸਾਫ਼ਟਵੇਅਰ 100% ਪ੍ਰਭਾਵਸ਼ਾਲੀ ਨਹੀਂ ਹੁੰਦਾ ਹੈ। ਸਟਾਫ਼ ਨੂੰ ਈਮੇਲਾਂ, ਵੈੱਬਸਾਈਟਾਂ ਅਤੇ ਫਾਈਲਾਂ ਡਾਊਨਲੋਡ ਕਰਦੇ ਸਮੇਂ ਚੌਕਸ ਰਹਿਣਾ ਚਾਹੀਦਾ ਹੈ, ਅਤੇ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਆਪਣੇ ਉਪਕਰਨਾਂ ਨੂੰ ਅੱਪਡੇਟ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ।

ਆਪਣੇ ਕਾਰੋਬਾਰ ਨੂੰ ਰੈਨਸਮਵੇਅਰ ਤੋਂ ਬਚਾਉਣ ਬਾਰੇ ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ ਹੇਠਾਂ ਦਿੱਤੇ ਸਰੋਤ ਦੇਖੋ:

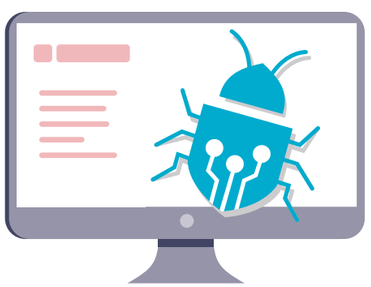
- ਰੈਨਸਮਵੇਅਰ
- ਆਪਣੇ ਆਪ ਨੂੰ ਰੈਨਸਮਵੇਅਰ ਹਮਲਿਆਂ ਤੋਂ ਬਚਾਓ
- ਜੇਕਰ ਤੁਹਾਨੂੰ ਫਿਰੌਤੀ ਲਈ ਬੰਧਕ ਬਣਾ ਲਿਆ ਜਾਵੇ ਤਾਂ ਕੀ ਕਰਨਾ ਹੈ।

ਮਾਮਲੇ ਦਾ ਅਧਿਐਨ (ਕੇਸ ਸਟੱਡੀ):

ਇੱਕ ਆਟੋ ਪਾਰਟਸ ਸਟੋਰ ਦੇ ਕਰਮਚਾਰੀ ਇੱਕ ਸਵੇਰ ਕੰਮ 'ਤੇ ਆਏ ਅਤੇ ਆਪਣੇ ਸਰਵਰ ਕੰਪਿਊਟਰ ਨੂੰ ਚਲਾਉਣ ਦੇ ਯੋਗ ਨਹੀਂ ਸਨ। ਜਦੋਂ ਉਹਨਾਂ ਦੇ ।T ਪ੍ਰਦਾਤਾ ਨੂੰ ਸਰਵਰ ਤੱਕ ਪਹੁੰਚ ਮਿਲੀ, ਤਾਂ ਉਹਨਾਂ ਨੂੰ ਇੱਕ ਵਿੰਡੋ ਖੁੱਲ੍ਹੀ ਮਿਲੀ ਜਿਸ ਵਿੱਚ ਕਿਹਾ ਗਿਆ ਸੀ ਕਿ ਸਾਰਾ ਕੰਪਿਊਟਰ ਡੇਟਾ ਇਨਕ੍ਰਿਪਟ ਕਰ ਦਿੱਤਾ ਗਿਆ ਹੈ। ਨੋਟ ਵਿੱਚ ਮੰਗ ਕੀਤੀ ਗਈ ਸੀ ਕਿ ਉਹ ਫਾਈਲਾਂ ਨੂੰ ਅਨਲੌਕ ਕਰਨ ਲਈ ਬਿਟਕੋਇਨ ਵਿੱਚ ਫਿਰੌਤੀ ਅਦਾ ਕਰਨ।

ਉੱਥੇ ਕੰਪਿਊਟਰ ਵਿੱਚ ਇੱਕ ਬੈਕਅੱਪ ਡਰਾਈਵ ਵੀ ਲੱਗੀ ਹੋਈ ਸੀ, ਉਸਨੂੰ ਵੀ ਇਨਕ੍ਰਿਪਟ ਕਰ ਲਿਆ ਗਿਆ ਸੀ। ਉਹਨਾਂ ਨੇ ਹੋਰ ਬੈਕਅੱਪ ਡਰਾਈਵਾਂ ਨੂੰ ਕਨੈਕਟ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕੀਤੀ, ਪਰ ਉਹਨਾਂ ਫਾਈਲਾਂ ਨੂੰ ਵੀ ਸਕਿੰਟਾਂ ਵਿੱਚ ਹੀ ਆਪਣੇ ਆਪ ਇਨਕ੍ਰਿਪਟ ਕਰ ਲਿਆ ਗਿਆ। **ਉਹ ਆਪਣਾ ਡੇਟਾ ਰਿਕਵਰ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਰੈਨਸਮਵੇਅਰ ਨੂੰ ਹਟਾਉਣ ਵਿੱਚ ਅਸਫ਼ਲ ਰਹੇ ਸਨ ਅਤੇ ਉਹਨਾਂ ਨੇ ਆਪਣੇ ਕੋਲ ਮੌਜੂਦ ਹਰੇਕ ਬੈਕਅੱਪ ਫਾਈਲ ਨੂੰ ਗੁਆ ਦਿੱਤਾ।**

ਉਹਨਾਂ ਕੋਲ ਸਰਵਰ ਨੂੰ ਫੈਕਟਰੀ ਰੀਸੈੱਟ ਕਰਨ ਅਤੇ ਨਵੇਂ ਸਿਸਟਮ ਨਾਲ ਨਵੇਂ ਸਿਰੇ ਤੋਂ ਸ਼ੁਰੂ ਕਰਨ ਦਾ ਇੱਕੋ ਇੱਕ ਵਿਕਲਪ ਬਚਿਆ ਸੀ। ਉਨ੍ਹਾਂ ਦਾ ਕਾਰੋਬਾਰ ਕਈ ਸਾਲਾਂ ਦਾ ਡੇਟਾ ਗੁਆ ਬੈਠਾ ਅਤੇ ਦੁਬਾਰਾ ਨਵੇਂ ਸਿਰੇ ਤੋਂ ਸ਼ੁਰੂ ਕਰਨਾ ਪਿਆ।



ਆਪਣੇ ਖਾਤਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ

ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ (MFA) ਨੂੰ ਚਾਲੂ ਕਰੋ

ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ (MFA) ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਨੂੰ ਔਖਾ ਬਣਾਉਂਦੀ ਹੈ।

MFA ਤੁਹਾਡੇ ਖਾਤੇ ਵਿੱਚ ਸੁਰੱਖਿਆ ਦੀ ਇੱਕ ਹੋਰ ਪਰਤ ਜੋੜਦੀ ਹੈ। ਇਹ ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਨੂੰ ਕਿਸੇ ਹੋਰ ਦੁਆਰਾ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰਨ ਤੋਂ ਬਚਾਉਣ ਦੇ ਸਭ ਤੋਂ ਪ੍ਰਭਾਵਸ਼ਾਲੀ ਤਰੀਕਿਆਂ ਵਿੱਚੋਂ ਇੱਕ ਹੈ, ਇਸ ਲਈ ਤੁਹਾਨੂੰ ਜਿੱਥੇ ਵੀ ਸੰਭਵ ਹੋਵੇ ਇਸਦੀ ਵਰਤੋਂ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ। ਜੇ ਕੋਈ ਵੀ ਤੁਹਾਡੇ ਖਾਤੇ ਵਿੱਚ ਲੌਗਇਨ ਕਰੇਗਾ ਉਸਨੂੰ ਤੁਹਾਡੇ ਯੂਜ਼ਰਨੇਮ ਅਤੇ ਪਾਸਵਰਡ ਤੋਂ ਇਲਾਵਾ ਵੀ ਕੁੱਝ ਹੋਰ ਜਾਣਕਾਰੀ ਪ੍ਰਦਾਨ ਕਰਨ ਦੀ ਲੋੜ ਹੋਵੇਗੀ। ਇਹ ਟੈਕਸਟ ਸੁਨੇਹੇ ਜਾਂ ਪੁਸ਼ਟੀਕਰਨ ਐਪ ਤੋਂ ਪੈਦਾ ਕੀਤਾ ਗਿਆ ਇੱਕ ਵਿਲੱਖਣ ਕੋਡ ਹੋ ਸਕਦਾ ਹੈ। ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ, ਸਾਡੀ MFA ਬਾਰੇ ਸਲਾਹ ਪੜ੍ਹੋ, ਜੋ ਕਿ **cyber.gov.au/mfa** 'ਤੇ ਉਪਲਬਧ ਹੈ।

✓ **ਆਪਣੇ ਸਭ ਤੋਂ ਵੱਧ ਅਹਿਮ ਖਾਤਿਆਂ ਤੋਂ ਸ਼ੁਰੂਆਤ ਕਰਦੇ ਹੋਏ, ਜਿੱਥੇ ਵੀ ਸੰਭਵ ਹੋਵੇ MFA ਨੂੰ ਚਾਲੂ ਕਰੋ।**

ਪਹੁੰਚ ਸੰਬੰਧੀ ਨਿਯੰਤਰਣ ਲਾਗੂ ਕਰੋ

ਉਪਭੋਗਤਾ ਪਹੁੰਚ ਨੂੰ ਸੀਮਤ ਕਰਨ ਨਾਲ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਘਟਨਾ ਕਾਰਨ ਹੋਏ ਨੁਕਸਾਨ ਨੂੰ ਸੀਮਤ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ।

ਪਹੁੰਚ ਨਿਯੰਤਰਣ ਕੁੱਝ ਫਾਈਲਾਂ ਅਤੇ ਪ੍ਰਣਾਲੀਆਂ ਤੱਕ ਪਹੁੰਚ ਨੂੰ ਸੀਮਤ ਕਰਨ ਦਾ ਇੱਕ ਤਰੀਕਾ ਹੈ। ਆਮ ਤੌਰ 'ਤੇ, ਸਟਾਫ਼ ਨੂੰ ਕਿਸੇ ਕਾਰੋਬਾਰ ਵਿਚਲੇ ਸਾਰੇ ਡੇਟਾ, ਖਾਤਿਆਂ ਅਤੇ ਪ੍ਰਣਾਲੀਆਂ ਤੱਕ ਪੂਰੀ ਪਹੁੰਚ ਦੀ ਲੋੜ ਨਹੀਂ ਹੁੰਦੀ ਹੈ। ਉਹਨਾਂ ਨੂੰ ਸਿਰਫ਼ ਉਹੀ ਚੀਜ਼ਾਂ ਤੱਕ ਪਹੁੰਚ ਦੀ ਆਗਿਆ ਹੋਣੀ ਚਾਹੀਦੀ ਹੈ ਜੋ ਉਹਨਾਂ ਨੂੰ ਆਪਣੀਆਂ ਡਿਊਟੀਆਂ ਨਿਭਾਉਣ ਲਈ ਲੋੜੀਂਦੀਆਂ ਹਨ।

ਪਹੁੰਚ ਨੂੰ ਸੀਮਤ ਕਰਨ ਨਾਲ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਘਟਨਾ ਕਾਰਨ ਹੋਏ ਨੁਕਸਾਨ ਨੂੰ ਸੀਮਤ ਕਰਨ ਵਿੱਚ ਮਦਦ ਮਿਲੇਗੀ। ਉਦਾਹਰਨ ਲਈ, ਜੇਕਰ ਕਿਸੇ ਸਟਾਫ਼ ਮੈਂਬਰ ਦਾ ਕੰਪਿਊਟਰ ਫਿਰੌਤੀ ਵਾਲੇ ਸਾਫ਼ਟਵੇਅਰ (ਰੈਨਸਮਵੇਅਰ) ਨਾਲ ਪ੍ਰਭਾਵਿਤ ਹੋ ਗਿਆ ਹੈ, ਤਾਂ ਸਹੀ ਪਹੁੰਚ ਨਿਯੰਤਰਣਾਂ ਦੇ ਨਾਲ ਇਹ ਪੂਰੇ ਕਾਰੋਬਾਰ ਦੀ ਬਜਾਏ ਸਿਰਫ਼ ਥੋੜ੍ਹੀਆਂ ਜਿਹੀਆਂ ਫ਼ਾਈਲਾਂ ਨੂੰ ਪ੍ਰਭਾਵਿਤ ਕਰ ਸਕਦਾ ਹੈ।

✓ **ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਹਰੇਕ ਵਰਤੋਂ ਕਰਨ ਵਾਲਾ ਸਿਰਫ਼ ਉਹੀ ਪਹੁੰਚ ਰੱਖਦਾ ਹੈ ਜਿਸਦੀ ਉਹਨਾਂ ਨੂੰ ਆਪਣੀ ਨੌਕਰੀ ਦੀ ਭੂਮਿਕਾ ਲਈ ਲੋੜ ਹੈ।**

ਮਜ਼ਬੂਤ ਪਾਸਵਰਡਾਂ ਜਾਂ ਪਾਸਫਰੇਜ਼ਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ

ਆਪਣੇ ਖਾਤਿਆਂ ਨੂੰ ਕਿਸੇ ਸੁਰੱਖਿਅਤ ਪਾਸਵਰਡ ਜਾਂ ਪਾਸਫਰੇਜ਼ ਨਾਲ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਤੋਂ ਸੁਰੱਖਿਅਤ ਕਰੋ।

ਜ਼ਿਆਦਾਤਰ ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਨੂੰ ਕਮਜ਼ੋਰ ਪਾਸਵਰਡ ਵਾਲਾ ਵਿਵਹਾਰ ਰੱਖਣ ਦੇ ਨਤੀਜੇ ਵਜੋਂ ਸਾਈਬਰ ਹਮਲਿਆਂ ਦਾ ਸਾਹਮਣਾ ਕਰਨਾ ਪੈਂਦਾ ਹੈ। ਉਦਾਹਰਨ ਲਈ, ਕਈ ਖਾਤਿਆਂ 'ਤੇ ਇੱਕੋ ਪਾਸਵਰਡ ਦੀ ਮੁੜ ਵਰਤੋਂ ਕਰਨਾ। ਤੁਸੀਂ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਉਣ ਲਈ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਅਤੇ ਪਾਸਫਰੇਜ਼ ਦੋਵਾਂ ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦੇ ਹੋ।

ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਤੁਹਾਡੇ ਪਾਸਵਰਡਾਂ ਲਈ ਇੱਕ ਵਰਚੁਅਲ ਤਿਜੋਰੀ ਵਾਂਗ ਕੰਮ ਕਰਦਾ ਹੈ। ਤੁਸੀਂ ਇਸਨੂੰ ਆਪਣੇ ਹਰੇਕ ਖਾਤੇ ਲਈ ਮਜ਼ਬੂਤ, **ਵਿਲੱਖਣ** ਪਾਸਵਰਡ ਬਣਾਉਣ ਅਤੇ ਸਟੋਰ ਕਰਨ ਲਈ ਵਰਤ ਸਕਦੇ ਹੋ। ਜੇਕਰ ਤੁਹਾਡੇ ਕੋਲ ਬਹੁਤ ਸਾਰੇ ਖਾਤੇ ਹਨ, ਤਾਂ ਇਹ ਵਿਲੱਖਣ ਪਾਸਵਰਡਾਂ ਨੂੰ ਯਾਦ ਰੱਖਣ ਦੇ ਬੋਝ ਨੂੰ ਖ਼ਤਮ ਕਰਦਾ ਹੈ। ਤੁਹਾਨੂੰ ਉਨ੍ਹਾਂ ਪਾਸਵਰਡਾਂ ਜਾਂ ਉਨ੍ਹਾਂ ਖਾਤਿਆਂ ਨੂੰ ਯਾਦ ਰੱਖਣ ਦੀ ਲੋੜ ਨਹੀਂ ਹੈ ਜਿਨ੍ਹਾਂ ਨਾਲ ਉਹ ਸੰਬੰਧਿਤ ਹਨ, ਕਿਉਂਕਿ ਇਹ ਸਭ ਤੁਹਾਡੇ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਵਿੱਚ ਦਰਜ ਹੁੰਦਾ ਹੈ।

ਉਨ੍ਹਾਂ ਖਾਤਿਆਂ ਲਈ ਜਿੰਨ੍ਹਾਂ ਵਿੱਚ ਤੁਸੀਂ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਸਾਈਨ ਇਨ ਕਰਦੇ ਹੋ, ਜਾਂ ਜੇ ਤੁਸੀਂ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਵਿੱਚ ਸਟੋਰ ਨਹੀਂ ਕਰਨਾ ਚਾਹੁੰਦੇ ਹੋ, ਉਨ੍ਹਾਂ ਲਈ ਇੱਕ ਪਾਸਫਰੇਜ਼ ਨੂੰ ਆਪਣੇ ਪਾਸਵਰਡ ਵਜੋਂ ਵਰਤਣ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ। ਪਾਸਫਰੇਜ਼ ਬੇਤਰਤੀਬ ਸ਼ਬਦਾਂ ਦਾ ਸੁਮੇਲ ਹੁੰਦਾ ਹੈ, ਉਦਾਹਰਨ ਲਈ 'ਕ੍ਰਿਸਟਲ ਓਨੀਅਨ ਕਲੇਅ ਪ੍ਰੈਟਜ਼ਲ'। ਇਹ ਉਦੋਂ ਲਾਭਦਾਇਕ ਹੁੰਦੇ ਹਨ ਜਦੋਂ ਤੁਸੀਂ ਇੱਕ ਅਜਿਹਾ ਸੁਰੱਖਿਅਤ ਪਾਸਵਰਡ ਚਾਹੁੰਦੇ ਹੋ ਜੋ ਯਾਦ ਰੱਖਣਾ ਆਸਾਨ ਹੋਵੇ। ਚਾਰ ਜਾਂ ਚਾਰ ਤੋਂ ਵੱਧ ਸ਼ਬਦਾਂ ਦੇ ਬੇਤਰਤੀਬੇ ਮਿਸ਼ਰਣ ਦੀ ਵਰਤੋਂ ਕਰੋ ਅਤੇ ਇਸਨੂੰ ਵਿਲੱਖਣ ਰੱਖੋ - ਕਈ ਖਾਤਿਆਂ ਵਿੱਚ **ਇੱਕੋ ਪਾਸਫਰੇਜ਼ ਦੁਬਾਰਾ ਨਾ ਵਰਤੋ**। ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ, ਸਾਡੀ ਪਾਸਫਰੇਜ਼ਾਂ ਅਤੇ ਪਾਸਵਰਡ ਮੈਨੇਜਰਾਂ ਬਾਰੇ ਸਲਾਹ ਪੜ੍ਹੋ, ਜੋ ਕਿ **cyber.gov.au/passphrases** 'ਤੇ ਉਪਲਬਧ ਹੈ।

✓ **ਆਪਣੇ ਹਰੇਕ ਮਹੱਤਵਪੂਰਨ ਖਾਤੇ ਲਈ ਵਿਲੱਖਣ ਪਾਸਵਰਡ ਬਣਾਉਣ ਅਤੇ ਸਟੋਰ ਕਰਨ ਲਈ ਇੱਕ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਦੀ ਵਰਤੋਂ ਕਰੋ।**

ਸਾਂਝੇ ਵਰਤੇ ਜਾਂਦੇ ਖਾਤਿਆਂ ਦਾ ਪ੍ਰਬੰਧਨ ਕਰੋ

ਖਾਤਿਆਂ ਨੂੰ ਸਾਂਝਾ ਵਰਤਣਾ ਸੁਰੱਖਿਆ ਨਾਲ ਸਮਝੌਤਾ ਕਰ ਸਕਦਾ ਹੈ ਅਤੇ ਖ਼ਤਰੇ ਵਾਲੀ ਗਤੀਵਿਧੀ ਨੂੰ ਟਰੈਕ ਕਰਨਾ ਮੁਸ਼ਕਲ ਬਣਾਉਂਦਾ ਹੈ।

ਇੱਕ ਛੋਟੇ ਕਾਰੋਬਾਰ ਵਿੱਚ, ਸਟਾਫ਼ ਲਈ ਕਿਸੇ ਖਾਤੇ ਨੂੰ ਸਾਂਝੇ ਵਰਤਣ ਦੀ ਲੋੜ ਦੇ ਜਾਇਜ਼ ਕਾਰਨ ਹੋ ਸਕਦੇ ਹਨ, ਪਰ ਜਿੰਨਾ ਸੰਭਵ ਹੋ ਸਕੇ ਇਸ ਤੋਂ ਬਚਣਾ ਚਾਹੀਦਾ ਹੈ। ਜਦੋਂ ਇੱਕ ਤੋਂ ਵੱਧ ਸਟਾਫ਼ ਇੱਕੋ ਖਾਤੇ ਦੀ ਵਰਤੋਂ ਕਰਦਾ ਹੈ ਤਾਂ ਕਿਸੇ ਖ਼ਾਸ ਕਰਮਚਾਰੀ ਦੀ ਗਤੀਵਿਧੀ ਨੂੰ ਟ੍ਰੈਕ ਕਰਨਾ ਔਖਾ ਹੋ ਸਕਦਾ ਹੈ ਅਤੇ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਨੂੰ ਟਰੈਕ ਕਰਨਾ ਵੀ ਔਖਾ ਹੋ ਸਕਦਾ ਹੈ। ਜਦੋਂ ਤੱਕ ਤੁਸੀਂ ਪਾਸਵਰਡ ਨਹੀਂ ਬਦਲਦੇ ਹੋ, ਕਰਮਚਾਰੀ ਕਾਰੋਬਾਰ ਛੱਡਣ ਤੋਂ ਬਾਅਦ ਵੀ ਖਾਤਿਆਂ ਤੱਕ ਪਹੁੰਚ ਕਰਨਾ ਜਾਰੀ ਰੱਖ ਸਕਦੇ ਹਨ।

✓ **ਸਾਂਝੇ ਖਾਤਿਆਂ ਦੀ ਵਰਤੋਂ ਨੂੰ ਸੀਮਤ ਕਰੋ ਅਤੇ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਵਿੱਚ ਵਰਤੇ ਗਏ ਕਿਸੇ ਵੀ ਖਾਤੇ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ।**

ਆਪਣੇ ਉਪਕਰਨਾਂ ਅਤੇ ਜਾਣਕਾਰੀ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ

ਆਪਣੇ ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਅੱਪਡੇਟ ਕਰੋ

ਆਪਣੇ ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਅੱਪ-ਟੂ-ਡੇਟ ਰੱਖਣਾ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਨੂੰ ਸਾਈਬਰ ਹਮਲੇ ਤੋਂ ਬਚਾਉਣ ਦੇ ਸਭ ਤੋਂ ਵਧੀਆ ਤਰੀਕਿਆਂ ਵਿੱਚੋਂ ਇੱਕ ਹੈ।

ਅੱਪਡੇਟ ਤੁਹਾਡੇ ਓਪਰੇਟਿੰਗ ਸਿਸਟਮ ਅਤੇ ਹੋਰ ਸਾਫ਼ਟਵੇਅਰ ਵਿੱਚ ਸੁਰੱਖਿਆ ਖਾਮੀਆਂ ਨੂੰ ਠੀਕ ਕਰ ਸਕਦੇ ਹਨ, ਤਾਂ ਜੋ ਕਿਸੇ ਸਾਈਬਰ ਅਪਰਾਧੀ ਲਈ ਇਸ ਨੂੰ ਤੋੜਨਾ ਔਖਾ ਹੋ ਜਾਵੇ। ਹਰ ਸਮੇਂ ਸਾਫ਼ਟਵੇਅਰ ਵਿੱਚ ਨਵੀਆਂ ਖਾਮੀਆਂ ਲੱਭੀਆਂ ਜਾਂਦੀਆਂ ਹਨ, ਇਸ ਲਈ ਅੱਪਡੇਟ ਕਰਨ ਲਈ ਆਏ ਸੁਨੇਹਿਆਂ (ਪ੍ਰੋਂਪਟਾਂ) ਨੂੰ ਨਜ਼ਰਅੰਦਾਜ਼ ਨਾ ਕਰੋ। ਤੁਹਾਡੇ ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਅੱਪਡੇਟ ਕਰਨ ਨਾਲ ਸਾਈਬਰ ਅਪਰਾਧੀ ਵੱਲੋਂ ਕਿਸੇ ਜਾਣੀ-ਪਛਾਣੀ ਕਮਜ਼ੋਰੀ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋਏ ਮੈੱਲਵੇਅਰ ਚਲਾਉਣ ਜਾਂ ਤੁਹਾਡੀ ਡਿਵਾਈਸ ਨੂੰ ਹੈਕ ਕਰਨ ਦੀ ਸੰਭਾਵਨਾ ਘੱਟ ਜਾਵੇਗੀ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਮੱਦਦ ਦੀ ਲੋੜ ਹੈ, ਤਾਂ ACSC ਨੇ ਅੱਪਡੇਟਾਂ ਬਾਰੇ ਮਾਰਗਦਰਸ਼ਨ ਜਾਣਕਾਰੀ ਪ੍ਰਕਾਸ਼ਿਤ ਕੀਤੀ ਹੈ।

ਜੇਕਰ ਤੁਹਾਡਾ ਉਪਕਰਨ ਜਾਂ ਸਾਫ਼ਟਵੇਅਰ ਬਹੁਤ ਪੁਰਾਣਾ ਹੈ, ਤਾਂ ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਅੱਪਡੇਟ ਉਪਲਬਧ ਨਾ ਹੋਣ। ਜੇਕਰ ਉਸ ਉਪਕਰਨ ਦੇ ਨਿਰਮਾਤਾ ਨੇ ਅੱਪਡੇਟਾਂ ਨਾਲ ਉਸ ਉਤਪਾਦ ਦਾ ਸਮਰਥਨ ਕਰਨਾ ਬੰਦ ਕਰ ਦਿੱਤਾ ਹੈ, ਤਾਂ ਤੁਹਾਨੂੰ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਇੱਕ ਨਵੇਂ ਉਪਕਰਨ ਨਾਲ ਅੱਪਗ੍ਰੇਡ ਕਰਨ ਬਾਰੇ ਵਿਚਾਰ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ। ਉਨ੍ਹਾਂ ਸਿਸਟਮਾਂ ਦੀਆਂ ਉਦਾਹਰਨਾਂ ਹਨ ਜੋ ਹੁਣ ਵੱਡੇ ਅੱਪਡੇਟ ਪ੍ਰਾਪਤ ਨਹੀਂ ਕਰਦੇ ਹਨ **iPhone 7** ਅਤੇ **Microsoft Windows 7**।

ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ ਸਾਡੀ ਅੱਪਡੇਟਾਂ ਬਾਰੇ ਮਾਰਗਦਰਸ਼ਨ ਜਾਣਕਾਰੀ ਨੂੰ ਪੜ੍ਹੋ, ਜੋ ਕਿ **cyber.gov.au/updates** 'ਤੇ ਉਪਲਬਧ ਹੈ।

✓ **ਆਪਣੇ ਉਪਕਰਨਾਂ ਅਤੇ ਸਾਫ਼ਟਵੇਅਰ ਲਈ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ ਚਾਲੂ ਕਰੋ।**

ਸਿਕਿਊਰਿਟੀ ਸਾਫ਼ਟਵੇਅਰ ਦੀ ਵਰਤੋਂ ਕਰੋ

ਸਿਕਿਊਰਿਟੀ ਸਾਫ਼ਟਵੇਅਰ ਜਿਵੇਂ ਕਿ ਐਂਟੀਵਾਇਰਸ ਅਤੇ ਰੈਨਸਮਵੇਅਰ ਸੁਰੱਖਿਆ ਤੁਹਾਡੇ ਉਪਕਰਨਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਵਿੱਚ ਮੱਦਦ ਕਰ ਸਕਦੇ ਹਨ।

ਸਿਕਿਊਰਿਟੀ ਸਾਫ਼ਟਵੇਅਰ ਜਿਵੇਂ ਕਿ ਐਂਟੀਵਾਇਰਸ ਅਤੇ ਰੈਨਸਮਵੇਅਰ ਸੁਰੱਖਿਆ ਤੁਹਾਡੇ ਉਪਕਰਨਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਵਿੱਚ ਮੱਦਦ ਕਰ ਸਕਦੇ ਹਨ। ਐਂਟੀਵਾਇਰਸ ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਸ਼ੱਕੀ ਫਾਈਲਾਂ ਅਤੇ ਪ੍ਰੋਗਰਾਮਾਂ ਦਾ ਪਤਾ ਲਗਾਉਣ ਲਈ ਸਕੈਨ ਕਰਨ ਲਈ ਸੈੱਟਅੱਪ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ। ਜਦੋਂ ਕੋਈ ਖ਼ਤਰਾ ਮਿਲਦਾ ਹੈ, ਤਾਂ ਤੁਹਾਨੂੰ ਇੱਕ ਚੇਤਾਵਨੀ ਪ੍ਰਾਪਤ ਹੋਵੇਗੀ ਅਤੇ ਸ਼ੱਕੀ ਫਾਈਲ ਨੂੰ ਅਲੱਗ ਕਰ ਦਿੱਤਾ ਜਾਵੇਗਾ ਜਾਂ ਹਟਾ ਦਿੱਤਾ ਜਾਵੇਗਾ।

ਬਹੁਤ ਸਾਰੇ ਛੋਟੇ ਕਾਰੋਬਾਰ ਆਪਣੇ ਆਪ ਨੂੰ ਵਾਇਰਸਾਂ ਅਤੇ ਮੈੱਲਵੇਅਰ ਤੋਂ ਬਚਾਉਣ ਲਈ **ਵਿੰਡੋਜ਼ ਸਕਿਊਰਿਟੀ ਦੀ ਵਰਤੋਂ** ਕਰ ਸਕਦੇ ਹਨ। ਵਿੰਡੋਜ਼ ਸਕਿਊਰਿਟੀ Windows 10 ਅਤੇ Windows 11 ਉਪਕਰਨਾਂ ਵਿੱਚ ਪਹਿਲਾਂ ਤੋਂ ਹੀ ਮੌਜੂਦ (ਬਿਲਟ-ਇਨ) ਹੁੰਦੀ ਹੈ ਅਤੇ ਇਸ ਵਿੱਚ ਮੁਫ਼ਤ ਵਾਇਰਸ ਅਤੇ ਖ਼ਤਰਿਆਂ ਤੋਂ ਸੁਰੱਖਿਆ ਮਿਲਣੀ ਸ਼ਾਮਲ ਹੈ। ਤੁਸੀਂ ਇਸਦੀ ਵਰਤੋਂ ਆਪਣੇ ਉਪਕਰਨ 'ਤੇ ਰੈਨਸਮਵੇਅਰ ਸੁਰੱਖਿਆ ਵਿਸ਼ੇਸ਼ਤਾਵਾਂ ਨੂੰ ਚਾਲੂ ਕਰਨ ਲਈ ਵੀ ਕਰ ਸਕਦੇ ਹੋ।

ਵਿਕਲਪਕ ਉਤਪਾਦਾਂ ਅਤੇ ਵਿਕਲਪਾਂ ਲਈ, cyber.gov.au 'ਤੇ ਐਂਟੀਵਾਇਰਸ ਖੋਜ ਕੇ, ਸਾਡੀ ਐਂਟੀਵਾਇਰਸ ਸਾਫ਼ਟਵੇਅਰ ਬਾਰੇ ਸਲਾਹ ਪੜ੍ਹੋ।

✓ **ਆਪਣੇ ਉਪਕਰਨ 'ਤੇ ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਸਕੈਨ ਨੂੰ ਕਰਨ ਲਈ ਸਿਕਿਊਰਿਟੀ ਸਾਫ਼ਟਵੇਅਰ ਸੈਟਅੱਪ ਕਰੋ।**

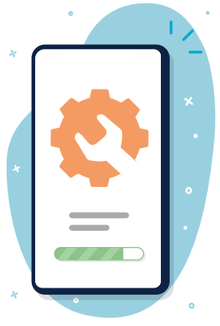
ਆਪਣੀ ਸਮੱਗਰੀ ਦਾ ਬੈਕਅੱਪ ਲਓ

ਜੇਕਰ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਗੁਆਚ ਜਾਂਦੀ ਹੈ ਜਾਂ ਚੋਰੀ ਹੋ ਜਾਂਦੀ ਹੈ ਤਾਂ ਨਿਯਮਤ ਬੈਕਅੱਪ ਇਸਨੂੰ ਮੁੜ ਪ੍ਰਾਪਤ ਕਰਨ ਵਿੱਚ ਤੁਹਾਡੀ ਮੱਦਦ ਕਰ ਸਕਦੇ ਹਨ।

ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਅੰਦਰ ਮਹੱਤਵਪੂਰਨ ਜਾਣਕਾਰੀ ਦਾ ਬੈਕਅੱਪ ਲੈਣਾ ਇੱਕ ਨਿਯਮਿਤ ਜਾਂ ਆਟੋਮੈਟਿਕ ਅਭਿਆਸ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ। ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਬੈਕਅੱਪ ਲੈਂਦੇ ਹੋਣ ਤੋਂ ਬਗ਼ੈਰ, ਸਾਈਬਰ ਹਮਲੇ ਤੋਂ ਬਾਅਦ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਨੂੰ ਮੁੜ ਪ੍ਰਾਪਤ ਕਰਨਾ ਤੁਹਾਡੇ ਲਈ ਅਸੰਭਵ ਹੋ ਸਕਦਾ ਹੈ।

ਇੱਥੇ ਬਹੁਤ ਸਾਰੇ ਤਰੀਕੇ ਅਤੇ ਉਤਪਾਦ ਹਨ ਜੋ ਤੁਸੀਂ ਆਪਣੀ ਜਾਣਕਾਰੀ ਦਾ ਬੈਕਅੱਪ ਲੈਣ ਲਈ ਵਰਤ ਸਕਦੇ ਹੋ। ਆਪਣੇ ਕਾਰੋਬਾਰ ਦਾ ਬੈਕਅੱਪ ਲੈਣ ਬਾਰੇ ਵਧੇਰੇ ਸਲਾਹ ਲੈਣ ਲਈ, ਸਾਡੀ ਬੈਕਅੱਪ ਲਈ ਸਲਾਹ ਪੜ੍ਹੋ, ਜੋ ਕਿ **cyber.gov.au/backups** 'ਤੇ ਉਪਲਬਧ ਹੈ। ਹਰੇਕ ਕਾਰੋਬਾਰ ਲਈ ਸਭ ਤੋਂ ਵਧੀਆ ਵਿਕਲਪ ਵੱਖੋ-ਵੱਖਰਾ ਹੋਵੇਗਾ, ਇਸ ਲਈ ਜੇਕਰ ਤੁਹਾਨੂੰ ਯਕੀਨ ਨਹੀਂ ਹੈ ਤਾਂ ਕਿਸੇ IT ਪੇਸ਼ੇਵਰ ਨਾਲ ਗੱਲ ਕਰੋ।

✓ **ਆਪਣੀ ਜਾਣਕਾਰੀ ਦਾ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਬੈਕਅੱਪ ਲੈਣ ਲਈ ਯੋਜਨਾ ਬਣਾਓ ਅਤੇ ਲਾਗੂ ਕਰੋ।**



ਆਪਣੇ ਨੈੱਟਵਰਕ ਅਤੇ ਬਾਹਰੀ ਸੇਵਾਵਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ

ਆਪਣੇ ਨੈੱਟਵਰਕ ਵਿਚਲੀਆਂ ਸੰਭਾਵਿਤ ਕਮਜ਼ੋਰੀਆਂ ਨੂੰ ਠੀਕ ਕਰਕੇ ਆਪਣੇ ਕਾਰੋਬਾਰ ਨੂੰ ਸਾਈਬਰ ਹਮਲੇ ਤੋਂ ਬਚਾਓ।

ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਤੁਹਾਡੇ ਨੈੱਟਵਰਕ ਵਿਚਲੇ ਉਪਕਰਨ ਅਤੇ ਸੇਵਾਵਾਂ ਮੁੱਖ ਨਿਸ਼ਾਨਾ ਹੋ ਸਕਦੀਆਂ ਹਨ। ਇਨ੍ਹਾਂ ਵਿੱਚੋਂ ਬਹੁਤ ਸਾਰੇ ਸਿਸਟਮ ਸੁਰੱਖਿਅਤ ਕਰਨ ਲਈ ਗੁੰਝਲਦਾਰ ਹੋ ਸਕਦੇ ਹਨ, ਇਸ ਲਈ ਕਿਸੇ IT ਪੇਸ਼ੇਵਰ ਨਾਲ ਹੇਠਾਂ ਦਿੱਤੀਆਂ ਸਿਫ਼ਾਰਸ਼ਾਂ 'ਤੇ ਚਰਚਾ ਕਰੋ।

- **ਆਪਣੇ ਸਰਵਰਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ**: ਜੇਕਰ ਤੁਸੀਂ ਆਪਣੇ ਘਰ ਜਾਂ ਕਾਰੋਬਾਰ ਵਿੱਚ NAS ਜਾਂ ਹੋਰ ਸਰਵਰ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋ, ਤਾਂ ਉਹਨਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਲਈ ਵਾਧੂ ਚੌਕਸੀ ਵਰਤੋ। ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਇਹ ਯੰਤਰ ਆਮ ਨਿਸ਼ਾਨੇ ਹਨ ਕਿਉਂਕਿ ਉਹ ਅਕਸਰ ਮਹੱਤਵਪੂਰਨ ਫਾਈਲਾਂ ਨੂੰ ਸਟੋਰ ਕਰਦੇ ਹਨ ਜਾਂ ਮਹੱਤਵਪੂਰਨ ਕਾਰਜ ਕਰਦੇ ਹਨ। ਇਨ੍ਹਾਂ ਯੰਤਰਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਲਈ ਬਹੁਤ ਸਾਰੀਆਂ ਸਾਈਬਰ ਹਮਲੇ ਨੂੰ ਰੋਕਣ ਵਾਲੀਆਂ ਰਣਨੀਤੀਆਂ ਦੀ ਲੋੜ ਪੈਂਦੀ ਹੈ। ਉਦਾਹਰਨ ਲਈ, ਇਹ ਯਕੀਨੀ ਬਣਾਉਣਾ ਮਹੱਤਵਪੂਰਨ ਹੈ ਕਿ ਕੋਈ ਵੀ ਸਰਵਰ ਜਾਂ NAS ਉਪਕਰਨ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਅੱਪਡੇਟ ਕੀਤੇ ਜਾ ਰਹੇ ਹਨ। ਪ੍ਰਬੰਧਕੀ ਖਾਤਿਆਂ ਨੂੰ ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਫਰੇਜ਼ ਜਾਂ ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ ਨਾਲ ਸੁਰੱਖਿਅਤ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ।
- **ਇੰਟਰਨੈੱਟ ਦੀ ਬਾਹਰੀ-ਦੁਨੀਆਂ ਦਾ ਸਾਹਮਣਾ ਕਰਨ ਵਾਲੀਆਂ ਸੇਵਾਵਾਂ ਦੇ ਫੁੱਟਪ੍ਰਿੰਟ ਨੂੰ ਘੱਟ ਤੋਂ ਘੱਟ ਕਰੋ**: ਆਪਣੇ ਨੈੱਟਵਰਕ 'ਤੇ ਕਿਸੇ ਵੀ ਇੰਟਰਨੈੱਟ ਦੇ ਸੰਪਰਕ ਵਿਚ ਆਉਣ ਵਾਲੀਆਂ ਸੇਵਾਵਾਂ ਦਾ ਆਡਿਟ ਕਰੋ ਅਤੇ ਸੁਰੱਖਿਅਤ ਕਰੋ। ਇਸ ਵਿੱਚ ਰਿਮੋਟ ਡੈਸਕਟਾਪ, ਫਾਈਲ ਸ਼ੇਅਰ, ਵੈਬਮੇਲ ਅਤੇ ਰਿਮੋਟ ਤੌਰ 'ਤੇ ਪ੍ਰਬੰਧਕੀ ਸੇਵਾਵਾਂ ਸ਼ਾਮਲ ਹੋ ਸਕਦੀਆਂ ਹਨ।
- **ਕਲਾਊਡ ਸੇਵਾਵਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਲੱਗੋ**: ਔਨਲਾਈਨ ਜਾਂ ਕਲਾਊਡ ਸੇਵਾਵਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ 'ਤੇ ਵਿਚਾਰ ਕਰੋ ਜੋ ਤੁਹਾਡੇ ਖੁਦ ਦੇ ਪ੍ਰਬੰਧਨ ਦੀ ਬਜਾਏ ਉਨ੍ਹਾਂ ਦੇ ਵਿੱਚ ਹੀ ਬਣੀ ਹੋਈ (ਬਿਲਟ-ਇਨ) ਸੁਰੱਖਿਆ ਪ੍ਰਦਾਨ ਕਰਦੇ ਹਨ। ਉਦਾਹਰਨ ਲਈ, ਇਨ੍ਹਾਂ ਸੇਵਾਵਾਂ ਨੂੰ ਖੁਦ ਚਲਾਉਣ ਅਤੇ ਸੁਰੱਖਿਅਤ ਕਰਨ ਦੀ ਬਜਾਏ ਈਮੇਲ ਜਾਂ ਵੈੱਬਸਾਈਟ ਹੋਸਟਿੰਗ ਵਰਗੀਆਂ ਚੀਜ਼ਾਂ ਲਈ ਔਨਲਾਈਨ ਸੇਵਾਵਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- **ਆਪਣੇ ਰਾਊਟਰ ਦੀ ਸੁਰੱਖਿਆ ਵਿੱਚ ਸੁਧਾਰ ਕਰੋ:** ਪੂਰਵ-ਨਿਰਧਾਰਤ ਪਾਸਵਰਡ ਅੱਪਡੇਟ ਕਰਨ, ਗਾਹਕਾਂ ਜਾਂ ਵਿਜ਼ਿਟਰਾਂ ਲਈ "ਮਹਿਮਾਨ" ਵਾਈ-ਫਾਈ ਨੂੰ ਚਾਲੂ ਕਰਨ, ਅਤੇ ਸਭ ਤੋਂ ਮਜ਼ਬੂਤ ਇਨਕ੍ਰਿਪਸ਼ਨ ਪ੍ਰੋਟੋਕੋਲ ਦੀ ਵਰਤੋਂ ਕਰਨ ਸਮੇਤ, ਆਪਣੇ ਰਾਊਟਰ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਦੇ ਤਰੀਕਿਆਂ ਬਾਰੇ ਸਾਡੇ ਮਾਰਗਦਰਸ਼ਨ ਦੀ ਪਾਲਣਾ ਕਰੋ। ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ **cyber.gov.au** 'ਤੇ ਰਾਊਟਰ ਲਿਖ ਕੇ ਖੋਜੋ।
- **ਆਪਣੀ ਸਾਈਬਰ ਸਪਲਾਈ ਚੇਨ ਨੂੰ ਸਮਝੋ:** ਆਧੁਨਿਕ ਕਾਰੋਬਾਰ ਅਕਸਰ ਕਈ ਸੇਵਾਵਾਂ ਨੂੰ ਬਾਹਰੋਂ ਕਰਵਾਉਂਦੇ (ਆਊਟਸੋਰਸ ਕਰਦੇ) ਹਨ। ਉਦਾਹਰਨ ਲਈ, ਆਪਣੇ ਕਾਰੋਬਾਰ ਦੇ IT ਹਿੱਸੇ ਦੇ ਰੱਖ-ਰਖਾਵ ਲਈ ਕਿਸੇ ਸੇਵਾ ਨੂੰ ਪ੍ਰਬੰਧਿਤ ਕਰਨ ਵਾਲੇ ਪ੍ਰਦਾਤਾ ਦੀ ਵਰਤੋਂ ਕਰਨਾ। ਇਨ੍ਹਾਂ ਸੇਵਾਵਾਂ ਜਾਂ ਪ੍ਰਦਾਤਿਆਂ ਨਾਲ ਸੰਬੰਧਿਤ ਸੁਰੱਖਿਆ ਸਮੱਸਿਆਵਾਂ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ 'ਤੇ ਕਾਫ਼ੀ ਜ਼ਿਆਦਾ ਪ੍ਰਭਾਵ ਪਾ ਸਕਦੀਆਂ ਹਨ। ਸਾਈਬਰ ਸਪਲਾਈ ਚੇਨ ਸੰਬੰਧੀ ਜ਼ੋਖਮ ਪ੍ਰਬੰਧਨ ਬਾਰੇ ਵਧੇਰੇ ਸਲਾਹ ਲਈ ਸਾਡੀ ਸਾਈਬਰ ਸਪਲਾਈ ਚੇਨ ਗਾਈਡੈਂਸ ਨੂੰ **cyber.gov.au** 'ਤੇ ਪੜ੍ਹੋ।

✓ **ਆਪਣੇ ਨੈੱਟਵਰਕ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਦੇ ਤਰੀਕਿਆਂ ਬਾਰੇ ਕਿਸੇ IT ਪੇਸ਼ੇਵਰ ਨਾਲ ਗੱਲ ਕਰੋ।**

ਆਪਣੀ ਵੈੱਬਸਾਈਟ ਨੂੰ ਮਜ਼ਬੂਤ ਬਣਾਓ

ਸਾਈਬਰ ਹਮਲਿਆਂ ਦਾ ਮੁੱਖ ਨਿਸ਼ਾਨਾ ਵੈੱਬਸਾਈਟਾਂ ਹੁੰਦੀਆਂ ਹਨ।

ਕੁੱਝ ਬੁਨਿਆਦੀ ਸੁਰੱਖਿਆ ਉਪਾਵਾਂ ਦੀ ਪਾਲਣਾ ਕਰਕੇ ਆਪਣੀ ਵੈੱਬਸਾਈਟ ਨੂੰ ਹਾਈਜੈਕ ਹੋਣ ਤੋਂ ਬਚਾਓ:

- ਆਪਣੇ ਵੈੱਬਸਾਈਟ ਲੌਗਇਨ ਨੂੰ ਮਲਟੀ-ਫੈਕਟਰ ਪੁਸ਼ਟੀਕਰਨ ਜਾਂ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਨਾਲ ਸੁਰੱਖਿਅਤ ਕਰੋ
- ਆਪਣੀ ਵੈੱਬਸਾਈਟ ਦੀਆਂ ਸਮੱਗਰੀ ਪ੍ਰਬੰਧਨ ਪ੍ਰਣਾਲੀਆਂ ਅਤੇ ਪਲੱਗਇਨਾਂ ਨੂੰ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਅੱਪਡੇਟ ਕਰੋ
- ਆਪਣੀ ਵੈੱਬਸਾਈਟ ਦਾ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਬੈਕਅੱਪ ਲਓ ਤਾਂ ਜੋ ਤੁਸੀਂ ਸਾਈਬਰ ਹਮਲੇ ਤੋਂ ਬਾਅਦ ਇਸਨੂੰ ਰੀਸਟੋਰ ਕਰ ਸਕੋ।

ACSC ਕੋਲ ਵੈੱਬਸਾਈਟ ਮਾਲਕਾਂ ਲਈ ਇਸਤੋਂ ਇਲਾਵਾ ਹੋਰ ਸਰੋਤ ਉਪਲਬਧ ਹਨ। ਇਨ੍ਹਾਂ ਸਰੋਤਾਂ ਨੂੰ **cyber.gov.au** 'ਤੇ ਖੋਜੋ:

- ਤੁਹਾਡੀ ਵੈੱਬਸਾਈਟ ਲਈ ਕੁਇੱਕ ਵਿੰਨਜ਼
- ਸਰਟੀਫ਼ਿਕੇਟ, TLS, HTTPS ਅਤੇ ਮੌਕਾਪ੍ਰਸਤ TLS ਨੂੰ ਲਾਗੂ ਕਰਨਾ
- ਡੋਮੇਨ ਮਾਲਕਾਂ ਲਈ ਡੋਮੇਨ ਨਾਮ ਸਿਸਟਮ ਸਕਿਊਰਿਟੀ
- ਸੇਵਾ-ਤੋਂ-ਮਨ੍ਹਾਂ ਕਰਨ ਵਾਲੇ ਹਮਲਿਆਂ ਪ੍ਰਤੀ ਤਿਆਰੀ ਅਤੇ ਜਵਾਬ ਦੇਣਾ

✓ **ACSC ਦੇ ਵੈੱਬਸਾਈਟ ਸੁਰੱਖਿਆ ਸਰੋਤਾਂ ਨੂੰ ਪੜ੍ਹੋ।**

ਆਪਣੇ ਉਪਕਰਨਾਂ ਨੂੰ ਵੇਚਣ ਜਾਂ ਨਿਪਟਾਰਾ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਰੀਸੈੱਟ ਕਰੋ

ਤੁਹਾਡੇ ਪੁਰਾਣੇ ਉਪਕਰਨਾਂ ਦੇ ਡੇਟੇ ਨੂੰ ਅਜਨਬੀਆਂ ਦੁਆਰਾ ਐਕਸੈਸ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ।

ਜੇਕਰ ਤੁਸੀਂ ਆਪਣੇ ਉਪਕਰਨਾਂ ਦਾ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਨਿਪਟਾਰਾ ਨਹੀਂ ਕਰਦੇ, ਤਾਂ ਸਾਈਬਰ ਅਪਰਾਧੀ ਇਸ 'ਤੇ ਮੌਜੂਦ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚ ਕਰ ਸਕਦੇ ਹਨ। ਇਸ ਵਿੱਚ ਈਮੇਲ, ਫਾਈਲਾਂ ਅਤੇ ਹੋਰ ਕਾਰੋਬਾਰੀ ਡੇਟਾ ਸ਼ਾਮਲ ਹੋ ਸਕਦਾ ਹੈ। ਆਪਣੇ ਕਾਰੋਬਾਰੀ ਡਿਵਾਈਸਾਂ ਨੂੰ ਵੇਚਣ, ਵਾਪਸ ਕਰਨ ਜਾਂ ਸੁੱਟਣ ਤੋਂ ਪਹਿਲਾਂ ਉਨ੍ਹਾਂ ਤੋਂ ਸਾਰੀ ਜਾਣਕਾਰੀ ਹਟਾਓ। ਉਦਾਹਰਨ ਲਈ, ਫੈਕਟਰੀ ਰੀਸੈੱਟ ਕਰਕੇ। ਇਹ ਕਿਸੇ ਵੀ ਜਾਣਕਾਰੀ ਨੂੰ ਖ਼ਤਮ ਕਰਨ ਅਤੇ ਉਪਕਰਨ ਨੂੰ ਇਸਦੀਆਂ ਮੂਲ ਸੈਟਿੰਗਾਂ ਵਿੱਚ ਰੀਸਟੋਰ ਕਰਨ ਵਿੱਚ ਮੱਦਦ ਕਰੇਗਾ।

ਆਪਣੇ ਉਪਕਰਨਾਂ ਨੂੰ ਰੀਸੈੱਟ ਕਰਨ ਬਾਰੇ ਸਲਾਹ ਲਈ ਸਾਡਾ ਮਾਰਗਦਰਸ਼ਨ, ਆਪਣੇ ਉਪਕਰਨ ਦਾ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਕਿਵੇਂ ਨਿਪਟਾਰਾ ਕਰਨਾ ਹੈ ਪੜ੍ਹੋ। **cyber.gov.au** 'ਤੇ ਨਿਪਟਾਰਾ ਲਿਖ ਕੇ ਖੋਜੋ।

✓ **ਕਾਰੋਬਾਰੀ ਉਪਕਰਨਾਂ ਨੂੰ ਵੇਚਣ ਜਾਂ ਨਿਪਟਾਉਣ ਤੋਂ ਪਹਿਲਾਂ ਫੈਕਟਰੀ ਰੀਸੈੱਟ ਕਰੋ।**

ਆਪਣੇ ਉਪਕਰਨਾਂ ਨੂੰ ਲਾਕ ਲਗਾ ਕੇ ਅਤੇ ਭੌਤਿਕ ਤੌਰ 'ਤੇ ਸੁਰੱਖਿਅਤ ਰੱਖੋ

ਆਪਣੇ ਕਾਰੋਬਾਰੀ ਉਪਕਰਨਾਂ ਤੱਕ ਪਹੁੰਚ ਨੂੰ ਸੀਮਤ ਕਰਨ ਨਾਲ ਖ਼ਤਰੇ ਵਾਲੀ ਗਤੀਵਿਧੀ ਹੋਣ ਦੇ ਮੌਕੇ ਘੱਟ ਜਾਣਗੇ।

ਆਪਣੇ ਕਾਰੋਬਾਰੀ ਉਪਕਰਨਾਂ ਤੱਕ ਭੌਤਿਕ ਪਹੁੰਚ ਨੂੰ ਸੀਮਤ ਕਰਨਾ ਡੇਟਾ ਚੋਰੀ ਹੋਣ ਜਾਂ ਹੋਰ ਖ਼ਤਰਨਾਕ ਗਤੀਵਿਧੀ ਨੂੰ ਰੋਕਣ ਦਾ ਇੱਕ ਸਧਾਰਨ ਤਰੀਕਾ ਹੈ। ਕਾਰੋਬਾਰੀ ਯੰਤਰਾਂ ਨੂੰ ਉਸ ਥਾਂ ਉੱਪਰ ਨਹੀਂ ਰੱਖਿਆ ਜਾਣਾ ਚਾਹੀਦਾ ਜਿੱਥੇ ਅਣ-ਅਧਿਕਾਰਤ ਸਟਾਫ਼ ਜਾਂ ਜਨਤਾ ਦੇ ਮੈਂਬਰ ਉਨ੍ਹਾਂ ਤੱਕ ਪਹੁੰਚ ਕਰ ਸਕਦੇ ਹਨ।

ਆਪਣੇ ਕਾਰੋਬਾਰੀ ਉਪਕਰਨਾਂ ਨੂੰ ਹੋਰ ਵਧੇਰੇ ਸੁਰੱਖਿਅਤ ਕਰਨ ਲਈ ਸੁਰੱਖਿਆ ਨਿਯੰਤਰਣਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ। ਉਹਨਾਂ ਨੂੰ ਘੱਟੋ-ਘੱਟ ਪਾਸਫਰੇਜ਼, ਪਿੰਨ ਜਾਂ ਬਾਇਓਮੈਟ੍ਰਿਕਸ ਨਾਲ ਲਾਕ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ। ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਇਹ ਉਪਕਰਨ ਥੋੜ੍ਹੇ ਸਮੇਂ ਦੀ ਅਕਿਰਿਆਸ਼ੀਲਤਾ ਤੋਂ ਬਾਅਦ ਆਪਣੇ ਆਪ ਬੰਦ (ਲਾਕ) ਹੋਣ ਲਈ ਸੈੱਟ ਕੀਤੇ ਗਏ ਹਨ।

✓ **ਉਪਕਰਨਾਂ ਨੂੰ ਅਕਿਰਿਆਸ਼ੀਲਤਾ ਦੇ ਥੋੜ੍ਹੇ ਸਮੇਂ ਬਾਅਦ ਆਪਣੇ-ਆਪ ਲਾਕ ਹੋਣ ਲਈ ਸੈੱਟ ਕਰੋ।**

ਆਪਣੇ ਕਾਰੋਬਾਰੀ ਡੇਟੇ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ

ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਦੁਆਰਾ ਰੱਖਿਆ ਗਿਆ ਡੇਟਾ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਲਈ ਇੱਕ ਦਿਲ-ਖਿੱਚਵਾਂ ਨਿਸ਼ਾਨਾ ਹੁੰਦਾ ਹੈ।

ਡੇਟਾ ਉਲੰਘਣਾਵਾਂ ਵੱਧ ਰਹੀਆਂ ਹਨ - ਆਪਣੇ ਕਾਰੋਬਾਰ ਨੂੰ ਇਸਦਾ ਸ਼ਿਕਾਰ ਨਾ ਹੋਣ ਦਿਓ। ਇਹ ਸਮਝਣਾ ਮਹੱਤਵਪੂਰਨ ਹੈ ਕਿ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਕੋਲ ਕਿਹੜਾ ਡੇਟਾ ਹੈ, ਅਤੇ ਕਿੱਥੇ ਹੈ। ਇੱਕ ਵਾਰ ਜਦੋਂ ਤੁਸੀਂ ਇਸ ਬਾਰੇ ਸੁਚੇਤ ਹੋ ਜਾਂਦੇ ਹੋ, ਤਾਂ ਤੁਹਾਡੇ ਡੇਟੇ ਨੂੰ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਦੁਆਰਾ ਐਕਸੈਸ ਕੀਤੇ ਜਾਣ ਤੋਂ ਬਚਾਉਣ ਵਿੱਚ ਮੱਦਦ ਲਈ ਇਸ ਗਾਈਡ ਵਿਚਲੀਆਂ ਸਿਫ਼ਾਰਸ਼ਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ। ਕੁੱਝ ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਦੀਆਂ ਕਾਨੂੰਨ ਅਧੀਨ ਵਧੀਕ ਕਾਨੂੰਨੀ ਜ਼ਿੰਮੇਵਾਰੀਆਂ ਵੀ ਹੋ ਸਕਦੀਆਂ ਹਨ।

- **ਆਪਣੇ ਕਾਰੋਬਾਰੀ ਡੇਟੇ ਨੂੰ ਇਕ ਥਾਂ ਇਕੱਠਾ ਕਰੋ।** ਤੁਹਾਡੇ ਕੋਲ ਕਈ ਉਪਕਰਨਾਂ ਜਾਂ ਸੇਵਾਵਾਂ ਵਿੱਚ ਡੇਟਾ ਸਟੋਰ ਕੀਤਾ ਗਿਆ ਹੋ ਸਕਦਾ ਹੈ। ਜਦੋਂ ਡੇਟਾ ਕਈ ਥਾਵਾਂ 'ਤੇ ਹੁੰਦਾ ਹੈ, ਤਾਂ ਇਹ ਉਨ੍ਹਾਂ ਸਿਸਟਮਾਂ ਦੀ ਸੰਖਿਆ ਨੂੰ ਵਧਾਉਂਦਾ ਹੈ ਜੋ ਤੁਹਾਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਅਤੇ ਬੈਕਅੱਪ ਲੈਣ ਲਈ ਕਰਨੇ ਹੁੰਦੇ ਹਨ। ਕਈ ਸਿਸਟਮਾਂ ਦਾ ਹੋਣਾ ਸਾਈਬਰ ਅਪਰਾਧੀ ਲਈ ਹਮਲਾ ਕਰਨ ਦੇ ਹੋਰ ਮੌਕੇ ਵੀ ਪੈਦਾ ਕਰ ਸਕਦਾ ਹੈ। ਜਿੱਥੇ ਵੀ ਸੰਭਵ ਹੋਵੇ, ਆਪਣੇ ਕਾਰੋਬਾਰੀ ਡੇਟੇ ਨੂੰ ਕੇਂਦਰੀ ਸਥਾਨ 'ਤੇ ਸਟੋਰ ਕਰੋ ਜੋ ਸੁਰੱਖਿਅਤ ਹੈ ਅਤੇ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਬੈਕਅੱਪ ਕੀਤਾ ਜਾਂਦਾ ਹੈ। ਜੇਕਰ ਤੁਹਾਡੇ ਸਿਸਟਮਾਂ ਨਾਲ ਸਮਝੌਤਾ (ਚੋਰੀ) ਕੀਤਾ ਜਾਂਦਾ ਹੈ ਤਾਂ ਤੁਹਾਡੇ ਡੇਟੇ ਨੂੰ ਇੱਕਠਾ ਕਰਨ ਨਾਲ ਇੱਕ ਵੱਡੀ ਡੇਟਾ ਉਲੰਘਣਾ ਹੋ ਸਕਦੀ ਹੈ, ਇਸ ਲਈ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਇਹ ਕੇਂਦਰੀ ਸਥਾਨ ਸੁਰੱਖਿਅਤ ਸੰਰਚਨਾਵਾਂ ਅਤੇ ਪਾਬੰਦੀਸ਼ੁਦਾ ਪਹੁੰਚ ਨਾਲ ਢੁੱਕਵੇਂ ਰੂਪ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਹੈ। ਸਲਾਹ ਲਈ ਕਿਸੇ IT ਜਾਂ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਪੇਸ਼ੇਵਰ ਨਾਲ ਗੱਲ ਕਰੋ।
- **ਡੇਟੇ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਆਪਣੀਆਂ ਕਾਨੂੰਨੀ ਜ਼ਿੰਮੇਵਾਰੀਆਂ ਨੂੰ ਜਾਣੋ।** ਕੁੱਝ ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਕੋਲ ਉਨ੍ਹਾਂ ਦੁਆਰਾ ਇਕੱਠੀ ਕੀਤੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਸੰਭਾਲਣ ਲਈ ਕਾਨੂੰਨੀ ਜ਼ਿੰਮੇਵਾਰੀਆਂ ਲਾਗੂ ਹੋ ਸਕਦੀਆਂ ਹਨ। ਹੋਰ ਜਾਣਨ ਲਈ ਆਸਟ੍ਰੇਲੀਆ ਦੇ ਸੂਚਨਾ ਕਮਿਸ਼ਨਰ ਦੇ ਦਫ਼ਤਰ ਦੀ ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਲਈ ਗਾਈਡ ਨੂੰ ਪੜ੍ਹੋ, ਜੋ ਕਿ **oaic.gov.au** 'ਤੇ ਉਪਲਬਧ ਹੈ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਯਕੀਨ ਨਹੀਂ ਹੈ ਤਾਂ ਕਿਸੇ ਕਾਨੂੰਨੀ ਪੇਸ਼ੇਵਰ ਨਾਲ ਸਲਾਹ ਕਰੋ।

✓ **ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਕੋਲ ਮੌਜੂਦ ਡੇਟਾ ਅਤੇ ਇਸਦੀ ਸੁਰੱਖਿਆ ਲਈ ਆਪਣੀਆਂ ਜ਼ਿੰਮੇਵਾਰੀਆਂ ਨੂੰ ਸਮਝੋ।**

ਆਪਣੇ ਸਟਾਫ਼ ਨੂੰ ਤਿਆਰ ਕਰੋ

ਕਰਮਚਾਰੀਆਂ ਨੂੰ ਸਿੱਖਿਅਤ ਕਰੋ

ਚੰਗੇ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਤਰੀਕਿਆਂ ਨਾਲ ਕੰਮ ਕਰਨ ਵਾਲੇ ਕਰਮਚਾਰੀ ਸਾਈਬਰ ਹਮਲਿਆਂ ਦੇ ਵਿਰੁੱਧ ਤੁਹਾਡੇ ਪਹਿਲੇ ਬਚਾਓ ਕਵਚ ਹਨ।

ਤੁਹਾਡੇ ਕਰਮਚਾਰੀਆਂ ਨੂੰ ਹੇਠਾਂ ਦਿੱਤੇ ਵਿਸ਼ਿਆਂ ਸਮੇਤ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਬਾਰੇ ਜਾਗਰੂਕਤਾ ਹੋਣੀ ਚਾਹੀਦੀ ਹੈ:

- ਆਮ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਖ਼ਤਰੇ ਜਿਵੇਂ ਕਿ ਕਾਰੋਬਾਰੀ ਈਮੇਲ ਸਮਝੌਤਾ ਅਤੇ ਰੈਨਸਮਵੇਅਰ
- MFA ਅਤੇ ਸਾਫ਼ਟਵੇਅਰ ਅੱਪਡੇਟ ਸਮੇਤ ਸੁਰੱਖਿਆ ਉਪਾਅ
- ਧੋਖਾਧੜੀ ਅਤੇ ਫਿਸ਼ਿੰਗ ਹਮਲਿਆਂ ਦਾ ਪਤਾ ਕਿਵੇਂ ਲਗਾਇਆ ਜਾਵੇ
- ਕਾਰੋਬਾਰੀ ਵਿਸ਼ੇਸ਼ ਨੀਤੀਆਂ (ਉਦਾਹਰਨ ਲਈ, ਸ਼ੱਕੀ ਈਮੇਲਾਂ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਜਾਂ ਭੁਗਤਾਨ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਇਨਵੌਇਸਾਂ ਦੀ ਪੁਸ਼ਟੀ ਕਰਨ ਦੀਆਂ ਪ੍ਰਕਿਰਿਆਵਾਂ ਕਿ ਉਹ ਅਸਲੀ ਹਨ)
- ਐਮਰਜੈਂਸੀ ਵਿੱਚ ਕੀ ਕਰਨਾ ਹੈ।

ACSC ਦੀ ਵੈੱਬਸਾਈਟ cyber.gov.au/learn 'ਤੇ ਇਨ੍ਹਾਂ ਵਿੱਚੋਂ ਜ਼ਿਆਦਾਤਰ ਵਿਸ਼ਿਆਂ ਲਈ ਸਰੋਤ ਹਨ। ਤੁਸੀਂ ਆਪਣੇ ਕਰਮਚਾਰੀਆਂ ਨੂੰ ਸਿੱਖਿਅਤ ਕਰਨ ਦੇ ਹੋਰ ਤਰੀਕਿਆਂ 'ਤੇ ਵੀ ਵਿਚਾਰ ਕਰ ਸਕਦੇ ਹੋ, ਉਦਾਹਰਨ ਲਈ ਰਸਮੀ ਕੋਰਸ ਜਾਂ ਅੰਦਰੂਨੀ ਸਿਖਲਾਈ। ਹਾਲਾਂਕਿ ਤੁਸੀਂ ਫ਼ੈਸਲਾ ਕਰਦੇ ਹੋ, ਯਾਦ ਰੱਖੋ ਕਿ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਸਿਖਲਾਈ ਇੱਕ ਵਾਰ ਕਰਨ ਵਾਲੀ ਜ਼ਰੂਰਤ ਨਹੀਂ ਹੈ ਅਤੇ ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਦੋਬਾਰਾ ਤਾਜ਼ਾ ਕੀਤੀ ਜਾਣੀ ਚਾਹੀਦੀ ਹੈ।

✓ **ਇਹ ਨਿਰਧਾਰਤ ਕਰੋ ਕਿ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਵਿੱਚ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਜਾਗਰੂਕਤਾ ਕਿਵੇਂ ਸਿਖਾਈ ਜਾਵੇਗੀ।**

ਐਮਰਜੈਂਸੀ ਯੋਜਨਾ ਬਣਾਓ

ਇੱਕ ਐਮਰਜੈਂਸੀ ਯੋਜਨਾ ਦਾ ਹੋਣਾ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ 'ਤੇ ਸਾਈਬਰ ਹਮਲੇ ਦੇ ਪ੍ਰਭਾਵ ਨੂੰ ਘਟਾ ਸਕਦਾ ਹੈ।

ਕਿਸੇ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਘਟਨਾ ਪ੍ਰਤੀ ਜਵਾਬੀ ਕਾਰਵਾਈ ਕਰਨ ਵੇਲੇ, ਹਰ ਪਲ ਮਾਇਨੇ ਰੱਖਦਾ ਹੈ। ਐਮਰਜੈਂਸੀ ਯੋਜਨਾ ਹੋਣ ਦਾ ਮਤਲਬ ਹੈ ਕਿ ਤੁਹਾਡੇ ਸਟਾਫ਼ ਨੂੰ ਇਹ ਪਤਾ ਲਗਾਉਣ ਵਿੱਚ ਘੱਟ ਸਮਾਂ ਲੱਗ ਸਕਦਾ ਕਿ ਕੀ ਕਰਨਾ ਹੈ ਅਤੇ ਕਾਰਵਾਈ ਕਰਨ ਵਿੱਚ ਜ਼ਿਆਦਾ ਸਮਾਂ ਮਿਲ ਸਕਦਾ ਹੈ।

ਆਪਣੀ ਐਮਰਜੈਂਸੀ ਯੋਜਨਾ ਬਣਾਉਂਦੇ ਸਮੇਂ ਹੇਠਾਂ ਦਿੱਤੇ ਸਵਾਲਾਂ 'ਤੇ ਵਿਚਾਰ ਕਰੋ:

- ਤੁਹਾਡੇ ਸਟਾਫ਼ ਲਈ ਕਿਸੇ ਸੰਭਾਵੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਘਟਨਾਵਾਂ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਲਈ ਕੀ ਪ੍ਰਕਿਰਿਆ ਲਾਗੂ ਹੈ?
- ਤੁਸੀਂ ਸਹਾਇਤਾ ਲਈ ਕਿਸ ਨਾਲ ਸੰਪਰਕ ਕਰੋਗੇ? ਉਦਾਹਰਨ ਲਈ, IT ਪੇਸ਼ੇਵਰ ਅਤੇ ਤੁਹਾਡਾ ਬੈਂਕ।
- ਇਸ ਘਟਨਾ ਬਾਰੇ ਤੁਹਾਡੇ ਸਟਾਫ਼, ਹਿੱਤਧਾਰਕਾਂ ਜਾਂ ਗਾਹਕਾਂ ਨੂੰ ਕਿਵੇਂ ਸੂਚਿਤ ਕੀਤਾ ਜਾਵੇਗਾ?
- ਜੇਕਰ ਕੋਈ ਨਾਜ਼ੁਕ ਸਿਸਟਮ ਬੰਦ ਹੋ ਜਾਂਦਾ ਹੈ ਤਾਂ ਤੁਸੀਂ ਆਮ ਵਾਂਗ ਕਾਰੋਬਾਰ ਕਿਵੇਂ ਕਰੋਗੇ?

ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡਾ ਸਟਾਫ਼ ਐਮਰਜੈਂਸੀ ਯੋਜਨਾ ਤੋਂ ਜਾਣੂ ਹੈ, ਜਿਸ ਵਿੱਚ ਉਹਨਾਂ ਦੀਆਂ ਕੋਈ ਵੀ ਭੂਮਿਕਾਵਾਂ ਜਾਂ ਜ਼ਿੰਮੇਵਾਰੀਆਂ ਸ਼ਾਮਲ ਹਨ। ਤੁਹਾਡੇ ਸਿਸਟਮ ਦੇ ਬੰਦ ਹੋਣ ਦੀ ਸਥਿਤੀ ਵਿੱਚ ਇਸ ਯੋਜਨਾ ਦੀ ਵਰਤੋਂ ਲਈ ਇੱਕ ਹਾਰਡ ਕਾਪੀ ਬਣਾਕੇ ਰੱਖੋ ਜੇਕਰ ਤੁਹਾਨੂੰ ਇਸਦੀ ਲੋੜ ਹੋਵੇ।

✓ **ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਘਟਨਾਵਾਂ ਲਈ ਇੱਕ ਐਮਰਜੈਂਸੀ ਯੋਜਨਾ ਬਣਾਓ।**

ਜਾਗਰੂਕ ਰਹੋ

ACSC ਤੋਂ ਨਵੀਨਤਮ ਜਾਣਕਾਰੀ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ ACSC ਭਾਈਵਾਲ ਬਣੋ।

ACSC ਭਾਈਵਾਲ ਬਣ ਕੇ ਨਵੀਨਤਮ ਸਾਈਬਰ ਖ਼ਤਰਿਆਂ ਅਤੇ ਕਮਜ਼ੋਰੀਆਂ ਬਾਰੇ ਸੂਚਿਤ ਰਹੋ। ਜਦੋਂ ਕਿਸੇ ਨਵੇਂ ਸਾਈਬਰ ਖ਼ਤਰੇ ਦੀ ਪਛਾਣ ਕੀਤੀ ਜਾਂਦੀ ਹੈ ਤਾਂ ਇਹ ਸੇਵਾ ਤੁਹਾਨੂੰ ਮਹੀਨਾਵਾਰ ਖਬਰਨਾਮੇ (ਨਿਊਜ਼ਲੈਟਰ) ਅਤੇ ਚੇਤਾਵਨੀਆਂ ਭੇਜੇਗੀ।

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਇੱਕ ਤੇਜ਼ੀ ਨਾਲ ਵਿਕਸਿਤ ਹੋ ਰਿਹਾ ਖੇਤਰ ਹੈ। ਸਾਈਬਰ ਅਪਰਾਧੀ ਆਪਣੀ ਖੋਜ ਦੇ ਕੁੱਝ ਮਿੰਟਾਂ ਦੇ ਅੰਦਰ ਹੀ ਸਿਸਟਮ ਦੀਆਂ ਕਮਜ਼ੋਰੀਆਂ ਦਾ ਸਰਗਰਮੀ ਨਾਲ ਸ਼ੋਸ਼ਣ ਕਰਦੇ ਹਨ। ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀ ਦੁਨੀਆਂ ਬਾਰੇ ਸੂਚਿਤ ਰਹਿਣਾ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਨੂੰ ਉਹਨਾਂ ਖ਼ਤਰਿਆਂ ਨੂੰ ਸਮਝਣ ਵਿੱਚ ਮੱਦਦ ਕਰੇਗਾ ਜਿਨ੍ਹਾਂ ਦਾ ਉਸ ਵੱਲੋਂ ਸਾਹਮਣਾ ਕਰਨ ਦੀ ਸੰਭਾਵਨਾ ਹੈ ਅਤੇ ਉਹਨਾਂ ਤੋਂ ਕਿਵੇਂ ਸੁਰੱਖਿਆ ਕੀਤੀ ਜਾਵੇ।

✓ **ਆਪਣੇ ਕਾਰੋਬਾਰ ਨੂੰ ACSC ਪਾਰਟਨਰਸ਼ਿਪ ਪ੍ਰੋਗਰਾਮ ਨਾਲ ਰਜਿਸਟਰ ਕਰੋ।**

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