Community Resilience to Foreign Interference

National Cyber Security Centre

ਆਪਣੇ ਸੰਗਠਨ ਨੂੰ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰੱਖਣਾ

ਭਾਈਚਾਰਕ ਸਮੂਹਾਂ ਅਤੇ ਸੰਗਠਨਾਂ ਲਈ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਮਹੱਤਵਪੂਰਨ ਕਿਉਂ ਹੈ?

ਇਸ ਪੰਨੇ ਉੱਤੇ ਸਲਾਹ ਅਤੇ ਕੁਝ ਕਦਮ ਹਨ ਜੋ ਤੁਸੀਂ ਆਪਣੇ ਭਾਈਚਾਰਕ ਸਮੂਹ ਜਾਂ ਸੰਗਠਨ ਨੂੰ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਖਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਲਈ ਚੁੱਕ ਸਕਦੇ ਹੋ। ਆਪਣੇ ਆਪ ਨੂੰ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਵਿਅਕਤੀਆਂ ਲਈ ਇੱਕ ਵੱਖਰੀ ਗਾਈਡ ਵੀ ਹੈ।

ਇਹ ਸਲਾਹ ਸਭ ਤੋਂ ਆਮ ਅਤੇ ਗੰਭੀਰ ਖਤਰਿਆਂ ਉੱਤੇ ਅਧਾਰਿਤ ਹੈ।

ਅੱਪਡੇਟ

ਸੁਰੱਖਿਆ ਵਿੱਚ ਕਿਸੇ ਵੀ ਛੇਕ ਨੂੰ ਬੰਦ ਕਰਨ ਲਈ ਆਪਣੀਆਂ ਡਿਵਾਈਸਾਂ ਉੱਤੇ ਸਾਫਟਵੇਅਰ ਨੂੰ ਅੱਪ ਟੂ ਡੇਟ ਰੱਖੋ।

- ਆਪਣੇ ਭਾਈਚਾਰਕ ਸਮੂਹ ਜਾਂ ਸੰਗਠਨ ਦੇ ਡਿਵਾਈਸਾਂ ਨੂੰ ਅਪਡੇਟ ਰੱਖੋ। ਇਸ ਵਿੱਚ ਫ਼ੋਨ, ਕੰਪਿਊਟਰ, ਵਾਈ-ਫਾਈ ਰਾਊਟਰ, ਅਤੇ ਸਮਾਰਟ ਡੀਵਾਈਸਾਂ ਸਮੇਤ ਇੰਟਰਨੈੱਟ ਨਾਲ ਜੁੜਣ ਵਾਲੀ ਕੋਈ ਵੀ ਚੀਜ਼ ਸ਼ਾਮਲ ਹੈ।
- ਜਿੱਥੇ ਵੀ ਮੁਮਕਿਨ ਹੋਵੇ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟ ਵਰਤੋ।

ਦੋ-ਕਾਰਕ ਪ੍ਰਮਾਣਿਕਤਾ (2FA)

ਇੱਕ ਪਾਸਵਰਡ ਅਤੇ ਇੱਕ ਹੋਰ ਕਦਮ ਦੀ ਲੋੜ ਕਰਕੇ ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਵਿੱਚ ਵਾਧੂ ਸੁਰੱਖਿਆ ਸ਼ਾਮਲ ਕਰਦਾ ਹੈ, ਜਿਵੇਂ ਕਿ ਤੁਹਾਡੇ ਫ਼ੋਨ ਉੱਤੇ ਇੱਕ ਐਪ ਤੋਂ ਕੋਡ।

- ਨੋਟ: ਇਸ ਨੂੰ ਬਹੁ-ਕਾਰਕ ਪ੍ਰਮਾਣਿਕਤਾ (MFA), ਦੋ-ਪੜਾਵੀ ਤਸਦੀਕ (2SV) ਅਤੇ ਕਈ ਹੋਰ ਨਾਂ ਵੀ ਕਹੇ ਜਾਂਦੇ ਹਨ।

- ਆਪਣੇ ਸਾਰੇ ਭਾਈਚਾਰਕ ਸਮੂਹ ਜਾਂ ਸੰਗਠਨ ਦੇ ਖਾਤਿਆਂ ਉੱਤੇ 2FA ਨੂੰ ਚਾਲੂ ਕਰੋ।
- ਜੇਕਰ ਸੰਭਵ ਹੋਵੇ, ਤਾਂ 2FA ਦੇ ਇੱਕ ਫਾਰਮ ਦੀ ਵਰਤੋਂ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ ਜੋ ਫਿਸ਼ਿੰਗ ਰੋਧੀ ਹੈ, ਜਿਸਦਾ ਮਤਲਬ ਹੈ ਕਿ ਤੁਹਾਨੂੰ ਇਸਨੂੰ ਦੇਣ ਲਈ ਧੋਖਾ ਨਹੀਂ ਦਿੱਤਾ ਜਾ ਸਕਦਾ ਹੈ। ਇਹ ਇੱਕ ਭੌਤਿਕ ਸੁਰੱਖਿਆ ਕੁੰਜੀ ਜਾਂ ਫਿੰਗਰਪ੍ਰਿੰਟ ਜਾਂ ਫੇਸ ID ਵਰਗੀ ਕੋਈ ਚੀਜ਼ ਹੋ ਸਕਦੀ ਹੈ।

ਆਪਣੇ ਔਨਲਾਈਨ ਖਾਤਿਆਂ ਉੱਤੇ ਨਜ਼ਰ ਰੱਖੋ

ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਸਾਬਕਾ ਮੈਂਬਰ ਭਾਈਚਾਰਕ ਸਮੂਹ ਜਾਂ ਸੰਗਠਨ ਨੂੰ ਛੱਡਣ ਤੋਂ ਬਾਅਦ ਖਾਤਿਆਂ ਤੱਕ ਆਪਣੀ ਪਹੁੰਚ ਨਾ ਰੱਖਣ।

- ਜੇਕਰ ਤੁਹਾਡੇ ਕੋਲ ਇੱਕੋ ਖਾਤੇ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਵਾਲੇ ਇੱਕ ਤੋਂ ਵੱਧ ਵਿਅਕਤੀ ਹਨ, ਤਾਂ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਉਹਨਾਂ ਸਾਰਿਆਂ ਦੇ ਵੱਖ-ਵੱਖ ਲੌਗਿਨ ਹਨ, ਅਤੇ ਸਾਰਿਆਂ ਕੋਲ 2FA ਚਾਲੂ ਹੈ।
- ਸਾਰੇ ਉਪਯੋਗਕਰਤਾ ਖਾਤਿਆਂ ਦੀ ਇੱਕ ਸੂਚੀ ਰੱਖੋ ਅਤੇ ਉਹਨਾਂ ਨੂੰ ਅਕਿਰਿਆਸ਼ੀਲ ਕਰੋ ਜਿਸਦੀ ਲੋੜ ਨਹੀਂ ਹੈ, ਜਿਵੇਂ ਕਿ ਜਦੋਂ ਸਟਾਫ ਛੱਡਦਾ ਹੈ।
- ਤੁਹਾਡੇ ਦੁਆਰਾ ਆਪਣੇ ਮੈਂਬਰਾਂ ਨੂੰ ਦਿੱਤੇ ਗਏ ਕਿਸੇ ਵੀ ਡਿਵਾਈਸ ਦਾ ਇੱਕ ਰਜਿਸਟਰ ਰੱਖੋ ਅਤੇ ਉਹਨਾਂ ਨੂੰ ਵਾਪਸ ਪ੍ਰਾਪਤ ਕਰਨਾ ਯਾਦ ਰੱਖੋ ਅਤੇ ਜੇਕਰ ਉਹ ਵਿਅਕਤੀ ਸੰਗਠਨ ਛੱਡ ਦਿੰਦਾ ਹੈ ਤਾਂ ਉਹਨਾਂ ਨੂੰ ਫੈਕਟਰੀ ਰੀਸੈਟ ਕਰੋ। ਤੁਹਾਨੂੰ ਬਿਲਡਿੰਗ ਵਿੱਚ ਪਹੁੰਚ ਲਈ ਭੌਤਿਕ ਕੋਡ ਬਦਲਣ ਦੀ ਵੀ ਲੋੜ ਹੋ ਸਕਦੀ ਹੈ।

ਜਾਂਚ ਕਰੋ ਕਿ ਤੁਹਾਡੇ ਔਨਲਾਈਨ ਖਾਤਿਆਂ ਤੱਕ ਕਿਸ ਕੋਲ ਪਹੁੰਚ ਹੈ

ਤੁਹਾਡੇ ਭਾਈਚਾਰਕ ਸਮੂਹ ਜਾਂ ਸੰਗਠਨ ਦੇ ਲੋਕਾਂ ਕੋਲ ਸਿਰਫ਼ ਉਹਨਾਂ ਚੀਜ਼ਾਂ ਤੱਕ ਪਹੁੰਚ ਹੋਣੀ ਚਾਹੀਦੀ ਹੈ ਜਿਨ੍ਹਾਂ ਦੀ ਉਹਨਾਂ ਨੂੰ ਲੋੜ ਹੈ।

- ਜੇਕਰ ਕਿਸੇ ਵਿਅਕਤੀ ਦਾ ਖਾਤਾ ਹੈਕ ਹੋ ਜਾਂਦਾ ਹੈਂ ਤਾਂ ਇਹ ਕਦਮ ਹਮਲਾਵਰ ਦੇ ਨੁਕਸਾਨ ਨੂੰ ਸੀਮਤ ਕਰਦੇ ਹਨ।
- ਨਿਯਮਿਤ ਤੌਰ ਉੱਤੇ ਜਾਂਚ ਕਰੋ ਅਤੇ ਬੇਲੋੜੀਆਂ ਇਜਾਜ਼ਤਾਂ ਨੂੰ ਹਟਾਓ।
- ਜੇਕਰ ਤੁਹਾਡੇ ਕੋਲ ਇੱਕ ਸਿੰਗਲ "ਐਡਮਿਨ" ਖਾਤਾ ਹੈ ਜਿਸਨੂੰ ਕਈ ਲੋਕ ਵਰਤਦੇ ਹਨ, ਤਾਂ ਅਸਾਧਾਰਨ ਗਤੀਵਿਧੀ ਲਈ ਇਸ ਦੀ ਨਿਗਰਾਨੀ ਕਰੋ। ਇਸ ਤਰ੍ਹਾਂ ਦੇ ਖਾਤਿਆਂ ਨੂੰ ਸੀਮਤ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ, ਖਾਸ ਕਰਕੇ ਰੋਜ਼ਾਨਾ ਦੇ ਕੰਮਾਂ ਲਈ।
- ਇਹ ਨਿਯਮ ਡਿਵਾਈਸਾਂ, ਜਿਵੇਂਕਿ ਰਾਊਟਰਾਂ ਤੱਕ ਪ੍ਰਬੰਧਕੀ ਪਹੁੰਚ ਉੱਤੇ ਵੀ ਲਾਗੂ ਹੁੰਦੇ ਹਨ।

ਸੇਵਾ ਪ੍ਰਦਾਤਾਵਾਂ ਨਾਲ ਆਪਣੇ ਇਕਰਾਰਨਾਮਿਆਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ

ਜੇਕਰ ਤੁਸੀਂ ਆਪਣੇ ਲਈ IT ਸੇਵਾਵਾਂ ਚਲਾਉਣ ਲਈ ਕਿਸੇ ਨੂੰ ਨੌਕਰੀ ਉੱਤੇ ਰੱਖਿਆ ਹੈ।

- ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਉਹਨਾਂ ਕੋਲ ਤੁਹਾਡੇ ਭਾਈਚਾਰਕ ਸਮੂਹ ਜਾਂ ਸੰਗਠਨ ਦੀਆਂ ਲੋੜਾਂ ਨੂੰ ਪੂਰਾ ਕਰਨ ਲਈ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਹਿਫਾਜ਼ਤ ਮੌਜੂਦ ਹੈ।

ਜਾਣੋ ਕਿ ਤੁਹਾਡੇ ਸਾਰੇ ਖਾਤੇ ਅਤੇ ਸਿਸਟਮ ਇਕੱਠੇ ਕਿਵੇਂ ਕੰਮ ਕਰਦੇ ਹਨ

ਕਨੈਕਸ਼ਨਾਂ ਨੂੰ ਸਮਝਣਾ ਤੁਹਾਨੂੰ ਇਹ ਜਾਣਨ ਵਿੱਚ ਮਦਦ ਕਰਦਾ ਹੈ ਕਿ ਹਮਲਾਵਰ ਕਿੱਥੇ ਦਾਖਲ ਹੋ ਸਕਦਾ ਹੈ।

- ਆਪਣੇ ਸਿਸਟਮਾਂ ਵਿਚਕਾਰ ਕਨੈਕਸ਼ਨਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ, ਉਦਾਹਰਨ ਲਈ, ਈਮੇਲ, ਕਲਾਉਡ ਸਟੋਰੇਜ, ਅਤੇ ਅਕਾਊਂਟਿੰਗ ਪਲੇਟਫਾਰਮ।
- ਵਾਧੂ ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ ਲਈ ਇੱਕ ਵਰਚੁਅਲ ਪ੍ਰਾਈਵੇਟ ਨੈੱਟਵਰਕ (VPN) ਦੀ ਵਰਤੋਂ ਕਰਨ ਉੱਤੇ ਵਿਚਾਰ ਕਰੋ। VPN ਦੀ ਵਰਤੋਂ ਕਰਨਾ ਤੁਹਾਡੀ ਔਨਲਾਈਨ ਗਤੀਵਿਧੀ ਨੂੰ ਕਿਸੇ ਵੀ ਉਸ ਵਿਅਕਤੀ ਤੋਂ ਲੁਕਾਉਂਦਾ ਹੈ ਜੋ ਤੁਹਾਨੂੰ ਟਰੈਕ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰ ਸਕਦਾ ਹੈ। ਇਹ ਖਾਸ ਤੌਰ ਉੱਤੇ ਚੰਗਾ ਹੁੰਦਾ ਹੈ ਜੇਕਰ ਤੁਹਾਡੇ ਭਾਈਚਾਰਕ ਸਮੂਹ ਜਾਂ ਸੰਗਠਨ ਦੇ ਕੋਈ ਮੈਂਬਰ ਰਿਮੋਟਲੀ ਜੁੜਦੇ ਹਨ।

ਆਪਣੇ ਲੋਕਾਂ ਨੂੰ 'ਸਾਈਬਰ ਸਮਾਰਟ' ਰੱਖੋ

ਤੁਹਾਡੇ ਭਾਈਚਾਰਕ ਸਮੂਹ ਜਾਂ ਸੰਗਠਨ ਦੇ ਲੋਕਾਂ ਨੂੰ ਤੁਹਾਡੇ ਸਿਸਟਮਾਂ ਨਾਲੋਂ ਜ਼ਿਆਦਾ ਨਿਸ਼ਾਨਾ ਬਣਾਏ ਜਾਣ ਦੀ ਸੰਭਾਵਨਾ ਹੈ।

- ਸਾਰੇ ਸਟਾਫ ਨੂੰ ਬੁਨਿਆਦੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਵਿੱਚ ਸਿਖਲਾਈ ਦਿਓ। ਔਨ ਯੋਰ ਔਨਲਾਈਨ (Own Your Online) ਵੈੱਬਸਾਈਟ ਔਨ ਯੋਰ ਔਨਲਾਈਨ | NCSC ਕੋਲ ਆਪਣੇ ਆਪ ਨੂੰ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਅਤੇ ਘੁਟਾਲਿਆਂ ਦਾ ਪਤਾ ਲਗਾਉਣ ਵਿੱਚ ਮਦਦ ਕਰਨ ਲਈ ਬਹੁਤ ਸਾਰੀਆਂ ਸਲਾਹਾਂ ਅਤੇ ਸੁਝਾਅ ਹਨ।
- ਉਹਨਾਂ ਨੂੰ ਯਾਦ ਦਿਵਾਓ ਕਿ ਇਹ ਉਹਨਾਂ ਦੇ ਨਿੱਜੀ ਖਾਤਿਆਂ ਦੇ ਨਾਲ-ਨਾਲ ਉਹਨਾਂ ਲਈ ਮਹੱਤਵਪੂਰਨ ਹੈ ਜਿਹਨਾਂ ਦੀ ਵਰਤੋਂ ਉਹ ਤੁਹਾਡੇ ਸੰਗਠਨ ਲਈ ਕਰਦੇ ਹਨ।
- ਸਾਡੇ ਕੋਲ ਵਿਅਕਤੀਆਂ ਲਈ ਆਪਣੇ ਆਪ ਨੂੰ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਇੱਕ ਗਾਈਡ ਹੈ।

ਕਿਸੇ ਘਟਨਾ ਲਈ ਯੋਜਨਾ ਬਣਾਓ

ਜਦੋਂ ਕੋਈ ਘਟਨਾ ਵਾਪਰਦੀ ਹੈ ਤਾਂ ਲੋਕਾਂ ਨੂੰ ਘਬਰਾਉਣ ਤੋਂ ਰੋਕਣ ਲਈ ਜਵਾਬੀ ਯੋਜਨਾ ਦਾ ਹੋਣਾ ਮਹੱਤਵਪੂਰਨ ਹੈ।

- ਇੱਕ ਘਟਨਾ ਦੀ ਜਵਾਬੀ ਯੋਜਨਾ ਇਹ ਦੱਸਦੀ ਹੈ ਕਿ ਘਟਨਾ ਦੌਰਾਨ ਕੌਣ ਕੀ ਕਰਦਾ ਹੈ। ਟੈਂਪਲੇਟ ਇੱਥੇ ਉਪਲਬਧ ਹਨ ਘਟਨਾ ਪ੍ਰਬੰਧਨ | NCSC
- ਜੇਕਰ ਫ਼ੋਨ, ਕੰਪਿਊਟਰ, ਜਾਂ ਹੋਰ ਸਿਸਟਮ ਫੇਲ ਹੋ ਜਾਂਦੇ ਹਨ ਤਾਂ ਕਰਨਾ ਕੀ ਹੈ ਇਸ ਬਾਰੇ ਇੱਕ ਯੋਜਨਾ ਸ਼ਾਮਲ ਕਰੋ। ਇਸ ਯੋਜਨਾ ਨੂੰ ਅੱਪਡੇਟ ਰੱਖੋ।
- ਲੋੜੀਂਦੇ ਹਰੇਕ ਵਿਅਕਤੀ ਦੇ ਸੰਪਰਕ ਵੇਰਵੇ ਅਤੇ ਬੈਕਅੱਪ ਵੇਰਵੇ ਰੱਖੋ ਜੇਕਰ ਉਹਨਾਂ ਨਾਲ ਸੰਪਰਕ ਕਰਨ ਦਾ ਮੁੱਖ ਤਰੀਕਾ ਟੁੱਟ ਗਿਆ ਹੈ (ਜਿਵੇਂਕਿ ਈਮੇਲ)।
- ਯੋਜਨਾ ਨੂੰ ਆਪਣੇ ਸਿਸਟਮ ਤੋਂ ਬਾਹਰ ਕਿਤੇ ਰੱਖੋ, ਜੇਕਰ ਤੁਸੀਂ ਇਸ ਉੱਤੇ ਨਹੀਂ ਪਹੁੰਚ ਸਕਦੇ ਹੋ।