[FRONTCOVER]

[Start Community Language Document 1]

ਸਾਈਬਰ ਸੁਚੇਤ

ਰਾਸ਼ਟਰੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਕੇਂਦਰ (ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਿਉਰਿਟੀ ਸੇਂਟਰ) ਵਿਕਲਪਿਕ ਸਰੂਪ ਸੰਸਕਰਣ।

ਇਹ ਸਮੱਗਰੀ ਲੀਡ ਸਕੋਟਲੈਂਡ ਦੁਆਰਾ ਭਾਗੀਦਾਰਾਂ ਦੇ ਮੇਲ ਅਤੇ ਸਕੋਟਿਸ਼ ਗਵਰਨਮੈਂਟ ਸਾਈਬਰ ਰਿਜ਼ਿਲੀਏਨ੍ਸ ਯੂਨਿਟ ਵੱਲੋਂ ਫੰਡਿੰਗ ਦੇ ਨਾਲ ਉਤਪੰਨ ਕੀਤੀ ਗਈ ਹੈ।

ਇਹ ਗਾਈਡ **ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਿਉਰਿਟੀ ਵੈਬਸਾਈਟ** 'ਤੇ ਉਪਲਬਧ ਸਮਗਰੀ 'ਤੇ ਅਧਾਰਤ ਹੈ

ਜਾਣਕਾਰੀ ਨੂੰ ਕਮਿਉਨਿਟੀ ਭਾਸ਼ਾ ਦੇ 7 ਦਸਤਾਵੇਜ਼ਾਂ ਵਿੱਚ ਵੰਡਿਆ ਗਿਆ ਹੈ, ਜੋ ਹਨ:

- ਇਹ ਦਸਤਾਵੇਜ਼, ਜਿਸ ਵਿੱਚ ਇੱਕ ਪਰਿਚੈ ਅਤੇ 6 ਕਿਰਿਆਵਾਂ ਦੀ ਸੰਖੇਪ ਜਾਣਕਾਰੀ ਸ਼ਾਮਲ ਹੈ ਜੋ ਤੁਸੀਂ ਆਪਣੀ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਵਿੱਚ ਸੁਧਾਰ ਲਈ ਕਰ ਸਕਦੇ ਹੋ।
- ਫਿਰ ਤੁਸੀਂ ਉਨ੍ਹਾਂ 6 ਕਿਰਿਆਵਾਂ ਜੋ ਤੁਸੀਂ ਕਰ ਸਕਦੇ ਹੋ, ਲਈ ਵਿਅਕਤੀਗਤ ਵੇਰਵੇ ਸਹਿਤ ਦਸਤਾਵੇਜ਼।
- ਜਿਕਰ ਕੀਤੇ ਗਏ ਸਾਰੇ ਲਿੰਕਾਂ ਤੱਕ ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਿਉਰਿਟੀ ਸੇਂਟਰ ਵੈਬਸਾਈਟ https://www.ncsc.gov.uk/cyberaware/ ‘ਤੇ ਜਾ ਕੇ ਪਹੁੰਚਿਆ ਜਾ ਸਕਦਾ ਹੈ।

ਆਪਣੀ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਵਿੱਚ ਸੁਧਾਰ ਲਿਆਉਣ ਦੇ 6 ਤਰੀਕੇ

ਕੋਰੋਨਾਵਾਇਰਸ ਦੇ ਕਾਰਨ, ਇਸ ਸਾਲ ਲੋਕ ਆਨਲਾਈਨ ਉੱਤੇ ਵਾਧੂ ਸਮਾਂ ਗੁਜ਼ਾਰ ਰਹੇ ਹਨ।

ਇਸਦਾ ਅਰਥ ਹੈ ਕਿ ਹੈਕਰਾਂ ਲਈ ਸਾਈਬਰ-ਹਮਲੇ ਕਰਨ ਦੇ ਵਧੇਰੇ ਮੌਕੇ ਹਨ। ਉਹ ਅਕਸਰ ਹੇਠਾਂ ਲਿਖੇ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਲੋਕਾਂ ਅਤੇ ਕਾਰੋਬਾਰਾਂ ਨੂੰ ਨਿਸ਼ਾਨਾ ਬਣਾ ਕੇ ਅਜਿਹਾ ਕਰਦੇ ਹਨ:

- ਈਮੇਲ ਅਤੇ ਵੈਬਸਾਈਟ ਘੋਟਾਲੇ।
- ਮਾਲਵੇਅਰ – ਇਹ ਇੱਕ ਸਾੱਫਟਵੇਅਰ ਹੈ ਜੋ ਤੁਹਾਡੇ ਉਪਕਰਣ ਨੂੰ ਨੁਕਸਾਨ ਪਹੁੰਚਾ ਸਕਦਾ ਹੈ ਜਾਂ ਹੈਕਰ ਨੂੰ ਅੰਦਰ ਆਉਣ ਦੇ ਸਕਦਾ ਹੈ।

ਜੇ ਹੈਕਰ ਤੁਹਾਡੇ ਉਪਕਰਣ ਜਾਂ ਖਾਤਿਆਂ ਵਿੱਚ ਦਾਖ਼ਲ ਹੋ ਜਾਂਦੇ ਹਨ, ਉਹ ਤੁਹਾਡੇ ਪੈਸੇ, ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਜਾਂ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਬਾਰੇ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚ ਸਕਦੇ ਹਨ।

ਤੁਸੀਂ ਛੇ ਕਿਰਿਆਵਾਂ ਕਰ ਕੇ ਆਪਣੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਸੁਧਾਰ ਸਕਦੇ ਹੋ:

ਕਿਰਿਆ 1 - ਆਪਣੀ ਈਮੇਲ ਲਈ ਇੱਕ ਤਗੜਾ ਅਤੇ ਵੱਖਰਾ ਪਾਸਵਰਡ ਵਰਤੋ।

ਕਿਰਿਆ 2 - 3 ਬੇਤਰਤੀਬੇ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਤਗੜਾ ਪਾਸਵਰਡ ਬਣਾਓ।

ਕਿਰਿਆ 3 - ਆਪਣੇ ਪਾਸਵਰਡ ਆਪਣੇ ਬ੍ਰਾਉਜ਼ਰ ਵਿੱਚ ਸੇਵ ਕਰੋ।

ਕਿਰਿਆ 4 - ਦੋ-ਗੁਣਕ ਪ੍ਰਮਾਣੀਕਰਣ (2ਐਫਏ) ਚਾਲੂ ਕਰੋ।

ਕਿਰਿਆ 5 – ਆਪਣੇ ਉਪਕਰਣ ਅੱਪਡੇਟ ਕਰੋ।

ਕਿਰਿਆ 6 – ਆਪਣਾ ਡੇਟਾ ਬੈਕਅੱਪ ਕਰੋ।

[End Community Language Document 1]

[Start Community Language Document 2]

ਕਿਰਿਆ 1 - ਆਪਣੀ ਈਮੇਲ ਲਈ ਇੱਕ ਤਗੜਾ ਅਤੇ ਵੱਖਰਾ ਪਾਸਵਰਡ ਵਰਤੋ

ਜੇ ਕੋਈ ਹੈਕਰ ਤੁਹਾਡੀ ਈਮੇਲ ਵਿੱਚ ਦਾਖ਼ਲ ਹੋ ਜਾਂਦਾ ਹੈ, ਤਾਂ ਉਹ ਤੁਹਾਡੇ ਹੋਰਨਾਂ ਖਾਤਿਆਂ ਦੇ ਪਾਸਵਰਡ ਅਤੇ ਪਹੁੰਚਣ ਦੀ ਜਾਣਕਾਰੀ ਜੋ ਤੁਸੀਂ ਆਪਣੇ ਬਾਰੇ ਜਾਂ ਆਪਣੇ ਕਾਰੋਬਾਰ ਬਾਰੇ ਸੇਵ ਕੀਤੀ ਹੈ, ਰੀਸੈੱਟ ਕਰ ਸਕਦਾ ਹੈ।

ਤੁਹਾਡਾ ਈਮੇਲ ਪਾਸਵਰਡ ਤਗੜਾ ਅਤੇ ਹੋਰਨਾਂ ਪਾਸਵਰਡਾਂ ਨਾਲੋਂ ਵੱਖ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ। ਇਹ ਇਸ ਨੂੰ ਤੋੜਨ ਜਾਂ ਅਨੁਮਾਨ ਲਗਾਉਣ ਨੂੰ ਹੋਰ ਮੁਸ਼ਕਲ ਬਣਾਏਗਾ।

ਤਿੰਨ ਬੇਤਰਤੀਬੇ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਇੱਕ ਤਗੜਾ, ਵਿਲੱਖਣ ਪਾਸਵਰਡ ਬਣਾਉਣਾ ਜੋ ਤੁਹਾਨੂੰ ਯਾਦ ਰਹੇਗਾ ਇੱਕ ਵਧੀਆ ਤਰੀਕਾ ਹੈ। ਅਸੀਂ ਅਗਲੇ ਦਸਤਾਵੇਜ਼ ਵਿੱਚ ਇਸ ਨੂੰ ਵਧੇਰੇ ਵਿਸਥਾਰ ਨਾਲ ਦੇਖਾਂਗੇ।

ਤੁਹਾਨੂੰ ਆਪਣੇ ਹੋਰਨਾਂ ਮਹੱਤਵਪੂਰਣ ਖਾਤਿਆਂ, ਜਿਵੇਂ ਬੈਂਕ ਦੇ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਦੀ ਵੀ ਰੱਖਿਆ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ।

ਈਮੇਲ ਇੰਨੀ ਮਹੱਤਵਪੂਰਣ ਕਿਉਂ ਹੈ?

ਈਮੇਲ ਤੁਹਾਡੇ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਨ ਖਾਤਿਆਂ ਵਿੱਚੋਂ ਇੱਕ ਹੈ। ਪਰ ਹੈਕਰ ਤੁਹਾਡੀਆਂ ਈਮੇਲਾਂ ਦੀ ਪਰਵਾਹ ਕਿਉਂ ਕਰਦੇ ਹਨ?

ਕਲਪਨਾ ਕਰੋ ਕਿ ਜੇ ਕੋਈ ਹੈਕਰ ਤੁਹਾਡੀ ਈਮੇਲ ਵਿੱਚ ਦਾਖ਼ਲ ਹੋ ਜਾਂਦਾ ਹੈ

ਉਹ ਹੁਣ ਉਸ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚ ਸਕਦੇ ਹਨ ਜੋ ਤੁਸੀਂ ਆਪਣੇ ਬਾਰੇ ਸੇਵ ਕਰ ਕੇ ਰਖੀ ਹੋਈ ਹੈ

ਜਾਂ ਆਪਣੇ ਆਪ ਨੂੰ ਤੁਸੀਂ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰਕੇ ਲੋਕਾਂ ਨਾਲ ਸੰਪਰਕ ਕਰ ਸਕਦੇ ਹਨ।

ਪਰ ਸਭ ਤੋਂ ਮਾੜੀ ਗੱਲ, ਉਹ ਤੁਹਾਨੂੰ ਤੁਹਾਡੇ ਕਿਸੇ ਵੀ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਤੋਂ ਬਾਹਰ ਲੌਕ ਕਰ ਸਕਦੇ ਹਨ।

ਉਹ ਤੁਹਾਡੇ ਕਿਸੇ ਵੀ ਖਾਤਿਆਂ ਵਿੱਚ ਜਾ ਕੇ ਅਤੇ 'ਪਾਸਵਰਡ ਭੁੱਲ ਗਿਆ' ਵਿਸ਼ੇਸ਼ਤਾ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਅਜਿਹਾ ਕਰ ਸਕਦੇ ਹਨ।

ਇਹ ਤੁਹਾਡੇ ਪਾਸਵਰਡ ਨੂੰ ਰੀਸੈਟ ਕਰਨ ਲਈ ਲਿੰਕ ਦੇ ਨਾਲ ਇੱਕ ਈਮੇਲ ਭੇਜਦਾ ਹੈ

ਜਿਸ ਨੂੰ ਹੈਕਰ ਤੁਹਾਨੂੰ ਆਪਣੇ ਖਾਤੇ ਤੋਂ ਬਾਹਰ ਲਾਕ ਕਰਨ ਲਈ ਵਰਤ ਸਕਦੇ ਹਨ

ਇੱਕ ਵਾਰ ਜਦੋਂ ਉਹ ਇੱਕ ਪਾਸਵਰਡ ਰੀਸੈਟ ਕਰ ਲੈਂਦੇ ਹਨ, ਤਾਂ ਉਹ ਤੁਹਾਡੇ ਹੋਰਨਾਂ ਖਾਤਿਆਂ ਲਈ ਵੀ ਪਾਸਵਰਡ ਰੀਸੈਟ ਕਰਨਾ ਜਾਰੀ ਰੱਖ ਸਕਦੇ ਹਨ

ਤਾਂ ਫਿਰ, ਤੁਸੀਂ ਆਪਣੀ ਈਮੇਲ ਦੀ ਰੱਖਿਆ ਅਤੇ ਹੈਕਰਾਂ ਨੂੰ ਆਪਣੇ ਸਾਰੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਤੋਂ ਬਾਹਰ ਰੱਖਣ ਵਿੱਚ ਆਪਣੀ ਸਹਾਇਤਾ ਕਿਵੇਂ ਕਰ ਸਕਦੇ ਹੋ?

ਆਪਣੀ ਈਮੇਲ ਲਈ ਇੱਕ ਤਗੜੇ ਪਾਸਵਰਡ ਦੀ ਵਰਤੋਂ ਕਰੋ ਅਤੇ ਸੁਨਿਸ਼ਚਿਤ ਕਰੋ ਕਿ ਤੁਹਾਡੀ ਈਮੇਲ ਦਾ ਪਾਸਵਰਡ ਤੁਹਾਡੇ ਬਾਕੀ ਸਾਰੇ ਪਾਸਵਰਡ ਜੋ ਤੁਸੀਂ ਵਰਤਦੇ ਹੋ ਨਾਲੋਂ ਵੱਖਰਾ ਹੈ
ਇਸਦਾ ਮਤਲਬ ਹੈ ਕਿ ਜੇ ਕੋਈ ਕਿਸੇ ਹੋਰ ਖਾਤੇ ਲਈ ਤੁਹਾਡਾ ਪਾਸਵਰਡ ਪਤਾ ਕਰ ਲੈਂਦਾ ਹੈ, ਤਾਂ ਉਹ ਤੁਹਾਡੀ ਈਮੇਲ ਅੰਦਰ ਦਾਖ਼ਲ ਹੋਣ ਲਈ ਇਸ ਦੀ ਵਰਤੋਂ ਨਹੀਂ ਕਰ ਸਕੇਗਾ।

ਯਾਦ ਰਖੋ, ਤੁਹਾਡੀ ਈਮੇਲ ਤੁਹਾਡੇ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਣ ਖਾਤਿਆਂ ਵਿੱਚੋਂ ਇੱਕ ਹੈ। ਇਸ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਓ

ਆਪਣਾ ਈਮੇਲ ਪਾਸਵਰਡ ਕਿਵੇਂ ਬਦਲਣਾ ਹੈ

ਇਹਨਾਂ ਵਿੱਚ ਪਾਸਵਰਡ ਕਿਵੇਂ ਬਦਲਣੇ ਹਨ:

- ਜੀਮੇਲ।
- ਯਾਹੂ!
- ਆਉਟਲੁੱਕ।
- ਬੀਟੀ।
- ਏਓਐਲ ਮੇਲ।

ਜੇ ਤੁਹਾਡੀ ਈਮੇਲ ਇੱਥੇ ਸੂਚੀਬੱਧ ਨਹੀਂ ਹੈ, ਤਾਂ ਤੁਹਾਨੂੰ ਆਪਣੇ ਪ੍ਰਦਾਤਾ ਵੱਲੋਂ ਆਨਲਾਈਨ ਸਲਾਹ ਲੱਭਣੀ ਚਾਹੀਦੀ ਹੈ ਕਿ ਆਪਣਾ ਈਮੇਲ ਪਾਸਵਰਡ ਕਿਵੇਂ ਬਦਲਣਾ ਹੈ।

ਇਕੱਲੇ ਵਪਾਰੀਆਂ ਅਤੇ ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਲਈ ਪਾਸਵਰਡਾਂ ਬਾਰੇ ਸਲਾਹ

ਜੇ ਤੁਸੀਂ ਇੱਕ ਕਾਰੋਬਾਰ ਦੇ ਮਾਲਿਕ ਹੋ, ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਵਿੱਚ ਤੁਹਾਡੇ ਗਾਹਕਾਂ, ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ, ਜਾਂ ਤੁਹਾਡੇ ਵਿੱਤੀ ਮਾਮਲਿਆਂ ਬਾਰੇ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਸ਼ਾਮਿਲ ਹੋ ਸਕਦੀ ਹੈ।

ਜੇ ਤੁਹਾਡੇ ਖਾਤੇ ਸੁਰੱਖਿਅਤ ਨਹੀਂ ਹਨ, ਤਾਂ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਨੂੰ ਕਿਸੇ ਸਾਈਬਰ ਘਟਨਾ ਦਾ ਵਾਧੂ ਖਤਰਾ ਹੋ ਸਕਦਾ ਹੈ। ਇਹ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਨੂੰ ਕਨੂੰਨੀ ਜਾਂ ਵਿੱਤੀ ਜੋਖ਼ਮ, ਅਤੇ ਜਨਰਲ ਡੇਟਾ ਪ੍ਰੋਟੈਕਸ਼ਨ ਰੈਗੂਲੇਸ਼ਨ (GDPR) ਨੂੰ ਤੋੜਨ ਦੇ ਖਤਰੇ ਵਿੱਚ ਪਾ ਸਕਦਾ ਹੈ।

ਜੇ ਤੁਹਾਡੇ ਕਾਰੋਬਾਰ ਵਿੱਚ ਸਟਾਫ਼ ਹੈ, ਤਾਂ ਤੁਹਾਨੂੰ ਇਹ ਨਿਸ਼ਚਿਤ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਉਹ ਆਪਣੇ ਪਾਸਵਰਡ ਆਪਣੇ ਉਪਕਰਣਾਂ ਦੇ ਕੋਲ ਨਾ ਰੱਖਣ, ਅਤੇ ਇਹ ਕਿ ਉਪਕਰਣ ਲਾਕ ਕੀਤੇ ਜਾਂ ਬੰਦ ਕੀਤੇ ਗਏ ਹਨ ਜਦੋਂ ਵਰਤੋਂ ਵਿੱਚ ਨਹੀਂ ਹਨ।

ਵਾਧੂ ਜਾਣਕਾਰੀ ਲਈ, ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਯੋਰਿਟੀ ਸੈਂਟਰ ਦੀ ਸਮਾਲ ਬਿਜ਼ਨਸ ਗਾਈਡ ਦੇਖੋ।

ਦੱਸੇ ਗਏ ਸਾਰੇ ਲਿੰਕਾਂ ਤੱਕ ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਯੋਰਿਟੀ ਸੈਂਟਰ ਦੀ ਵੈਬਸਾਈਟ https://www.ncsc.gov.uk/cyberaware/ 'ਤੇ ਜਾ ਕੇ ਪਹੁੰਚਿਆ ਜਾ ਸਕਦਾ ਹੈ।

[End Community Language Document 2]

[Start Community Language Document 3]

ਕਿਰਿਆ 2 - ਤਿੰਨ ਬੇਤਰਤੀਬੇ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਸਖ਼ਤ ਪਾਸਵਰਡ ਬਣਾਓ।

ਜਦੋਂ ਤੁਸੀਂ ਆਪਣੇ ਮਹੱਤਵਪੂਰਣ ਖਾਤਿਆਂ ਲਈ ਵੱਖਰੇ ਪਾਸਵਰਡ ਵਰਤਦੇ ਹੋ, ਤਾਂ ਉਨ੍ਹਾਂ ਸਾਰਿਆਂ ਨੂੰ ਯਾਦ ਰੱਖਣਾ ਮੁਸ਼ਕਲ ਹੋ ਸਕਦਾ ਹੈ।

ਤਗੜੇ, ਯਾਦਗਾਰ ਪਾਸਵਰਡ ਬਣਾਉਣ ਦਾ ਇੱਕ ਵਧੀਆ ਤਰੀਕਾ ਤਿੰਨ ਬੇਤਰਤੀਬ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨਾ ਹੈ।

ਉਹਨਾਂ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਨਾ ਕਰੋ ਜਿਨ੍ਹਾਂ ਦਾ ਅਨੁਮਾਨ ਲਗਾਇਆ ਜਾ ਸਕਦਾ ਹੈ (ਜਿਵੇਂ ਤੁਹਾਡੇ ਪਾਲਤੂ ਜਾਨਵਰ ਦਾ ਨਾਂ)।

ਜੇ ਲੋੜ ਹੈ ਤਾਂ ਤੁਸੀਂ ਨੰਬਰ ਅਤੇ ਚਿੰਨ੍ਹ ਸ਼ਾਮਲ ਕਰ ਸਕਦੇ ਹੋ। ਉਦਾਹਰਣ ਲਈ: ਲਾਲਪਤਲੂਨਦਰਖ਼ਤ4!

ਆਪਣੇ ਬ੍ਰਾਉਜ਼ਰ ਵਿੱਚ ਆਪਣੇ ਪਾਸਵਰਡ ਸੁਰੱਖਿਅਤ ਕਰਨ ਨਾਲ ਤੁਹਾਨੂੰ ਉਹਨਾਂ ਦੇ ਪ੍ਰਬੰਧਨ ਵਿੱਚ ਸਹਾਇਤਾ ਮਿਲੇਗੀ, ਅਸੀਂ ਅਗਲੇ ਦਸਤਾਵੇਜ਼ ਵਿੱਚ ਇਸ ਨੂੰ ਵਧੇਰੇ ਵਿਸਥਾਰ ਨਾਲ ਦੇਖਾਂਗੇ।

ਇੱਕ ਤਗੜਾ ਪਾਸਵਰਡ ਬਣਾਉਣ ਲਈ ਆਪਣੀ ਜਾਣਕਾਰੀ ਦੀ ਪਰੀਖਿਆ ਲਓ

ਕੀ ਤੁਸੀਂ ਅੰਦਾਜ਼ਾ ਲਗਾ ਸਕਦੇ ਹੋ ਕਿ ਇਹਨਾਂ ਵਿੱਚੋਂ ਕਿਹੜਾ ਪਾਸਵਰਡ ਚੋਟੀ ਦੇ 100,000 ਵਿੱਚੋਂ ਸਭ ਤੋਂ ਵੱਧ ਪਤਾ ਕੀਤੇ ਪਾਸਵਰਡਾਂ ਵਿੱਚ ਨਹੀਂ ਆਉਂਦਾ?

- ਆਰਸਨਲ22 (arsenal22)
- 1ਵੀ&ਯੂਪੀਜੇਡਬਲਯੂ3ਐਨਟੀ (1v&upjw3nt)
- ਪੀ@55ਡਬਲਯੂ0ਆਰਡੀ (p@55w0rd)
- ਰੈਡਪੈਂਟਸਟ੍ਰੀ (RedPantsTree)
- ਵਿਕਟੋਰੀਯਾ! (Victoria!)
- 2011977

ਉੱਤਰ ਰੈਡਪੈਂਟਸਟ੍ਰੀ (RedPantsTree) ਹੈ।

ਹੈਕਰ ਲੱਖਾਂ ਪਤਾ ਕੀਤੇ ਪਾਸਵਰਡਾਂ ਵਾਲੀਆਂ ਆਨਲਾਈਨ ਸੂਚੀਆਂ ਸਾਂਝਾ ਕਰਦੇ ਹਨ।

3 ਬੇਤਰਤੀਬ ਸ਼ਬਦ ਨਵੇਂ ਪਾਸਵਰਡ ਬਣਾਉਣ ਦਾ ਇੱਕ ਅਸਾਨ ਤਰੀਕਾ ਹਨ ਜਿਸਦੇ ਤੁਹਾਡੇ ਲਈ ਵਿਲੱਖਣ ਹੋਣ ਦੀ ਵਾਧੂ ਸੰਭਾਵਨਾ ਹੈ ਅਤੇ ਇਸਦਾ ਅਨੁਮਾਨ ਲਗਾਏ ਜਾਣ ਦੀ ਘੱਟ ਸੰਭਾਵਨਾ ਹੈ।
ਦੱਸੇ ਗਏ ਸਾਰੇ ਲਿੰਕਾਂ ਤੱਕ ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਯੋਰਿਟੀ ਸੈਂਟਰ ਦੀ ਵੈਬਸਾਈਟ

https://www.ncsc.gov.uk/cyberaware/ 'ਤੇ ਜਾ ਕੇ ਪਹੁੰਚਿਆ ਜਾ ਸਕਦਾ ਹੈ।

[End Community Language Document 3]

[Start Community Language Document 4]

ਕਿਰਿਆ 3 - ਆਪਣੇ ਪਾਸਵਰਡ ਆਪਣੇ ਬ੍ਰਾਉਜ਼ਰ ਵਿੱਚ ਸੇਵ ਕਰੋ

ਤੁਹਾਡੇ ਪਾਸਵਰਡ ਤੁਹਾਡੇ ਆਪਣੇ ਬ੍ਰਾਉਜ਼ਰ ਵਿੱਚ ਸੇਵ ਕਰਨ ਦਾ ਅਰਥ ਹੈ ਤੁਹਾਡੇ ਵੈਬ ਬ੍ਰਾਉਜ਼ਰ (ਜਿਵੇਂ ਕ੍ਰੋਮ, ਸਫਾਰੀ ਜਾਂ ਐੱਜ) ਨੂੰ ਤੁਹਾਡੇ ਲਈ ਤੁਹਾਡੇ ਪਾਸਵਰਡ ਯਾਦ ਰਖਣ ਦੇਣਾ।

ਇਹ ਸਹਾਇਤਾ ਕਰ ਸਕਦਾ ਹੈ:

- ਇਹ ਸੁਨਿਸ਼ਚਿਤ ਕਰਨ ਵਿੱਚ ਕਿ ਤੁਸੀਂ ਆਪਣੇ ਪਾਸਵਰਡ ਗੁਆਉਂਦੇ ਜਾਂ ਭੁੱਲਦੇ ਨਹੀਂ ਹੋ।
- ਤੁਹਾਨੂੰ ਕੁਝ ਸਾਈਬਰ-ਅਪਰਾਧ, ਜਿਵੇਂ ਕਿ ਨਕਲੀ ਵੈਬਸਾਈਟਾਂ ਤੋਂ ਬਚਾਓਣ ਵਿੱਚ।

ਇਹ ਕਮਜ਼ੋਰ ਪਾਸਵਰਡਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਜਾਂ ਇੱਕੋ ਪਾਸਵਰਡ ਨੂੰ ਇਕ ਤੋਂ ਵੱਧ ਜਗ੍ਹਾ 'ਤੇ ਵਰਤਣ ਨਾਲੋਂ ਜਿਆਦਾ ਸੁਰੱਖਿਅਤ ਹੈ।

ਸੁਨਿਸ਼ਚਿਤ ਕਰੋ ਕਿ ਤੁਸੀਂ ਆਪਣੇ ਸੇਵ ਕੀਤੇ ਪਾਸਵਰਡਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਦੇ ਹੋ ਜੇ ਤੁਹਾਡਾ ਉਪਕਰਣ ਗੁੰਮ ਜਾਂ ਚੋਰੀ ਹੋ ਜਾਂਦਾ ਹੈ।

ਤੁਹਾਡੇ ਸੇਵ ਕੀਤੇ ਪਾਸਵਰਡਾਂ ਨੂੰ ਕਿਵੇਂ ਸੁਰੱਖਿਅਤ ਕਰਨਾ ਹੈ

ਕੋਈ ਵਿਅਕਤੀ ਜੋ ਤੁਹਾਡੇ ਉਪਕਰਣ ਤੱਕ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰਦਾ ਹੈ ਉਹ ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਤੱਕ ਪਹੁੰਚਣ ਲਈ ਤੁਹਾਡੇ ਸੇਵ ਕੀਤੇ ਪਾਸਵਰਡਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਦੇ ਯੋਗ ਹੋ ਸਕਦਾ ਹੈ।
ਇਸ ਕਿਸਮ ਦਾ ਸਾਈਬਰ-ਅਪਰਾਧ ਇੰਟਰਨੈਟ ਉੱਤੇ ਕਿਸੇ ਹੋਰ ਥਾਂ ਤੋਂ ਕੀਤੇ ਹਮਲਿਆਂ ਨਾਲੋਂ ਬਹੁਤ ਘੱਟ ਆਮ ਹੈ, ਜਿੱਥੇ ਵਿਸ਼ੇਸ਼ ਸਾੱਫਟਵੇਅਰ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਪਾਸਵਰਡ ਪਤਾ ਕੀਤੇ ਜਾਂਦੇ ਹਨ।

ਇਹ ਸੁਨਿਸ਼ਚਿਤ ਬਣਾਉਣ ਲਈ ਕਿ ਤੁਸੀਂ ਸੁਰੱਖਿਅਤ ਹੋ, ਤੁਹਾਨੂੰ ਚਾਹੀਦਾ ਹੈ:

- ਕਿ ਤੁਸੀਂ ਆਪਣਾ ਉਪਕਰਣ ਬੰਦ ਜਾਂ ਲਾਕ ਕਰੋ ਜਦੋਂ ਤੁਸੀਂ ਇਸਦੀ ਵਰਤੋਂ ਨਹੀਂ ਕਰ ਰਹੇ।
- ਆਪਣੇ ਉਪਕਰਣ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਇੱਕ ਤਗੜੇ ਪਾਸਵਰਡ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- ਕਿ ਆਪਣੇ ਸਾਰੇ ਉਪਕਰਣਾਂ ਅਤੇ ਖਾਤਿਆਂ ਲਈ ਦੋ-ਗੁਣਕ ਪ੍ਰਮਾਣੀਕਰਣ (2ਐਫਏ) ਚਾਲੂ ਕਰੋ।
- ਬਾਇਓਮੈਟ੍ਰਿਕਸ (ਚਿਹਰੇ ਦੀ ਪਛਾਣ ਜਾਂ ਫਿੰਗਰਪ੍ਰਿੰਟ ਮਾਨਤਾ) ਚਾਲੂ ਕਰੋ ਜੇ ਤੁਹਾਡੇ ਉਪਕਰਣ ਵਿੱਚ ਇਹ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ।

ਤੁਹਾਨੂੰ ਆਪਣਾ ਡੇਟਾ ਨਿਯਮਿਤ ਤੌਰ ਤੇ ਬੈਕ-ਅੱਪ ਵੀ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ। ਇਹ ਤੁਹਾਡੀ ਮਹੱਤਵਪੂਰਣ ਜਾਣਕਾਰੀ ਨੂੰ ਮੁੜ ਪ੍ਰਾਪਤ ਕਰਨ ਵਿੱਚ ਤੁਹਾਡੀ ਮਦਦ ਕਰੇਗਾ ਜੇ ਤੁਹਾਡਾ ਉਪਕਰਣ ਗੁੰਮ ਜਾਂਦਾ ਹੈ ਜਾਂ ਚੋਰੀ ਹੋ ਜਾਂਦਾ ਹੈ।

ਆਪਣੇ ਪਾਸਵਰਡ ਨੂੰ ਆਪਣੇ ਬ੍ਰਾਉਜ਼ਰ ਵਿੱਚ ਕਿਵੇਂ ਸੇਵ ਕਰੀਏ

ਪਤਾ ਕਰੋ ਆਪਣੇ ਪਾਸਵਰਡ ਹੇਠਲਿਆਂ ਵਿੱਚ ਕਿਵੇਂ ਸੇਵ ਕਰਨੇ ਹਨ:

- ਗੂਗਲ ਕ੍ਰੋਮ।
- ਮਾਈਕ੍ਰੋਸਾਫਟ ਐੱਜ।
- ਫਾਇਰਫਾਕਸ।
- ਸਫਾਰੀ।

ਕੀ ਤੁਹਾਨੂੰ ਪਤਾ ਸੀ?

ਤੁਸੀਂ ਆਪਣੇ ਸੇਵ ਕੀਤੇ ਹੋਏ ਪਾਸਵਰਡਾਂ ਤੱਕ ਕਿਸੇ ਵੀ ਐਸੇ ਉਪਕਰਣ ਤੋਂ ਪਹੁੰਚ ਸਕਦੇ ਹੋ ਜਿੱਥੇ ਤੁਸੀਂ ਉਸੇ ਬ੍ਰਾਉਜ਼ਰ ਵਿੱਚ ਸਾਈਨ-ਇਨ ਕੀਤਾ ਹੈ।

ਵਾਧੂ ਸੁਰੱਖਿਆ ਸ਼ਾਮਲ ਕਰੋ

ਇੱਕ ਵਾਰ ਜਦੋਂ ਤੁਸੀਂ ਆਪਣੇ ਸਾਰੇ ਉਪਕਰਣਾਂ ਅਤੇ ਸੇਵਾਵਾਂ ਲਈ ਤਗੜੇ, ਵੱਖਰੇ ਪਾਸਵਰਡ (ਕਿਰਿਆ 1 ਤੋਂ 3) ਸੈਟ ਕਰ ਲੈਂਦੇ ਹੋ, ਹੋਰ ਚੀਜ਼ਾਂ ਹਨ ਜੋ ਤੁਸੀਂ ਆਪਣੇ ਹੈਕ ਹੋਣ ਦੇ ਜੋਖ਼ਮ ਨੂੰ ਘਟਾਉਣ ਲਈ ਕਰ ਸਕਦੇ ਹੋ (ਕਿਰਿਆ 4 ਤੋਂ 6)।

ਦੱਸੇ ਗਏ ਸਾਰੇ ਲਿੰਕਾਂ ਤੱਕ ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਯੋਰਿਟੀ ਸੈਂਟਰ ਦੀ ਵੈਬਸਾਈਟ

https://www.ncsc.gov.uk/cyberaware/ 'ਤੇ ਜਾ ਕੇ ਪਹੁੰਚਿਆ ਜਾ ਸਕਦਾ ਹੈ।

[End Community Language Document 4]

[Start Community Language Document 5]

ਕਿਰਿਆ 4 - ਦੋ-ਗੁਣਕ ਪ੍ਰਮਾਣੀਕਰਣ (2FA) ਚਾਲੂ ਕਰਨਾ

ਦੋ-ਗੁਣਕ ਪ੍ਰਮਾਣੀਕਰਣ (2FA) ਹੈਕਰਾਂ ਨੂੰ ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਅੰਦਰ ਆਉਣ ਤੋਂ ਰੋਕਣ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰਦਾ ਹੈ, ਭਾਵੇਂ ਉਹਨਾਂ ਕੋਲ ਤੁਹਾਡਾ ਪਾਸਵਰਡ ਹੈ।

ਕੁਝ ਆਨਲਾਈਨ ਬੈਂਕਿੰਗ ਆਪ ਹੀ 2FA ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਨ। ਇਹ ਅਜਿਹਾ ਤੁਹਾਡੀ ਪਛਾਣ ਨੂੰ ਸਾਬਤ ਕਰਣ ਲਈ ਵਧੇਰੇ ਜਾਣਕਾਰੀ ਮੰਗ ਕੇ ਕਰਦਾ ਹੈ, ਜਿਵੇਂ ਕਿ ਇੱਕ ਕੋਡ ਜੋ ਤੁਹਾਡੇ ਫੋਨ 'ਤੇ ਭੇਜਿਆ ਜਾਂਦਾ ਹੈ।

ਦੋ-ਗੁਣਕ ਪ੍ਰਮਾਣੀਕਰਣ (2FA) ਕਿਵੇਂ ਚਾਲੂ ਕਰੀਏ

ਤੁਹਾਨੂੰ ਆਪਣੇ ਜ਼ਿਆਦਾਤਰ ਖਾਤਿਆਂ ਲਈ 2FA ਨੂੰ ਹੱਥੀਂ ਚਾਲੂ ਕਰਨ ਦੀ ਜ਼ਰੂਰਤ ਹੋਏਗੀ। ਸਾਰੇ ਖਾਤੇ 2FA ਦੀ ਪੇਸ਼ਕਸ਼ ਨਹੀਂ ਕਰਣਗੇ। ਆਨਲਾਈਨ ਬੈਂਕਿੰਗ ਆਟੋਮੈਟਿਕ ਤੌਰ ਤੇ 2FA ਦੀ ਵਰਤੋਂ ਕਰਦੀ ਹੈ।
2FA ਨੂੰ ਦੋ-ਕਦਮ ਦੀ ਤਸਦੀਕ ਜਾਂ ਮਲਟੀ-ਫੈਕਟਰ ਪ੍ਰਮਾਣੀਕਰਣ ਵੀ ਕਿਹਾ ਜਾਂਦਾ ਹੈ।

ਵੀਡੀਓ: 2FA ਕਿਵੇਂ ਕੰਮ ਕਰਦਾ ਹੈ

2FA ਕਿਵੇਂ ਕੰਮ ਕਰਦਾ ਹੈ 'ਤੇ ਵਿਡੀਓ ਤੱਕ ਪਹੁੰਚ ਯੂਟਿਊਬ ਉੱਤੇ ਉਪਲਬਧ ਹੈ।

ਈਮੇਲ ਲਈ 2FA ਚਾਲੂ ਕਰਨਾ

- ਜੀਮੇਲ।
- ਯਾਹੂ।
- ਆਉਟਲੁੱਕ।
- ਏਓਐਲ।

ਸੋਸ਼ਲ ਮੀਡੀਆ ਲਈ 2FA ਚਾਲੂ ਕਰਨਾ

- ਇੰਸਟਾਗ੍ਰਾਮ।
- ਫੇਸਬੁੱਕ।
- ਟਵਿੱਟਰ।
- ਲਿੰਕਡਿਨ।

ਦੱਸੇ ਗਏ ਸਾਰੇ ਲਿੰਕਾਂ ਤੱਕ ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਯੋਰਿਟੀ ਸੈਂਟਰ ਦੀ ਵੈਬਸਾਈਟ

https://www.ncsc.gov.uk/cyberaware/ 'ਤੇ ਜਾ ਕੇ ਪਹੁੰਚਿਆ ਜਾ ਸਕਦਾ ਹੈ।

[End Community Language Document 5]

[Start Community Language Document 6]

ਕਿਰਿਆ 5 – ਆਪਣੇ ਉਪਕਰਣ ਅੱਪਡੇਟ ਕਰੋ

ਪੁਰਾਣੇ ਸਾੱਫਟਵੇਅਰ, ਐਪਾਂ ਅਤੇ ਓਪਰੇਟਿੰਗ ਸਿਸਟਮਾਂ ਵਿੱਚ ਕਮਜ਼ੋਰੀਆਂ ਹੁੰਦੀਆਂ ਹਨ। ਇਹ ਉਨ੍ਹਾਂ ਨੂੰ ਹੈਕ ਕਰਨਾ ਸੌਖਾ ਬਣਾਉਂਦਾ ਹੈ।

ਕੰਪਨੀਆਂ ਅੱਪਡੇਟਾਂ ਜਾਰੀ ਕਰਕੇ ਕਮਜ਼ੋਰੀਆਂ ਦੀ ਮੁਰੰਮਤ ਕਰਦੀਆਂ ਹਨ। ਜਦੋਂ ਤੁਸੀਂ ਆਪਣੇ ਉਪਕਰਣ ਅਤੇ ਸਾੱਫਟਵੇਅਰ ਅੱਪਡੇਟ ਕਰਦੇ ਹੋ, ਤਾਂ ਇਹ ਹੈਕਰਾਂ ਨੂੰ ਬਾਹਰ ਰੱਖਣ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰਦਾ ਹੈ।

ਆਪਣੇ ਉਹਨਾਂ ਉਪਕਰਣਾਂ ਲਈ ਅਤੇ ਸਾੱਫਟਵੇਅਰ ਲਈ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਾਂ ਚਾਲੂ ਕਰੋ ਜੋ ਇਹ ਪੇਸ਼ ਕਰਦੇ ਹਨ। ਇਸਦਾ ਅਰਥ ਇਹ ਹੋਵੇਗਾ ਕਿ ਤੁਹਾਨੂੰ ਆਪਣੇ ਆਪ ਇਹ ਕਰਨਾ ਯਾਦ ਨਹੀਂ ਰੱਖਣਾ ਪਏਗਾ।
ਕੁਝ ਉਪਕਰਣਾਂ ਅਤੇ ਸਾੱਫਟਵੇਅਰ ਨੂੰ ਹੱਥੀਂ ਅਪਡੇਟ ਕਰਨ ਦੀ ਜ਼ਰੂਰਤ ਹੁੰਦੀ ਹੈ। ਤੁਹਾਨੂੰ ਤੁਹਾਡੇ ਫੋਨ ਜਾਂ ਕੰਪਿਉਟਰ 'ਤੇ ਰਿਮਾਈਂਡਰ ਮਿਲ ਸਕਦੇ ਹਨ। ਅੱਪਡੇਟ ਕਰਨਾ ਤੁਹਾਨੂੰ ਆਨਲਾਈਨ ਉੱਤੇ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰੇਗਾ।

ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਾਂ ਕਿਵੇਂ ਚਾਲੂ ਕਰੀਏ

ਪਤਾ ਕਰੋ ਹੇਠਲਿਆਂ ਲਈ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਾਂ ਕਿਵੇਂ ਚਾਲੂ ਕਰਨੀਆਂ ਹਨ:

- ਐੱਪਲ - ਮੈੱਕ
- ਐੱਪਲ – ਆਈਫੋਨ ਅਤੇ ਆਈਪੈਡ
- ਮਾਈਕ੍ਰੋਸਾੱਫਟ ਵਿਨਡੋਜ਼ 10 – ਅੱਪਡੇਟ ਲਈ ਵਿਨਡੋਜ਼ 10 ਲੱਭੋ
- ਵਿਨਡੋਜ਼ 7 ਹੁਣ ਸਮਰਥਿਤ ਨਹੀਂ ਹੈ। ਤੁਹਾਨੂੰ ਵਿਨਡੋਜ਼ 10 'ਤੇ ਅਪਗ੍ਰੇਡ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ
- ਐਂਡਰਾਇਡ ਸਮਾਰਟਫੋਨ ਅਤੇ ਟੈਬਲਟਾਂ
- ਐਂਡਰਾਇਡ ਐੱਪਸ

ਪ੍ਰਸ਼ਨ: ਕੰਪਨੀਆਂ ਆਪਣੇ ਸਾੱਫਟਵੇਅਰ ਵਿੱਚ ਕਮਜ਼ੋਰੀਆਂ ਨੂੰ ਕਿਵੇਂ ਠੀਕ ਕਰਦੀਆਂ ਹਨ?

- ਪੱਟੀ
- ਟਾਕੀ (ਪੈਚ)
- ਮੁਰੰਮਤ

ਉੱਤਰ: ਜਦੋਂ ਇੱਕ ਕੰਪਨੀ ਨੂੰ ਆਪਣੇ ਸਾੱਫਟਵੇਅਰ ਵਿੱਚ ਕਮਜ਼ੋਰੀਆਂ ਲੱਭਦੀਆਂ ਹਨ, ਉਹ ਇਸਨੂੰ ਠੀਕ ਕਰਨ ਲਈ ਇੱਕ 'ਟਾਕੀ' (ਪੈਚ) ਜਾਰੀ ਕਰਦੀ ਹੈ। ਇਹ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਣ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰਦਾ ਹੈ।

ਦੱਸੇ ਗਏ ਸਾਰੇ ਲਿੰਕਾਂ ਤੱਕ ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਯੋਰਿਟੀ ਸੈਂਟਰ ਦੀ ਵੈਬਸਾਈਟ https://www.ncsc.gov.uk/cyberaware/ 'ਤੇ ਜਾ ਕੇ ਪਹੁੰਚਿਆ ਜਾ ਸਕਦਾ ਹੈ।

[End Community Language Document 6]

[Start Community Language Document 7]

ਕਿਰਿਆ 6 – ਆਪਣਾ ਡੇਟਾ ਬੈਕਅੱਪ ਕਰੋ

ਬੈਕਅੱਪ ਕਰਨ ਦਾ ਅਰਥ ਹੈ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਦੀ ਇੱਕ ਕਾਪੀ ਬਣਾਉਣਾ ਅਤੇ ਕਿਸੇ ਹੋਰ ਉਪਕਰਣ ਜਾਂ ਆਨਲਾਈਨ ਕਲਾਉਡ ਸਟੋਰੇਜ 'ਤੇ ਇਸਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨਾ।

ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਬੈਕਅੱਪ ਕਰਣ ਦਾ ਅਰਥ ਹੈ ਕਿ ਤੁਹਾਡੇ ਕੋਲ ਹਮੇਸ਼ਾ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਦਾ ਨਵਾਂ ਸੰਸਕਰਣ ਸੰਭਾਲਿਆ ਰਹੇਗਾ। ਜੇ ਤੁਹਾਡਾ ਡੇਟਾ ਗੁੰਮ ਜਾਂਦਾ ਹੈ ਜਾਂ ਚੋਰੀ ਹੋ ਜਾਂਦਾ ਹੈ ਤਾਂ ਇਹ ਤੁਹਾਨੂੰ ਜਲਦੀ ਮੁੜ ਪ੍ਰਾਪਤ ਕਰਨ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰੇਗਾ।

ਤੁਸੀਂ ਆਟੋਮੈਟਿਕ ਬੈਕਅੱਪ ਵੀ ਚਾਲੂ ਕਰ ਸਕਦੇ ਹੋ। ਇਹ ਤੁਹਾਡੇ ਵੱਲੋਂ ਯਾਦ ਕਰਨ ਦੀ ਲੋੜ ਦੇ ਬਗੈਰ ਨਿਯਮਿਤ ਤੌਰ ਤੇ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਨੂੰ ਕਲਾਉਡ ਸਟੋਰੇਜ ਵਿੱਚ ਸੇਵ ਕਰੇਗਾ।

ਜੇ ਤੁਸੀਂ ਆਪਣੀ ਜਾਣਕਾਰੀ ਨੂੰ ਇੱਕ USB ਸਟਿੱਕ ਜਾਂ ਬਾਹਰੀ ਹਾਰਡ ਡਰਾਈਵ 'ਤੇ ਬੈਕਅੱਪ ਕਰਦੇ ਹੋ, ਤਾਂ ਇਸਨੂੰ ਆਪਣੇ ਕੰਪਿਉਟਰ ਤੋਂ ਡਿਸਕਨੈਕਟ ਕਰੋ ਜਦੋਂ ਬੈਕਅੱਪ ਨਹੀਂ ਕੀਤਾ ਜਾ ਰਿਹਾ।

ਕੀ ਤੁਹਾਨੂੰ ਪਤਾ ਸੀ?

ਤੁਹਾਨੂੰ ਆਪਣੇ ਉਪਕਰਣ ਨੂੰ ਅੱਪਡੇਟ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਹਮੇਸ਼ਾਂ ਆਪਣੇ ਡੇਟਾ ਦਾ ਬੈਕਅੱਪ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ। ਇਹ ਇਸ ਲਈ ਹੈ ਕਿਉਂਕਿ ਅੱਪਡੇਟਾਂ ਕਈ ਵਾਰ ਫਾਈਲਾਂ ਨੂੰ ਹਟਾ ਜਾਂ ਬਦਲ ਸਕਦੀਆਂ ਹਨ।

ਆਟੋਮੈਟਿਕ ਬੈਕਅੱਪ ਕਿਵੇਂ ਚਾਲੂ ਕਰੀਏ

ਹੇਠਲਿਆਂ ਲਈ ਆਟੋਮੈਟਿਕ ਬੈਕਅੱਪ ਕਿਵੇਂ ਚਾਲੂ ਕਰੀਏ:

- ਐੱਪਲ – ਮੈੱਕ।
- ਐੱਪਲ – ਆਈਫੋਨ ਅਤੇ ਆਈਪੈਡ।
- ਐਂਡਰਾਇਡ।
- ਮਾਈਕ੍ਰੋਸਾੱਫਟ ਵਿਨਡੋਜ਼ 10 ਅਤੇ ਵਿਨਡੋਜ਼ 8 ਵਨ ਡ੍ਰਾਇਵ।

ਇਕੱਲੇ ਵਪਾਰੀਆਂ ਅਤੇ ਛੋਟੇ ਕਾਰੋਬਾਰਾਂ ਲਈ ਬੈਕਅੱਪ ਬਾਰੇ ਸਲਾਹ

ਤੁਹਾਡੇ ਡੇਟਾ ਨੂੰ ਬੈਕਅੱਪ ਕਰਨ ਦਾ ਅਰਥ ਇਹ ਹੋਵੇਗਾ ਕਿ ਜੇ ਕੋਈ ਸਾਈਬਰ ਘਟਨਾ ਵਾਪਰਦੀ ਹੈ ਤਾਂ ਤੁਹਾਡਾ ਕਾਰੋਬਾਰ ਚਲਣਾ ਜਾਰੀ ਰਹਿ ਸਕਦਾ ਹੈ।

ਆਪਣੇ ਕਾਰੋਬਾਰ ਲਈ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਣ ਡੇਟਾ ਦੀ ਪਛਾਣ ਕਰਕੇ ਸ਼ੁਰੂਆਤ ਕਰੋ। ਇਹ ਵਿੱਤੀ, ਇਕਰਾਰਨਾਮਾ, ਗਾਹਕ, ਜਾਂ ਸਪਲਾਇਰ ਦੀ ਜਾਣਕਾਰੀ ਹੋ ਸਕਦੀ ਹੈ। ਇਹ ਸੁਨਿਸ਼ਚਿਤ ਕਰੋ ਕਿ ਇਸਦਾ ਨਿਯਮਿਤ ਰੂਪ ਵਿੱਚ ਬੈਕਅੱਪ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।

ਤੁਹਾਨੂੰ ਇਹ ਵੀ ਪਤਾ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਡੇਟਾ ਗੁੰਮਣ ਦੀ ਸਥਿਤੀ ਵਿੱਚ ਬੈਕਅਪ ਨੂੰ ਕਿਵੇਂ ਬਹਾਲ ਕਰਨਾ ਹੈ।

ਵਾਧੂ ਜਾਣਕਾਰੀ ਲਈ, ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਯੋਰਿਟੀ ਸੈਂਟਰ ਦੀ ਸਮਾਲ ਬਿਜ਼ਨਸ ਗਾਈਡ ਦੇਖੋ।

ਦੱਸੇ ਗਏ ਸਾਰੇ ਲਿੰਕਾਂ ਤੱਕ ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਸਿਕਯੋਰਿਟੀ ਸੈਂਟਰ ਦੀ ਵੈਬਸਾਈਟ

https://www.ncsc.gov.uk/cyberaware/ 'ਤੇ ਜਾ ਕੇ ਪਹੁੰਚਿਆ ਜਾ ਸਕਦਾ ਹੈ।

[End Community Language Document7]

[END OF DOCUMENT]