ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਦੀ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਵਰਤੋਂ ਕਰਨ ਦੇ ਸੁਝਾਅ

ਬੁਰੇ ਅਦਾਕਾਰ ਤੁਹਾਡਾ ਔਨਲਾਈਨ ਫਾਇਦਾ ਉਠਾ ਸਕਦੇ ਹਨ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਦੀ ਵਰਤੋਂ ਕਰਨ ਦੀ ਲੋੜ ਪੈਂਦੀ ਹੈ ਤਾਂ ਨੀਚੇ ਕੁਝ ਵਿਚਾਰ ਕਰਨ ਯੋਗ ਸੁਝਾਅ ਪੜ੍ਹੋ।

ਕੋਰੋਨਾਵਾਇਰਸ ਪ੍ਰਕੋਪ ਫੈਲਣ ਅਤੇ ਵਪਾਰਾਂ ਅਤੇ ਲਾਈਬ੍ਰੇਰੀਆਂ ਦੇ ਬੰਦ ਹੋਣ ਦੀ ਪ੍ਰਤੀਕਿਰਿਆ ਵਜੋਂ, ਸਾਡੇ ਵਿੱਚੋਂ ਕਈ ਲੋਗ ਔਨਲਾਈਨ ਵੱਧ ਸਮਾਂ ਬਿਤਾ ਰਹੇ ਹਨ। ਨਤੀਜੇ ਵਜੋਂ, ਸਾਨੂੰ ਇੰਟਰਨੈੱਟ ਨਾਲ ਕਨੈਕਟ ਹੋਣ ਲਈ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਦੀ ਵਰਤੋਂ ਕਰਨ ਦੀ ਲੋੜ ਪੈ ਸਕਦੀ ਹੈ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਦੀ ਵਰਤੋਂ ਕਰਨ ਦੀ ਲੋੜ ਪੈਂਦੀ ਹੈ ਤਾਂ ਕਿਰਪਾ ਕਰਕੇ ਆਪਣੇ ਡੇਟਾ ਦੀ ਸੁਰੱਖਿਆ ਕਰਨ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰਨ ਲਈ ਸਟੇਟ ਪ੍ਰਮੁੱਖ ਪਰਦੇਦਾਰੀ ਅਫਸਰ (Chief Privacy Officer) ਦੇ ਹੇਠਲੇ ਸੁਝਾਵਾਂ 'ਤੇ ਵਿਚਾਰ ਕਰੋ:

1. ਪੁਸ਼ਟੀ ਕਰੋ ਕਿ ਤੁਹਾਡੇ ਕੋਲ ਸਹੀ ਨੈੱਟਵਰਕ ਹੈ।

ਯਕੀਨੀ ਕਰੋ ਕਿ ਤੁਸੀਂ ਸਹੀ ਨੈੱਟਵਰਕ ਨਾਲ ਕਨੈਕਟ ਕਰ ਰਹੇ ਹੋ। ਬੁਰੇ ਅਦਾਕਾਰ ਅਜਿਹੇ ਨੈੱਟਵਰਕ ਬਣਾ ਸਕਦੇ ਹਨ ਜੋ ਉਹਨਾਂ ਦੇ ਨਾਮ ਦੇ ਅਧਾਰ 'ਤੇ ਨੁਕਸਾਨ ਮੁਕਤ ਦਿਖਾਈ ਦੇ ਸਕਦੇ ਹਨ ਪਰ ਅਸਲ ਵਿੱਚ ਉਹ ਤੁਹਾਡੀ ਇੰਟਰਨੈੱਟ ਸਰਫਿੰਗ ਨੂੰ ਦੇਖਣ ਲਈ ਨੈੱਟਵਰਕ ਸੈੱਟ-ਅੱਪ ਨਾਲ ਕਨੈਕਟ ਕਰਨ ਲਈ ਤੁਹਾਨੂੰ ਡਾਇਰੈਕਟ ਕਰ ਰਹੇ ਹਨ। ਇਸ ਤੋਂ ਭਾਵ ਹੈ ਕਿ ਜੇਕਰ ਤੁਸੀਂ ਵੈੱਬਸਾਈਟਾਂ ਵਿੱਚ ਲੌਗ ਇਨ ਕ੍ਰਿਡੈਨਸ਼ੀਅਲ ਜਾਂ ਪਾਸਵਰਡ ਦਾਖਲ ਕਰਦੇ ਹੋ ਤਾਂ ਹੈਕਰ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਨੂੰ ਚੁਰਾ ਸਕੇਗਾ। ਇਸ ਤੋਂ ਸੁਰੱਖਿਆ ਕਰਨ ਲਈ, ਨੈੱਟਵਰਕ ਦੇ ਨਾਮ ਨੂੰ ਧਿਆਨ ਨਾਲ ਪੜ੍ਹੋ ਅਤੇ ਜੇਕਰ ਸੰਭਵ ਹੋਵੇ ਤਾਂ, ਕਿਸੇ ਕਰਮਚਾਰੀ ਨੂੰ ਉਸ ਵਪਾਰ ਦੇ ਸਾਈਨੇਜ ਦੀ ਜਾਂਚ ਕਰਨ ਲਈ ਕਹੋ ਤਾਂ ਜੋ ਇਹ ਯਕੀਨੀ ਹੋ ਸਕੇ ਕਿ ਨੈੱਟਵਰਕ ਸਹੀ ਹੈ।

ਮਸ਼ਹੂਰ ਨੈੱਟਵਰਕ, ਜਿਵੇਂ ਕਿ ਉਹਨਾਂ ਪਰਿਚਿਤ ਕੌਫੀ-ਚੇਨਾਂ ਦੇ ਨੈੱਟਵਰਕ 'ਤੇ ਸੰਭਵ ਤੌਰ 'ਤੇ ਘੱਟ ਸੰਦੇਹ ਹੈ, ਕਿਉਂਕਿ ਉਹ ਕੰਪਨੀ ਨੈੱਟਵਰਕ ਨੂੰ ਆਪਣੇ ਵਪਾਰ ਦੀ ਸੇਵਾ ਦੇ ਵਜੋਂ ਚਲਾ ਰਹੀ ਹੈ। ਗਿਆਤ ਨੈੱਟਵਰਕ ਆਮ ਤੌਰ 'ਤੇ ਉਹਨਾਂ ਮੁਫਤ ਵਾਈ-ਫਾਈ ਨੈੱਟਵਰਕਾਂ ਤੋਂ ਵੱਧ ਸੁਰੱਖਿਅਤ ਹੁੰਦੇ ਹਨ ਜੋ ਕਿ ਕਿਸੇ ਸਾਵਰਜਨਿਕ ਸਥਾਨ 'ਤੇ ਤੁਹਾਡੇ ਫੋਨ 'ਤੇ ਦਿਖਾਈ ਦੇ ਸਕਦੇ ਹਨ।

2. ਆਟੋ-ਕਨੈਕਟ ਵਿਸ਼ੇਸ਼ਤਾ ਨੂੰ ਬੰਦ ਕਰੋ।

ਕਈ ਡਿਵਾਈਸਾਂ (ਸਮਾਰਟਫੋਨਾਂ, ਲੈਪਟੌਪਾਂ, ਅਤੇ ਟੈਬਲੇਟਾਂ) 'ਤੇ ਆਟੋਮੈਟਿਕ ਕਨੈਕਟੀਵਿਟੀ ਸੈਟਿੰਗਾਂ ਹਨ। ਇਹ ਸੈਟਿੰਗ ਤੁਹਾਡੇ ਡਿਵਾਈਸਾਂ ਨੂੰ ਸੁਵਿਧਾਜਨਕ ਢੰਗ ਨਾਲ ਨੇੜਲੇ ਨੈੱਟਵਰਕਾਂ ਨਾਲ ਕਨੈਕਟ ਕਰਨ ਦੀ ਅਨੁਮਤੀ ਦਿੰਦੀ ਹੈ। ਵਿਸ਼ਵਾਸਯੋਗ ਨੈੱਟਵਰਕਾਂ ਦੇ ਸੰਬੰਧ ਵਿੱਚ ਕੋਈ ਚਿੰਤਾ ਨਹੀਂ ਹੁੰਦੀ ਹੈ, ਪਰ ਇਸ ਨਾਲ ਤੁਹਾਡੇ ਡਿਵਾਈਸ ਉਹਨਾਂ ਨੈੱਟਵਰਕਾਂ ਨਾਲ ਵੀ ਕਨੈਕਟ ਹੋ ਸਕਦੇ ਹਨ ਜੋ ਕਿ ਸੁਰੱਖਿਅਤ ਨਹੀਂ ਹਨ। ਤੁਸੀਂ ਇਸ ਵਿਸ਼ੇਸ਼ਤਾ ਨੂੰ ਆਪਣੇ ਡਿਵਾਈਸ 'ਤੇ ਸੈਟਿੰਗ ਵਿਸ਼ੇਸ਼ਤਾ ਦੇ ਰਾਹੀਂ ਅਸਮਰੱਥ ਕਰ ਸਕਦੇ ਹੋ। ਇਹਨਾਂ ਸੈਟਿੰਗਾਂ ਨੂੰ ਬੰਦ ਰੱਖੋ, ਖਾਸ ਤੌਰ 'ਤੇ ਜੇਕਰ ਤੁਸੀਂ ਨਵੀਆਂ ਜਗ੍ਹਾਵਾਂ 'ਤੇ ਜਾ ਰਹੇ ਹੋ। ਇੱਕ ਵਾਧੂ ਸਾਵਧਾਨੀ ਦੇ ਤੌਰ 'ਤੇ, ਤੁਸੀਂ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਬਾਅਦ "ਨੈੱਟਵਰਕ ਨੂੰ ਭੁੱਲੋ" ਦੀ ਚੋਣ ਕਰ ਸਕਦੇ ਹੋ।

ਤੁਹਾਨੂੰ ਪਬਲਿਕ ਜਗ੍ਹਾਵਾਂ ‘ਤੇ ਆਪਣੇ Bluetooth ਦੀ ਵੀ ਨਿਗਰਾਨੀ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ। Bluetooth ਕਨੈਕਟੀਵਿਟੀ ਕਈ ਡਿਵਾਈਸਾਂ ਨੂੰ ਇੱਕ-ਦੂਜੇ ਨਾਲ ਕਨੈਕਟ ਕਰਨ ਦੀ ਅਨੁਮਤੀ ਦਿੰਦੀ ਹੈ, ਅਤੇ ਕੋਈ ਹੈਕਰ ਤੁਹਾਡੇ ਡਿਵਾਈਸਾਂ ‘ਤੇ ਐਕਸੈਸ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ ਖੁੱਲ੍ਹੇ Bluetooth ਸਿਗਨਲਾਂ ਦੀ ਖੋਜ ਕਰ ਸਕਦਾ ਹੈ। ਜਦੋਂ ਤੁਸੀਂ ਕਿਸੇ ਨਵੀਂ ਜਗ੍ਹਾਂ ‘ਤੇ ਹੋਵੋ ਤਾਂ ਆਪਣੇ ਫੋਨ ਜਾਂ ਹੋਰਨਾਂ ਡਿਵਾਈਸਾਂ ‘ਤੇ ਇਸ ਵਿਸ਼ੇਸ਼ਤਾ ਨੂੰ ਬੰਦ ਰੱਖੋ।

3. ਫਾਈਲ ਸ਼ੇਅਰਿੰਗ ਵਿਸ਼ੇਸ਼ਤਾਂ ਨੂੰ ਬੰਦ ਕਰੋ।

ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਸਮੇਂ ਫਾਈਲ ਸ਼ੇਅਰਿੰਗ ਵਿਕਲਪ ਨੂੰ ਬੰਦ ਕਰਨਾ ਯਕੀਨੀ ਬਣਾਓ। ਤੁਸੀਂ ਆਪਣੇ ਆਪਰੇਟਿੰਗ ਸਿਸਟਮ ‘ਤੇ ਨਿਰਭਰ ਕਰਦੇ ਹੋਏ ਸਿਸਟਮ ਪ੍ਰਾਥਮਿਕਤਾਵਾਂ ਜਾਂ ਕੰਟ੍ਰੋਲ ਪੈਨਲ ਤੋਂ ਫਾਈਲ ਸ਼ੇਅਰਿੰਗ ਨੂੰ ਬੰਦ ਕਰ ਸਕਦੇ ਹੋ। AirDrop ਫਾਈਲ ਸ਼ੇਅਰਿੰਗ ਵਿਸ਼ੇਸ਼ਤਾ ਦੀ ਉਦਾਹਰਨ ਹੈ ਜਿਸ ਨੂੰ ਤੁਸੀਂ ਬੰਦ ਰੱਖਣਾ ਚਾਹੁੰਦੇ ਹੋਵੋਗੇ। ਕੁਝ ਆਪਰੇਟਿੰਗ ਸਿਸਟਮ ਜਿਵੇਂ ਕਿ Windows/PC ਪਹਿਲੀ ਵਾਰ ਕਿਸੇ ਨਵੇਂ ਪਬਲਿਕ ਨੈੱਵਰਕ ਨਾਲ ਕਨੈਕਟ ਕਰਦੇ ਸਮੇਂ “ਪਬਲਿਕ” ਵਿਕਲਪ ਨੂੰ ਚੁਣ ਕੇ ਤੁਹਾਡੇ ਲਈ ਫਾਈਲ ਸ਼ੇਅਰਿੰਗ ਵਿਕਲਪ ਨੂੰ ਬੰਦ ਕਰ ਦੇਣਗੇ।

ਫਾਈਲ ਸ਼ੇਅਰਿੰਗ ਨੂੰ ਬੰਦ ਕਰਨ ਲਈ ਕਦਮ

PC **ਨੂੰ ਚਾਲੂ ਕਰੋ**:

1. ਨੈੱਟਵਰਕ ਅਤੇ ਸ਼ੇਅਰਿੰਗ ਸੈਂਟਰ ਵਿੱਚ ਜਾਓ।
2. ਫਿਰ ਐਡਵਾਂਸਡ ਸ਼ੇਅਰਿੰਗ ਸੈਟਿੰਗਾਂ ਨੂੰ ਬਦਲੋ।
3. ਫਾਈਲ ਅਤੇ ਪ੍ਰਿੰਟਰ ਸ਼ੇਅਰਿੰਗ ਨੂੰ ਬੰਦ ਕਰੋ।

Macs **ਦੇ ਲਈ**:

1. ਸਿਸਟਮ ਪ੍ਰਾਥਮਿਕਤਾਵਾਂ ‘ਤੇ ਜਾਓ
2. ਸ਼ੇਅਰਿੰਗ ਨੂੰ ਚੁਣੋ।
3. ਹਰੇਕ ਚੀਜ਼ ਤੋਂ ਚੋਣ ਨੂੰ ਹਟਾ ਦਿਓ।
4. ਫਿਰ ਫਾਈਂਡਰ ਵਿੱਚ, AirDrop ‘ਤੇ ਕਲਿੱਕ ਕਰੋ ਅਤੇ ਮੈਨੂੰ ਇਸ ਵੱਲੋਂ ਲੱਭੇ ਜਾਣ ਦੀ ਅਨੁਮਤੀ ਦਿਓ ਨੂੰ ਚੁਣੋ: ਕੋਈ ਨਹੀਂ।

iOS ਦੇ ਲਈ, ਬੱਸ ਕੰਟਰੋਲ ਸੈਂਟਰ ਵਿੱਚ AirDrop ਨੂੰ ਲੱਭੋ ਅਤੇ ਇਸ ਨੂੰ ਬੰਦ ਕਰੋ।

4. VPN ਦੀ ਵਰਤੋਂ ਕਰੋ।

ਆਪਣੇ ਡਿਵਾਈਸ ‘ਤੇ VPN (ਵਰਚੁਅਲ ਪ੍ਰਾਈਵੇਟ ਨੈੱਟਵਰਕ) ਨੂੰ ਇੰਸਟਾਲ ਕਰਨ ‘ਤੇ ਵਿਚਾਰ ਕਰੋ। VPN ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ‘ਤੇ ਡਿਜਿਟਲ ਪਰਦੇਦਾਰੀ ਲਈ ਸਭ ਤੋਂ ਵੱਧ ਸੁਰੱਖਿਅਤ ਵਿਕਲਪ ਹੈ। ਇਹ ਤੁਹਾਡੇ ਡਿਵਾਈਸ ਵਿੱਚ ਆਉਣ ਵਾਲੇ ਅਤੇ ਬਾਹਰ ਨਿਕਲਣ ਵਾਲੇ ਡੇਟਾ ਨੂੰ ਏਨਕ੍ਰਿਪਟ ਕਰਦਾ ਹੈ ਅਤੇ ਇੱਕ ਸੁਰੱਖਿਅਤ “ਟਨਲ” ਦੇ ਤੌਰ ‘ਤੇ ਕੰਮ ਕਰਦਾ ਹੈ ਤਾਂ ਜੋ ਕਿਸੇ ਨੈੱਟਵਰਕ ਵਿੱਚੋਂ ਲੰਘਣ ਵੇਲੇ ਤੁਹਾਡਾ ਡੇਟਾ ਨਾ ਦਿਖੇ।

5. ਏਨਕ੍ਰਿਪਟੇਡ ਵੈੱਬਸਾਈਟਾਂ ਦੇ ਬਾਰੇ FBI ਦੀ ਚੇਤਾਵਨੀ – HTTPS.

FBI ਨੇ ਉਹਨਾਂ ਵੈੱਬਸਾਈਟਾਂ ਦੇ ਬਾਰੇ ਚੇਤਾਵਨੀ ਦਿੱਤੀ ਹੈ ਜਿੰਨ੍ਹਾਂ ਦਾ ਪਤਾ "https."ਤੋਂ ਸ਼ੁਰੂ ਹੁੰਦਾ ਹੈ। "https" ਅਤੇ ਲੌਕ ਆਈਕਨ ਦੀ ਮੌਜੂਦਗੀ ਇਹ ਦਰਸਾਉਂਦੀ ਹੈ ਕਿ ਵੈੱਬ ਟ੍ਰੈਫਿਕ ਏਨਕ੍ਰਿਪਟੇਡ ਹੈ ਅਤੇ ਇਹ ਕਿ ਦਰਸ਼ਕ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਡੇਟਾ ਸਾਂਝਾ ਕਰ ਸਕਦੇ ਹਨ। ਹਾਲਾਂਕਿ, ਸਾਈਬਰ ਕ੍ਰਿਮਿਨਲ ਹੁਣ ਲੋਕਾਂ ਨੂੰ ਉਹਨਾਂ ਖਰਾਬ ਵੈੱਬਸਾਈਟਾਂ ਦੇ ਨਾਲ ਭਰਮਾ ਕੇ ਉਹਨਾਂ ਤੋਂ ਪੈਸਾ ਕਮਾ ਰਹੇ ਹਨ ਜਿੰਨ੍ਹਾਂ ਵਿੱਚ https ਸ਼ਾਮਲ ਹੈ ਅਤੇ ਜੋ ਕਿ ਸੁਰੱਖਿਅਤ ਦਿਖਾਈ ਦਿੰਦੇ ਹਨ ਜਦੋਂ ਕਿ ਉਹ ਨਹੀਂ ਹਨ।

FBI ਦੇ ਸੁਝਾਅ

- ਕਿਸੇ ਈ-ਮੇਲ 'ਤੇ ਸਿਰਫ਼ ਨਾਮ 'ਤੇ ਭਰੋਸਾ ਨਾ ਕਰੋ: ਈਮੇਲ ਸਮੱਗਰੀ ਦੇ ਇਰਾਦੇ 'ਤੇ ਪ੍ਰਸ਼ਨ ਉਠਾਓ।
- ਜੇ ਤੁਸੀਂ ਕਿਸੇ ਜਾਣੇ ਪਛਾਣੇ ਸੰਪਰਕ ਦੇ ਲਿੰਕ ਦੇ ਨਾਲ ਇੱਕ ਸੰਦੇਹਯੋਗ ਈਮੇਲ ਪ੍ਰਾਪਤ ਕਰਦੇ ਹੋ, ਤਾਂ ਸੰਪਰਕ ਨੂੰ ਕਾਲ ਕਰਕੇ ਜਾਂ ਈਮੇਲ ਕਰਕੇ ਪੁਸ਼ਟੀ ਕਰੋ ਕਿ ਸੁਨੇਹਾ ਜਾਇਜ਼ ਹੈ। ਕਿਸੇ ਸੰਦੇਹਯੋਗ ਈਮੇਲ ਨੂੰ ਸਿੱਧੇ ਜਵਾਬ ਨਾ ਦਿਓ।
- ਲਿੰਕ ਦੇ ਵਿੱਚ ਗਲਤ ਸਪੈਲਿੰਗਾਂ ਜਾਂ ਗਲਤ ਡੋਮੇਨਾਂ ਦੇ ਲਈ ਜਾਂਚ ਕਰੋ (ਉਦਾਹਰਨ ਲਈ, ਜੇਕਰ ਕੋਈ ਅਜਿਹਾ ਪਤਾ ਹੈ ਜਿਸ ਦੀ ਸਮਾਪਤੀ ".gov" ਨਾਲ ਹੋਣੀ ਚਾਹੀਦੀ ਸੀ ਪਰ ".com" ਨਾਲ ਹੁੰਦੀ ਹੈ)।
- ਕਿਸੇ ਵੀ ਵੈੱਬਸਾਈਟ 'ਤੇ ਕੇਵਲ ਤਾਂ ਭਰੋਸਾ ਨਾ ਕਰੋ ਕਿਉਂਕਿ ਉਸਦੇ ਬ੍ਰਾਊਜ਼ਰ ਪਤੇ ਬਾਰ 'ਤੇ ਲੌਕ ਆਈਕਨ ਜਾਂ "https" ਹੈ।

6. ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਨੂੰ ਐਕਸੈਸ ਕਰਨ ਲਈ ਸਿਫਾਰਿਸ਼ ਨਹੀਂ ਕੀਤੀ ਜਾਂਦੀ ਹੈ।

ਭਾਵੇਂ ਤੁਹਾਡੇ ਕੋਲ VPN ਹੈ, ਫਿਰ ਵੀ ਅਸੁਰੱਖਿਅਤ ਪਬਲਿਕ ਨੈੱਟਵਰਕਾਂ 'ਤੇ ਨਿੱਜੀ ਬੈਂਕ ਖਾਤਿਆਂ ਜਾਂ ਸਮਾਜਕ ਸੁਰੱਖਿਆ ਨੰਬਰਾਂ ਵਰਗੇ ਸਮਾਨ ਸੰਵੇਦਨਸ਼ੀਲ ਨਿੱਜੀ ਡੇਟਾ ਨੂੰ ਐਕਸੈਸ ਕਰਨ ਦੀ ਸਿਫਾਰਸ਼ ਨਹੀਂ ਕੀਤੀ ਜਾਂਦੀ। ਇੱਥੋਂ ਤੱਕ ਕਿ ਪਬਲਿਕ ਸੁਰੱਖਿਅਤ ਨੈੱਟਵਰਕ ਵੀ ਜੋਖਮ ਭਰਪੂਰ ਹੋ ਸਕਦੇ ਹਨ। ਜੇਕਰ ਤੁਸੀਂ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ 'ਤੇ ਇਹਨਾਂ ਖਾਤਿਆਂ ਨੂੰ ਐਕਸੈਸ ਕਰਨ ਲੱਗੇ ਹੋ ਤਾਂ ਚੰਗੀ ਤਰ੍ਹਾਂ ਸੋਚ ਵਿਚਾਰ ਕਰੋ। ਵਿੱਤ ਲੈਣ-ਦੇਣਾਂ ਲਈ, ਇਹਨਾਂ ਦੀ ਬਜਾਏ ਆਪਣੇ ਸਮਾਰਟਫੋਨ ਦੀ ਹੌਟਸਪੋਟ ਵਿਸ਼ੇਸ਼ਤਾਂ ਨੂੰ ਵਰਤਣਾ ਬਿਹਤਰ ਹੋਵੇਗਾ।

7. ਸੁਰੱਖਿਅਤ ਬਨਾਮ ਅਸੁਰੱਖਿਅਤ।

ਬੁਨਿਆਦੀ ਤੌਰ 'ਤੇ ਦੋ ਤਰ੍ਹਾਂ ਦੇ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਨੈੱਟਵਰਕ ਹੁੰਦੇ ਹਨ: ਸੁਰੱਖਿਅਤ ਅਤੇ ਅਸੁਰੱਖਿਅਤ।

ਜਦੋਂ ਵੀ ਸੰਭਵ ਹੋਵੇ, ਹਮੇਸ਼ਾ ਸੁਰੱਖਿਅਤ ਪਬਲਿਕ ਨੈੱਟਵਰਕਾਂ ਦੇ ਨਾਲ ਕਨੈਕਟ ਕਰੋ। ਇੱਕ ਅਸੁਰੱਖਿਅਤ ਨੈਟਵਰਕ ਨੂੰ ਪਾਸਵਰਡ ਜਾਂ ਲੌਗਇਨ ਵਰਗੇ ਕਿਸੇ ਵੀ ਕਿਸਮ ਦੀ ਸੁਰੱਖਿਆ ਵਿਸ਼ੇਸ਼ਤਾ ਦੇ ਬਿਨਾਂ ਜੋੜਿਆ ਜਾ ਸਕਦਾ ਹੈ। ਇੱਕ ਸੁਰੱਖਿਅਤ ਨੈਟਵਰਕ ਲਈ ਆਮ ਤੌਰ 'ਤੇ ਉਪਭੋਗਤਾ ਨੂੰ ਨਿਯਮਾਂ ਅਤੇ ਸ਼ਰਤਾਂ ਨਾਲ ਸਹਿਮਤ ਹੋਣਾ, ਖਾਤਾ ਰਜਿਸਟਰ ਕਰਨਾ ਜਾਂ ਨੈੱਟਵਰਕ ਨਾਲ ਜੁੜਨ ਤੋਂ ਪਹਿਲਾਂ ਇੱਕ ਪਾਸਵਰਡ ਟਾਈਪ ਕਰਨਾ ਹੁੰਦਾ ਹੈ।

8. ਆਪਣੀ ਫਾਇਰਵਾਲ ਨੂੰ ਸਮਰੱਥ ਰੱਖੋ।

ਜੇ ਤੁਸੀਂ ਲੈਪਟਾਪ ਦੀ ਵਰਤੋਂ ਕਰ ਰਹੇ ਹੋ, ਤਾਂ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਨੂੰ ਵਰਤਣ ਵੇਲੇ ਆਪਣੇ ਫਾਇਰਵਾਲ ਨੂੰ ਸਮਰੱਥ ਰੱਖੋ। ਇੱਕ ਫਾਇਰਵਾਲ ਇੱਕ ਰੁਕਾਵਟ ਵਜੋਂ ਕੰਮ ਕਰਦਾ ਹੈ ਜੋ ਤੁਹਾਡੀ ਡਿਵਾਈਸ ਨੂੰ ਮਾਲਵੇਅਰ ਖਤਰੇ ਤੋਂ ਬਚਾਉਂਦਾ ਹੈ। ਪੌਪ ਅਪਸ ਅਤੇ ਨੋਟੀਫਿਕੇਸ਼ਨਾਂ ਕਾਰਨ ਉਪਭੋਗਤਾ Windows ਫਾਇਰਵਾਲ ਨੂੰ ਅਸਮਰੱਥ ਕਰ ਸਕਦੇ ਹਨ ਅਤੇ ਫਿਰ ਇਸ ਬਾਰੇ ਭੁੱਲ ਜਾਂਦੇ ਹਨ। ਜੇਕਰ ਤੁਸੀਂ PC 'ਤੇ ਇਸ ਨੂੰ ਰਿਸਟਾਰਟ ਕਰਨਾ ਚਾਹੁੰਦੇ ਹੋ ਤਾਂ ਕੰਟਰੋਲ ਪੈਨਲ 'ਤੇ ਜਾਓ, "ਸਿਸਟਮ ਅਤੇ ਸੁਰੱਖਿਆ" ਅਤੇ ਫਿਰ

"Windows ਫਾਇਰਵਾਲ" ਨੂੰ ਚੁਣੋ। ਜੇਕਰ ਤੁਸੀਂ ਇੱਕ Mac ਉਪਭੋਗਤਾ ਹੋ ਤਾਂ "ਸਿਸਟਮ ਪ੍ਰਾਥਮਿਕਤਾਵਾਂ" 'ਤੇ ਜਾਓ ਅਤੇ ਫਿਰ "ਸੁਰੱਖਿਆ ਅਤੇ ਪਰਦੇਦਾਰੀ" 'ਤੇ ਜਾਓ ਅਤੇ ਫਿਰ ਵਿਸ਼ੇਸ਼ਤਾ ਨੂੰ ਸਮਰੱਥ ਕਰਨ ਲਈ "ਫਾਇਰਵਾਲ" ਟੈਬ 'ਤੇ ਜਾਓ।

9. ਐਂਟੀਵਾਇਰਸ ਸਾਫਟਵੇਅਰ ਦੀ ਵਰਤੋਂ ਕਰੋ।

ਇਸ ਦੇ ਨਾਲ ਹੀ ਆਪਣੇ ਲੈਪਟੌਪ 'ਤੇ ਇੱਕ ਐਂਟੀਵਾਇਰਸ ਪ੍ਰੋਗ੍ਰਾਮ ਦੇ ਨਵੀਨਤਮ ਸੰਸਕਰਣ ਨੂੰ ਇੰਸਟਾਲ ਕਰਨਾ ਯਕੀਨੀ ਬਣਾਓ। ਐਂਟੀਵਾਇਰਸ ਪ੍ਰੋਗਰਾਮ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋਏ ਮਾਲਵੇਅਰ ਦਾ ਪਤਾ ਲਗਾ ਕੇ ਤੁਹਾਡੀ ਸੁਰੱਖਿਆ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰ ਸਕਦੇ ਹਨ ਜੋ ਸਾਂਝੇ ਨੈੱਟਵਰਕ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਸਮੇਂ ਤੁਹਾਡੇ ਸਿਸਟਮ ਵਿੱਚ ਦਾਖਲ ਹੋ ਸਕਦੇ ਹਨ। ਇੱਕ ਚੇਤਾਵਨੀ ਤੁਹਾਨੂੰ ਸਾਵਧਾਨ ਕਰੇਗੀ ਜੇਕਰ ਗਿਆਤ ਵਾਇਰਸ ਤੁਹਾਡੇ ਡਿਵਾਇਸ 'ਤੇ ਲੋਡ ਹੋ ਗਏ ਹਨ ਜਾਂ ਜੇ ਕੋਈ ਸੰਦੇਹਯੋਗ ਗਤੀਵਿਧੀ, ਹਮਲਾ ਹੈ, ਜਾਂ ਜੇਕਰ ਮਾਲਵੇਅਰ ਤੁਹਾਡੇ ਸਿਸਟਮ ਵਿੱਚ ਆ ਜਾਂਦਾ ਹੈ।

10. ਟੂ-ਫੈਕਟਰ ਜਾਂ ਮਲਟੀ-ਫੈਕਟਰ ਪ੍ਰਮਾਣੀਕਰਨ ਦੀ ਵਰਤੋਂ ਕਰੋ।

ਆਪਣੀ ਵਿਅਕਤੀਗਤ ਜਾਣਕਾਰੀ ਦੇ ਨਾਲ ਵੈੱਬਸਾਈਟਾਂ 'ਤੇ ਦਾਖਲ ਹੁੰਦੇ ਸਮੇਂ ਮਲਟੀ-ਫੈਕਟਰ ਪ੍ਰਮਾਣੀਕਰਨ (MFA) ਦੀ ਵਰਤੋਂ ਕਰੋ। ਇਸਦਾ ਅਰਥ ਹੈ ਕਿ ਤੁਹਾਡੇ ਕੋਲ ਇੱਕ ਦੂਜਾ ਤਸਦੀਕ ਕੋਡ ਹੈ (ਤੁਹਾਡੇ ਫੋਨ 'ਤੇ ਟੈਕਸਟ ਕੀਤਾ ਗਿਆ ਹੈ ਜਾਂ ਇੱਕ ਐਪ ਜਾਂ ਭੌਤਿਕ ਕੁੰਜੀ ਦੁਆਰਾ ਦਿੱਤਾ ਗਿਆ ਹੈ) ਜੋ ਤੁਹਾਡੀ ਵਧੇਰੇ ਸੁਰੱਖਿਆ ਕਰਦਾ ਹੈ। ਤਾਂ ਵੀ ਜੇ ਕੋਈ ਹੈਕਰ ਤੁਹਾਡਾ ਯੂਜ਼ਰ ਨਾਮ ਅਤੇ ਪਾਸਵਰਡ ਪ੍ਰਾਪਤ ਵੀ ਕਰ ਲੈਂਦਾ ਹੈ, ਤਾਂ ਉਹ ਪ੍ਰਮਾਣੀਕਰਨ ਕੋਡ ਤੋਂ ਬਗੈਰ ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਤੱਕ ਨਹੀਂ ਪਹੁੰਚ ਸਕਦੇ।

11. ਆਪਣੇ ਵਿਅਕਤੀਗਤ ਡਿਵਾਈਸਾਂ ਦਾ ਟ੍ਰੈਕ ਰੱਖੋ।

ਆਪਣੇ ਲੈਪਟੌਪ, ਟੈਬਲੇਟ, ਜਾਂ ਸਮਾਰਟਫੋਨ ਨੂੰ ਪਬਲਿਕ ਜਗ੍ਹਾਂ ਜਾਂ ਵਾਹਨ ਵਿੱਚ ਇਕੱਲੇ ਨਾ ਰੱਖੋ। ਜੇਕਰ ਤੁਸੀਂ ਕਿਸੇ ਵਾਈ-ਫਾਈ ਨੈੱਟਵਰਕ 'ਤੇ ਸਾਵਧਾਨੀਆਂ ਵੀ ਵਰਤ ਰਹੇ ਹੋ, ਤਾਂ ਇਸ ਨਾਲ ਕਿਸੇ ਵੱਲੋਂ ਤੁਹਾਡੇ ਸਮਾਨ ਨੂੰ ਲੈਣ ਜਾਂ ਤੁਹਾਨੂੰ ਜਾਣਕਾਰੀ ਨੂੰ ਚੋਰੀ ਨਾਲ ਵੇਖਣ 'ਤੇ ਰੋਕ ਨਹੀਂ ਲੱਗੇਗੀ। ਆਪਣੇ ਆਲੇ-ਦੁਆਲੇ ਦੇ ਵਾਤਾਵਰਣ ਅਤੇ ਆਪਣੇ ਆਲੇ-ਦੁਆਲੇ ਦੇ ਲੋਕਾਂ ਤੋਂ ਸਚੇਤ ਰਹੋ।

12. ਹੋਰ ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ ਸੁਝਾਅ।

ਇੱਥੇ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਕੁਝ ਸੁਝਾਅ ਦਿੱਤੇ ਹੋਏ ਹਨ, ਖਾਸ ਤੌਰ 'ਤੇ ਜੇਕਰ ਤੁਸੀਂ ਕੋਈ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਕਨੈਕਸ਼ਨ ਦੀ ਵਰਤੋਂ ਕਰ ਰਹੇ ਹੋ:

- ਮਜ਼ਬੂਤ ਪਾਸਵਰਡਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- ਆਪਣੇ ਡਿਵਾਈਸਾਂ ਨੂੰ ਏਨਕ੍ਰਿਪਟ ਕਰੋ।
- ਨਕਲੀ ਈਮੇਲਾਂ ਤੋਂ ਸਚੇਤ ਰਹੋ।
- ਇਸ ਬਾਰੇ ਸਾਵਧਾਨ ਰਹੋ ਕਿ ਤੁਸੀਂ ਸੋਸ਼ਲ ਮੀਡਿਆ 'ਤੇ ਕੀ ਪੋਸਟ ਕਰਦੇ ਹੋ। ਬਹੁਤ ਵੱਧ ਵਿਅਕਤੀਗਤ ਵੇਰਵੇ ਹੈਕਰਾਂ ਨੂੰ ਪਾਸਵਰਡਾਂ ਦੀ ਪਛਾਣ ਕਰਨ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰ ਸਕਦੇ ਹਨ।
- ਉਸ ਪੁਰਾਣੀ ਜਾਣਕਾਰੀ ਨੂੰ ਮਿਟਾ ਦਿਓ ਜਿਸ ਦੀ ਤੁਹਾਨੂੰ ਲੋੜ ਨਹੀਂ ਹੈ।
- ਜੇਕਰ ਕੋਈ ਨੈੱਟਵਰਕ ਤੁਹਾਨੂੰ ਕੋਈ ਵਾਧੂ ਸੌਫਟਵੇਅਰ ਜਾਂ ਬ੍ਰਾਊਜ਼ਰ ਐਕਸਟੈਸ਼ਨਾਂ ਨਾਲ ਕਨੈਕਟ ਕਰਨ ਲਈ ਕਹਿੰਦਾ ਹੈ ਤਾਂ ਕਨੈਕਟ ਨਾ ਕਰੋ।
- ਯਕੀਨੀ ਕਰੋ ਕਿ ਤੁਹਾਡੇ ਡਿਵਾਈਸ 'ਤੇ ਗਿਆਤ ਸਮੱਸਿਆਵਾਂ ਦੇ ਵਿਰੁੱਧ ਸੁਰੱਖਿਆ ਕਰਨ ਲਈ ਨਵੀਨਤਮ ਪੈਚ ਅਤੇ ਸਾਫਟਵੇਅਰ ਅਪਡੇਟ ਇੰਸਟਾਲ ਹਨ।