TELUS Wise® ਸਿੱਖਿਆ ਪ੍ਰੋਗਰਾਮ

ਸਾਡੇ ਡਿਜ਼ੀਟਲ ਸੰਸਾਰ ਲਈ ਸੇਫ਼ਟੀ ਅਤੇ ਪ੍ਰਾਈਵੇਸੀ ਸੁਝਾਅ

TELUS Wise ਇੱਕ ਮੁਫ਼ਤ ਵਿਦਿਅਕ ਪ੍ਰੋਗਰਾਮ ਹੈ, ਜੋ ਸਾਡੇ ਡਿਜ਼ੀਟਲ ਸੰਸਾਰ ਵਿਚ ਕੈਨੇਡੀਅਨਜ਼ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਬਲ ਪ੍ਰਦਾਨ ਕਰਦਾ ਹੈ। ਇਹ ਸੁਝਾਅ ਤੁਹਾਨੂੰ ਅਤੇ ਤੁਹਾਡੇ ਪਰਿਵਾਰ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਵਿੱਚ ਸਹਾਈ ਹੋ ਸਕਦੇ ਹਨ।

ਇੰਟਰਨੈੱਟ ਸੇਫ਼ਟੀ

1. **ਆਪਣੀ ਰੱਖਿਆ ਕਰੋ:** ਐਂਟੀ-ਵਾਇਰਸ, ਐਂਟੀ-ਸਪਾਈਵੇਅਰ, ਫ਼ਾਇਰਵਾਲ ਸਿਕਿਉਰਿਟੀ ਹੱਲ ਅਤੇ ਆਪਣੇ ਡਾਟਾ ਨੂੰ ਨਿਯਮਤ ਰੂਪ ਵਿਚ ਬੈਕਅਪ ਕਰਨਾ ਯਾਦ ਰੱਖੋ।
2. **ਸੌਫ਼ਟਵੇਅਰ, ਆਪਰੇਟਿੰਗ ਸਿਸਟਮ ਅਤੇ ਬ੍ਰਾਊਜ਼ਰ ਨੂੰ ਅੱਪ-ਟੂ-ਡੇਟ ਰੱਖੋ** ਤਾਂ ਕਿ ਤੁਸੀਂ ਅਜੋਕੇ ਨਵੇਂ ਖ਼ਤਰਿਆਂ ਖਿਲਾਫ਼ ਹਮੇਸ਼ਾ ਸੁਰੱਖਿਅਤ ਰਹੋ।
3. **ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਸੈੱਟ ਕਰੋ** ਅਤੇ ਵਧੇਰੇ ਸੁਰੱਖਿਆ ਲਈ ਉਨ੍ਹਾਂ ਨੂੰ ਅਕਸਰ ਬਦਲੋ।
4. **ਆਪਣੀ ਈਮੇਲ ਦੀ ਜਾਂਚ ਕਰੋ:** ਸ਼ੱਕੀ ਅਟੈਚਮੈਂਟਸ/ਲਿੰਕਸ, ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਲਈ ਬੇਨਤੀਆਂ, ਟਾਈਪੋ ਅਤੇ ਵਿਆਕਰਣ ਦੀਆਂ ਗ਼ਲਤੀਆਂ ਸੰਭਾਵਿਤ ਰੂਪ ਵਿਚ ਹਾਨੀਕਾਰਕ ਈਮੇਲ ਲਈ ਚੰਗੇ ਸੰਕੇਤ ਹਨ।

ਸਮਾਰਟਫ਼ੋਨ ਅਤੇ ਟੇਬਲੈਟ ਸੇਫ਼ਟੀ

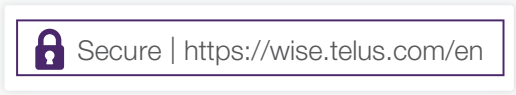
1. **ਆਪਣਾ ਫ਼ੋਨ ਲੌਕ ਕਰੋ:** ਆਪਣਾ ਫ਼ੋਨ ਪ੍ਰੋਗਰਾਮ ਕਰੋ, ਤਾਂ ਜੋ ਇਹ ਨਾ-ਵਰਤੋਂ ਦੇ ਸਮੇਂ ਦੌਰਾਨ ਆਪਣੇ-ਆਪ ਲੌਕ ਹੋ ਜਾਏ। ਨਿਯਮਤ ਰੂਪ ਨਾਲ ਪਾਸਵਰਡ ਸੈੱਟ ਕਰਨਾ ਅਤੇ ਬਦਲਣਾ ਨਾ ਭੁੱਲੋ।
2. **ਪ੍ਰੋਗਰਾਮ ਲੌਕ, ਟ੍ਰੈਕ, ਇਰੇਜ਼ ਕਰੋ:** ਜੇ ਫ਼ੋਨ ਗਵਾਚ ਜਾਂਦਾ ਹੈ ਜਾਂ ਚੋਰੀ ਹੋ ਜਾਂਦਾ ਹੈ ਤਾਂ ਤੁਹਾਡੇ ਆਪਰੇਟਿੰਗ ਸਿਸਟਮ 'ਤੇ ਨਿਰਭਰ ਕਰਦਿਆਂ, ਤੁਸੀਂ ਇੱਕ ਐਪ ਦੀ ਵਰਤੋਂ ਕਰ ਕੇ ਆਪਣੇ ਫ਼ੋਨ ਵਿਚਲੀ ਜਾਣਕਾਰੀ ਨੂੰ ਲੌਕ, ਟ੍ਰੈਕ ਜਾਂ ਰਿਮੋਟਲੀ ਮਿਟਾ ਸਕਦੇ ਹੋ (iPhone ਲਈ ਇਸ ਨੂੰ Find my Phone, Blackberry ਲਈ, ਇਹ Blackberry Protect ਹੈ ਅਤੇ Android ਲਈ ਇਹ ਨਿਰਮਾਤਾ 'ਤੇ ਨਿਰਭਰ ਕਰਦਿਆਂ ਵੱਖਰੀ ਹੈ)। ਇਸ ਤੋਂ ਬਿਨਾ, ਆਪਣੇ ਡਿਵਾਇਸ ਨੂੰ ਵੇਚਣ ਜਾਂ ਰੀਸਾਈਕਲ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਇਸ ਤੋਂ ਸਭ ਕੁੱਝ ਮਿਟਾ ਦੇਣਾ ਯਾਦ ਰੱਖੋ।
3. **ਅਜੋਕੇ ਨਵੇਂ ਖ਼ਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਲਈ** ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਆਪਣਾ ਸਿਸਟਮ ਅੱਪਡੇਟ ਕਰੋ।
4. **ਲੋਕੇਸ਼ਨ ਸੈਟਿੰਗਜ਼ ਮੈਨੇਜ ਕਰੋ:** ਤੁਹਾਡਾ ਸਥਾਨ ਜਾਨਣ ਲਈ ਪਹੁੰਚ ਦੀ ਪ੍ਰਵਾਨਗੀ ਸਿਰਫ਼ ਅਜਿਹੀਆਂ ਐਪਸ ਲਈ ਦੇਵੋ, ਜਿਨ੍ਹਾਂ ਵਾਸਤੇ ਤੁਹਾਡਾ ਸਥਾਨ ਜਾਨਣ ਦੀ ਜ਼ਰੂਰਤ ਹੈ, ਜਿਵੇਂ GPS ਜਾਂ ਨਕਸ਼ੇ ਦੀਆਂ ਐਪਸ। ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਤੇ ਹੋਰ ਬਹੁਤ ਸਾਰੀਆਂ ਐਪਸ ਬਿਨਾ ਤੁਹਾਡੇ ਸਥਾਨ ਦੀ ਜਾਣਕਾਰੀ ਲਏ ਚੱਲ ਸਕਦੀਆਂ ਹਨ।
5. **ਆਪਣੇ ਫ਼ੋਨ 'ਤੇ ਕੋਈ ਮਾਲਵੇਅਰ ਇੰਸਟਾਲ ਹੋਣ ਤੋਂ ਬਚਾਅ ਲਈ** ਡਾਊਨਲੋਡਿੰਗ ਤੋਂ ਪਹਿਲਾਂ ਅਣਪਛਾਤੇ ਸਰੋਤਾਂ ਅਤੇ ਰਿਸਰਚ ਐਪਸ ਰਾਹੀਂ ਆਈਆਂ ਅਟੈਚਮੈਂਟਸ ਨਾ ਖੋਲ੍ਹੋ।
6. **ਮੁਫ਼ਤ Wi-Fi ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ:** ਜੇ ਤੁਸੀਂ ਕਿਸੇ ਜਨਤਕ ਸਥਾਨ 'ਤੇ ਮੁਫ਼ਤ Wi-Fi ਵਰਤਦੇ ਹੋ, ਤਾਂ ਹੈਕਰਜ਼ ਉਸ ਰਾਹੀਂ ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਤੱਕ ਆਸਾਨੀ ਨਾਲ ਪਹੁੰਚ ਕਰ ਸਕਦੇ ਹਨ, ਸਿਰਫ਼ ਬ੍ਰਾਊਜ਼ਿੰਗ ਲਈ ਆਪਣੀ ਅਜਿਹੀ ਗਤੀਵਿਧੀ ਸੀਮਤ ਕਰੋ। ਕਿਸੇ ਜਨਤਕ Wi-Fi ਰਾਹੀਂ ਆਪਣੀ ਕੋਈ ਨਿੱਜੀ ਜਾਂ ਵਿੱਤੀ ਜਾਣਕਾਰੀ ਕਦੇ ਸਾਂਝੀ ਨਾ ਕਰੋ।
7. **Bluetooth ਦੇ ਖ਼ਤਰਿਆਂ ਤੋਂ ਚੌਕਸ ਰਹੋ:** Bluetooth ਦੇ ਯੋਗ ਉਪਕਰਣਾਂ 'ਤੇ ਹੈਕਰਜ਼ ਵਲੋਂ ਆਸਾਨੀ ਨਾਲ ਪਹੁੰਚ ਦੀ ਸੰਭਾਵਨਾ ਬਣੀ ਰਹਿੰਦੀ ਹੈ ਜਾਂ ਉਹ ਅਣ-ਅਧਿਕਾਰਤ ਤੌਰ 'ਤੇ ਉਨ੍ਹਾਂ ਨਾਲ ਕੁਨੈਕਸ਼ਨ ਕਾਇਮ ਕਰ ਸਕਦੇ ਹਨ। ਸਿਰਫ਼ ਭਰੋਸੇਯੋਗ ਉਪਕਰਨਾਂ ਨਾਲ ਹੀ ਕੁਨੈਕਸ਼ਨ ਜੋੜੋ ਅਤੇ/ਜਾਂ Bluetooth ਨੂੰ ਬੰਦ ਕਰ ਦੇਵੋ ਜੇ ਉਸ ਦੀ ਜ਼ਰੂਰਤ ਨਾ ਹੋਵੇ।

ਸੋਸ਼ਲ ਮੀਡੀਆ ਸੇਫ਼ਟੀ

1. **ਪਰਮਿਸ਼ਨ ਅਤੇ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਜ਼ 'ਤੇ ਨਜ਼ਰ ਰੱਖੋ:**
   - **ਪਰਮਿਸ਼ਨ ਸੈਟਿੰਗਜ਼** ਨਾਲ ਕਿਸ ਤੱਕ ਪਹੁੰਚ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ ਅਤੇ ਤੁਹਾਡੇ ਬਾਰੇ (ਉਦਾਹਰਣ ਵਜੋਂ ਸੰਪਰਕ ਸੂਚੀਆਂ, ਤਸਵੀਰਾਂ ਅਤੇ ਤੁਹਾਡੀ ਪ੍ਰੋਫ਼ਾਈਲ ਜਾਣਕਾਰੀ) ਕੀ ਸ਼ੇਅਰ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ ਜਾਂ ਨਹੀਂ; ਉਸ ਸਭ ਨੂੰ ਕੰਟਰੋਲ ਕਰੋ।
   - **ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਜ਼** ਕੰਟਰੋਲ ਕਰੋ ਕਿ ਕੌਣ ਤੁਹਾਡੀ ਪ੍ਰੋਫ਼ਾਈਲ ਅਤੇ ਪੋਸਟ ਕੀਤੀ ਜਾਣਕਾਰੀ ਵੇਖ ਸਕਦਾ ਹੈ ਅਤੇ ਕੌਣ ਨਹੀਂ।
2. **ਇੱਕ Google Alert ਬਣਾਓ:** google.com/alerts 'ਤੇ ਆਪਣੇ ਨਾਮ ਲਈ Google Alert ਸੈੱਟ ਕਰੋ, ਤਾਂ ਜੋ ਜਦੋਂ ਵੀ ਕਦੇ ਤੁਹਾਡਾ ਨਾਮ ਔਨਲਾਈਨ ਆਵੇ, ਤਾਂ ਤੁਹਾਨੂੰ ਈਮੇਲ ਰਾਹੀਂ ਉਸ ਦੀ ਸੂਚਨਾ ਪੁੱਜੇ।
3. **ਸ਼ੇਅਰ ਕਰਨਾ ਘਟਾਓ:** ਤੁਹਾਡੀ ਜਨਮ ਤਾਰੀਖ਼, ਪਤਾ ਅਤੇ ਛੁੱਟੀਆਂ ਬਿਤਾਉਣ ਦੇ ਵੇਰਵੇ ਜਿਹੀ ਬਹੁਤ ਜ਼ਿਆਦਾ ਜਾਣਕਾਰੀ ਸ਼ੇਅਰ ਕਰਨ ਨਾਲ ਤੁਹਾਡਾ ਖ਼ਤਰਾ ਵਧ ਸਕਦਾ ਹੈ।
4. **ਕੁਨੈਕਟ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਦੋ ਵਾਰ ਸੋਚੋ:** ਸਿਰਫ਼ ਉਨ੍ਹਾਂ ਲੋਕਾਂ ਨਾਲ ਹੀ ਜੁੜੋ, ਜੋ ਤੁਹਾਨੂੰ ਚੰਗੀ ਤਰ੍ਹਾਂ ਜਾਣਦੇ ਹਨ।
5. **ਕਲਿੱਕ ਕਰਦੇ ਸਮੇਂ ਧਿਆਨ ਰੱਖੋ:** ਸ਼ੱਕੀ ਕਿਸਮ ਦੇ ਲਿੰਕਸ ਜਾਂ ਆਫ਼ਰਜ਼ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ, ਜੋ ਤੁਹਾਨੂੰ ਸਹੀ ਨਾ ਜਾਪਦੇ ਹੋਣ।
6. **ਜਿਓਟੈਗਿੰਗ ਬੰਦ ਕਰ ਦੇਵੋ:** ਜ਼ਿਆਦਾਤਰ ਸਮਾਰਟਫ਼ੋਨਜ਼ ਤੋਂ ਲਈਆਂ ਤਸਵੀਰਾਂ ਦਾ ਇੱਕ ਜਿਓ-ਟੈਗ (ਉਸ ਸਥਾਨ ਦੇ ਸਹੀ ਵੇਰਵੇ, ਜਿੱਥੇ ਤਸਵੀਰਾਂ ਖਿੱਚੀਆਂ ਗਈਆਂ ਸਨ) ਹੁੰਦਾ ਹੈ। ਤਸਵੀਰਾਂ ਔਨਲਾਈਨ ਸ਼ੇਅਰ ਕਰਦੇ ਸਮੇਂ ਆਪਣੀ ਨਿੱਜਤਾ ਵਧਾਉਣ ਲਈ ਇਸ ਫ਼ੀਚਰ ਨੂੰ ਬੰਦ ਕਰ ਦੇਵੋ।
7. **ਲੌਗ ਔਫ਼ ਕਰਨਾ ਨਾ ਭੁੱਲੋ:** ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਕਾਊਂਟਸ, ਐਪਸ ਜਾਂ ਗੇਮਜ਼ ਨਾ ਵਰਤਦੇ ਸਮੇਂ ਉਨ੍ਹਾਂ ਨੂੰ ਖੁੱਲ੍ਹਾ ਛੱਡ ਦੇਣ ਨਾਲ ਤੁਹਾਡੀ ਸੁਰੱਖਿਆ ਅਤੇ ਨਿੱਜਤਾ ਨੂੰ ਖ਼ਤਰਾ ਪੈਦਾ ਹੋ ਜਾਂਦਾ ਹੈ।
8. **ਆਪਣਾ ਡਿਜੀਟਲ ਹਾਊਸਹੋਲਡ ਸਾਫ਼ ਰੱਖੋ:** ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਕਾਊਂਟਸ ਅਤੇ ਐਪਸ 'ਤੇ ਪ੍ਰਾਈਵੇਸੀ ਅਤੇ ਪਰਮਿਸ਼ਨ ਸੈਟਿੰਗਜ਼ ਚੈੱਕ ਕਰਨ ਲਈ ਆਪਣੇ ਕੈਲੰਡਰ 'ਤੇ ਹਰੇਕ ਤਿੰਨ ਤੋਂ ਛੇ ਮਹੀਨਿਆਂ ਦਾ ਸਮਾਂ ਸੈੱਟ ਕਰੋ। ਪਾਸਵਰਡ ਬਦਲੋ, ਆਪਣੇ ਦੋਸਤਾਂ ਦੀਆਂ ਸੂਚੀਆਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ ਅਤੇ ਉਨ੍ਹਾਂ ਦੀ ਸਫ਼ਾਈ ਕਰੋ ਅਤੇ ਜਿਹੜੇ ਅਕਾਊਂਟ ਤੁਸੀਂ ਨਹੀਂ ਵਰਤਦੇ, ਉਨ੍ਹਾਂ ਨੂੰ ਡੀਐਕਟੀਵੇਟ ਕਰ ਦੇਵੋ।

ਔਨਲਾਇਨ ਸ਼ੌਪਿੰਗ ਸੁਰੱਖਿਆ

1. **ਵਿਕਰੇਤਾ ਦਾ ਸਾਖ਼ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ:** ਨਿੱਜਤਾ ਬਾਰੇ ਬਿਆਨ, ਅਸਲ ਪਤਾ, ਫ਼ੋਨ ਨੰਬਰ ਅਤੇ ਵਾਪਸ ਕਰਨ ਦੀ ਨੀਤੀ ਵੈੱਬਸਾਈਟ 'ਤੇ ਵੇਖੋ ਅਤੇ ਹੋਰ ਗਾਹਕਾਂ ਦੇ ਹਾਂ-ਪੱਖੀ ਰੀਵਿਊਜ਼ ਚੈੱਕ ਕਰੋ।
2. **ਸੁਰੱਖਿਆ ਯਕੀਨੀ ਬਣਾਓ:** ਲੌਕ ਦਾ ਨਿਸ਼ਾਨ ਅਤੇ ਪਤੇ ਵਾਲੇ ਬਾਰ ਵਿੱਚ "https" ਵਿੱਚ 'S' ਲੱਭੋ।



3. **ਆਪਣੀ ਜਾਣਕਾਰੀ ਸੁਰੱਖਿਅਤ ਰੱਖੋ:** ਜਨਤਕ ਕੰਪਿਊਟਰਜ਼ ਜਾਂ Wi-Fi 'ਤੇ ਕੋਈ ਖ਼ਰੀਦਦਾਰੀ ਨਾ ਕਰੋ ਅਤੇ ਤੁਹਾਡੇ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਦੀ ਜਾਣਕਾਰੀ ਸੇਵ ਕਰਨ ਦੀ ਪੇਸ਼ਕਸ਼ ਨੂੰ ਸਦਾ ਨਕਾਰ ਦੇਵੋ।

ਧਿਆਨ-ਭਟਕਾਊ ਡਰਾਈਵਿੰਗ ਵਿਰੁੱਧ ਡਟੋ

ਧਿਆਨ-ਭਟਕਾਊ ਡਰਾਈਵਿੰਗ ਨੂੰ ਸਮਾਜਿਕ ਤੌਰ 'ਤੇ ਕਦੇ ਪ੍ਰਵਾਨ ਨਾ ਕਰੋ। ਆਪਣੇ ਹੱਥ ਸਟੀਅਰਿੰਗ 'ਤੇ ਅਤੇ ਅੱਖਾਂ ਸੜਕ 'ਤੇ ਰੱਖੋ ਅਤੇ ਇਨ੍ਹਾਂ ਨੁਕਤਿਆਂ ਦਾ ਧਿਆਨ ਰੱਖੋ:

1. ਆਪਣਾ ਫ਼ੋਨ ਨਜ਼ਰ ਅਤੇ ਦਿਮਾਗ਼ ਤੋਂ ਦੂਰ ਰੱਖੋ (ਉਦਾਹਰਣ ਵਜੋਂ ਗਲੱਵ ਬੌਕਸ 'ਚ ਰੱਖੋ)
2. ਇਸ ਨੂੰ ਸਾਇਲੈਂਟ 'ਤੇ ਜਾਂ ਸਵਿੱਚ ਆਫ਼ ਕਰ ਕੇ ਰੱਖੋ
3. ਨਾਲ ਬੈਠੀ ਭਰੋਸੇਯੋਗ ਸਵਾਰੀ ਨੂੰ ਫ਼ੋਨ ਫੜਾ ਦੇਵੋ
4. ਗੱਡੀ ਚਲਾਉਣ ਤੋਂ ਪਹਿਲਾਂ ਸਾਰੇ ਸੁਨੇਹੇ ਚੈੱਕ ਕਰੋ ਅਤੇ ਆਪਣੇ GPS ਦਾ ਪ੍ਰੋਗਰਾਮ ਸੈੱਟ ਕਰੋ
5. ਜੇ ਤੁਸੀਂ ਆਪਣਾ ਫ਼ੋਨ ਜ਼ਰੂਰ ਵਰਤਣਾ ਹੀ ਹੈ ਤਾਂ ਉਸ ਨੂੰ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਵਰਤੋ

ਇੰਟਰਨੈੱਟ ਆਫ਼ ਥਿੰਗਜ਼ (IoT) ਸੇਫ਼ਟੀ

IoT ਤੋਂ ਭਾਵ ਹੈ ਸਮਾਰਟ ਜਾਂ ਜੁੜੇ ਹੋਏ ਉਪਕਰਣ, ਜਿਵੇਂ ਹੋਮ ਸੁਰੱਖਿਆ ਸਿਸਟਮਜ਼, ਬੇਬੀ ਮਾਨੀਟਰਜ਼, ਸਮਾਰਟ ਵਾਚੇਜ਼ ਅਤੇ ਹੋਰ, ਜੋ ਇੰਟਰਨੈੱਟ ਰਾਹੀਂ ਇੱਕ-ਦੂਜੇ ਨੂੰ ਜੋੜਦੇ ਹਨ। ਇਨ੍ਹਾਂ ਉਪਕਰਣਾਂ ਨਾਲ ਸਾਡੇ ਜੀਵਨ ਵਿੱਚ ਇਨਕਲਾਬ ਆਉਂਦਾ ਹੈ, ਪਰ ਡਾਟਾ ਇਕੱਠਾ ਕਰੋ ਅਤੇ ਟ੍ਰਾਂਸਮਿਟ ਕਰੋ, ਅਜਿਹੇ ਵੇਲੇ ਹੇਠ ਲਿਖੇ ਨੁਕਤਿਆਂ 'ਤੇ ਵਿਚਾਰ ਕਰਨਾ ਅਹਿਮ ਹੁੰਦਾ ਹੈ:

1. ਇਹ ਸਮਝੋ ਕਿ ਕਿਹੜਾ ਡਾਟਾ ਇਕੱਠਾ ਕੀਤਾ ਜਾ ਰਿਹਾ ਹੈ ਅਤੇ ਉਸ ਦੀ ਵਰਤੋਂ ਕਿਵੇਂ ਕੀਤੀ ਜਾਂਦੀ ਹੈ।
2. ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਜ਼ ਸੈੱਟ ਕਰੋ, ਤਾਂ ਜੋ ਤੁਹਾਡਾ ਉਹੀ ਡਾਟਾ ਸ਼ੇਅਰ ਹੋਵੇ, ਜੋ ਤੁਸੀਂ ਕਰਨਾ ਚਾਹੋ ਅਤੇ ਤੁਸੀਂ ਸ਼ੇਅਰਿੰਗ ਆਪਣੀ ਸਹੂਲਤ ਮੁਤਾਬਕ ਕਰ ਸਕੋ।
3. IoT ਉਪਕਰਣ ਬੰਦ ਕਰ ਦੇਵੋ, ਜੇ ਉਹ ਵਰਤੇ ਨਹੀਂ ਜਾ ਰਹੇ (ਖ਼ਾਸ ਤੌਰ 'ਤੇ ਕੈਮਰੇ/ਮਾਈਕ ਵਾਲੇ ਉਪਕਰਣਾਂ ਦਾ ਕੰਮ)।
4. IoT ਉਪਕਰਣ ਇੱਕ ਵੱਖਰੇ "guest" ਨੈੱਟਵਰਕ 'ਤੇ ਰੱਖੋ, ਤਾਂ ਜੋ ਹੈਕ ਹੋਣ ਦੀ ਹਾਲਤ 'ਚ ਤੁਹਾਡਾ ਨਿੱਜੀ ਨੈੱਟਵਰਕ ਸੁਰੱਖਿਅਤ ਰਹੇ।

ਕੀ ਤੁਸੀਂ ਜਾਣਦੇ ਹੋ? 42% ਨੌਜਵਾਨਾਂ ਨੂੰ ਇੰਟਰਨੈੱਟ 'ਤੇ ਧੱਕੇਸ਼ਾਹੀ ਦਾ ਸਾਹਮਣਾ ਕਰਨਾ ਪੈਂਦਾ ਹੈ। ਇਹ ਕਈ ਤਰ੍ਹਾਂ ਨਾਲ ਹੋ ਸਕਦੀ ਹੈ ਅਤੇ ਇਸ ਦਾ ਅਸਰ ਸਿਰਫ਼ ਨੌਜਵਾਨਾਂ 'ਤੇ ਹੀ ਨਹੀਂ ਪੈਂਦਾ।

ਇਨ੍ਹਾਂ ਚਾਰ ਨੁਕਤਿਆਂ ਨਾਲ ਇੰਟਰਨੈੱਟ 'ਤੇ ਧੱਕੇਸ਼ਾਹੀ (cyberbullying) ਤੋਂ ਬਚੋ:

1. **ਜੋ ਵੀ ਤੁਸੀਂ ਔਨਲਾਈਨ ਕਰ ਰਹੇ ਹੋ,** ਉਸ ਨੂੰ ਛੱਡ ਕੇ ਤੁਰੰਤ ਉੱਥੋਂ ਬਾਹਰ ਆ ਜਾਓ, ਬਹਿਸਬਾਜ਼ੀ ਨਾਲ ਗੜਬੜੀ ਵਧ ਸਕਦੀ ਹੈ।
2. **ਸਾਰੇ ਸੁਨੇਹੇ ਬਲੌਕ ਕਰ ਦੇਵੋ,** ਜੇ ਤੁਸੀਂ ਕਰ ਸਕਦੇ ਹੋ, ਅਤੇ/ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਮੰਚ ਰਾਹੀਂ ਉਸ ਵਿਅਕਤੀ ਬਾਰੇ ਰਿਪੋਰਟ/ਉਸ ਨੂੰ ਬਲੌਕ ਕਰੋ।
3. **ਸੁਨੇਹੇ ਰਿਕਾਰਡ ਕਰੋ,** ਜੇ ਬਾਅਦ 'ਚ ਕਿਸੇ ਜਾਂਚ ਲਈ ਲੋੜ ਹੋਵੇ ਤਾਂ ਇਹ ਸਬੂਤ ਬਚਾਉਣ ਲਈ ਸਕ੍ਰੀਨ ਸ਼ਾਟ ਲਵੋ।
4. **ਕਿਸੇ ਨਾਲ ਗੱਲ ਕਰੋ** ਅਤੇ ਅਗਲੇਰੀ ਕਾਰਵਾਈ ਬਾਰੇ ਫ਼ੈਸਲਾ ਲਵੋ। ਜੇ ਤੁਸੀਂ ਉਸ ਸਮੱਸਿਆ 'ਚੋਂ ਨਹੀਂ ਨਿਕਲ ਰਹੇ ਅਤੇ/ਜਾਂ ਤੁਹਾਨੂੰ ਖ਼ਤਰਾ ਮਹਿਸੂਸ ਹੁੰਦਾ ਹੈ, ਤਾਂ ਤੁਹਾਨੂੰ ਆਪਣੀ ਸਥਾਨਕ ਲਾਅ ਇਨਫੋਰਸਮੈਂਟ ਏਜੰਸੀ ਨਾਲ ਸੰਪਰਕ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ।

ਹੋਰ ਸਰੋਤਾਂ ਲਈ telus.com/**riseabove** 'ਤੇ ਜਾਓ।

ਸਿੱਖਿਆ ਵਰਕਸ਼ਾਪ ਦੀ ਬੇਨਤੀ ਕਰਨ ਲਈ **wise@telus.com** 'ਤੇ ਸੰਪਰਕ ਕਰੋ ਜਾਂ telus.com/**wise** 'ਤੇ ਹੋਰ ਜਾਣੋ। **#TELUSWise** ਰਾਹੀਂ ਔਨਲਾਈਨ ਗੱਲਬਾਤ ਵਿਚ ਸ਼ਾਮਲ ਹੋਵੋ।

ਕੈਨੇਡੀਅਨ ਐਸੋਸੀਏਸ਼ਨ ਆਫ਼ ਚੀਫ਼ਸ ਆਫ਼ ਪੁਲਿਸ ਤੋਂ ਸਮਰਥਨ ਪ੍ਰਾਪਤ। TELUS Wise ਹੁਣ ਤੱਕ 3 ਮਿਲੀਅਨ ਤੋਂ ਵੱਧ ਕੈਨੇਡੀਅਨਜ਼ ਦੇ ਮਸਲੇ ਹੱਲ ਕਰ ਚੁੱਕਾ ਹੈ।

TELUS