CYBERSAFE LEGAL

Tip 2: Safe use of Public Wifi

Public wifi is now a standard service that consumers expect whether in a shopping mall, at a restaurant, having a cup of coffee, in a hotel or at the airport.

Free wifi users are not just checking Facebook or posting an Instagram, but often working on the go and accessing work networks and information systems from their remote devices.

Utilising public wifi exposes any information system users to an increased risk of cyberattack – especially if they have no security and no password log ins.

Cyber threats over publicly used wifi can take many forms but there are two main types of attacks through which cyber-criminals can use shared public Wi-Fi to gain access to your personal information and steal your identity. These are when either a hacker is on the same network and uses his skills to take over the network and gain access to the personal information of any of the users or when hackers trick you into joining a false network created by them and access your personal information as soon as you log in.

There is no doubt that the best way to stay safe on a public wifi is NOT to log in to it at all but if you are in desperate need of a wifi connection, there are some tips that can boost your cyber security.

1. **Use a secure public network whenever possible:** An unsecured network can be connected into by anyone within range and without any type of security feature like a password or login. On the other hand, a secured network requires a user to agree to certain terms and conditions, register an account, and/or set a password for access.

2. **Never access personal or financial information:** It is never OK to access personal financial or confidential information when logged in to a public wifi system. When absolutely desperate, hotspot off one of your other devices connected directly to the internet not via wifi.

3. **Take care of the physical security of your mobile devices:** They are like a wallet or a passport – never leave them unattended in a public place. Even if you have accessed a secure network, that does not stop someone form stealing your device or looking at your search history and activity and learning more about the private you.

4. **Use a Virtual Private Network (VPN):** This will allow a user to connect to servers via secure connections. VPN services can encrypt data that you send and receive from a public wifi spot securing your information from access by other users of that public wifi. When it comes to a VPN - paying up is worth it, Free or uber cheap VPNs may not be trustworthy.

5. T**urn off Automatic Connectivity:** Make sure you change the settings on your devices so they do not automatically connect when they are exposed to an open wifi network or Bluetooth connection. Bluetooth connectivity allows various devices to connect with each other, and hackers often look for open Bluetooth signals to try and infiltrate your devices. Even when not using public or shared wifi, it is best practice to leave your file sharing and Bluetooth capabilities turned off until you need them.

6. **Don't shop online when using public Wifi:** This may give cybercriminals complete access to your credit card details, bank accounts and other personal information. This is especially important if you use your mobile devices to access your work information systems.