resolution

your identity at risk, our solutions at work™

WiFi - The Dangers of Connecting to "Free" Public Networks

We've all been there... airport lounge, coffee store, shopping mall, sports event...we want some wifi access to get onto the internet so we open our phone settings and see a "Free Wifi" access point.

It may seem legit, a store name or a business name and it has public access. BUT, are they who they say they are?

Is it real or is it a bogus access point set up by hackers to lure you in and steal your data?

Don't Think It's A Real Problem?

Watch this video showing how easy it is for a hacker to set up a fake wifi address and dupe you. Click on the arrow below...

Public Wifi Hacking

- **Use VPN services on public Wi-Fi networks**
- **Never connect to open unsecured public Wi-Fi**. Even if this is the only Wi-Fi available, do not connect to it. Providing your email address and accepting the terms and conditions of the Wi-Fi owner does not mean you are connecting to a secure Wi-Fi.
- **Only use HTTPS-protected websites**. In the URL address bar, check to ensure the URL uses HTTPS and that the green lock icon is present. Never provide personal confidential information such as passwords, credit card details, or bank information on a website that does not use HTTPS.
- **Turn off auto-connect**. Ensure your mobile devices are not configured to connect to public Wi-Fi that is not password protected automatically.
- **Configure your mobile devices and laptop to "forget" public Wi-Fi network connections**. This prevents you from telling cybercriminals that you have used this public network in the past, making it difficult for them to trick you into connecting to a fake network.
- **Disable Bluetooth auto-discovery**. Cybercriminals listen for Bluetooth signals that they can hack to connect to mobile devices.
- **Be aware of your surroundings.** Do not leave your laptop open on a coffee shop table or leave your mobile device unattended at the charging station. Do not ask someone to "watch" your laptop while ordering a coffee or going to the bathroom. Be aware of people sitting too close who may be listening to your conversations or looking at your screens.
- **Always install the latest updates, patches, and versions.** Ensure your computer and mobile devices have the latest applications, operating systems, network tools, and internal software installed. Ask the IT/support team to verify that your devices are up to date.

More Information? Call Us... 877 308 9167

www.idresolution.net