Public WiFi Best Practices - To Use or Not to Use?

Public WiFi networks are everywhere – in airports, coffee shops, restaurants, malls, and hotels – convenient and easy for anyone to connect to the Internet wherever they are. But it's not always secure, especially if you're conducting financial transactions, checking sensitive email, or need to transmit your sensitive information (CC#, SS#, other Personally Identifiable Information).

Before you log onto any public WiFi, it's important to understand the risks and consider the following best practice tips.

- First, **use your mobile network connection**. Using your wireless hotspot, if included in your mobile plan, is generally more secure than using a public wireless network.
- **Confirm the network name and login procedures** with the appropriate staff before you connect to confirm it's the legitimate one. Cybercriminals can easily create a similarly-named network hoping to fool you into connecting to theirs. Additionally, most hotspots are not secure and do not encrypt the information you send over the Internet, leaving it vulnerable to cybercriminals.
- **Avoid conducting sensitive activities** through public networks – this includes things like shopping, banking, and sensitive work that requires passwords or your credit card and other personal information.
- **Keep software up-to-date**. Install updates for apps and your device's operating system as soon as they're available, or better yet, set up auto-updates so that none get missed. These prevent cybercriminals from being able to take advantage of known vulnerabilities.
- **Use strong passwords and different passwords for different accounts and devices**. Don't choose options that allow your device to remember your passwords. Although it's convenient to store the password, that potentially allows a cybercriminal into your accounts if your device is ever lost or stolen.
- **Disable auto-connect features and always log out**. Turn off features on your computer or mobile devices that allow you to connect automatically to WiFi. Once you've finished using a network or account, you should log out!
- **Ensure your websites are encrypted**. When entering personal information over the Internet, verify that the website is encrypted. Look for https:// on every page, not just the login or welcome page. Where an encrypted option is available, you can add an "s" to the "http" address prefix and force the website to display the encrypted version.

You now know the risks and best practices to stay safe, so enjoy your away time with a better sense of security and peace of mind.

west protect℠