ENTERPRISE INFORMATION SECURITY PROGRAM
Keeping our organization's data safe.

Monthly Security Tips NEWSLETTER

Tacoma

July 2013 Volume 8, Issue 7

Using Wi-Fi: Connect With Care

From the Desk of Paul Federighi, Chief Information Security Officer

If you're traveling this summer, chances are you'll encounter a Wi-Fi hotspot (network) or two.

Wi-Fi in airports, hotels, train stations, coffee shops, and other public places can be convenient, but they're often not secure, and can leave you at risk.

Whether you're entertaining the kids by streaming a video on a tablet, downloading new travel apps on your smartphone or even taking your tablet poolside, there are precautions you should take to make sure your personal information is safe.

First and foremost, connect with care. If you're online through an unsecured network, you should be aware that individuals with malicious intent may have established a Wi-Fi network with the intent to eavesdrop on your connection. This could allow them to steal your credentials, financial information, or other sensitive and personal information. It's also possible that they could infect your system with malware. Any free Wi-Fi should be considered to be "unsecure." Therefore, be cautious about the sites you visit and the information you release.

STOP. THINK. CONNECT.

Here are 6 tips to remember when using Wi-Fi:

- Keep an updated machine. Having the latest security software, operating system, web browser and apps can help protect you from the malware and other threats you may encounter when using Wi-Fi.
- Don't assume that the Wi-Fi connection is secure. Many hotspots don't encrypt the information you send on the Wi-Fi network.
- Do not log into accounts, especially financial accounts, when using public wireless networks.
- Do not log onto sites that don't seem legitimate, (clues could include the URL being misspelled, or not matching the name that you were given by the place of business). It's not uncommon for cybercriminals to set up a Wi-Fi network called "free Wi-Fi" in airports, hotels, and other public places.
- A cellular 3G/4G connection is generally safer than a Wi-Fi connection.
- Consider turning off features on your computer or mobile devices that allow you to automatically connect to Wi-Fi.

For More Information:

For additional information, please visit:

- OnGuardOnline.gov: Tips for Using Public Wi-Fi Networks
- US CERT: Cyber Threats to Mobile Phones
- US CERT: Holiday Traveling with Personal Internet-Enabled Devices
- Microsoft Security: Four Safety Tips for Using Public Wi-Fi

- Sophos: Hot Tips for Securing Your Wi-Fi Network

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY

STOP | THINK | CONNECT™