National Cyber Security Awareness Month
October 2015
OUR SHARED RESPONSIBILITY

Keep an Eye on Public Wi-Fi

Most people use some kind of mobile device, tablet, or laptop on a daily basis, and most of us take advantage of open wireless networks. Whether at work or at school, at your local coffee shop or public library, we take for granted how often we use public Wi-Fi. While these hotspots are convenient and, for some of us, a necessary part of our daily lives, they are certainly not secure. Free Wi-Fi is an easy way for someone to collect your personal data. When you're connected, information sent through websites or mobile apps can be easily hijacked, including passwords. Things like mobile banking, bill-pay, or business transactions are prime targets for network trespassers to sniff out passwords, credit cards, and other personal information. However, there are ways to protect your information from potential intruders.

Hotspot Precautions for Personal Devices

- Before connecting, verify the name of the free network you're about to use with any available staff.
- When using Windows, disable file sharing and identify the Wi-Fi connection as "public." Go to **Control Panel>Network and Sharing Center>Change Advanced Sharing Settings.** Under the Public heading, turn off the file sharing toggle.
- Turn **ON** the Windows Firewall if it isn't already activated. Go to **Control Panel>Windows Firewall.** Under the Public settings, turn OFF Network Discovery, file and printer sharing, and Public folder sharing.
- In Mac, open **System Preferences>Sharing**. Uncheck **Filesharing** and remove all public home folder sharing options.
- **Check for https** (the **S** means "secure") in the browser bar of every webpage you visit, **not just the sign in page.** Browser extensions like *HTTPS Everywhere* ensure that **https** is being used.
- **Install updates as soon as they're available.** Make sure all updates are done at home, on a secure private network.
- Don't assume your apps are automatically secure, updated, or using **https**. It's safer to assume they are NOT. For online banking or financial transactions, use the company's website rather than their mobile app to ensure the transmission is encrypted. Make sure to validate the correct spelling of the website address.
- **Use two-factor authentication** when utilizing a service that supports it, such as Gmail, Twitter, and Facebook. This gives you an added layer of protection in case someone manages to crack your password.
- **Use a Virtual Private Network (VPN)** to secure your documents and browsing sessions. VPNs encrypt traffic between the device and the server, making it much more difficult for an intruder to get to your data. Private VPN options like SecurityKISS, CyberGhost, and Disconnect.me are available for personal use.

National Cyber Security Awareness Month
October 2015
OUR SHARED RESPONSIBILITY

Keep an Eye on Public Wi-Fi

Wireless Security for Government Equipment

Government furnished equipment (GFE) already has several security features enabled. However, there are additional steps you can take when using GFE outside of the office.

- **Make it a habit to shut down your laptop when not in use to enable full disk encryption.**
- **Don't allow your computer to automatically join the nearest network. Manually select the hotspot each time you connect. Make sure your IHS VPN is being used any time you're connected to a network not personally owned by you.**
- **NEVER work on sensitive material when using an unsecure connection. Make sure you have prior approval to work on sensitive information outside of the office.**

- **Turn off bluetooth and wireless capabilities when not in use.**
- **A laptop's wireless connection isn't automatically disabled when you connect with a LAN cable (or Ethernet cable). Make sure to turn OFF the wireless capability when reconnecting to an Ethernet cable or port. Always be aware of whether you're connected to a wired or wireless network, and only use ONE connection at a time.**
- **NEVER leave your laptop or handheld device unattended - not even for a moment.**
- **Be cautious when establishing a wireless connection through a non-secure environment (e.g., at a hotel or in-flight). Use a VPN connection whenever possible. If you need VPN access, contact your local IT staff.**

For questions or assistance regarding Wi-Fi Security, contact HQ_OITSecurity@ihs.gov.