Security Tips

Using Public Wireless Networks

May 2012

Tips for Using Public Wireless Networks

Public wireless networks are located in coffee shops, libraries, airports, hotels, universities, and other public places. They allow access to the internet through a shared network. While convenient, they are often not secure.

Is this hotspot secure?

- If a hotspot doesn't require a password, it's not secure.
- If a hotspot asks for a password through your browser simply to grant access, or it asks for a WEP password, it's best to assume it's not secure.
- You can be confident a hotspot is secure only if you are asked to provide a WPA password. If you're not sure, the information you enter could be at risk. WPA2 is more secure.

How to Identify an Encrypted Website

To determine if a website is encrypted, look for **https** at the beginning of the web address (the "s" is for secure), and a **lock icon** at the top or bottom of your browser window.

Public Wireless Networks

Most Wi-Fi hotspots **don't** encrypt the information you send over the internet and are **not** secure. If you use an unsecured network to log in to an unencrypted site – or a site that uses encryption only on the sign-in page – other users on the network can see what you see and what you send.

Protect Your Information

- When using a Wi-Fi hotspot, only log in or send personal information to websites that you know are fully encrypted.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Do not use the same password on different websites.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN).

