i.t.solutions
uahuntsville

CONNECTING TO PUBLIC WI-FI SECURELY

AUDIENCE

This document is for UAHunstville faculty, staff, and students.

ACCESSING A PUBLIC WIRELESS HOTSPOT SECURELY

Follow these recommendations to be safe when connecting to public wireless.

- Be careful when connecting in a coffee shop or hotel. Make sure that the Service Set Identifier (SSID) which is the public wireless LAN name your computer recognizes when connecting is the one that the actual coffee shop or hotel is broadcasting. It is easy for a hacker to name an SSID similar to the legitimate one. For example a hacker might call his SSID HolidayAP whereas the hotel might call theirs HolidayInn. If it in doubt ask the concierge or barista for the Access Point SSID name. You don't want to connect to a rogue, hacker controlled, access point.
- Always try to connect to a secured Wi-Fi network. These are displayed with a lock and will prompt for a password to connect. WPA2 is the most secure Wi-Fi network type to connect to.

  Note: Most coffee shops and hotels have unsecured Wi-Fi networks.

- Use your company VPN, if available, or a free third-party VPN product like Hotspot Shield. This will create a virtual private network between your machine and the network you are connecting to. This tunnel is secured against anyone such as hackers, snoopers, or bots who may try to intercept your Web session while connected to a public hotspot.

  Note: Using a VPN may cause some slow down in your web surfing or downloading.

- Avoid storing your username and password for any site, especially those that are access points to financial information. When prompted by your browser to remember a password, select Never for This Site.

If you want the convenience of stored passwords and form fillers, use a utility like LastPass to manage passwords. LastPass encrypts passwords and form information for secure web browsing.

- Avoid bill paying, accessing your bank account, or using your credit card when connected to public Wi-Fi. It is safer to access the bank from your home computer with a wired or secured wireless connection.
- With Windows 7, when you connect to a new network or Wi-Fi hotspot, the Set Network Location window allows you to apply appropriate settings according to the type of network you are accessing. Select the option Public Network when connecting to any public Wi-Fi hotspot. This adds an extra layer of security by blocking file and print sharing and turning off network discovery.

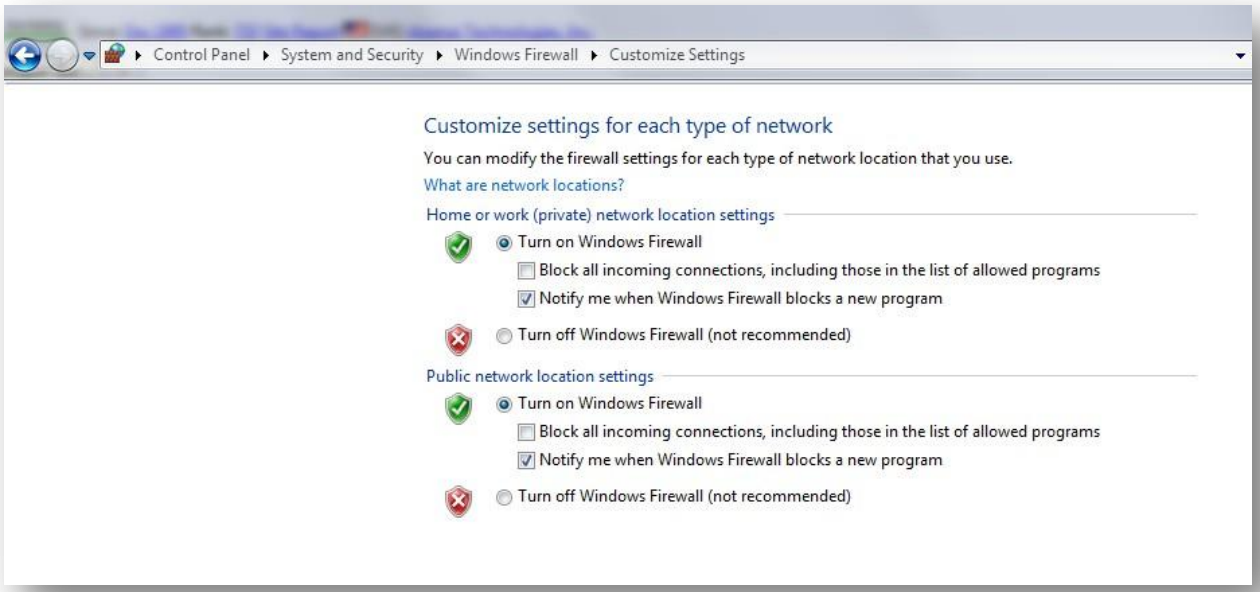
Note: You should also turn off file sharing and network discovery settings on other operating systems like MAC OSX.

- Harden your system by having an up-to-date Anti-Virus software package. Make sure it is updating to the latest virus definitions.

- If you system contains sensitive data, then consider using TrueCrypt, a free open source on-the-fly encryption software.
- If possible, use HTTPS and SSL for connection to sensitive websites like banks and email. Quite a few websites now use HTTPS and SSL to secure and encrypt your data communications For example; you can access Gmail via http://www.gmail.com or https://www.gmail.com. The latter is a more secure option.

  Example: When you access a site with HTTPS a padlock will display indicating that the connection is secure. Notice the difference between an unsecure and secure site.

- Make sure that you have the Windows Firewall turned on. Never attempt to turn it off in a public Wi-Fi. It will only take a few seconds to get hacked or infected with some type of malware.



- Make sure that you have all Microsoft Windows Updates installed. Also consider updating all other programs like Adobe Reader, Adobe Flash Players, ITunes, and QuickTime etc. These can all provide a way to break into your system.

- Turn off your wireless card (Wi-Fi) when you are not using it. .