WiFi Dos and Don’ts

Protect your computer, tablet and phone before joining a WiFi network by following these dos and don’ts.

Dos

- Before joining a network, ask an employee the official name of the business’ WiFi. Be sure you are connected to the right WiFi spot and not a rogue location.

- Select a secure WiFi network that requires a password to connect. A secure connection is indicated by an icon that looks like a lock.

- Stay up-to-date with your antivirus software, applications, and your operating system’s security patches, especially before traveling.

- Connect only to secure websites when accessing sensitive information. Secure websites are indicated in your browser by an icon shaped like a lock or https in the address bar.

- Use encryption software to protect confidential data on your desktop or laptop.

- Reset your WiFi connection after moving to a new location (turn WiFi off and back on again to reset the connections).

- Turn WiFi off when not in use.

Don’ts

- Do NOT connect to an unknown WiFi network.

- Do NOT pay bills, access bank accounts, or make purchases over public WiFi.

- In Windows 7, do NOT select anything other than Public Network when setting a network location. Public Network blocks file and print sharing and turns off network discovery. This can also be disabled in MAC OS X.

- Avoid using wireless connections when wired connections are readily available.

- Avoid using wireless in crowded areas wherever possible.

- Avoid using streaming media, Skype, or other high bandwidth applications over shared wireless connections.

- Do NOT use WiFi hotspot features of your cell phone or set up wireless routers, printers, or hotspot appliances in areas where wireless services are available.