The following are safe practices when connecting to a public wireless hotspot:

- Ask the concierge or barista the official name of the establishment’s WiFi so that you are certain 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
- Faculty/Staff should use a Virtual Private Network connection (VPN) to connect back to the UA Network when off-campus
- Stay up-to-date with your antivirus software, applications, and your operating system’s security patches
- Connect only to secure websites when accessing sensitive information. Secure Web sites 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
WiFi Security Things Not to Do

Take the following precautions when connecting to a public WiFi hotspot:

- Do NOT connect to an unknown WiFi network
- Do NOT pay bills, access bank accounts, or make online 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