

Is Wireless Networking Safe?



A wireless network sends signals through the air instead of over a wire. Because of this others can easily intercept the information you are sending when using a “unsecured” public or open access wireless connection, such as “UAPublic”. Imagine your phone line at home. If you were in the middle of a call, at any time someone else could pick up another receiver in the house and listen to what you are saying without your knowledge. Wireless access has the same issue. If your wireless router or access point is not secure anybody within its range can use it. This is like having a phone receiver sitting outside on your front lawn. Anyone can wander by, listen to what you say, or make calls from your phone. The same rules apply for “public” or “open” access points. Anyone within range of your wireless device can easily monitor everything you do over your wireless connection!

What you can do to protect yourself

When possible you should **use a secure wireless connection** such as “UAWiFi” which is configured to use WPA2 to secure your internet traffic and PEAP which encrypts your username and password during the authentication process.

There are times when you may find yourself in a situation where you have a need to use open public access wireless. Be aware of what information you are transmitting. We strongly recommend that you limit what you do to simple browsing and checking webmail.

Additionally if you have a wireless router at home or apartment, you should to configure it to use encryption and MAC filtering. SSID broadcasting should also be disabled and the administrative password changed from the default. More information about securing home wireless is available on the other side of this document.

When Browsing the Internet while using open wireless access:

Always assume that (almost) ANYTHING that you type or any info that appears on your screen while you're using an “open” wireless connection can be seen by others nearby. If you are accessing a page that requires a login and password, or if you are entering ANY personal data (credit card, SSN, etc) make sure that you are on a secure site. That's easy enough -- just check that the web address begins with **https** instead of the usual **http** -- and your information will be safely encrypted before transmission. As long as you're on a page with an address that begins with https, the data you send and receive is protected from sniffers and snoopers.

When checking email while using open wireless access:

Use the UA and/or your ISP's webmail, as long as it supports a secure connection, and most do. You'll need to check what the exact URL is for your ISP, but do it before you wander off to the coffee shop, and add it to your bookmarks/favorites, so you don't have to remember it. Check that both when logging in to your email, and when reading your email, there is a small padlock icon on the bottom bar of your browser. If there is, then you are safe to read your email from prying eyes.

BE PARANOID when accessing the Internet while using open “unsecured” wireless access!

More Information on  is available at uawifi.arizona.edu





10 Steps to Secure Your Home Wireless

The recommendations below summarize the steps you should take to improve the security of your home wireless network. Details on how to implement the following steps will be found in the instructions specific to your wireless router.

1. **Change Default Administrator Passwords (and Usernames)** - At the core of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately.
2. **Turn on (Compatible) Encryption** - All Wi-Fi equipment supports some form of encryption. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Make sure you pick the strongest form of encryption that works with your wireless network. This encryption type (WEP, WPA, WPA2, etc) must be compatible with all the Wi-Fi devices that you want to connect to your wireless.
3. **Change the Default SSID** - Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "Linksys". While knowing the SSID alone does not allow others to break into your network, it's a start. More importantly, when someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring your wireless network.
4. **Enable MAC Address Filtering** - Each piece of Wi-Fi gear possesses a unique identifier called the physical address or MAC address. Access points and routers keep track of the MAC addresses of all devices that connect to them. You can restrict your wireless network to only allow devices on your network for you have entered the MAC address.
5. **Disable SSID Broadcast** - In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature is unnecessary, and it increases the likelihood someone will try to log in to your home network.
6. **Do Not Auto-Connect to Open Wi-Fi Networks** - Connecting to an open Wi-Fi network such as a free wireless hotspot or your neighbor's router exposes your computer to security risks. Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying you (the user). This setting should be disabled except in temporary situations.
7. **Assign Static IP Addresses to Devices** - Most home networkers gravitate toward using dynamic IP addresses. DHCP technology is indeed easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from your network's DHCP pool. Turn off DHCP on the router or access point, set a fixed IP address range instead, and then configure each connected device to match. Use a private IP address range (like 10.0.0.x) to prevent computers from being directly reached from the Internet.
8. **Enable Firewalls On Each Computer and the Router** - Modern network routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on. For extra protection, consider installing and running personal firewall software on each computer connected to the router.
9. **Position the Router or Access Point Safely** - Wi-Fi signals normally reach to the exterior of a home. A small amount of signal leakage outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach through neighboring homes and into streets, for example. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the center of the home rather than near windows to minimize leakage.
10. **Turn Off the Network During Extended Periods of Non-Use** - The ultimate in wireless security measures, shutting down your network will most certainly prevent outside hackers from breaking in! While impractical to turn off and on the devices frequently, at least consider doing so during travel or extended periods offline. Computer disk drives have been known to suffer from power cycle wear-and-tear, but this is a secondary concern for broadband modems and routers.