

Home Wireless Setup:

The question has come up several times, "How do I setup my home wireless network to be secure?" Some thoughts have been compiled below on how to best fortify (notice we aren't securing) your wireless connection at home.

Basic definitions (most taken in part from <http://www.wikipedia.org>):

- Wireless networking: in general when we talk about wireless networking we are talking about the Radio Frequency (RF) communication that occurs according to the 802.11 IEEE standards. These transmissions generally take place in the 2.4GHz radio frequency (RF) spectrum (known as 802.11b or 802.11g,) however, could also take place in the 5GHz RF spectrum (known as 802.11a.)
- 802.11a: uses the 5GHz RF spectrum. This is advantageous because there are fewer devices to interfere with it. The downside is the support, price and distance that can be covered are less than the 802.11b/g standards.
- 802.11b: the standard that propelled wireless networking to take off! It uses the 2.4GHz spectrum and there are several devices that can interfere with this such as your 2.4GHz cordless phones, microwave ovens, or baby monitors. It is the most commonly used standard and can cover distance beyond that of 802.11a.
- 802.11g: basically a speed increase over the 802.11b standard. It uses the 2.4GHz spectrum and there are several devices that can interfere with this such as your 2.4GHz cordless phones, microwave ovens, or baby monitors. It is backwards compatible with the 802.11b standard and can cover distance beyond that of 802.11a.
- 802.11n: this is a new standard for which the specifications have not been finalized. Despite this fact many companies are offering Pre-N products with the promise that you'll be able to upgrade them once the standard has been ratified.
- AP or WAP: AP stands for Access Point, WAP standard for Wireless Access Point. This is a device that connects wireless communication devices together to form a wireless network.
- Wireless Network Interface Card: a WNIC is a network card which connects your computer to a radio-based computer network. The WNIC allows your computer to connect to the WAP. A WNIC can be PCI, USB, PCMCIA or mini-PCI based.

Hardware Recommendations:

Because of the variety of brands and models of WAPs and WNICs it's impossible to make a recommendation. At the consumer level you generally see these names: Linksys (owned by Cisco), Netgear, Belkin and D-Link. There are others that we've seen more of lately (Buffalo Technology) etc. If you look for deals or rebates you should expect to spend ~\$0 - \$100 dollars for a WAP and \$0 - \$100 for the WNIC. If you buy the "router" version with switch ports the price may vary on the AP and these features may be helpful if you are building a network in which you need to support both wired and wireless devices. We make no warranties about any of the brands above. For reviews on wireless equipment check out:

- <http://www.tomsnetworking.com>
- Amazon reviews
- Search Google for wireless access point reviews

Configuration Recommendations:

- Ideally your WAP & WNIC should support 802.11abg - yes all three standards. Using the 802.11a standard when possible will help mitigate the effects of devices that interfere with with 802.11b/g only WAPs.
- Steer clear of Pre-N devices – you have been warned. The standard has not been finalized and may change before it is ratified. For that reason we (and we are not alone) are recommending you do not purchase these products.
- Your WAP & WNIC should support at a minimum WPA-PSK. If you can find support for WPA2 (WPA2 being the more secure option) that is preferable. Don't bother with an AP or WNIC if it does not support one of these. When you setup WPA or WPA2 you should be asked to use TKIP or AES. AES provides a higher level of security and should be used when possible, but some operating systems and WNICs won't support it – in which case you will select TKIP. You may have to go through trial an error to verify AES does not work. WEP can be broken in less than 10 minutes by monkeys and should not be used.
- Your WPA or WPA2 password or key should be 24+ characters long and make use of upper and lower case letters, numbers and special characters. Everything that make a password hard to remember – right? The longer password (or Pre-shared Key = PSK) the better, the more upper and lower case letters, numbers and special characters the better too. If you want to make the key this long write it down so you don't have to remember it. Please do not use the WEP key used for “uhosp1” that is over 5 years old.
- Change the default SSID or name of your wireless network to something that doesn't identify you or your home (don't use your address, your family name, etc.) Something generic that indicates your mildly interested in fortifying your wireless network such as “home” or “closed” will do nicely and deter most people looking for access points to connect to.
- Don't broadcast the SSID or name of your wireless network if possible. This feature is supported by every device created in the past 5 years or so and while it provides no actual protection (security by obscurity) it may give someone a reason to pass your AP by in favor of an easier target.

What wireless traffic should be encrypted?

- Transmissions between the UUHSC and your home computer – YES PLEASE!
 - By making a connection to the UUHSC you are essentially putting your computer back on the UUHSC network from a remote location and all reasonable efforts should be made to protect that connection.
- Your TIVO video streams – NO, it's probably not important enough to encrypt.
- A PSP “Wipeout Pure” session between your children – NO, it's probably not important enough to encrypt.
- When I log into my bank website – even though they use SSL/HTTPS to encrypt it at my web browser? YES!
 - Anytime you put a username and password/pin into a web application for work or personal use that leads to the access of personal information (yours or someone else's) you should take all reasonable efforts to protect that data and the connection made to that data.

If you plan to transmit any data that maybe sensitive over a wireless network you should take reasonable efforts to ensure the data you transmit is protected. Otherwise you need to understand that anything you send may be viewable or intercepted by someone.

What if I'm on the road?

Let's say you're in Las Vegas waiting for a flight back to SLC and you grab an iced caramel macchiato from Starbucks, and while you're there decide to try your luck accessing a "hotspot" wireless network. What can you expect?

1. It is very likely that ANYTHING you send is being viewed by someone else.
2. Even if you are connecting to an SSL web site you should be wary...check that the certificate appears to be valid and if something looks out of place don't enter your credentials.

Can I connect to anything and be safe?

- Exercise caution: do you really need to access the application from a "hotspot" or are you just killing time?
- Did you check the certificate for the application before you put in your username and password?
- Did you initiate a VPN connection before connecting to a UUHSC resource?
- There is no silver bullet to securing a wireless connection while on the road, but by taking a few precautions you can reduce the risk.
- If your Outlook client has been configured properly you should be able to securely access your e-mail – but again exercise caution.

Some recommended wireless resources:

- A wireless security FAQ guide can be found here:
http://www.tomsnetworking.com/2006/06/30/wireless_faq_security/
- A wireless networking FAQ guide can be found here:
http://www.tomsnetworking.com/2006/06/26/wireless_faq_setup_and_configuration/
- A wireless need to know guide can be found here:
http://www.tomsnetworking.com/2006/02/27/wireless_networking_ntk_2006/