

## Wireless

### Wireless Security

When you are physically connected to Hamline's network via a network cable, your computer's network communication is restricted to the cable that links your computer to the network jack in the wall. You can be reasonably assured that your communication is safe, as the only way to "sniff" your information is to have physical access to the cables that connect your computer to its destination.

In a wireless world, it is completely the opposite. Since your computer communicates with the network through the air, it is much easier for someone to "sniff" that information, and piece it back together to find your usernames, passwords, credit card numbers, etc. Any sort of information that is sent through the air unencrypted can be seen with the appropriate tools.

As I hinted in the previous paragraph, the solution to this problem is using encryption such that even if someone does listen to your computer's conversations, all the information being sent is encrypted, and the person or device listening would have to know the encryption key to be able to decipher the data. So, in the wireless world, we have a few different encryption options:

- No encryption - no key required, but obviously insecure
- Wired Equivalent Privacy (WEP) encryption - uses a pre-set 26 digit key, somewhat secure
- Wifi Protected Access (WPA) encryption - the wireless transmitter and your computer periodically negotiate a key, very secure

The methods are listed in order of their effectiveness. Obviously, not using encryption is very ineffective, but it is very insecure. Using WEP adds a layer of encryption, but since that key is stays the same, and it's shared among everyone using the wireless access point, a hacker just needs to get the key to be able to decrypt the data. The most secure option, WPA, uses dynamic keys that are negotiated between your computer, and the wireless transmitter, so this is the most secure, as each computer gets its own key, and that key changes periodically. However, WPA also requires certain hardware, drivers, and adds a layer of potential problems. Therefore, it is somewhat hard to manage in a large environment.

That being said, probably the easiest to manage, and most secure option wasn't listed: SSL. Even before wireless hit its peak, secure sockets layer (SSL) was used widely through the internet. As we all know, the internet isn't secure, so SSL was created for those sites that wanted to make sure the information being transferred couldn't be intercepted by a hacker. This allows your online banking, credit card transactions, loan, and other sites that ask you to transmit personal/confidential information to operate securely.

This same technology can be used to transfer information over the wireless network securely, as even if someone is able to intercept the data, they aren't going to be able to decrypt it. If you are using a wireless network, it's important to make sure that your connection is secure when you are transferring any private information such as:

- usernames/passwords
- credit card info
- social security numbers
- bank account information

The only downfall of this is that many applications aren't built with this technology, as in the past it's been primarily a solution for web sites. Other applications, such as internal authentication programs, don't have that type of encryption builtin, as it was designed to operate on an internal network, which normally cannot be sniffed by other people.

In the initial deployment of wireless on campus, we won't be implementing any security, so it's important that any sites you enter any confidential information that you make sure it's using SSL encryption. When you type in your username and password to log into the wireless network, that is encrypted, as is accessing groupwise and netmail webaccess. These applications should be safe from someone sniffing the traffic.

We will continue to try to broaden the services available over the wireless network in a safe manner. Please continue to watch the forum for further developments.

[Help Desk Support](#)  
Hamline University

**Need more help?** Please contact the [Help Desk by email](#) or by phone at **651-523.2220**