WIRELESS

**Each of us is the solution to securing your wireless.**

**Wireless computing** is flexible and convenient. Having the ability to move freely while computing provides great opportunities for each of us both in the work environment and at home. However, if you are not careful, it unknowingly provides the same opportunities to others. Your wireless network must be secured properly so that criminals cannot access your files and information or engage in illegal activity on your network while disguised as you.

**Secure your home wireless network**

Properly securing your home wireless network is critical to securing your information and your reputation. Don’t be an easy victim. Here are some ideas that work together to keep your information and home network safe. The more solutions you apply, the stronger your defense will be.

1. **Change the default password and logon name for your router.** [more...](http://www.montgomerycollege.edu/cybersecurity/homewire.html#home1)
2. **Enable the strongest encryption that your equipment will support.** [more...](http://www.montgomerycollege.edu/cybersecurity/homewire.html#home2)
3. **Disable SSID broadcasting and change the SSID.** [more...](http://www.montgomerycollege.edu/cybersecurity/homewire.html#home3)
4. **Restrict the devices that can connect to your wireless network.** [more...](http://www.montgomerycollege.edu/cybersecurity/homewire.html#home4)
5. **Turn off your wireless router when you know you won't be using it.** [more...](http://www.montgomerycollege.edu/cybersecurity/homewire.html#home5)

**Be careful computing in Wi-Fi hotspots**

When you are on the move and computing in a Wi-Fi hotspot provided in a coffee shop, bookstore, campus, or airport you need to be wary of hackers waiting to access your network or steal your information. Most public wi-fi hotspots do not provide security protection for their users. Here are some ideas to make those hotspots safer. As mentioned in setting up a home wireless network, these ideas work together to build a stronger defense.

1. **Hackers are able to capture network traffic with little effort and chance of being caught.** Make sure that sensitive data is encrypted during transport and not sent in clear-text. [more...](http://www.montgomerycollege.edu/cybersecurity/wifi.html)
2. **Configure your laptop to allow only connections to approved access points.**
	1. Disable Automatic Wireless connections.
	2. Verify that you are connecting to the appropriate SSID.
	3. Disable ad-hoc capability which allows other wireless users to connect directly to your laptop.
	4. Disable your wireless card when not in use.
3. **Disable File and Printer Sharing** to prevent disclosure of your shared files and to reduce the chances of your computer being compromised. You can always turn it back on when you return to your home network.
	1. Disable the service or restrict access with your personal firewall.
4. **Use a personal firewall.**
5. **Use anti-virus and anti-spyware protection software.**
6. **Consistently apply patches.** Keep all applications, including your operating system up to date.