Wireless technology (often called Wi-Fi) makes it simple to connect to the Internet. However, this technology can also make it easier for cyber attackers to monitor and steal your information.

What is Wi-Fi?
When the Internet first became popular, the only way you could connect to a network was to do so physically. This meant you had to manually connect a network cable to your computer or laptop. While inconvenient for people, physical cables helped protect our organization. They allowed us to control who had access to our networks. However, people needed a simpler and faster way to connect to networks, one that did not require physical cables. As a result, a new wireless technology was created in the 1990s Fi works by allowing a computer to connect to any network without the need of a cable. To use Wi-Fi, you simply select a wireless network from your computer or mobile device and connect. In some cases, you may also be asked for a login or password. However, you need to be aware of the unique risks that come with Wi-Fi networks.

What information can be monitored on Wi-Fi?
Everything you do over a Wi-Fi network can potentially be monitored. Wireless is like a conversation; without precautions, anyone close to you can listen in on what is said. In addition to eavesdropping, attackers can sometimes use your unsecured connection to compromise your computer or online accounts. As a result, you should encrypt all online activity whenever you connect via Wi-Fi. This is especially important on public Wi-Fi networks, since their security cannot be trusted.

How can you connect safely to a Wi-Fi Network?
To connect to a wireless network, you must first select the network you want to connect to. There are often multiple networks to choose from in crowded or public places. However, always be careful which networks you connect to. Cyber criminals can create counterfeit or fake wireless networks designed to harm or monitor everything you do. To protect yourself, always be sure you are joining a trusted Wi-Fi network. Otherwise, you have to assume that devices on non-trusted networks can scan, probe or hack any other device connected to that network. By making sure you only connect to trusted wireless networks, you protect yourself against these and other attacks.

When working remotely, use the University's VPN (Virtual Private Network) to connect when using a wireless network other than the University's. The University's VPN secures your network connection by building a virtual tunnel between your computer and the UChicago network. It is especially useful if you wish to use fileshares or other services restricted to the UChicago network. The University's VPN will require your CNET ID and password.

Finally, make sure your laptop and mobile devices are using is the most current version and has the latest patches and software. In addition, be sure your encryption software is installed and you have anti-virus running on your laptop.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about the University or downloaded malware contact the BSD-ISO team via the following phone numbers or e-mail addresses:

Plamen Martinov, BSD Chief Information Security Officer	O: 773-834-1714	pmartinov@bsd.uchicago.edu
Kim Cooke, IT Security and Compliance Analyst	O: 773-834-7897	kcooke3@bsd.uchicago.edu

You may also send an e-mail to the BSD Security mailbox: security@bsd.uchicago.edu
Visit the BSD-ISO website: http://security.bsd.uchicago.edu