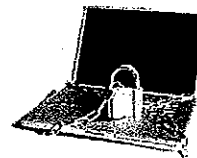



WI-FI SECURITY ADVICE



You're at the airport, anxiously awaiting your flight. You have some time to kill so you power up your laptop computer and connect to the airport's Wi-Fi to check your office emails or perhaps to do some online financial transactions.

Stop!  Before you do this, consider: odds are there is a hacker nearby, with his own laptop, attempting to "eavesdrop" on your computer to obtain personal data that could provide access to your money or even to your credit union's sensitive information.

Remember also the connection between your laptop and the attacker's runs both ways. While he is taking information from you, you may be unknowingly downloading viruses, worms, and other malware from him.

There are over 68,000 Wi-Fi "hot spots" in the U.S., at airports, coffee shops, hotels, bookstores and other locations where hundreds of people pass through every day. According to the FBI Cyber Division, many have secure networks but some do not.

What can you do to protect yourself?

The best advice is, don't connect to an unknown Wi-Fi network.

If you do have to connect, there are other precautions you can take to decrease the risk:

- Make sure your laptop security is up to date, with current versions of your operating system, firewalls and antivirus and antispyware software.
- Do not conduct financial transactions or instant messaging.
- Change the default setting on your laptop so you have to manually select the Wi-Fi network you're connecting to.
- Turn off your laptop's Wi-Fi capabilities when you're not using them.

The most important thing is to be aware of possible threats around you and take necessary steps to protect yourself, your information and the information of your credit union.