Information Security Awareness Program

PUBLIC WI-FI SECURITY RISKS

The main threat to free Wi-Fi security is the ability for the hacker to position himself between you and the connection point. So instead of talking directly with the hotspot, you're sending your information to the hacker, who then relays it on.

While working in this setup, the hacker has access to the information that you're sending out on the Internet: important emails, credit card information and even security credentials.

Summary: What to do?

1. Do not use Public Wi-Fi for Government of the Northwest (GNWT) Territories business.

2. If you **must** use Public Wi-Fi for GNWT business, use a secure connection that requires a user name and password.

3. A virtual private network (VPN) is an example of a secure connection to the GNWT's network.

MALWARE

Hackers can also use an unsecured Wi-Fi connection to distribute malware. If you allow file-sharing across a network, the hacker can easily plant infected software on your computer. Some ingenious hackers have even managed to hack the connection point itself, causing a pop-up window to appear during the connection process offering an upgrade to a piece of popular software. Clicking the window installs the malware.

Internet security issues and public Wi-Fi risks are on the rise. However, this doesn't mean that you can't be *aware* of the risks and take mitigating measures. The vast majority of hackers are simply going after easy targets, and taking a few precautions will help to keep your information safe.

The easiest way to avoid the risk is to *not* use public Wi-Fi. Unfortunately, often there is a business need to connect. What are some solutions to this problem?

WHAT CAN YOU DO TO AVOID THE RISK?

Use a VPN

A virtual private network (VPN) connection is a must when connecting to government business through an unsecured connection, like a Wi-Fi hotspot. Even if a hacker manages to position himself in the middle of your connection, the data will be strongly encrypted. Since most hackers are after an easy target, they'll likely discard stolen information rather than put it through a lengthy decryption process.

Visit Secure Sites

Enable the "Always Use HTTPS" option on websites that you visit frequently, or that require you to enter some kind of credentials. The information that you send over these sites becomes encrypted and protected. Remember, hackers understand how people reuse passwords, so your username and password for some forum may be the same as it is for your bank or corporate network, and sending these credentials in an unencrypted manner could open the door to getting hacked.

Turn Off Sharing

When connecting to the Internet at a public place, you can turn off sharing from the system preferences or Control Panel, depending on your OS, or let Windows turn it off for you by choosing the "Public" option the first time you connect to a new, unsecured network.

Disable Autoconnect, and Keep Wi-Fi Off When You Don't Need It

Even if you haven't actively connected to a network, the Wi-Fi hardware in your computer is still transmitting data between networks within range. If you're just using your device to work on a Word or Excel document, keep your Wi-Fi off. As a bonus, you'll also save on the battery life.