CYBER SECURITY
newsletter

WI-FI SECURITY

Problem

When the Internet first became popular, the only way you could connect to it was physically. This meant you had to manually take a cable (often an Ethernet cable) and connect it to your computer or laptop. This cable then connected you to a local network which connected to the Internet. While inconvenient for the end user, physical cables helped protect our organization. They allowed us to control who had and did not have access to our networks.

However, users 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 called IEEE 802.11; or more commonly known as Wi-Fi. Wi-Fi works by allowing a computer to connect to any network without the need of a cable. This makes accessing the Internet much simpler as you simply select a wireless network for your computer and connect. In some cases, you may also be asked for a login or password. Unfortunately, Wi-Fi networks come with their own unique risks which you need to be aware of.

Solution

Here are three simple steps to remember when using Wi-Fi technology.

1. Monitoring: First, remember that when you connect to a wireless network that anyone else can intercept and monitor your activity. All your online activity is simply converted into radio signals that are broadcast into the open air. These signals can then be intercepted by anyone close enough to you. This is especially true in public places such as hotels, airports, cafes, or conferences. Since anyone can intercept your Wi-Fi signals, just about anything you do online can be monitored.

The best way to protect yourself is encrypt all your online activities. Make sure you visit websites using HTTPS, the encryption standard for browsing. For email make sure your email client is configured to connect to the mail server using encryption. In addition, check to see if you can use a VPN (Virtual Private Network) for remotely connecting back to our organization. For encryption options contact the IT help desk or your information security team.

Wireless Networks

Wireless technology (often called Wi-Fi) makes it simple for you to connect to the Internet. However, this technology can also make it simple for cyber criminals to monitor and steal your information. In this newsletter, we cover the most effective steps in protecting yourself when using wireless networks.

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

Hacking 45 Million Credit Cards

Weak or insecure Wi-Fi networks are one of the simplest ways cyber criminals can bypass our security and break into our organization. This is exactly how criminals were able to break into the multi-billion dollar company TJX, one of the largest apparel companies in the world.

These criminals practiced what is called war-driving. They turned on their laptops and simply drove around their town looking for any organizations that had insecure Wi-Fi networks. They soon found several stores that were insecure. The cyber criminals simply parked their car in the company's parking lot. From there, they were able to break into and join the company's Wi-Fi network and gain access to their internal networks.

Once they had access to the internal networks, they were able to quickly find and hack into many of the organization's confidential servers. They then created accounts and were able to remotely access the company whenever they wanted to for the next 18 months. Over this time, they were able to steal at least 45 million credit cards, all as a result of an insecure Wi-Fi network.

2. Connecting To A Wi-Fi Network: Connecting to a wireless network first begins by selecting the network you want to connect to. In crowded or public places, there is often multiple networks to choose from. However, always be careful which network you are connecting to. Cyber criminals can create counterfeit or fake wireless networks that are designed to harm or monitor everything you do. To protect yourself, always be sure you are joining a trusted Wi-Fi network.

When you are at work, your network administrator will tell you which wireless networks you can join. These networks almost always will require a login and password. You can trust these networks as they are administered by our organization. When you want to connect to Wi-Fi networks in public places (such as hotels or airports) look for posted signs telling you which wireless networks are legitimate and how to join them. By making sure you only connect to trusted wireless networks, you protect yourself against these and other attacks.

3. Installing Your Own Wi-Fi Network: Remember it is against organization policy to install unauthorized Wi-Fi networks within our organization. If you need to add a new Wi-Fi network in one of our facilities, you must get authorization first. All Wi-Fi networks in our organization are required to meet strict security configurations so cyber attackers cannot gain access.

If you are going to install a Wi-Fi wireless network at home, take the following steps to protect yourself.

• Be sure to change the default administrative login and password on your Wi-Fi access point. The simplest way for cyber criminals to hack into any Wi-Fi network is simply scan the entire Internet and log into Wi-Fi access points with default logins and passwords.

• By default, most Wi-Fi networks are open, allowing anyone to join them. Make sure your wireless network requires a login and password to join it. This protects your home network from cyber criminals accessing your computers, or protects you from criminals using your wireless network to attack others.

• By default, most Wi-Fi networks are in the clear, meaning anyone can intercept and monitor your activity. Make sure you enable the latest version of encryption in your Wi-Fi network. This ensures your activities cannot be monitored. Remember, older versions of encryption (such as WEP) are outdated and offer little security.