Wi-Fi Security

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. In this newsletter, we cover the most effective steps for protecting yourself when using wireless networks.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE
TECHNOLOGY SOLUTIONS & SERVICES

Wi-Fi Security

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 called Wi-Fi. Wi-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.

Monitoring

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. If your computer supports technology called a Virtual Private Network (VPN), connect with your VPN when using public Wi-Fi points. This creates an encrypted tunnel that allows you to work online more securely.

Connecting 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.

When you are at work, your network administrator will tell you which wireless networks you can join. These networks will almost always 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 that say 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.

Finally, when connecting to public networks, you have to assume these networks are hostile. Anyone connected on that network can scan, probe or hack any other device connected to that network. This is why it is so important that your laptop and mobile devices are secure. Make sure whatever you are using is the most current version and has the latest patches and software. In addition, be sure your firewall is enabled and you have anti-virus running on your laptop.

Our Facilities

Finally, you must have prior authorization to install Wi-Fi networks at work. This ensures any Wi-Fi networks in our facilities meet our security standards and are protected against cyber attackers.

Wardriving

Wardriving is a technique attackers use to find and hack into organizations with vulnerable or open wireless networks. Their ultimate goal is usually to find a wireless network that has no authentication and that anyone can join. If they find one of these, they can simply park their car in our parking lot and wirelessly access our internal network from there. They use a method call wardriving to find these unsecured wireless networks. Wardriving is nothing more than driving around with a laptop open, trying to connect to any wireless networks they find. Since they are driving in a car, they can cover a great deal of territory quickly and potentially find hundreds of vulnerable Wi-Fi networks. This is why we take security so seriously and require any new Wi-Fi networks to go through security procedures before they can connect to any of our networks.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE
TECHNOLOGY SOLUTIONS & SERVICES