TLP:WHITE

# Security Tip (ST05-003)

## Securing Wireless Networks

Original release date: March 11, 2010 | Last revised: June 28, 2018

Wireless networks introduce additional security risks. If you have a wireless network, make sure to take appropriate precautions to protect your information.

In today's connected world, almost everyone has at least one Internet-connected devices. With the number of these devices on the rise, it is important to implement a security strategy to minimize their potential for exploitation (see Securing the Internet of Things). Internet-connected devices may be used by nefarious entities to collect personal information, steal identities, compromise financial data, and silently listen to—or watch—users. However, taking a few precautions in the configuration and use of your devices can help prevent this type of activity.

### What are the risks to your wireless network?

Whether it's a home or business network, the risks to an unsecured wireless network are the same. Some of the risks include:

#### Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can utilize your connection. The typical indoor broadcast range of an access point is 150 – 300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could potentially open your internet connection to many unintended users. These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files.

#### Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections available outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna— searching for unsecured wireless networks. This practice is known as "wardriving."

#### Evil Twin Attacks

In an evil twin attack, an adversary gathers information about a public network access point, then sets up their system to impersonate it. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point, then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information. Always confirm the name and password of a public Wi-Fi hotspot prior to use. This will ensure you are connecting to a trusted access point.

TLP:WHITE

**Wireless Sniffing**

Many public access points are not secured and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted “in the clear,” malicious actors could use sniffing tools to obtain sensitive information such as passwords or credit card numbers. Ensure that all the access points you connect to use at least WPA2 encryption.

**Unauthorized Computer Access**

An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing. Ensure that when you connect your devices to public networks that you deny sharing files and folders. Only allow sharing on recognized home networks, and only while it is necessary to share items. When not needed, ensure that file sharing is disabled. This will help prevent an unknown attacker from accessing your device’s files.

**Shoulder Surfing**

In public areas malicious actors can simply glance over your shoulder as you type. By simply watching you, they can steal sensitive or personal information. Screen protectors which prevent shoulder-surfers from seeing your device screen can be purchased for little money. For smaller devices, such as phones, be cognizant of your surroundings while viewing sensitive information or entering passwords.

**Theft of Mobile Devices**

Not all attackers rely on gaining access to your data via wireless means. By physically stealing your device, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts. Taking measures to protect your devices from loss or theft is important, but should the worst happen, a little preparation may protect the data inside. Most mobile devices, including laptop computers, now have the ability to fully encrypt their stored data—making devices useless to attackers who cannot provide the proper password or PIN. In addition to encrypting device content, it is also advisable to configure your device’s applications to request login information before allowing access to any cloud-based information. Lastly, individually encrypt or password-protect files that contain personal or sensitive information. This will afford yet another layer of protection in the event an attacker is able to gain access to your device (see Protecting Portable Devices: Physical Security).

**What can you do to minimize the risks to your wireless network?**

- **Change default passwords** - Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default passwords makes it harder for attackers to access a device. Use and periodic changing of complex passwords is your first line of defense in protecting your device (see Choosing and Protecting Passwords).
- **Restrict access** - Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the “guest” account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.
- **Encrypt the data on your network** - Encrypting your wireless data prevents anyone who might be able to access your network from viewing it (see Understanding Encryption). There are several encryption protocols available to provide this protection. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2 encrypt information being transmitted between wireless routers and wireless devices. WPA2 is currently the strongest encryption. WEP and WPA are both still available; however, it is advisable to use equipment that specifically supports WPA2, as using the other protocols could leave your network

open to exploitation.



- **Protect your Service Set Identifier (SSID)** - To prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device's SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer's default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.
- **Install a firewall** - Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer (see Understanding Firewalls).
- **Maintain antivirus software** - Install antivirus software and keep your virus definitions up-to-date. Many antivirus programs also have additional features that detect or protect against spyware and adware (see Understanding Anti-virus Software, Recognizing and Avoiding Spyware, and Why is Cyber Security a Problem?).
- **Use file sharing with caution** - File sharing between devices should be disabled when not needed. You should always choose to only allow file sharing over home or work networks, never on public networks. You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories. In addition, you should password protect anything you share. Never open an entire hard drive for file sharing (see Choosing and Protecting Passwords).
- **Keep your access point software patched and up-to-date** - The manufacturer of your wireless access point will periodically release updates to and patches for a device's software and firmware. Be sure to check the manufacturer's website regularly for any updates or patches for your device.
- **Check your Internet provider's, or router manufacturer's, wireless security options** - Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions.
- **Connect using a virtual private network** - Many companies and organizations have a virtual private network (VPN). VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

**Author**

NCCIC