PROTECTING YOUR ORGANIZATION WHILE USING WI-FI

October 2020

ITSAP.80.009

Wi-Fi is often an essential technology to support your business functions. However, Wi-Fi can also expose your organization to vulnerabilities that can be exploited by threat actors. To stay safe while staying connected, you should ensure that you have security measures in place to protect your networks, systems, and information.

WHAT IS WI-FI?

Wi-Fi is a wireless technology that connects devices, like laptops and smart phones, to the Internet. It uses radio waves and a wireless router instead of a physical wired connection. The router allows devices to interface and exchange information with others, which creates a network. Users can access Wi-Fi through networks that are specific to an organization or publicly available.

HOW CAN THREAT ACTORS TAKE ADVANTAGE OF WI-FI?

Threat actors can use Wi-Fi networks to access and damage your systems and devices. They can also use Wi-Fi networks to steal sensitive information. Public Wi-Fi networks are especially vulnerable as they usually don't require authentication for users to connect, and they may rely on weak encryption protocols that are easily hacked. Once a threat actor is positioned on a network, they can access unsecured devices that are on the same network.

SPOOFING

A threat actor creates a fraudulent network to mimic a legitimate network. For example, a threat actor may create a network with the same name as an airport, library, or café network to trick users into connecting to it. If your employees work remotely and connect to a spoofed network, a threat actor can intercept sensitive business or personal data and infect their devices with malware.

MAN IN THE MIDDLE ATTACKS OR EAVESDROPPING

A threat actor can use Wi-Fi networks (particularly unsecured networks) to exploit security flaws and intercept data that is sent over the network. Information sent over a public or unsecure Wi-Fi network is particularly vulnerable to this attack. A threat actor can capture and read information such as login credentials and credit card numbers.

SIGNAL JAMMING

A threat actor can overwhelm a wireless access point to disrupt the network and prevent legitimate traffic from communicating with that access point. Signal jamming can compromise the availability of your organization's services.

If your organization's physical network is not secured, a threat actor may attempt to install a wireless access point on your network. They can use this rogue access point to connect devices or carry out attacks on your network.

HOW CAN I PROTECT MY ORGANIZATION?

Whether using Wi-Fi in your organization or in public spaces, take the following actions to protect your networks, systems, and information.

CHANGE YOUR NETWORK NAME

Your Wi-Fi comes with a default service set identifier (SSID), or network name. Change this name to something that is unique but does not contain any personal information or reveal the manufacturer of the router or access point you are using.

USE A PASSPHRASE

Change the default passwords for the network and the administrator account. Use a unique, complex passphrase or password, avoiding single dictionary words or other easily guessed passwords.

USE A VIRTUAL PRIVATE NETWORK

Installing a virtual private network (VPN) on your network can protect your organization's information. A VPN is a secure, encrypted tunnel through which information is sent. If your employees are working remotely and must use unsecured or public networks, they should use a VPN to establish a secure connection that uses authentication and protects data.

USE SECURITY TOOLS TO DEFEND YOUR NETWORK

Install a firewall on your network. A firewall monitors the flow of traffic moving in and out of your network and filters out known-bad traffic. You can set rules to control the amount and types of traffic that can pass between networks. Consider enabling media access control (MAC) address filtering to ensure only authorized devices can connect to your network.

If you have the resources available, consider investing in a wireless intrusion detection systems (WIDS) or wireless intrusion prevention systems (WIPS), which can monitor your networks for anomalies.

SET UP A GUEST NETWORK

A guest network is a separate access point on your wireless router. It provides devices with access to the Internet but not your internal network. You should consider connecting Internet of Things (IoT) devices to a guest network to reduce the risk of malware infections on your main network.

DISABLE NETWORK BROADCASTING

Optionally, you can disable network broadcasting. When your network name is broadcasted, anyone scanning for available networks can see it. By disabling network broadcasting, users must enter the name manually to find and join the network.

WHAT ELSE SHOULD I CONSIDER?

Ensure that all employees know how to protect your organization from cyber threats. Provide your employees with cyber security training, and encourage employees working remotely to secure their home Wi-Fi networks with the actions mentioned in this document. Some additional best practices include the following:

- Avoid using public Wi-Fi networks when working remotely. If you must use public Wi-Fi, use a VPN to keep information secure.
- Avoid using "remember me" features when logging into accounts and always sign out of accounts when you are done.
- Remove saved networks ("forget the network") that you connected to in the past and no longer use.
- Disable automatic connection features on your mobile devices to prevent automatic connection to unsecure networks.
- Turn off Wi-Fi and Bluetooth when they are not in use.
- Update and patch operating systems and applications regularly.
- Update the software and firmware on IoT devices, including routers, regularly.

WHERE CAN I LEARN MORE?

For more security tips, visit the Cyber Centre's website at **cyber.gc.ca** to find more publications on similar topics:

- *ITSAP.80.101 Virtual Private Networks*
- *ITSAP.10.016 Security Tips for Organizations with Remote Workers*
- *ITSAP.70.111 Using Virtual Desktop at Home and in Office*
- *ITSAP.70.002 Security Considerations for Mobile Device Deployments*
- *ITSAP.10.096 How Updates Secure Your Device*
- *ITSAP.00.057 Protect Your Organization from Malware*
- *ITSAP.30.032 Best Practices for Passphrases and Passwords*