Guest Wi-Fi

AUGUST 2022 ITSAP.80.023

Setting up guest Wi-Fi networks at home and within your organization is an important part of keeping your primary network secure. A guest network provides an access point to the internet that is separate from your primary network. Although there are many benefits, guest networks can also expose your organization or home to vulnerabilities that can be exploited by threat actors. Implementing and securing a guest network is important to improve your cyber security posture.

Why you should use guest networks

Guest Wi-Fi networks provide guests and devices access to the Internet using separate network access points from your primary network. Guest networks are easy to set up, cost effective, and enhance your cyber security in your home and organization in the following ways:

At home:

- Offers guests internet access
- Avoids sharing passwords
- Secludes smart devices and possible unpatched devices from the primary network
- Isolates company network access and devices remotely

Organization:

- Offers visitors internet access
- Reduces the risk of attackers accessing primary network devices and information (e.g. spreading malware)
- Offers a logical separation network for new and out-dated devices (e.g. unpatched software)

Most modern virtual local area networks (VLANs) can create multiple separated networks to offer your system availability to have separated networks for primary, devices, and guests. Many devices, such as smart devices, need an internet connection to function accordingly, but do not need direct access to your primary networks. Guest Wi-Fi networks reduce the risk of compromised devices from accessing important sensitive information.

Threats to your guest networks

Guest Wi-Fi networks are common targets for threat actors as they are often poorly secured. Some common cyber threats should be considered when having a guest network:

- **Eavesdropping attacks:** Threat actors use eavesdropping attacks to take advantage of unsecure open Wi-Fi to compromise information transmitted over the network.
- **Phishing attacks:** If someone falls victim to a phishing attack either while using or prior to using your guest network, other connected devices may become compromised.
- **Malware:** If a device is infected with malware, it will likely spread to other connected devices. Any connected device and information residing on the guest network is at risk of being compromised.
- **Denial of service (DoS) attacks:** Threat actors use DoS attacks to overwhelm target networks. A DoS attack can overload the router and cause processes to malfunction or offer threat actors access to your primary network.

Most of these threats emphasize why a guest Wi-Fi network is useful to protect your primary network (e.g. isolating threats from accessing sensitive information). In order for your guest Wi-Fi network to keep connected devices and your primary network secure, it must be implemented and managed using appropriate security tools.

Cat. No. D97-1/80-023-2022E-PDF
ISBN 978-0-660-44766-7

How can I secure my guest networks?

Although a guest network is often used to keep potentially unsecured devices from accessing the primary network, it is important to keep it as secure as possible. Mitigating the risks posed by your guest network will keep devices and information that need to reside on the guest network as secure as possible. Here are some security measures for you to consider:

Separate passwords

Your guest Wi-Fi network should have a password for access, but a separate one from all other networks and accounts. Ensure the password is changed from the default, and be mindful of who access is shared with. A trusted guest might not directly share the password, but if their compromised device accesses your guest network, other connected devices could become compromised.

Update software

Keep your router and all devices on the guest network updated and patched with the latest versions of software and firmware. This will help patch security vulnerabilities and reduce the risk of spreading malicious software.

Isolating networks

Ensure the settings in your VLAN restrict guests and devices in the guest networks from interacting with devices and information in the primary network. Firewalls can also offer these security settings with advanced configuration if your organization has the financial and technical support to implement them.

Monitor connected devices

Monitor what devices are connected to your guest Wi-Fi network. Limit the period of time that guest passwords can be used to ensure only current guests can access the network. Set up a start and end access feature for new connecting devices.

Network broadcasting

For extra security, you can disable network broadcasting (e.g. network ID or service set identifier [SSID]). If your guest network is broadcasting, anyone can attempt to access it by scanning available networks. By disabling it, users must enter the network name manually to find and gain access.

Use WPA2 or WPA3

Use WPA2 or WPA3 security protocols if the option is available when configuring your guest network. These security protocols offer advanced Wi-Fi encryption to keep your devices and information secure.

Web Filtering

Use web filtering to control what sources are accessible while using your guest network. Using allow lists and deny lists can help manage specific websites and applications from being accessed. You can also use keyword and content filters to restrict websites that contain the specific content.

You may also want to consider media access control (MAC) address filtering. Like allow lists and deny lists, MAC address filtering can allow you to specify which devices should and should not have access to your network.

Learn more

Visit our website at cyber.gc.ca to find a catalogue of cyber security publications, including:

- *Wi-Fi Security (ITSP.80.002)*
- *Protecting your organization while using Wi-Fi (ITSAP.80.009)*
- *How updates secure your device (ITSAP.10.096)*
- *Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101)*
- *Protect your organization from malware (ITSAP.00.057)*
- *Protecting your organization against denial of service attacks (ITSAP.80.100)*
- *Best practices for passphrases and passwords (ITSAP.30.032)*
- *Application allow list (ITSAP.10.095)*

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**