Routers cyber security best practices

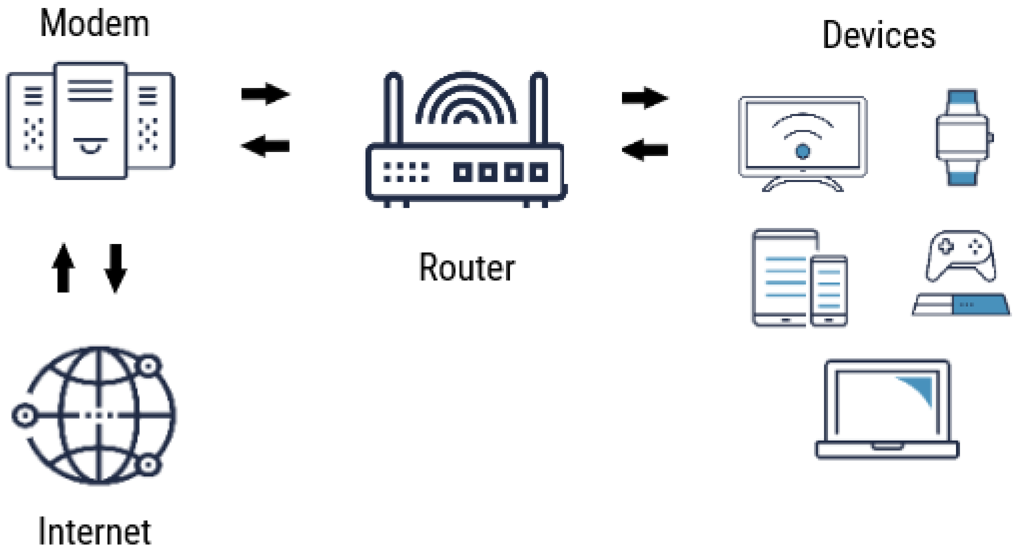
CANADIAN CENTRE FOR
CYBER SECURITY

October 2022 | ITSAP.80.019

Chances are your office and your home have a wide range of internet-connected devices, such as computers, tablets, smartphones, printers, smart TVs, and various Internet of Things (IoT) devices. Routers enable multiple devices to connect to the internet using the same connection. A router without an internet connection is often used to wirelessly connect devices within a local area so that you can access wireless/network printers, share files, and communicate among connected devices. Unfortunately, routers are attractive targets for cybercriminals trying to infiltrate the network to conduct cyber attacks. This document provides information on cyber security best practices to protect your routers from being compromised.

What is a router?

A router is a piece of hardware used to create a network for devices within a local area. A modem then connects that network to the internet. Some units combine both functions and are often referred to as routers also. Routers are responsible for forwarding messages (data packets) between devices within a network. To do so, the router assigns a unique local Internet Protocol (IP) address to each of the devices on the network. On receiving a data packet for delivery, the router reads the destination IP address, searches its routing table to determine the next hop, and forwards the packet accordingly.



What are the **impacts** of a compromised router?

Threat actors use various techniques to automatically scan for hardware like routers that can be vulnerable to cyber attacks. Routers are vulnerable if they are poorly or improperly configured. When your router is compromised, threat actors can:

- Steal personally identifiable information (PII) from any device connected to your network and use it for malicious purposes.
- Access login credentials of user accounts and use them to gain unauthorized access to networks and devices. Threat actors can gain access to login credentials by altering your router's ability to resolve to legitimate websites and redirect you to malware-serving websites.
- Monitor, modify, and deny traffic to and from your organization, or maintain persistent access to your networks for future attacks.
- Leverage exposed data or intellectual property to perform advanced cyber attacks, such as supporting espionage.
- Hijack or assimilate your router into a network of infected devices to create a botnet. Threat actors use botnets to conduct Distributed Denial of Service (DDoS) attacks, which will overwhelm your server with internet traffic and disrupt your ability to provide essential business operations and services.

The following publications are available on our website:

- Protecting your organization while using Wi-Fi (ITSAP.80.009)
- Protective Domain Name System (ITSAP.40.019)
- Wi-Fi security (ITSP.80.002)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Guest Wi-Fi (ITSAP.80.023)

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

Routers cyber security best practices

CANADIAN CENTRE FOR CYBER SECURITY

October 2022 | ITSAP.80.019

How to **prevent** your router from being compromised

The following actions can be taken to secure your router from cyber attacks. Start with the basics and implement the additional measures over time.

Basic measures

Change all default passwords for your Wi-Fi network and the router. Use a passphrase, whenever possible, or a strong, unique, and complex password. Passphrases/ passwords are important to protect your router from brute-force attacks to crack passwords.

Turn on Wi-Fi Protected Access (WPA) to protect internet traffic from unauthorized access. WPA2 or the newer WPA3 provide strong encryption between the router and your devices.

Disable Service Set Identifier (SSID) broadcast so that your wireless network name will not be easily visible to threat actors scanning networks within the vicinity.

Change the default wireless network SSID name. This prevents threat actors from easily identifying the make and model of your router and potentially determining if a vulnerability exists for that device.

Disable WPS (Wi-Fi Protected Setup). This is a convenient feature to simplify the process of connecting devices to your Wi-Fi router. However, a threat actor within range can brute-force the PIN authentication method.

Keep the router's firmware up to date. This ensures you have the latest security patch installed to address known vulnerabilities. Turn on automatic firmware updates if your router model has this feature.

Set up a guest network to enable internet connection for your guests and for your IoT devices. This avoids sharing passwords and reduces the risk of threat actors accessing your primary network devices and sensitive information.

Physical security. Ensure physical access to the devices is restricted and access to Wi-Fi access points is equally secured.

Additional measures

Schedule routine reboots to clear the system memory and refresh all connections. Rebooting the router may disrupt any potential malware that may have been implanted.

Disable remote access management, if possible, to prevent unauthorized people from remotely accessing your router and tampering with it.

Disable Simple Network Management Protocol (SNMP) to reduce risk of threat actors collecting basic system configuration information about your network.

Set up each router administrator with their own login username, unique password and appropriate privilege level. If event logging is enabled, then the login information will be important for auditing and incident investigation purposes.

Use Media Access Control (MAC) filtering to choose which trusted devices connect to your network.

Enable port filtering. For example, the SANS Institute recommends blocking outbound traffic that uses the following ports to prevent unwanted traffic out to the internet:

- MS RPC - TCP & UDP port 135
- NetBIOS/IP - TCP & UDP ports 137-139
- SMB/IP - TCP port 445
- Trivial File Transfer Protocol (TFTP) - UDP port 69
- Syslog - UDP port 514
- Simple Network Management Protocol (SNMP) - UDP ports 161-162
- Internet Relay Chat (IRC) - TCP ports 6660-6669

Enable event logging and regularly monitor activity. This will allow you to detect what types of attacks are being attempted against the router and implement proactive mitigation measures. If using a Syslog server for monitoring, change the default UDP port 514 to use alternatives such as TCP 514 or TCP 6514.

Communications Security Establishment | Centre de la sécurité des télécommunications

Cat. No. D97-1/80-019-2022E-PDF ISBN 978-0-660-45678-2

Canada