How to:

Safely use Wi-Fi networks

Public wireless networks

Wireless networks are everywhere, however using them comes with risks as they can be targeted and attacked from a distance. This makes them vulnerable to cyber attacks.

There are two types of wireless networks: Private and public. The wireless network you use in your home is private and can be tightly controlled. The wireless network you use at the coffee shop or in the airport is public. You are more at risk of a cyber attack when using public networks.

Here are four precautions you can take when using public wireless networks:

Use legitimate wireless networks

Fraudsters sometimes set up fake Wi-Fi sites that look similar to the network you are searching for.

Use a VPN

A VPN encrypts data traveling to and from your device, making it harder for fraudsters to steal your information.

Don't access personal information

Be careful of the information you share through a public wireless network and avoid tasks like online banking or shopping online.

Keep to https sites

Https is the secure version of http in the website address you are visiting. The 's' stands for 'Secure' and all communications between your browser and the website are encrypted.

How to: **Safely use Wi-Fi networks**

Private wireless networks

Secure your home network for personal use and from your internet connected devices (IoT). It starts with securing your Wi-Fi router from your Wi-Fi provider. This device controls who and what connects to your home network.

Start by going to your internet provider's website or use the IP address documented in your device's manual. You should find a Wi-Fi management section where you can make the following changes:

Make the network undiscoverable

Changing the network name makes it harder for hackers to exploit potential vulnerabilities. Do not use your name, home address, or identifying information.

Change the default password

Change it to a strong, unique password that has a minimum of 8 characters (preferably much longer) and combines numbers, letters and characters.

Create a guest network

Use the guest network for untrusted devices when guests visit your home and for your personal smart home devices.

Ensure your network is encrypted

Change wireless settings to WPA2 or WPA3.

Patch firmware

Enable automatic updates for all devices. If an automatic update is not an option, periodically log into your provider's account and check for updates.