Protecting your home from cybercrimes

Cyber crimes? Not in my home!

We all know that "Home is where the heart is", but it's also where all of our most personal and private information is! In this month's newsletter, you'll find tips to help secure your home Wi-Fi from cybercrimes.

Securing your private Wi-Fi

Many devices such as your computer, voice assistants, TVs, gaming consoles and even smart refrigerators are on your home Wi-Fi network. It's important to ensure that your network is secure so none of your information is at risk.

5 tips for securing your home network

1. Update your router name

Routers come with a SSID (Service Set ID), which is the technical name for your Wi-Fi network. If you were to keep the given SSID provided by your service provider, it makes it easy for a hacker to breach your network. This is because the information is traceable to the make and model of the Wi-Fi router, giving someone a better chance of finding a way into your network.

2. Change router and Wi-Fi passwords

When you first receive your router, there will be preset passwords for the router itself (admin password) and for the Wi-Fi. These passwords are often written down on a card or even directly on the router. This is an easy way for someone to get into your network. It's important to change both the router admin password and the Wi-Fi network password.

- **Changing the router admin password:** This password allows you to make all setting changes for your home network. Changing this password is important because if someone were to get into your network, they have access to your Wi-Fi password.
- **Changing the Wi-Fi password:** This password is used to connect all of your devices to your network. Be sure to choose a password that is unique to you and easy to remember but hard to guess.

You can find instructions on how to change your passwords by searching "how to change [your router manufacturer] admin or Wi-Fi network password".

3. Encrypt your network

When you encrypt your network, it makes it harder for hackers to see what you are doing or any of the personal information you have. To encrypt your network, you need to update your router settings to WPA3 Personal (newest and best encryption) or WPA2 Personal. Both of these settings will scramble your information and help add a layer of security to your home Wi-Fi network.

If your router is older or does not have the WPA2 or WPA3 settings:

- Older routers have WPA and WEP, but those are insecure and outdated. Try to update your router software and see if WPA2 or WPA3 becomes available. If not, you may need to upgrade your router to better secure your network.

4. Turn off "Remote Management," WPS (Wi-Fi Protected Setup) and UPnP (Universal Plug and Play)

These features, although convenient, are not helping to secure your network.

- Remote management allows you to make network changes over the internet.
- WPS allows you to press a button on your router and connect a device to your network without having to put in a password.
- UPnP lets devices on your network find and connect to one another.

Ring doorbells: Can they be hacked?

Just as your phone, laptop and other devices are connected to your home Wi-Fi, the Ring doorbell has the same security concerns. The Ring doorbell is now mandating two-factor authentication (which adds an extra layer of security), along with notifications that alert you about other devices that have logged in to the account. Even though the added security features are available, it is crucial to stay ahead of any issues. Here are some additional tips to keep in mind if you have or are thinking of getting a smart doorbell.

- Create a strong username and password
- Do not share your login information. Check your shared users to be certain who all has access to your device
- Avoid sharing videos or pictures on social media
- Keep the software up to date

5. Set up a guest network

Setting up a guest network allows you to connect your guests to Wi-Fi while keeping your primary network safe and secure. This is a good security measure for two reasons:

1. Having a different login means fewer people have access to your primary Wi-Fi
2. If your guest were to have malware (malicious software designed to cause harm to a computer or computer user) on their device, this would prevent that from getting onto your network.

Update, update, update!

Malware often uses old security defects in our programs to install itself or cause harm. This can easily be prevented by updating your technology frequently. Updates become available when low-risk issues are found. These are called "patches."

Many popular operating systems will automatically patch themselves every few days. Some hackers will use this opportunity to send you a fake update alert that, if clicked, allows them to get into your system. To avoid this, make sure you are only updating when you get an official notification from the provider. Turning on automatic updates will ensure that you stay on top of updated software.