Safety Tip of the Week #24

Tips To Protect Your Home Wi-Fi Network

1. Change default username and password

The first and most important thing you should do to secure your home Wi-Fi network is to change the default username and password to something more secure.

Wi-Fi providers automatically assign a username and password to the network and hackers can easily find these default passwords online. If they can gain entry to the network, they can change the password to whatever they like, lock the owner out and hijack the network.

Changing the username and password makes it more difficult for attackers to identify whose Wi-Fi it is and gain entry to the network. Hackers have sophisticated tools to test thousands of possible password and username combinations, so it's vital to choose a strong password that combines letters, numbers, and symbols to make it more difficult to crack.

2. Turn on Wireless Network Encryption

Encryption is one of the most effective ways of safeguarding your network data. Encryption works by scrambling your data or the contents of a message so that it cannot be deciphered by hackers.

The most secure type of encryption to use for your home Wi-Fi network is WPA2. If you have older devices that are up to 10 years old, they may not be compatible with WPA2 so it will be vital to upgrade your home devices for enhanced security and performance.

To check if your router uses WPA2 encryption, look at your network settings and check the wireless properties. This will enable you to select the best encryption method when you join a wireless network.

3. Use a VPN (Virtual Private Network)

A VPN is a network that allows you to communicate over an unsecured, unencrypted network in a private way. A VPN encrypts your data so that a hacker cannot tell what you are doing online or where you are located.

A VPN will also alter your IP address, making it appear that you are using your computer from another location other than your home address. In addition to a desktop, it can also be used on a laptop, phone or tablet.

4. Hide your network from view

When you are initially setting up your home network you will be asked to create a publicly visible network name, otherwise known as a SSID (Service Set identifier). Most devices are configured with a default network name that has been allocated by the manufacturer. There's a good chance that if your neighbours have a device from the same manufacturer they will also the same SSID which could be a security nightmare if both networks are unencrypted.

SSID hiding is a feature that will enable you to hide your network name from the list of people in the surrounding area. Changing the default name makes it a lot more difficult for a hacker to know what type of router you have, reducing the chance of attack.

info@protectivegroup.com.au
www.protectivegroup.com.au
+61 3 9699 4257
27 Ballantyne Street,
Southbank VIC 3006

Safety Tip of the Week #24

Tips To Protect Your Home Wi-Fi Network

5. Turn off your Wi-Fi Network when not at home

It sounds simple but one of the easiest ways to protect your home network from attack is to turn it off when you're not at home. Your home Wi-Fi network doesn't need to be running 24 hours a day, seven days a week. Turning off your Wi-Fi when you're away from home reduces the chances of opportunistic hackers attempting to break into your home network when you're not in.

6. Keep your router software up to date

Wi-Fi software should be updated to protect the network security of your home. The router's firmware like any other type of software can contain vulnerabilities that hackers are keen to exploit. Most routers won't have the option of an auto-update so you'll need to manually update the software to ensure your home network is protected.

7. Use Firewalls

Most W-Fi routers will contain a built-in network firewall that will protect broadband connections and prevent any network attacks from intruders. They will also have an option to be disabled so it's important to check that your home router's firewall is turned on to add another layer of protection to your home security.

8. Place the router in the centre of your home

Homeowners often don't realise that the location of their router can have an impact on security. If your router is positioned near a door or window it increases the chance of your wi-fi signal being intercepted by someone with malicious intent. To improve the security of your home Wi-Fi, it's best to place your Wi-Fi router as close to the centre of your home as possible and this will reduce the chance of hackers connecting to your network.

9. Enable MAC Address Filtering

Most broadband routers will have a unique identifier called the physical address or Media Access Control (MAC) address. This address aims to improve security by limiting the number of devices that can hook up to the home network. Homeowners have the option to type in the MAC addresses of all devices in the home and this restricts the network to only allow connections from these approved addresses. This provides another layer of security to help keep hackers at bay.

10. Disable Remote Administration

Another way hackers can gain entry to a home network connection is through the remote administration feature on a router. Remote administration allows anyone close enough to your home to view or change your Wi-Fi settings. If you don't need to remotely connect to your Wi-Fi router, it's best to turn this feature off. This can be done by going into the administration section of the Wi-Fi settings and clicking on the disable button.