Know More About Home Internet Security

TechRounder PDF Edition

Live article: https://www.techrounder.com/internet/know-more-about-home-internet-security/

By Vipin PG | Published May 27, 2022 | Updated March 8, 2026 | Format: Article | 4 min read

In brief

A secure home network means your family can surf the web more securely. However, keeping your home internet and home network secure requires the right tools and the assurance that family members are safe online.

A secure home network means your family can surf the web more securely. However, keeping your home internet and home network secure requires the right tools and the assurance that family members are safe online.

Your home network can have many wireless devices connected, from computers and phones to smart TVs and other appliances. By following a few simple steps to secure your home Wi-Fi network, you can protect your devices from being hacked and your information being stolen.

However, the first thing to do would be to ensure that your Internet Service Provider (ISP) offers a secure connection. Leading ISPs, like Cox internet, provide a safe connection and make sure that all customers with a wireless network enable their security once the installation is complete. Furthermore, their customer representatives are available around the clock to guide you on making further your network connection safer.

Home Wi-Fi Network

Your Wi-Fi network is the wireless Internet connection in your home. This is usually a wireless router that sends a signal through airwaves. You can connect to the web using this connection. However, if your network is not password protected, any device within its range can pick up a signal out of nowhere and use your internet connection.

How to make your home WiFi Secure

You will need to make sure that all internet devices have the newest operating system, security software, and web browser installed.

Network Encryption

Encryption encodes information sent over your network. This prevents other people from seeing what you are doing or getting your private information. You encrypt your network by updating your router’s settings to WPA3 or WPA2 Personal. WPA3 is the recent and better version of encoding accessible but combined, and they work well to encrypt your information.

Routinely Change Passwords

Some routers come with passwords already set into the system. However, hackers can effortlessly find these passwords, so modifying them to something more difficult is significant. There are two steps to doing this:

WiFi Password

This includes the password you use to connect your devices. A secure and unique network password will help prevent anyone from accessing it.

Admin Password

This is the one that gives you access to the device management page. You can change the settings. If a hacker manages to log into your router's administration page, they can change its settings (including the password to your Wi-Fi). This will override any other precautions you might have taken.

Update router

Before setting up a new router or updating an existing one, check the manufacturer's webpage to see if a recent version of the software is available for installation. Get your router registered with the respective manufacturer and subscribe to receive up to ensure that you are getting the newer dates to ensure that you are getting the newer one. If you got your router from your ISP, check with them to see if they send programmed updates.

Switch off Unnecessary Features

Many routers have preset features that may be practical but deteriorate the security of your network. For example, your router control may have remote access enabled that permits you to modify settings over the Internet. With WPS, you can press a button on your router to connect any device to your network instead of reentering the password. Finally, universal plug and play (UPnP) allow your devices to connect to the network. These functions can make adding devices to your network easier or allow visitors to connect to your WiFi, but they can reduce the security of your network.

Separate Network for Guests

Most WiFi routers give you the option of creating a guest network with a new name and password. This is a reasonable precaution in two ways: Separate login means fewer people know your master Wi-Fi network password, and If a guest's phone or tablet has malware, it won't reach your main network and devices.

Disable Broadcasting Network Name

If you are using a wireless router at home, it is highly suggested that you deactivate network name broadcasting. When anyone in the proximity tries to find a Wi-Fi network, their device displays a list of close-by networks to choose from. However, turning off broadcasting settings will not reveal your network, leaving your Wi-Fi connection unseen to those who do not know about it.

This feature is valuable for restaurants, companies, hotels, and libraries who wish to offer customers wireless Internet access. Still, it is not required for a private wireless network, such as the WiFi network at your home.

Good Firewall

A firewall is intended to guard computers against intruders such as viruses and malware. WiFi routers usually have pre-installed firewalls, but sometimes these are disabled. Make sure your wireless router's firewall is enabled. If your router does not have such a firewall, ensure you get it installed on your system to protect against malicious attempts to access your wireless network.

Use VPNs

A VPN, i.e., a virtual private network, is a group of networks or computers working together online. You can use VPN services to secure and encrypt your communications. Once connected, a VPN client is started on your computer. When you log in with your authorizations, your computer contacts another server to exchange keys. After both computers have mutually authenticated, all your online communications are encoded and hidden from prying eyes from the outside.

Most importantly, check which devices are connected to your home network and have reliable anti-virus and anti-spyware software such as Norton Security installed.

Conclusion

By implementing the steps shown above, you can get the best out of the security of your wireless network, giving you more peace of mind when using the Internet in your house. There are probably many devices linked to your router, from phones to smart devices, and you need to block and secure them all. Once you connect them to WiFi, they will also be linked to your router. If your device does not require Wi-Fi, turn it off. You will not regret it.

References

1. localcabledeals.com - Cox / Internet - https://www.localcabledeals.com/Cox/Internet