IMC HEALTH
MEDICAL CENTERS

Securing Your Home Wi-Fi Network

Many of us enjoy the convenience of home Wi-Fi but an unsecured home Wi-Fi network can invite malicious or criminal access to every device that connects to that network. There are several important steps you can take to better secure your home Wi-Fi network to reduce the likelihood of becoming a victim of fraud, identify theft, loss of personal information etc. Some are easier to implement than others, but all can be done by following instructions readily available online. While this list is not inclusive of every possible step you could take to further secure your network, these are the easiest and the ones generally considered by security experts to offer the most benefit.

1. **Change the name of your default Wi-Fi.** Your router likely came with a default SSID which stands for Service Set Identifier. It is the name you see when you search for available wireless networks. Change it to something unique and avoid a name that would make it easier for hackers to associate that network with you or your home. Visit this link for detailed instructions:
https://www.wikihow.com/Change-the-Name-of-a-Wireless-Network

2. **Add a strong wireless network password.** Every wireless router comes with a default username and password, both of which are easy for hackers to guess, especially if they can determine the router manufacturer. Change your password to one that includes letters, symbols, and numbers. The longer the password the better. Visit this link for detailed instructions:
https://www.wikihow.com/Add-a-Password-to-Your-Wireless-Internet-Connection-(WiFi)

3. **Enable network encryption.** Turning on encryption goes a long way towards ensuring that personal and confidential information that you are sharing online is not visible to hackers. While the steps to do so many vary based on your router, this link provides an overview of the steps required:
https://www.wikihow.com/Encrypt-Wireless

4. **Ensure you are using a Firewall.** Most routers come with a firewall, but sometimes it is turned off. This article explains how to check to see if your router comes with a firewall, and how to ensure it is operational: https://www.lifewire.com/how-to-enable-your-wireless-routers-built-in-firewall-2487668

5. **Ensure your router's software is up to date.** Router firmware updates often provide both performance improvements and critical security protections. While the steps may vary depending on the hardware you are using, this link provides a good overview of the process:
https://www.hellotech.com/guide/for/how-to-update-router-firmware

6. **Remember the security of devices connecting to your network.** Even with a secure network you are still at risk if the devices connecting to your network are not protected. Whether it be a PC, phone, or tablet, always ensure that the software on your device is current and that security patches are applied.