CYBER SECURITY NEWSLETTER

PROTECTING YOUR HOME NETWORK

Wi-Fi networks (sometimes called by their technical name, 802.11) allow people to wirelessly connect devices to the Internet using smartphones, laptops, tablets, and gaming consoles. Because Wi-Fi networks are fairly easy to set up, many people install their own networks at home. However, many home Wi-Fi networks are configured insecurely, allowing strangers or unauthorized individuals to easily access your home network or anonymously abuse your Internet connection. To ensure you have a safe and secure home Wi-Fi network, here are a few simple steps you should take.

Protecting Your Home Network

Your home network, just like your network at work, is under constant attack. Here are some steps you can take to help protect you and your family at home.

Solution

Your Wi-Fi network is controlled by something called a Wi-Fi access point. This is a physical device you can buy at your local electronics store, or that may be built into your Internet router. The access point is what wirelessly connects your devices to the Internet.

One of the first steps to securing your Wi-Fi network is limiting who can administer your Wi-Fi access point and how they can access it. We recommend you follow the following steps when configuring your Wi-Fi access point for the first time:

1. For many Wi-Fi access points, the default administrator login and password is well-known. In fact, these default accounts can often be found listed on the Internet. Always change the default administrator login and password to something only you know.

2. For administrative access to your Wi-Fi access point, we recommend you disable wireless access and instead require a physical network connection using an Ethernet cable. If you must have wireless administrative access, then, at a minimum, disable HTTP access and require HTTPS, which supports encryption.

St Luke's

This newsletter is published by St. Luke's IT Security.

For more information or to report an IT Security incident, please contact the St. Luke's Cyber Security Incident Response Team (CSIRT) at csirt@slhs.org

Another option you will need to configure is the name of your Wi-Fi network (often called SSID). This is the name your devices will see when they search for local Wi-Fi networks. We recommend changing your default Wi-Fi network name. Give your network name something unique so you can easily identify it, but make sure it does not contain any personal information. Also, there is little value in configuring your Wi-Fi network as hidden (or non-broadcast). Today most Wi-Fi scanning tools or any skilled attacker can easily discover the details of a hidden network. The recommended option is to leave your Wi-Fi network visible, but secure it using the other steps covered in this newsletter.

3. Next, ensure only people you know and trust can connect to and use your Wi-Fi network, and that those connections are encrypted. You want to be sure neighbors or nearby strangers cannot connect to or monitor your Wi-Fi network. Fortunately, these dangers are easily mitigated by simply enabling strong security on your Wi-Fi access point. Currently, one of the best options to use is the security mechanism WPA2. By simply enabling this, you require a password for people to connect to your Wi-Fi network, and once authenticated, those connections are encrypted.

Be sure you do not use older, outdated security methods, such as WEP, or no security at all, which is called an open Wi-Fi network. An open network allows anyone to connect to your Wi-Fi network without any authentication. The recommended encryption method for WPA2 is AES only, versus other options such as TKIP or TKIP+AES.

When configuring your password, make sure it is different from the administrator password and cannot be easily figured out; we recommend passwords be at least 20 characters long. This may sound like a very long password, but remember that you most likely have to enter it only once for each of your devices, as they will store and remember the password for future network access. If your Wi-Fi access point is in a physically secure location and only trusted members of your family have access to it, one option may be to tape the user password to the bottom of the Wi-Fi access point for easy recall. Remember, anyone you have given the password to will have access to your Wi-Fi network, so from time to time you may want to change it.

OpenDNS

Once you have your home network secured, one of the last steps we recommend is configuring your network to use OpenDNS as your DNS servers. When you type a name into your browser, DNS is how your browser knows which sever to connect to. DNS converts the name of the website into a routable IP address.

OpenDNS is a free service that helps ensure you connect only to safe websites. It does this by having a list of known malicious websites, and then stops you from accidently attempting to connect to one. In addition, OpenDNS gives you the ability to manage what websites your family can connect to. For example, you can block any websites that have adult content, focus on hate crimes, or contain any other objectionable material. The OpenDNS website walks you through step-by-step how to configure your Wi-Fi access point to use OpenDNS, helping secure any devices connected to your Wi-Fi network. Learn more about OpenDNS at:

http://www.opendns.org