OUCH! | February 2016

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Your Wireless Network
- Your Devices

Securing Your Home Network

Overview

Several years ago, home networks were relatively simple. They were usually nothing more than a wireless access point and computer or two used for surfing the Internet, online shopping, or gaming. However, home networks have become increasingly complex. We now connect far more devices to these networks and use them for more than just web browsing or consuming media. In this newsletter, we cover how you can create a secure network at home for you and your family.

Guest Editor

Cheryl Conley leads the Security Education and Awareness team at Lockheed Martin, leveraging The I Campaign™, which reaches over 100,000 employees. This includes alliance and advocate focus groups across the enterprise, in addition to a global phishing program. Follow Cheryl at **@conleychera**.

Your Wireless Network

Almost every home network starts with a wireless network (sometimes called a Wi-Fi network). This is what enables you to wirelessly connect any of your devices to the Internet, from laptops and tablets to gaming consoles and televisions. Most home wireless networks are controlled by your Internet router, which is the device your Internet service provider installed in your house to connect you to the Internet. However, in some cases, your wireless network may be controlled by a separate system called a wireless access point, which connects to your Internet router. Regardless which one your wireless network uses, they both work the same way: by broadcasting wireless signals. The different devices in your house connect to your wireless network via these signals. From there, these devices can then connect to the Internet, as well as any other devices on your home network. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

- Change the default administrator password for your Internet router or wireless access point, whichever is controlling your wireless network. The admin account is what allows you to configure the settings for your wireless network. The problem is many Internet routers or wireless access points are shipped with a default admin login and password that are well known and often posted on the Internet. As such, be sure to change

Securing Your Home Network

the admin password to a strong, unique password that only you know.

- Change the default name of your wireless network (sometimes called SSID). This is the name your devices will see when they search for a local wireless network. Give your network name something unique so you can easily identify it, but make sure it does not contain any personal information. There is little value in configuring your network as hidden (or non-broadcast), as most wireless scanning tools or any skilled attacker can easily discover hidden networks.
- Ensure that only people you trust can connect to and use your wireless network, and that those connections are encrypted. Do this by enabling strong security. Currently, the best option is to use the security mechanism called WPA2. By enabling this, a password is required for people to connect to your home network. Once connected, their online activities are encrypted. Be sure you do not use older, outdated security methods, such as WEP, or no security at all, which is an open network. Open networks allow anyone to connect to your wireless network without any authentication.
- Ensure the password people use to connect to your wireless network is a strong one and that it is different from the admin password. Remember that you most likely only need to enter the password once for each of your devices, as they can store and remember the password.
- Many wireless networks support what is called a guest network. This allows visitors to connect to the Internet, but protects your home network, as they cannot connect to any of the other devices on your home network. If you add a guest network, be sure to enable WPA2 and a unique password for this network.
- Disable Wi-Fi Protected Setup or other mechanisms that allow a new device to connect to the network without knowing the password and configuration options.
- If you have difficulty remembering all these different passwords, we highly recommend you use a password manager to securely store them for you.

To protect your home network, secure your wireless network and update and password protect all devices on your network.

Securing Your Home Network

Not sure how to do these steps? Ask your Internet service provider, check the documentation that came with your Internet router or wireless access point, or refer to their respective websites.

Your Devices

The next step is knowing what is connected to your home network and making sure all of those devices are secure. This used to be simple, when there were only a few devices connected. However, in today's "always connected" world, almost anything can connect to your home network, including TVs, gaming consoles, baby monitors, speakers, your thermostat, and even your car. One simple way to discover what is on your home network is to use a simple network scanner, such as Fing. These apps, which you can install on your computer or mobile device, scan your wireless network and report every device connected to it. Once you have identified all of the devices on your home network, you need to ensure that each of them is secure. The best way to do this is to ensure that they are always running the latest version of their operating system/firmware. Whenever possible, enable automatic updating on them. If any of your devices require a password, always use a unique, strong password. Finally, be sure to visit your Internet service provider's website, as they may provide free tools to help you secure your home network.

ICS: Anatomy of a Cyber Attack

Be sure to check out our free resources, including our blog and Video of the Month. This month, we cover Engineer: Anatomy of a Cyber Attack. View the video at: https://www.securingthehuman.org/u/8x9.

Resources

Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Manager:	https://securingthehuman.sans.org/ouch/2015#october2015
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Mapping Your Home Network:	http://l.rud.is/home-network-mapping

License