OUCH! | January 2014

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Your Wireless Network
- OpenDNS
- Your Devices

Securing Your Home Network

Overview

Home networks were relatively simple several years ago,, perhaps nothing more than a wireless access point and a computer or two used to surf the Internet or play games online. However, home networks have become increasingly complex. Not only are we connecting more devices to our home networks, but we are doing more things with them. In this edition we will cover some basic steps to creating a more secure home network.

Guest Editor

Kevin Johnson is the CEO at Secure Ideas, runs **MySecurityScanner.com** and is a senior instructor with the SANS Institute. You can find more information at **www.secureideas.com**.

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. For this to happen, your wireless network needs something called a wireless access point. This is a physical device that connects to your Internet router (or may be built into your Internet router) and sends out a wireless signal that your devices connect to. Once your devices connect to the access point, they can then connect to other devices on your home network and the Internet. As a result, your wireless access point is one of the key parts of your home network. As such, we recommend the following steps to securing it:

- For most wireless access points, the default administrator login and password is well-known and often even posted on the Internet. As such, be sure to change the default administrator login and password to something that only you know. Make sure that it is a unique password and is not used for any of your other accounts.
- Another option you will need to configure is the name of your wireless network (sometimes called your SSID). This is the name your devices will see when they search for local wireless networks. 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 network as hidden (or non-broadcast). Most wireless scanning tools or any skilled attacker can easily discover the details of a hidden network.

To protect your home network, make sure you have a secured wireless network, you are using OpenDNS or a similar service and all the devices on your home network are updated and current.

- The next step is ensuring that only people you know and trust can connect to and use your wireless network, and that those connections are encrypted. You want to be sure that neighbors or strangers cannot connect to or monitor your network. You can easily mitigate these risks by enabling strong security on your wireless access point. Currently, the best option is to use the security mechanism WPA2. By simply enabling this, you require a password for people to connect to your home 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 network). An open network allows anyone to connect to your wireless network without any authentication.
- Make sure the password people will use to connect to your wireless network is a strong, hard-to-guess password and that it is different from the administrator password. Remember, you most likely have to enter the password only once for each of your devices, as they will each store and remember the password.
- Many wireless access points support what is called a Guest Network. A Guest Network allows visitors to connect to your wireless access point and access the Internet, but they cannot connect to any of the devices on your home network. If you add a Guest Network, be sure to enable WPA2 and a different password for this network.
- If you can't remember the different passwords then use a password manager to securely store them.

OpenDNS

Once you have your wireless network configured, we recommend you configure your home network to use OpenDNS as your DNS servers (or a similar service, such as Norton ConnectSafe for Home). When you type a name into your browser, DNS is how your browser knows which server on the Internet to connect to. Services such as OpenDNS identify known, infected websites and stop any device connected to your home wireless network from accidentally visiting these infected websites. In addition, these services often give you the ability to filter and block objectionable websites. What makes this approach so effective is there is no software to install on your devices, you just make a change to your wireless access point.

Your Devices

The next step involves knowing what is connected to your home network and making sure those devices are secure. This used to be simple, as you only had a few devices connected in the past. Nowadays, however, almost anything can connect to your home network, including TVs, gaming consoles, baby monitors, speakers, your house thermometer and even your car. Once you identify all the devices on your home network, you may be surprised by just how many you have. The best way to keep all of these devices secure is to ensure they are always running the latest version of their operating system. Be sure you have auto-update enabled when possible. If this is not an option, then review and update your devices monthly, if possible. In addition, be sure to visit your Internet service provider's website, as they may provide free tools and services to help you secure your home network.

Become A Security Professional - SANS 2014

If you haven't been to SANS 2014 training in Orlando, you can't miss this on April 5-14! One of our biggest events of the year, you will have countless opportunities to develop and expand your network of security experts and friends, and learn more than you can imagine from the top instructors in the cybersecurity industry. For more information, please visit http://www.sans.org/event/sans-2014/welcome.

Resources

OpenDNS:	http://www.opendns.org
Norton ConnectSafe:	http://dns.norton.com/dnsweb/dnsForHome.do
Network Security Scanner:	http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
Password Managers:	http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

License