OUCH! | January 2012

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE…

- Administration
- Your Network Name
- Encryption & Authentication
- OpenDNS

Securing Your Home Wi-Fi Network

GUEST EDITOR

Raul Siles is the guest editor for this issue. Raul is the founder of and a senior security analyst with Taddong (www.taddong.com), a SANS author and instructor, and security passionate (www.raulsiles.com). You can follow Raul on Twitter at @taddong and on his blog at blog.taddong.com.

OVERVIEW

Wi-Fi networks (sometimes called by their technical name 802.11) allow people to wirelessly connect devices to the Internet, such as smartphones, gaming consoles, tablets, and laptops. Because Wi-Fi networks are simple to setup, many people install their own Wi-Fi networks at home. However, many home Wi-Fi networks are configured insecurely, allowing strangers or unauthorized people 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.

ADMINISTRATION

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 take the following steps when configuring your Wi-Fi access point for the first time.

- 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. So be sure to change the default administrator login and password to something that only you know.
- For administrative access to your Wi-Fi access point, we recommend you disable wireless access and instead require a physical network connection,

such as using an Ethernet cable. If you must have wireless administrative access, then at a minimum disable HTTP access and require HTTPS, which supports encryption.

SETTING YOUR WI-FI NETWORK NAME

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.

The key to a secure home Wi-Fi network is making sure only you have administrative access, your communications are encrypted, and that people have to authenticate to use your network.

ENCRYPTION & AUTHENTICATION

The next step is to ensure that only people you know and trust can connect to and use your Wi-Fi network and that those connections are encrypted. We want to be sure that 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 is to use 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 the password people will use to connect to your Wi-Fi network, make sure it is different from the administrator password and that the password cannot be easily guessed; we recommend at least 20 characters long. This may sound like a very long password, but remember 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 that 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.

Finally, we recommend you turn off or disable WPS (Wi-Fi Protected Setup). WPS is a specification designed to ease the process of securely setting up your Wi-Fi access point. At the time of publishing this newsletter, recent vulnerabilities were found that may allow an attacker full access to your wireless network if WPS is enabled.

OPENDNS

Once you have your Wi-Fi connection configured, 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 on the Internet to connect to. OpenDNS is a free service that helps ensure you connect only to safe websites. In addition, OpenDNS gives you the ability to manage what websites your family can connect to. If you want to filter and block objectionable material, this is a great resource. The OpenDNS website walks you through step-by-step how to configure your Wi-Fi access point to use OpenDNS.

RESOURCES

Some of the links shown below have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

OnGuard Online Wi-Fi Security:
http://preview.tinyurl.com/7sylsul

Security Encyclopedia:
http://preview.tinyurl.com/bpc2h23

WPS Vulnerability:
http://preview.tinyurl.com/cjs4l4w

OpenDNS:
http://www.opendns.org

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org