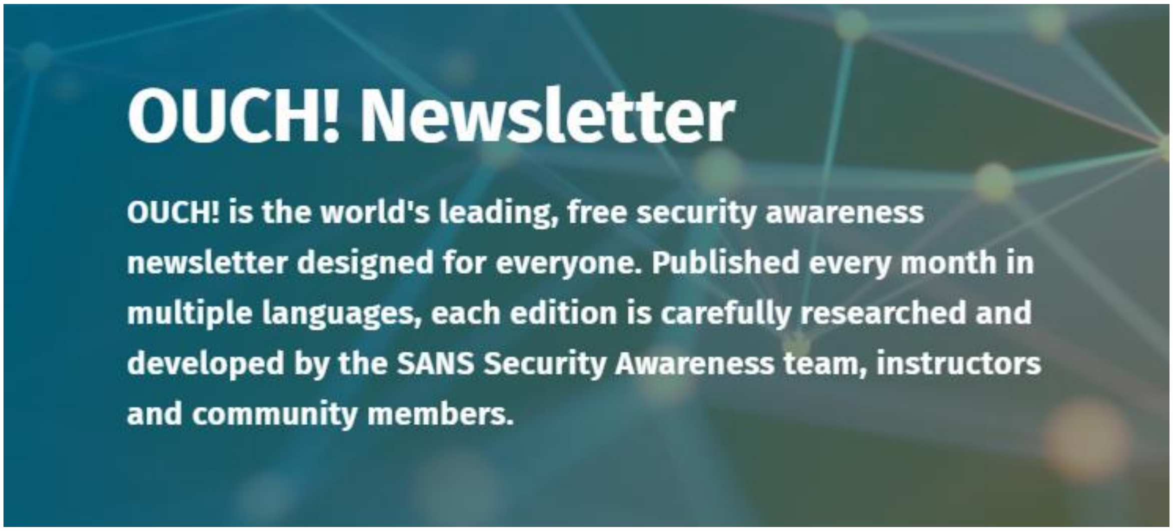

OUCH! Newsletter

OUCH! is the world's leading, free security awareness newsletter designed for everyone. Published every month in multiple languages, each edition is carefully researched and developed by the SANS Security Awareness team, instructors and community members.

June 2020 • The Monthly Security Awareness Newsletter for Everyone

Creating a Cyber Secure Home

Overview

In the past, building a home network was nothing more than installing a wireless router and several computers. Today, as so many of us are working, connecting, or learning from home, we have to pay more attention to creating a strong cyber secure home. Here are four simple steps to do just that.

Your Wireless Network

Almost every home network starts with a wireless (or Wi-Fi) network. This is what enables your devices to connect to the Internet. Most home wireless networks are controlled by your Internet router or a separate, dedicated wireless access point. They both work the same way: by broadcasting wireless signals which allow the devices in your house to connect to the Internet. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it.

1. Change the default administrator password to your Internet router or wireless access point, whichever is controlling your wireless network. The administrator account is what allows you to configure the settings for your wireless network.
2. Ensure that only devices you trust can connect to your wireless network. Do this by enabling strong security. Doing so requires a password to connect to your home network and encrypts online activities once connected.
3. Ensure the password used to connect to your wireless network is a strong password that is different from the administrator password. Remember, your devices store passwords, so you only need to enter the password once for each device.

If you’re not sure how to do these steps, check your Internet Service Provider’s website or check the website of the vendor for your router or wireless access point.

Passwords

Use a strong, unique password for each of your devices and online accounts. The key words here are *strong* and *unique*. The longer your password the stronger it is. Try using a series of words that are easy to remember, such as ***sunshine-doughnuts-happy***.

A unique password means using a different password for each device and online account. Use a password manager to remember all those strong passwords, which is a security program that securely stores all your passwords for you in an encrypted, virtual safe.

Additionally, enable two-step verification whenever available, especially for your online accounts. It uses your password, but also adds a second authentication step, such as a code sent to your smartphone or an app on your smartphone that generates the code for you. This is probably the most important step you can take, and it's much easier than you think.

Your Devices

The next step is knowing what devices are connected to your wireless home network and making sure all of those devices are trusted and secure. This used to be simple when you had just a computer. However, today almost anything can connect to your home network, including your smartphones, TVs, gaming consoles, baby monitors, printers, speakers, or perhaps even your car. Once you have identified all the devices on your home network, ensure that each of them is secure. The best way to do this is to change any default passwords on them and enable automatic updating wherever possible.

Backups

Sometimes, no matter how careful you are, you may be hacked. If that is the case, often the only way you can recover your personal information is to restore from a backup. Make sure you are doing regular backups of any important information and verify that you can restore from them. Most mobile devices support automatic backups to the Cloud. For most computers, you may have to purchase some type of backup software or service, which are relatively low-priced and simple to use.

Guest Editor

Randy Marchany is the CISO of Virginia Tech. He is also a Senior SANS instructor, and teaches the SEC566, SEC440, Implementing & Auditing the Critical Security Controls courses. Follow Randy @randymarchany.

To sign up for these monthly newsletters (or check out prior newsletters from SANS) copy and paste this link into your browser:
https://www.sans.org/security-awareness-training/ouch-newsletter