SANS SECURITY AWARENESS

OUCH! | January 2018

The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- Your Wireless Network
- Your Devices
- Passwords
- Backups

Creating a Cybersecure Home

Overview

Several years ago, creating a cybersecure home was simple; most homes consisted of nothing more than a wireless network and several computers. Today, technology has become far more complex and is integrated into every part of our lives, from mobile devices and gaming consoles to your home thermostat and your refrigerator. Here are four simple steps for creating a cybersecure home.

Guest Editor

Matt Bromiley is an incident responder by day, where he helps clients of all sizes deal with data breaches. He is also a SANS instructor, where he teaches FOR508, the Advanced Digital Forensics and Incident Response course. Follow Matt **@mbromileyDFIR**.

Your Wireless Network

Almost every home network starts with a wireless (or Wi-Fi) network. This is what enables all 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. The devices in your house can then connect via these signals. 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 to your Internet router or wireless access point. (Whichever one is controlling your wireless network.) The admin account is what allows you to configure the settings for your wireless network.
- Ensure that only people you trust can connect to your wireless network. 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, and once connected, their online activities are encrypted.
- Ensure the password used to connect to your wireless network is strong and that it is different from the admin password. Remember, you only need to enter the password once for each of your devices, as they store and remember the password.

Creating a Cybersecure Home

- 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 the network.

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

Follow these four simple steps to creating a cyber secure home: secure your Wi-Fi network, enable automatic updating, use unique passphrases, and enable backups.

Your Devices

The next step is knowing what devices are connected to your wireless home network and making sure all of those devices are secure. This used to be simple when you had just a computer or two. However, almost anything can connect to your home network today, including your smartphones, TVs, gaming consoles, baby monitors, speakers, or perhaps even your car. Once you have identified all the devices on your home network, ensure that each one of them is secure. The best way to do this is ensure you have automatic updating enabled on them wherever possible. Cyber attackers are constantly finding new weaknesses in different devices and operating systems. By enabling automatic updates, your computer and devices are always running the most current software, which makes them much harder for anyone to hack into.

Passwords

The next step is to use a strong, unique password for each of your devices and online accounts. The key words here are strong and unique. Tired of complex passwords that are hard to remember and difficult to type? So are we. Use a passphrase instead. This is a type of password that uses a series of words that is easy to remember, such as “Where is my coffee?” or “sunshine-doughnuts-happy-lost”. The longer your passphrase is, the stronger. A unique password means using a different password for each device and online account. This way, if one password is compromised, all your other accounts and devices are still safe. Can’t remember all those strong, unique passwords? Don’t worry, neither can we. That is why we recommend you use a password manager, which is a special security program that securely stores all your passwords for you in an encrypted, virtual safe.

Creating a Cybersecure Home

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

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 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.

Subscribe to OUCH!

Get the OUCH! security awareness newsletter every month for free, in the language of your choice. Simply subscribe at https://securingthehuman.sans.org/ouch.

Resources

Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Password Manager:	https://securingthehuman.sans.org/ouch/2017#september2017
Two-factor Authentication:	https://securingthehuman.sans.org/ouch/2017#december2017
Backups:	https://securingthehuman.sans.org/ouch/2017#august2017

License