Creating a Cyber Secure Home

1 Securing Yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true, it may be an attack. Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing; they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to craft customized phishing attacks.

Someone calls you pretending to be Microsoft tech support. They claim that your computer is infected, when they are really just cyber criminals that want access to your computer or want you to buy their fake anti-virus software.

2 Securing Your Home Network

Your Wi-Fi router (also called a Wi-Fi Access Point) is a physical device that controls who can connect to your wireless network at home:

Always change the default admin password on your Wi-Fi router to a strong password only you know.

Configure your Wi-Fi network so that if anyone wants to join it, they have to use a password. In addition, always configure your wireless network to use the latest encryption, which is currently WPA2.

Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, TVs or perhaps even your car.

3 Securing Your Computers / Devices

Here are some steps to protect any device connected to your home network:

Ensure all devices are protected by a strong PIN or passcode and always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged access.

Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."

Lori Rosenberg - Intuit

To learn more, subscribe to our monthly security awareness newsletter

securingthehuman.sans.org/ouch



4 Securing Your Accounts / Passwords

You most likely have a tremendous number of accounts online and on your devices and computers. Here are some key steps to protecting them:

Always use long passwords that are hard to guess. Use passphrases when possible. These are passwords that have multiple words, such as "Where Is My Coffee?"

Use a different password for each of your accounts and devices. Can't remember all of your strong passwords? We recommend you use a password manager to securely store them. This is a computer program that securely stores all of your passwords in an encrypted vault.

Use two-step verification whenever possible. Two-step verification is when you need a password and something else to log in to your account, such as a code sent to your smartphone.

On social media sites, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

5 What to Do When Hacked

No matter how secure you are, sooner or later, you may be hacked:

Create regular backups of all your personal information. If your computer or mobile device is hacked, the only way you can recover all of your personal information may be from backups.

If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password. If you no longer have access, contact the company.

Monitor your credit cards. If you see any charges you do not recognize, call the credit card company right away.

About the Poster

This poster was developed as a community project by the following security professionals:

Lori Rosenberg, eBay - Tonia Dudley, Charles Schwab - Rhonda Kelly, Oshkosh Corporation - Jonathan Matys, GM Financial - Karen McDowell, University of Virginia - Michele D'Anna, JHU/APL - Kitty Berra, Saint Louis University - Sorina Dunose, Ubisoft Divertissements Inc - Mark Merkow, Charles Schwab - Roberto Rodriguez, MySherpa - Antonio Merola, Poste Italiane - Barbara Filkins, skWorks - Vaman Amarjeet - James McQuiggan, Central Florida ISSA - Karla Thomas, Tower International - Tim Harwood, HS and TC - Denise Fredregill - Christopher Sorensen

© SANS Institute - You are free to print, distribute and post as many copies as you like; the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit securingthehuman.sans.org/ouch