OUCH! December 2020

Securing the Generation Gap

Overview

Trying to securely make the most of today's technology can be overwhelming for almost all of us, but it can be especially challenging for family members not as used to or as familiar with technology. Therefore, we wanted to share some key steps to help secure family members who may be struggling with technology and might misunderstand the risks that come with using it.

Focus on The Basics

Frequently, the best way to help secure others is to make security as simple as possible for them. Focus on the fewest steps that will have the biggest impact.

1. **Social Engineering:** Social engineering attacks are one of the primary ways most of us are targeted. Explain how scammers and con artists have operated for thousands of years, the only difference now is bad guys are using the Internet to fool us. Give examples, such as phishing emails pretending to be your bank or a package shipment or scammers calling pretending to be Tech Support or the government. Make sure family members understand they should never give their password, credit card, personal information or access to their computer to anyone. Remind them the more urgent the message is the more likely it is an attack. Some criminals prey on our loved ones longing for love and will pretend to be their dream prospect. Finally, be sure they know that if they feel uncomfortable or have questions about an email or someone calling them, that they call you first.
2. **Home Wi-Fi Network:** Take time to make sure their home Wi-Fi network is password protected and has the default admin password changed. You may also want to consider configuring the Wi-Fi network to use a secure form of DNS such as the free https://www.opendns.com. Secure DNS services not only help stop people from visiting infected websites but can give you control over the websites people can or cannot visit, which can be especially valuable if kids are visiting.
3. **Updating:** Emphasize that keeping systems, software and devices updated and current makes it much harder for criminals to compromise them. The simplest way to ensure this is to enable automatic updating wherever possible. If you have a device or system that is so old that you cannot update it, we recommend you replace it with a new device that does support updating.

© SANS Institute 2020

4. **Passwords:** Strong and secure passwords are key to protecting both devices and any online accounts. Walk your family members through how to create long passphrases. Passphrases may be easiest for them to both use and remember. Another idea is to install a password manager and teach them how to use it. It can allow your loved ones to use the Internet in an easy and secure manner, only having to remember a single password to unlock the vault. Depending on the solution, you may be even able to virtually administer it for them. If that does not work, perhaps have them write their passwords in a book and then store it in a convenient and secure place. For any critical online accounts, such as their financial accounts, you may also want to set up two-step verification. Be sure to have a legacy plan for any online accounts the same way you would prepare a will for physical assets.
5. **Backups:** When all else fails, backups will save the day. Make sure family members have a simple, reliable backups in place. For many, a cloud-based approach is often the simplest.

If you have family members feeling overwhelmed, help them by just focusing on the basics, keeping security as simple as possible. Also, be patient, give time and space to make mistakes, and help others to not repeat them. Finally, consider having them sign up for the OUCH! newsletter.

Guest Editor

Chris Dale (Twitter @chrisadale) is a principal consultant at River Security, an European security consulting firm, and a certified SANS instructor (https://www.sans.org/profiles/chris-dale/).
Find Chris at LinkedIn here: https://www.linkedin.com/in/chrisad/

Resources

Social Engineering: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Password Managers: https://www.sans.org/security-awareness-training/resources/password-managers-0
Updating: https://www.sans.org/security-awareness-training/resources/power-updating
Backups: https://www.sans.org/security-awareness-training/resources/got-backups
Digital Inheritance: https://www.sans.org/security-awareness-training/resources/digital-inheritance

OUCH! is published by SANS Security Awareness and is distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Walter Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley