OUCH! | October 2017

The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

Helping Others Secure Themselves

Overview

Many of us feel comfortable with technology, to include how to use it safely and securely. However, other friends or family members may not feel so comfortable. In fact, they may be confused, intimidated, or even scared by it. This makes them very vulnerable to today's cyber attackers. Cyber security does not have to be scary; it's actually quite simple once you understand the basics. They most likely just need a guide like you to help them understand the basics.

Guest Editor

Randy Marchany (Twitter: **@randymarchany**) is the CISO at Virginia Tech and a certified SANS Institute instructor.

Five Simple Steps

Here are five simple steps you can take to help others overcome those fears and securely make the most of today's technology. For more information on each of these points, refer to the References section at the end of this newsletter.

1. Social Engineering: Social engineering is a common technique used by cyber attackers to trick or fool people into doing something they should not do, such as sharing their password, infecting their computer, or sharing sensitive information. This is nothing new. Scams and con artists have existed for thousands of years. The only difference now is bad guys are applying these same concepts to the Internet. You can help others by explaining to them the most common clues of a social engineering attack, such as when someone creates a tremendous sense of urgency, when something is too good to be true, or when a cyber attacker pretends to be someone you know but their messages don't sound like them. Share examples of common social engineering attacks, such as phishing emails or the infamous Microsoft tech-support phone calls. If nothing else, make sure family members understand they should never give their password to anyone or allow remote access to their computer.
2. Passwords: Strong passwords are key to protecting devices and any online accounts. Walk your family members through how to create strong passwords. We recommend passphrases, as they are the easiest to both type and remember. Passphrases are nothing more than passwords made up of multiple words. In addition, help

Helping Others Secure Themselves

them to install and use a password manager. It is important to have a unique password for each of your devices and accounts. If a password manager is overwhelming, perhaps teach them to write their passwords down, then store those passwords in a secure location. Finally, help them enable two-step verification (often called two-factor authentication) for important accounts. Two-step verification is one of the most effective steps you can take to secure any account.

Help others securely make the most of technology by sharing these five simple steps with them.

3. Patching: Keeping systems current and fully up-to-date is a key step anyone can take to secure their devices. This is not only true for your computers and mobile devices, but anything connected to the Internet, such as gaming consoles, thermometers, or even lights or speakers. The simplest way to ensure all devices are current is to enable automatic updating whenever possible.
4. Anti-Virus: People make mistakes. We sometimes click on or install things we probably should not, which could infect our systems. Anti-virus is designed to protect us from those mistakes. While anti-virus cannot stop all malware, it does help detect and stop the more common attacks. As such, make sure any home computers have anti-virus installed and that it is current and active. In addition, many of today's anti-virus solutions include other security technology, such as firewalls and browser protection.
5. Backups: When all else fails, backups are often the only way you can recover from mistakes (like deleting the wrong files) or cyber attacks (like ransomware). Make sure family and friends have an automated file backup system in place. Often, the simplest solutions are Cloud-based. They back up your devices hourly or whenever you make a change to a file. These solutions make it easy not only to back up data, but to recover it.

Securing Kids When Visiting Others

If you are comfortable with technology, you most likely not only have secured yourself, but helped secure your kids. However, when kids visit a relative who is not comfortable with technology, such as grandparents, these relatives may not be aware of how to best protect kids online or your expectations. Here are some steps you can take to help protect kids when they visit others, especially family:

Helping Others Secure Themselves

- Rules. Be sure that if there are any rules or expectations you have for kid's security, others know about them. For example, are there any rules on how long kids can be online, whom they can talk to, or what games they can or cannot play? Trust us, don't plan on kids explaining the rules to other family members. One idea is to create a 'rules sheet' and share that with any relatives your kids frequently visit.
- Control. If a child understand technology better than their guardians, they may take advantage of that. For example, kids may ask for or gain administrative rights to a grandparent's computer and then do whatever they want, such as installing that game you may not want them playing. Make sure relatives understand they should not give the kids any additional access beyond what has been established.

Finally, suggest to people that they subscribe to resources, such as the OUCH! newsletter, so they can continue to learn on their own. This newsletter is published every month for free in over 20 languages. Sign up at https://securingthehuman.sans.org/ouch.

2017 Security Awareness Report

Learn the latest trends and lessons learned in building mature awareness programs from over 1,000 security awareness professionals. https://securingthehuman.sans.org/report.

Resources

Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Password Manager:	https://securingthehuman.sans.org/ouch/2017#september2017
Two-Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Backup and Recovery:	https://securingthehuman.sans.org/ouch/2017#august2017
Securing Today's Online Kids:	https://securingthehuman.sans.org/ouch/2017#may2017

License