The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Overview
- Five Key Steps

Five Steps to Staying Secure

Overview

As technology gains a more important role in our lives, it also grows in complexity. Given how quickly technology changes, keeping up with security advice can be confusing. It seems like there is always new guidance on what you should or should not be doing. However, while the details of how to stay secure may change over time, there are fundamental things you can always do to help protect yourself. Regardless of what technology you are using or where you are using it, we recommend the following five key steps.

Guest Editor

Lenny Zeltser focuses on safeguarding customers' IT operations at NCR Corp and teaches malware combat at the SANS Institute. Lenny is active on Twitter as **@lennyzeltser** and writes a security blog at **blog.zeltser.com**.

Five Key Steps

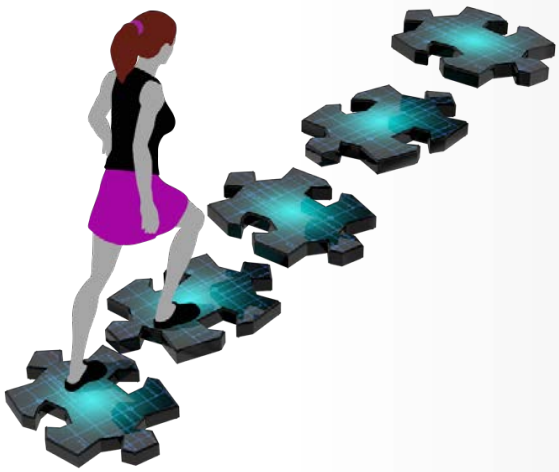
Each of the five steps below is a simple overview. To learn more about each step, refer to the Resources section at the end of this newsletter.

1. You: First and foremost, keep in mind that technology alone can't protect you. Attackers have learned that the easiest way to bypass most security technology is by attacking you. If they want your password or your credit card, the easiest thing for them to do is to trick you into giving them this information. For example, they can call you pretending to be Microsoft tech support and claim that your computer is infected, when they are really just cyber criminals that want you to give them access to it. They could even send you an email explaining that your package could not be delivered and asks you to click on a link to confirm your address. You are then taken to a malicious website that will hack into your computer. Ultimately, the greatest defense against attackers is you. Be suspicious. By using common sense, you can spot and stop most attacks.

2. Updating: Make sure your computers, mobile devices, apps and anything else connected to a network are running the latest version of their software. Cyber criminals are constantly looking for vulnerabilities in the technologies you use. When they discover these weaknesses, they use special programs to exploit the vulnerability and hack

Five Steps to Staying Secure

into whatever technology you are using, including your network, your computer and your mobile devices. Meanwhile, the companies that created the technology you are using work hard to keep it up-to-date. Once a vulnerability is known, they create a patch to fix it and release this patch to the public. By ensuring your computers and mobile devices have these updates, you reduce the number of known vulnerabilities, making it much harder for someone to hack you. To stay current, enable automatic updating whenever possible. This rule applies to almost any technology connected to a network, including Internet-connected TVs, baby monitors, home routers, gaming consoles or even your car. If your computer's operating system, mobile device or any other technology you are using is no longer supported and will no longer receive any updates, we recommend you get a new version or device that is supported.



By following these five key steps, you will go a long way towards protecting yourself while leveraging the latest technology.

3. Passwords: The next step to protecting yourself involves using a strong, unique password for each of your devices, online accounts and applications. The key words here are strong and unique. A strong password means one that cannot be easily guessed by hackers or by their automated programs. Instead of a single word, use a long passphrase of multiple words with some symbols and numbers thrown in for good measure. Unique means using a different password for each device and online account. This way, if one password is compromised, all of 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. This is a specialized application for your smartphone or computer that can securely store all of your passwords in an encrypted format. Finally, if any of your accounts support two-step verification, we highly recommend you always enable it, as this is one of the strongest ways to protect your account.

4. Encryption: Next we recommend the use of encryption. Encryption makes sure that only you or people you trust can access your information. Data can be encrypted in two places: at rest and in motion. Encrypting data at rest means protecting it when it is stored as files on places like your hard drive or a USB stick. Most

Five Steps to Staying Secure

operating systems allow you to automatically encrypt all of your data using features such as Full Disk Encryption. We recommend you enable this whenever possible. Encrypting data in motion means encrypting data as it's transmitted from your computer or device to others, such as when you are banking online. A simple way to verify if encryption is enabled is to make sure that the address of the website you're visiting starts with "https:" and has the image of a closed padlock next to it.

5. Backups: Sometimes, no matter how careful you are, one of your devices or accounts may be compromised. If that is the case, often your only option to ensure your computer or mobile device is free of malware is to fully wipe it and rebuild it from scratch. The attacker might even prevent you from accessing your personal files, photos and other information stored on the compromised system. Your only option might be to restore all of your personal information from a backup. Make sure you are doing regular backups of any important information and verify that you can restore from them. Most operating systems and mobile devices support automatic backups.

National Cyber Security Awareness Month (NCSAM)

Cyber security awareness month is here and, as a result, SANS Securing The Human is offering some free resources! You can attend one of our webinars, download a free tip sheet to share with your employees and/or take our Security Awareness Survey to receive access to the results. To learn more, visit us at: http://www.sans.org/info/167527.

Resources

Email Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Securing Your New Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Strong Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Encryption:	http://www.securingthehuman.org/ouch/2014#august2014
Personal Backup and Recovery:	http://www.securingthehuman.org/ouch/2013#september2013

License