The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- You
- Passwords
- Updating
- Backups

Four 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 protect yourself. Regardless of what technology you are using or where you are using it, we recommend the following four key steps. To learn more about any of the steps below, refer to the Resources section at the end of this newsletter.

Guest Editor

Ryan Johnson focuses on ensuring that organizations are prepared to respond to the inevitable breach and teaches Advanced Network Forensics at the SANS Institute. Ryan is active on Twitter as **@ForensicRJ**.

1. You: First and foremost, keep in mind that technology alone will never be able to fully protect you. Attackers have learned that the easiest way to bypass even the most advanced security technology is by attacking you. If they want your password, credit card, or personal data, 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 in reality they are just cyber criminals that want you to give them access to your computer. Or perhaps they will send you an email explaining that your package could not be delivered and ask you to click on a link to confirm your mailing address, when in reality they are tricking you into visiting a malicious website that will hack into your computer. This is how attacks such as Ransomware or CEO Fraud start. Ultimately, the greatest defense against attackers is you. Be suspicious. By using common sense, you can spot and stop most attacks.

2. Passwords: The next step to protecting yourself involves using a strong, unique password for each of your devices and online accounts. The key words here are strong and unique. A strong password means one that

Four Steps to Staying Secure

cannot be easily guessed by hackers or by their automated programs. Tired of complex passwords that are hard to remember and difficult to type? Try using a passphrase instead. Instead of a single word, use a series of words that is easy to remember, such as “Where is my coffee?” 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 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, which is a specialized application for your smartphone or computer that securely stores all of your passwords in an encrypted format.

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

Finally, one of the most important steps you can take to protect any account is enable two-step verification. Passwords alone are no longer enough to protect accounts; we all need something stronger. Two-step verification is much stronger. It uses your password, but also adds a second step, either something you are (biometrics) or something you have (such as a code sent to your smartphone or an app on your smartphone that generates the code for you). Enable this option on every account you can, including your password manager, if possible. Two-step verification is probably the single most important step you can take to protect yourself, and it’s much easier than you think.

3. Updating: Make sure your computers, mobile devices, apps, and anything else connected to the Internet are running the latest software versions. Cyber criminals are constantly looking for new vulnerabilities in the software your devices use. When they discover vulnerabilities, they use special programs to exploit them and hack into the devices you are using. Meanwhile, the companies that created the software for these devices are hard at work fixing them by releasing updates. By ensuring your computers and mobile devices install these updates,

Four Steps to Staying Secure

you make it much harder for someone to hack you. To stay current, simply 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 perhaps even your car. If your operating systems or devices are old and no longer supported with security updates, we recommend you replace them with new ones that are.

4. Backups: Sometimes, no matter how careful you are, you may be hacked. 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 hacked system. Often the only way to restore all of your personal information is from 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. In addition, we recommend you store your backups in either the Cloud or offline to protect them against cyber attackers.

An Easier Way to Manage Your Security Awareness Program

SANS Institute's new Advanced Cybersecurity Learning Platform (ACLP) makes deploying, maintaining, and measuring awareness programs easier and more effective. Learn more at https://securingthehuman.sans.org/u/jGf.

Resources

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
Two-Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015

License