OUCH!

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

Four Simple Steps to Staying Secure

Overview

Making the most of technology safely and securely can seem overwhelming and confusing. However, regardless of what technology you are using or how you are using it, here are four simple steps that will help you stay secure.

1. You: First and foremost, technology alone cannot fully protect you; you are your best defense. Attackers have learned that the easiest way to get what they want is to target you rather than your computer or other devices. If they want your password, credit card, or control of your computer, they'll attempt to trick you into giving it to them, often by creating a sense of urgency. For example, they might call you pretending to be Microsoft tech support and claim that your computer is infected, when in reality they are just cyber criminals who want you to give them access to your computer. Or perhaps they send you an email warning that your package could not be delivered and pressuring you into clicking 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. Ultimately, the greatest defense against attackers is you. By using common sense, you can spot and stop many attacks.

2. Passphrases: Modern computing speeds have made the old, eight-character password outdated and vulnerable. When a site asks you to create a password, create a strong and unique passphrase instead. A passphrase is a type of password that uses a series of words that is easy to remember, such as *bee honey bourbon rain*. The longer your passphrase is, the stronger. A unique passphrase means using a different one for each device or online account. This way, if one passphrase is compromised, all of your other accounts and devices are still safe. Can't remember all those passphrases? Use a password manager, which is a specialized program that securely stores all your passphrases in an encrypted format (and offers lots of other great features as well).

Finally, enable two-step verification (also called two-factor or multi-factor authentication). It uses your password but also adds a second step, such as entering a code sent to your smartphone or from an app that generates the code for you. Enabling two-step verification is probably the most important step you can take to protect your online accounts, and it's much easier than you may think.

3. Updating: Make sure each of your computers, mobile devices, programs, and apps is running the latest version of its software. Cyber attackers 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 the vulnerabilities by releasing updates. By ensuring your computers and mobile devices install these updates promptly, 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, security cameras, home routers, gaming consoles, and even your car.

4. Backups and recovery: No matter how careful you are, you still may be hacked. If that is the case, often the only way to restore all of your personal information is from backup. Make sure you make regular backups of any important information and verify that you can restore your data from them. Most operating systems and mobile devices support automatic backups, either to external drives or to the cloud.

Subscribe to OUCH! and receive the latest security tips in your email every month - sans.org/ouch.

Do you think you've got what it takes to get into the cyber security industry? Or are you looking to improve your existing skillset? Training with SANS helps you achieve your goals. Level Up with SANS today! sans.org/Level-Up-Ouch

Guest Editor

SANS Certified Instructor **Steve Anson** *provides guidance to IT security teams and governments around the world to improve their security posture. Steve is the author of the upcoming book* Applied Incident Response *and provides free resources for IT security practitioners at* AppliedIncidentResponse.com.

Resources

Social Engineering:	https://www.sans.org/u/W3G
Personalized Scams:	https://www.sans.org/u/W3Q
Making Passwords Simple:	https://www.sans.org/u/W3V
Got Backups:	https://www.sans.org/u/W40