OUCH! | December 2012

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE…

- **Starting Secure**
- **Staying Secure**
- **Recovery**

Seven Steps to a Secure Computer

GUEST EDITOR

Guy Bruneau is the guest editor for this issue. Guy holds the GIAC Security Expert (GSE) certification and successfully completed the SANS Cyber Guardian (Blue Team) program. He is a SANS certified instructor and a SANS Incident Storm Center handler. Learn more and follow him on Twitter at @guybruneau.

OVERVIEW

While handheld devices such as smartphones and tablets provide new ways for us to leverage technology, computers are often still the primary tool we use for our professional and personal lives.

As a result, your computer, whether at work or at home, still remains a primary target for cyber criminals. By following the seven simple steps outlined below, you can help secure your computer and protect it against most known attacks.

1. STARTING SECURE

The first step to a secure computer is starting with a computer you can trust. If you purchased a new computer directly from a well-known vendor, then you should be able trust it and the pre-installed software. If you have purchased a used computer, then do not trust it. The used computer may have been accidentally (or intentionally) infected by the previous owner. Trying to secure a computer that is already infected does no good. The first step you should take after acquiring a used computer is reformat the hard drive and reinstall the operating system (be sure to ask someone you trust for help if you are not sure how to do this).

2. UPDATING

The next step is updating your computer. Cyber attackers are always identifying new weaknesses in computers and their applications. When computer and software vendors learn about these new vulnerabilities, they develop and release fixes, called updates or patches, to fix the problem. When you purchase a new computer or reinstall the operating system, your computer is most likely already out of date. As such, the first step you want to take is connect to the Internet and update your computer's operating system. Be sure that when you do connect to the Internet, your new computer is protected behind a firewall or home Wi-Fi access point. In addition, most computer operating systems, including Windows and OS X (and even many applications), have an automatic updating feature built-in. Enable automated updating to check for updates at least once a day; this helps ensure your computer will remain updated and secure. If a vendor releases a patch that you have to manually install, be sure to install it as soon as possible.

3. SECURITY SOFTWARE

Once your computer is updated you want to ensure you have security software installed and enabled. The two most common types of security software are anti-virus and firewalls. Anti-virus helps identify infected files you may have downloaded or shared with others and stops these malicious files from harming your computer. Firewalls act like a virtual policeman; they determine who can and cannot talk to your computer. Many security vendors now offer entire security software suites that include firewall, anti-virus and other software options. You may want to consider purchasing an entire security package.

4. ACCOUNTS

Every person that has authorized access to your computer should have their own separate account protected by a unique, strong password. Never share accounts. If this is a personal computer for home use, create a separate account for each member of your own family, especially children.

By following these simple steps you can help ensure a secure computer.

This way you can apply different controls to each user (such as parental controls for your children) and track who did what. In addition, grant each user the minimum privileges they need to use the computer. Never give someone administrative access unless they absolutely need it, including yourself. Only use administrative privileges when you need them, such as to install software or changing a system configuration.

5. SECURITY ON THE GO

If your computer is portable, such as a laptop, you may want to consider full disk encryption (FDE). Encryption helps ensure that the data on your computer is protected even if you lose it. You may also want to ensure the computer screen is password locked, so people cannot

Seven Steps to a Secure Computer

access the system when you are away from it. Finally, some laptops now support remote location and/or wiping to help you locate a missing laptop or permanently erase sensitive data if it cannot be recovered.

6. USING THE COMPUTER

No amount of technology can protect your computer against every threat. While everything we have covered so far will help secure your computer, the last element we have to secure is you, the computer user. Know and understand that bad guys are always trying to trick you. If you receive a message that seems odd or suspicious, don't click on any links or attachments. If someone calls you telling your computer is infected and you need to install software, this is most likely a scam. In many ways you are the best defense for your computer, not technology.

7. BACKUPS

Finally, even if you take all the steps we have covered, there is always a chance your computer can get hacked, have a hard drive failure or some other catastrophe. Your last defense is backups. We highly recommend you regularly backup any important information (documents, pictures, videos, etc) to either an external hard drive or use a backup Cloud service, or perhaps even both.

RESOURCES

Some of the links have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

Free Security Checkups:
http://preview.tinyurl.com/bxph6a8

Microsoft Security:
http://www.microsoft.com/security

Mac OS X Security:
http://preview.tinyurl.com/abl6xm7

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

BECOME A SECURITY PROFESSIONAL

Become a certified security professional from the largest and most trusted security training organization in the world at SANS 2013. Over 40 security classes taught by the world's leading experts. March 08-15, 2013 in Orlando, FL. http://www.sans.org/event/sans-2013/