OUCH! February 2023

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for You

Do I Need Security Software?

Overview

When you bought a new computer years ago, you often had to install additional security software on your computer to help ensure it was secure against cyber attackers. However, most of today's computers and devices have numerous security features already built into them, such as automatic-updating, firewalls, disk encryption, and file protection. In addition, Microsoft provides on Windows computers security functionality called Microsoft Defender, which includes additional features such as anti-virus. In many ways today's systems by default are much more secure. In fact, YOU are most likely now the greatest weakness. This is why cyber attackers continually target people, attempting to trick you into doing things you should not do, such as give up your passwords, click on links, or open email attachments that install malware on your computers or share your credit card information.

Which tools should I consider?

If you want to take some additional steps to secure your systems, there are some additional security programs you can consider.

Password Manager: Passwords can be complex and overwhelming, especially having to remember potentially hundreds of different passwords. A Password Manager is a secure vault that protects and stores all your passwords for you so you have to only remember one master password. In addition, they can log you into websites, generate passwords for you, and help validate certain websites.

Virtual Private Network (VPN): VPNs primarily focus on protecting your privacy by encrypting your connection to the Internet and hiding your source location.

Security Suites: These are packages of security software that provide a collection of additional security features above and beyond what your operating system already provides. For example, filtering for dangerous websites, parental controls, and often a VPN. Each suite has different features, so research the one that you feel is best if you need one.

Selecting a Security Vendor

If you need to purchase additional security tools or software, there are many different vendors from which to choose. Which one should you choose? Quite often different vendors are more similar in the features they offer than they are different. The key is to use a solution from a trusted vendor. You don't want to accidentally purchase and install something distributed by cyber criminals that is infected with malware.

Purchase tools from only well-known vendors that you have heard of and trust. Never purchase a tool from a company you know nothing about, that is brand new, or has no comments or lots of negative comments. You want to be sure that the solution you are purchasing is legitimate and actively updated and maintained. You may even want to consider in what country the vendor is based. There are numerous online sites that have reviews of trusted vendors showcasing the differences in features and costs of their security software.

Be careful of free tools. While excellent free security tools do exist, there can be some concerns. These tools may be limited in features, difficult to use, or not updated frequently. In some cases, free tools may be developed by cyber attackers and then infected with malware.

Remember, while these security tools are helpful, start first with your computer's built-in security features, to include enabling automatic updating. Today's operating systems are very secure by default. Finally, you are your own best defense. Be cautious with any odd or suspicious phone calls, emails, or text messages. No security software in the world can protect you from someone trying to trick or fool you into something you should not do.

Guest Editor

Nico "Dutch_OsintGuy" Dekens is a Certified SANS instructor and former Government Intelligence Analyst specialized in Open-Source Intelligence (OSINT).
More info about Nico here: https://www.sans.org/profiles/nico-dekens/
and here https://www.dutchosintguy.com.

Resources

Password Managers: https://www.sans.org/newsletters/ouch/password-managers/
The Power of Updating: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Virtual Private Networks: https://www.privacyguides.org/vpn/
Social Engineering: https://www.youtube.com/watch?v=lc7scxvKQOo
Security Suite Reviews: https://www.pcmag.com/picks/the-best-security-suites