The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- How anti-virus software works
- How it can and cannot protect your computer
- Tips for using anti-virus software
- Trusted sources for anti-virus programs

# Understanding Anti-Virus Software

## GUEST EDITOR

Lenny Zeltser served as the guest editor for this issue of OUCH! Lenny leads the security consulting team at Savvis (www.savvis.com) and teaches malware defense courses (http://www.CombatingMalware.com) for the SANS Institute. He is active on Twitter at @lennyzeltser and writes regularly on his security blog at blog.zeltser.com.

## OVERVIEW

Any computer can be infected by malware. Malware is a catch-all term for malicious programs, such as viruses, worms, Trojans, and spyware, which are designed to infect and take control of your computer. Once your computer has been infected, bad guys can capture all your keystrokes, steal your documents, and use your computer to attack other computers. Anti-virus software is designed to protect your computer against malware. It is available as a stand-alone product and is also included in most security software packages.

Anti-virus detects and blocks attempts by the bad guys to infect your computer. The problem is that anti-virus can no longer keep up with the bad guys. There are so many new versions of malware being released every day that no anti-virus can detect and protect against all of them. For this reason, it is possible for your computer to be infected even with the latest version of anti-virus installed. To understand why this is so, let's look at how most anti-virus programs work.

## SIGNATURE DETECTION

Most anti-virus programs work like the human immune system by scanning your computer for the signatures (patterns) of digital pathogens and infections. They refer to a dictionary of known malware, and if something in a file matches a pattern in the dictionary, the anti-virus software attempts to neutralize it. Like the human immune system, the dictionary approach requires updates, like flu shots, to provide protection against new strains of malware. Anti-virus can only protect against what it recognizes as harmful. Again, the problem is the bad guys are developing new malware so fast that anti-virus developers cannot keep up. Your computer is vulnerable during the delay between the time new malware is identified and the time a dictionary

# Understanding Anti-Virus Software

update is released by anti-virus vendors. This is why it is important that you keep your anti-virus product as up-to-date as possible.

## BEHAVIOR DETECTION

In this approach, instead of attempting to identify known malware, anti-virus software monitors the behavior of software installed on your computer. When a program acts suspiciously, such as trying to access a protected file or to modify another program, anti-virus spots the suspicious activity and alerts you to it. This approach provides protection against brand new types of malware that do not yet exist in any dictionary. The problem with this approach is that it can generate a large number of false warnings. You, the computer user, may be unsure about what to allow or not allow and over time become desensitized to all those warnings. You might be tempted to click *Accept* on every warning, leaving your computer wide open to attack and infection.

## ANTI-VIRUS TIPS

***1. Don't Assume You're Not At Risk***

Every computer, regardless of its operating system, is vulnerable to attack. While anti-virus cannot protect against all types of malware, the security of your computer is enhanced substantially when anti-virus software is installed, up to date, and working properly.

***2. Download Only From Trusted Sources***

Obtain security software only from known, trusted sources and vendors. It is a common ploy of cybercriminals to pretend to be selling anti-virus programs that are in fact malware. We list several trusted sources for anti-virus solutions at the end of this newsletter.

***3. Keep Your Software Current***

Make sure you have the latest version of your anti-virus

***It is important to keep your anti-virus product as up-to-date as possible.***

# Understanding Anti-Virus Software

product installed and that it is set to update automatically. Check the status of the signature updates periodically to make sure they are current.

***4. Don't Delay Updates***

If your computer has been offline or powered off for a while, your anti-virus will most likely need an update when you turn it back on or reconnect it to the Internet. Do not postpone these updates.

***5. Scan Additional Devices***

Make sure your anti-virus automatically scans portable devices, such as USB sticks, when you plug them into your computer.

***6. Track Warnings And Alerts***

Pay attention to the onscreen warnings and alerts generated by your anti-virus software. Most alerts include the option of clicking on a link to get more information or a recommendation about what to do next. At the office, write down the alert messages and contact your computer help desk or security team.

***7. Don't Disable The Software***

Do not disable your security software because you feel it is slowing down your computer, blocking a website, or preventing you from installing an app or program. Disabling your anti-virus will expose your computer to unnecessary risk and could result in a serious security incident. If problems persist, replace your anti-virus with another product.

***8. Install One Program Only***

Do not install multiple anti-virus programs on your computer at the same time. Doing so may leave your computer with less protection instead of providing more protection.

***9. Consider A Security Suite***

Understand that anti-virus cannot protect your computer against all threats. We recommend you install a security suite that includes additional tools, such as a firewall, browser protection, and other advanced security features.

## TRUSTED SOURCES

PC Magazine – http://preview.tinyurl.com/48tc9y5

Consumer Reports – http://preview.tinyurl.com/5ve99ck

## LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org.



*Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy*