

# Overview

- Overview
- How Anti-Virus Works
- Anti-Virus Tips

## Overview

Anti-virus is a security program you install on your computer or mobile device to protect it from getting infected by malware. The term “malware” is a catch-all phrase for any type of malicious software, such as viruses, worms, Trojans and spyware. In fact, the term malware comes from combining the words malicious and software. If your computer has become infected by malware, a cyber attacker can capture all of your keystrokes, steal your documents or use your computer to attack others. Contrary to what some people believe, any operating system, including Mac OS X and Linux, can be infected.

### Guest Editor

Jake Williams is the founder of Rendition Infosec ([www.renditioninfosec.com](http://www.renditioninfosec.com)) SANS instructor and course author. He is active on Twitter as [@MalwareJake](https://twitter.com/MalwareJake) and writes on his blog at [malwarejake.blogspot.com](http://malwarejake.blogspot.com).

You can purchase anti-virus software as a standalone solution or it is often included as part of a security package. The problem is that anti-virus can no longer keep up with cyber attackers; they are constantly developing and releasing new types of malware. There are so many new versions of malware released every day that no anti-virus program can detect and protect against all of them. This is why it is important for you to understand that while anti-virus will help protect your computer, it cannot detect or stop all types of malware. To better understand better why, let's look at how most of these programs work.

## How Anti-Virus Works

Signature detection works like the human immune system. It scans your computer for characteristics or signatures of programs known to be malicious. It does this by referring to a dictionary of known malware. If something on your computer matches a pattern in the dictionary, the program attempts to neutralize it. Like the human immune system, the program looks for patterns against what it recognizes as harmful. The problem is that cyber attackers are developing new malware so fast that



anti-virus vendors cannot keep up. As a result, no matter how recently your anti-virus was updated, there is always some new variant of malware that can potentially bypass your anti-virus software.

With behavior detection, anti-virus does not attempt to identify known malware, but monitors the behavior of software installed on your computer. When a program or to modify another program, behavior-based anti-virus software 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 false warnings. You, the computer user, may be unsure about what to allow or not allow and become desensitized to all those warnings over time. You might be tempted to click on “Accept” on every warning, leaving your computer open to attack and infection. In addition, by the time the behavior is detected, the malware most likely has already run on your machine and you may not know what actions the malware took

*While anti-virus is an important part of your security, it cannot detect or stop all attacks. Ultimately, you are the best defense, not just technology.*

Anti-virus is an important part to securing your computer and mobile devices. Whenever possible, we recommend you install and actively use it. However, the key point to remember is that regardless of how your anti-virus works, it can never protect you from all types of malware. Ultimately, you, and not just technology, are the best defense against today’s cyber attackers.

## What Is Anti-Virus?

Make sure your anti-virus automatically scans portable media, such as USB sticks, and ensure real-time protection is on. Pay attention to the on-screen warnings and alerts generated by your anti-virus software. Most alerts include the option of getting more information or a recommendation about what to do next. If you get an alert on a work-supplied computer, be sure to contact the help desk or your supervisor immediately.

Do not disable or uninstall your anti-virus 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 you to unnecessary risk and could result in a serious security incident. If problems persist on a work computer, contact your help desk. If the problems persist on your personal computer, try contacting the anti-virus vendor, visiting their website for more information or replacing your anti-virus with another product.

Do not install multiple anti-virus programs on your computer at the same time. Doing so will most likely cause the  
 Learn to recognize the warnings that your anti-virus software produces. Cyber attackers can set up malicious websites  
 buttons on these websites can actually harm your computer.

## Security Awareness Posters

Be sure to check out our free security awareness posters at [@cc|KDD, É•æ}•É\[!\\*Dà}~\[DFÍGÉÍG](#). To get hard copies of future posters, register for a SANS portal account at [@cc|KDD, É•æ}•É\[!\\*Dà}~\[DFÍGÉÍÍ](#).

### Resources

- [@cc|KDD, É•æ}•É\[!\\*Dà}~\[DFÍGÉÍG](#)
- [@cc|KDD, É•æ}•É\[!\\*Dà}~\[DFÍGÉÍÁ}\[ç^{à^!GÉFI](#)
- [@cc|KDD, É•æ}•É\[!\\*Dà}~\[DFÍGÉFHÀ-^à!~æ!^GÉFH](#)
- [@cc|KDD, É•æ}•É\[!\\*Dà}~\[DFÍGÉFI{æ^GÉFI](#)

### License

OUCH! is published by SANS Securing The Human and is distributed under the [Ô!^æçç^ÁÔ\[ { { \[ \] •ÁÓÏÈPÔÈPÖÄIÈÁ\[ä&^}•^](#). You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit [É•æ}•É\[!\\*Dà}~\[DFÍGÉÍÍ](#).



[É•æ}•É\[!\\*Dà}~\[DFÍGÉÍÍ](#)

[@securethehuman](#)

[@securethehuman](#)



[É•æ}•É\[!\\*Dà}~\[DFÍGÉÍÍ](#)