Avoiding Malware on a Windows Computer

By: Mike Young – Apr. 4, 2013

The term “malware”, a portmanteau of “malicious” and “software”, is an all-encompassing term for all types of malicious software; viruses, trojans, worms, rootkits, keyloggers, adware, and spyware, among other classifications. With the explosion of Internet use on home computers in the past decade and a half, coupled with security somewhat being an afterthought in the design of many versions of Windows, and the fact that Windows dominates the home computing market, making it a large and lucrative target for malicious hackers, malware has run rampant. A joke suggests the ultimate in Internet/network security; a pair of scissors, to cut your connection to the Internet. Some of the most common ways to get infected with malware from the Internet are by downloading and running infected files sent via email, clicking on dangerous links in email or instant messages that lead to malicious websites and malware downloads, and accidentally or mistakenly downloading software that claims to fix to an alleged problem, when in fact the downloaded software actually is malware.

In late 2009, Microsoft released Security Essentials, free (for home and limited commercial use) anti-malware software for currently supported versions of its Windows operating systems. Some portions of this guide assume that you are using Microsoft Security Essentials (available for Windows XP, Vista, and 7) or Windows Defender (built into Windows 8, though possibly disabled if your Windows 8 system came preloaded with commercial anti-malware software). However, many general suggestions and information in this guide will apply even if you choose to use some other anti-malware software. This guide isn't exhaustive because malicious hackers are constantly developing new ways of exploiting software and tricking unsuspecting users in the already rapidly changing landscape of personal computing and Internet technology. The general suggestions in this guide should still help you avoid the more common ways of getting infected with malware. If you have Windows XP, Vista, or 7 you can download Microsoft Security Essentials from:

http://windows.microsoft.com/en-US/windows/security-essentials-download

Email Threats

Email is a very common means of malware infection. Files attached to emails containing malware can infect computers when downloaded and opened if anti-malware software is unable to identify the threat. That said, malware infection from infected email attachments has been reduced in part by people using web-based email services, such as Yahoo! Mail and Gmail, among others. Many reputable web-based email (webmail) service providers scan file attachments for malware on their end, the “server-side”, as opposed to solely relying on anti-malware detection and removal on the user's computer, the “client-side”. In addition, some people have learned to be more skeptical and aware of email malware threats and are perhaps a little less likely than they once were to open attachments that seem odd or contain strange looking files. When it comes to avoiding malware, an old saying, with some adaption, certainly applies: An ounce of skepticism is worth a pound of cure. That theme holds true for all of the various malware threats you may encounter on the Internet.

If you receive an email that has a strange looking file attachment, if you don't know the sender, or if the context of receiving a file attachment does make much sense, such as an email from someone you know that's very non-specific, it's best to err on the side of caution and not download and run any attachments or click on any links in such a message. If someone you know has their email account compromised and you're one of their contacts, you could be a target for such malicious emails sent by a hacker trying to compromise your email account or get your computer infected with malware.

Phishing Scams

Another dangerous type of threat is that of phishing. You might receive an email initially appearing to be from a financial institution or some other business or service that claims you need to update your account information, or otherwise provide sensitive information in light of some alleged incident. You then might be presented with a link to click on to log into a website to enter such information. In phishing scams, the link actually takes you to a malicious website that is designed to look legitimate. Information you enter in such a website is actually gathered by criminals who will try and use it to access your account or gather information for identity theft. Just as you wouldn't give a stranger sensitive information over the phone, you also should never provide sensitive information solicited over the Internet.

It's best to practice much caution when clicking on links in an email or from other sources, such as messaging systems and social networking services, like Facebook. That advise is especially pertinent when accessing highly sensitive websites, like online banking, online payment websites, and even email, as if your email account were able to be accessed by a thief, just think of all the information they would have access to for trying to hijack other various accounts of yours linked to your email address. It's best to type in website links (also known as "URLs") directly into your web browser's address bar or use a saved "favorite" or "bookmark" that you know to be correct when you need to access a specific website, as opposed to clicking on a link from a questionable source.

Strong Passwords

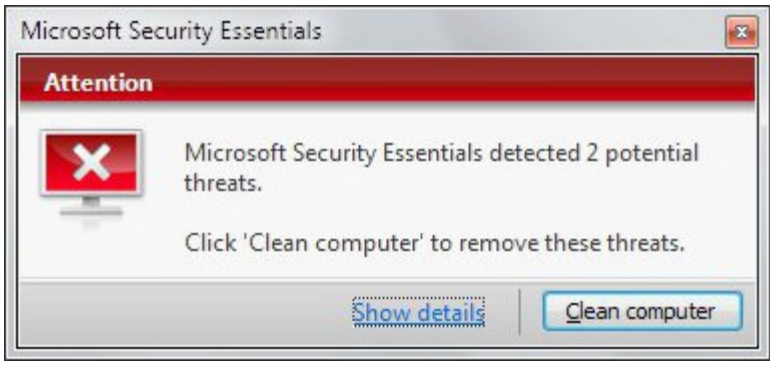
It's important to choose strong passwords for your various accounts, whether they're on the web or on your computer. It's best to use mixed case, numbers, and even symbols if possible. It's also best to make your password as long as you can reasonably tolerate. Long passwords with mixed case, numbers, and symbols are significantly harder or even impossible to crack in a timely manner by sophisticated computer password cracking programs.

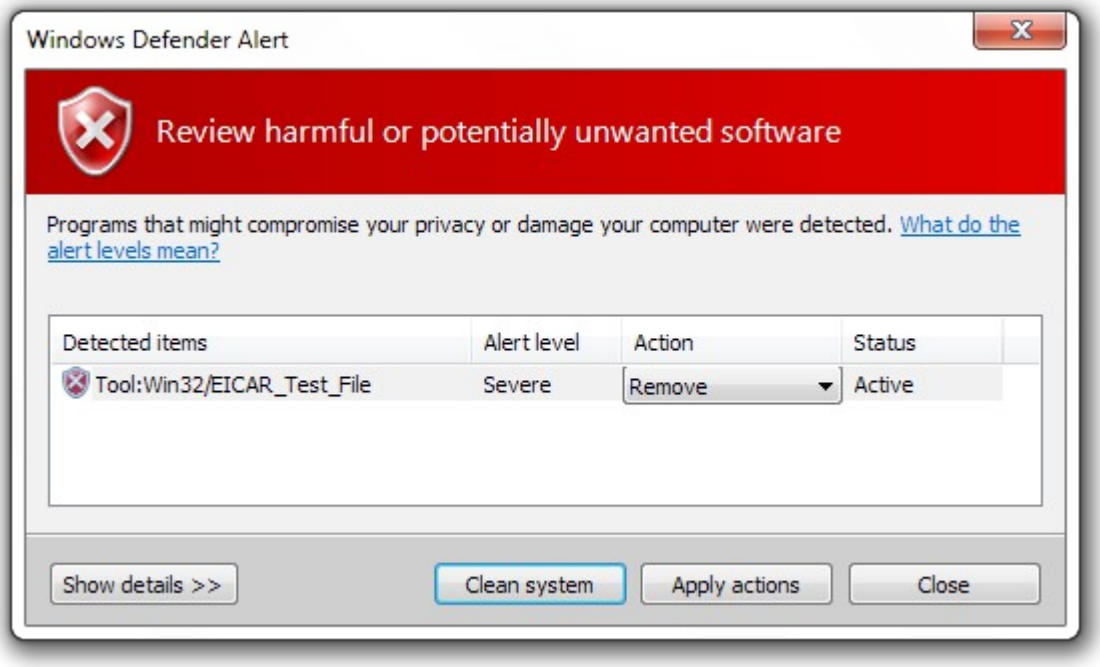
In addition, just as it's good to choose strong passwords, is also good to have them physically written down somewhere in a secure location, just in case you forget a password. Also, in the event an account ever becomes compromised and you still have access to your account, such as in the case of a compromised email account, changing your email account password, as well as other passwords that may be referenced in saved email messages, should be your first step to minimize damage.

Fake Anti-Malware Threats

One of the most common ways people get infected lately comes from being tricked into willingly downloading and running malware from the Internet. The typical case involves a malicious webpage, often a pop-up window, displaying what appears to be a virus scan or some other important or severe looking notice claiming there's a problem with your computer or with how it has been used. These fake notices vary in how legitimate they appear. Some have misspellings, grammatical errors, and tacky graphics. Others have overly aggressive and sometimes very vague language that if action isn't taken, bad things will happen. That said, others fake notices can look very legitimate, even using similar or exact graphics and wording from legitimate malware detection notices. Some are even sophisticated enough to display information about the user's location or other specific user information, which it might be able to obtain from your IP address (basically, your address on the Internet) or web browser cookies (temporary data stored in your web browser). These fake notices are usually web-based, meaning they appear in a web browser, as opposed to appearing in their own application

window, such as a legitimate infection notice from your anti-virus software, or some other information notice from Windows, like a notice that there are updates to download. A great way to deal with these tricky types of threats is to be familiar with what an actual infection notice looks like on your computer. If you are using Microsoft Security Essentials or Windows Defender, here are some examples of what legitimate malware detection notices look like:





If a notice appears different than the first detection notification (Microsoft Security Essentials) or the second detection notification (Windows Defender) then it likely should not be trusted. Due to the popularity of Microsoft's free anti-virus software, some malicious hackers have made fake infection notices that imitate the look and language of Microsoft's anti-malware programs. If clicking on a pop-up window leads to a file download and a prompt to run a program, that is a major indication of trouble. In that situation it's very important to not download and especially not run any program downloaded because its very likely to be malware.

Sometimes when you encounter a fake anti-malware website and try to close the fake pop-up notice, or back out of a malicious webpage, you might be redirected right back to the malicious webpage, or you might be prompted if you really want to close the window and still get redirected back to the malicious webpage. If you are having problems closing or backing-out of a fake notice or malicious website and you are unable to close your web browser then it might be easier to just restart

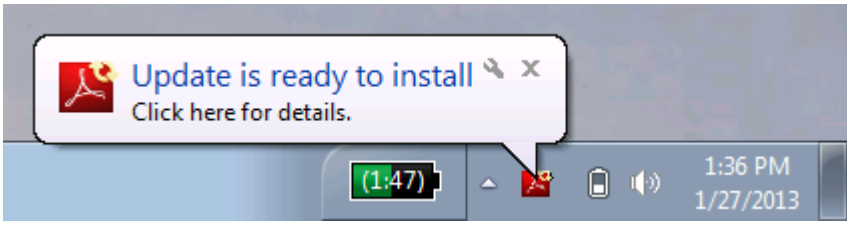
your computer and run a malware scan with Microsoft Security Essentials, Windows Defender, or whatever legitimate anti-malware program you use. It's best to restart or shutdown your computer through the start menu as forcefully powering-down your computer can cause other problems. Forcefully powering-down your computer should only be a last resort. Some computers are configured to power-down gracefully if you tap the power button once, whereas holding the power button in for six seconds should forcefully power it down.

After restarting your computer, if a malware scan doesn't indicate you're infected, and if you don't notice any new pop-ups or software running that wasn't running before, then you're likely not infected. However, if you do notice odd behavior or software that wasn't previously installed, or if your web browser doesn't seem to be behaving, such as redirecting to websites you aren't telling it to go to, or pop-ups appearing out of nowhere, then you probably got infected and your computer may need professional attention. Sometimes after an infection you can use anti-malware software to scan and remove an infection, but results vary because sometimes an anti-malware program cannot identify an infection or an infection may have damaged the anti-malware software or other critical software components. In such cases, your computer will certainly need professional attention.

It is important to note that there are many variations of fake anti-malware threats. Some other threats include fake notices that the computer's hardware (memory, hard drive, etc.) is failing or that the computer was used for illegal activity and that authorities have been contacted, with a link to take proper action that really links to a malicious download, sensitive information gathering, or to make an online payment for a bogus fine or fee. The bottom line is that if a notice looks strange in any way, it's probably malicious, and it best to err on the side of caution. Do not download or run any programs unless you know exactly what they are. Close the web browser, restart your computer if necessary, run an anti-malware scan, remove all threats, and monitor the system for any further peculiar behavior.

Keeping Software Updated

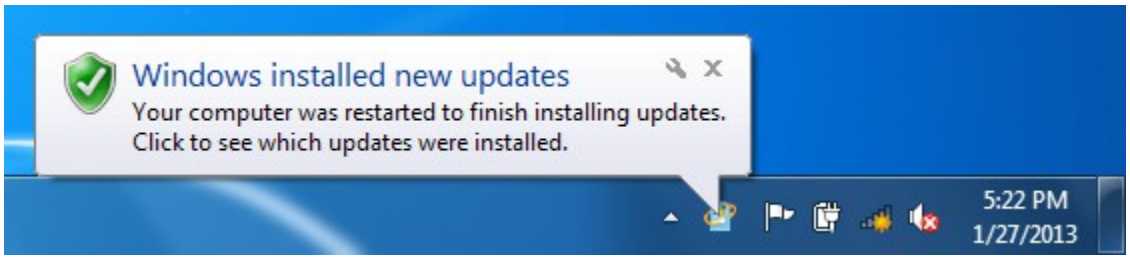
Keeping software on your computer updated is very important as sometimes malicious hackers will uncover vulnerabilities in various widely-used software, such as Windows itself, Adobe software (such as Adobe Flash, which is used to play multimedia content, such as YouTube videos; Adobe Shockwave, which is similar to Flash; and Adobe Reader, which is used to view PDF files, which can also be infected), Java (used by some programs and websites for various functions), and Microsoft Office, among others. If legitimate software prompts to update then doing so is recommended. However, caution should still be exercised as malicious hackers have been known to create malicious software that appears to be legitimate software performing updates for the above listed software. If an update pops-up from the taskbar (in the lower right of the screen, by the clock) then it's either likely legitimate or you've already been infected. If you are unsure if an update is legitimate then it's recommended you seek professional advise, or at the very least, run a malware scan after performing such an update. Here's an example of a legitimate Adobe update appearing in the taskbar:



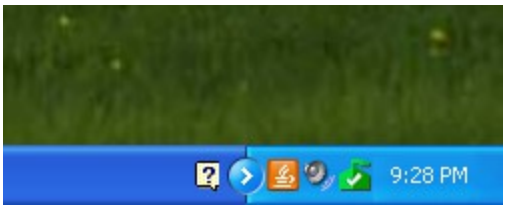
In the case of keeping Windows and Office updated, among other Microsoft programs, that update functionality, called Windows Update, is built into Windows. In Windows XP you may

occasionally see a yellow shield with an exclamation mark. In Windows Vista and 7 the update icon is that of a box with a Windows symbol and a yellow ring (pictured below). It's best to download and install any such updates for Windows and other Microsoft software because malicious hackers are always looking for exploitable vulnerabilities in such widely used software.

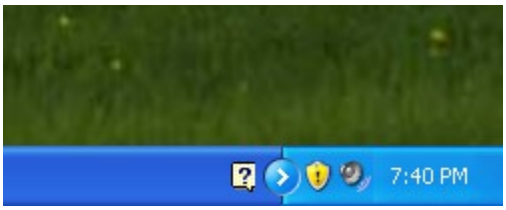
Below are some examples of Windows Update and other update icons that may appear in the taskbar for various legitimate software updates:



Windows Update notification in Windows 7



Java Update in Windows XP (orange icon)



Windows Update notification in Windows XP (yellow shield)

Keeping your anti-malware program updated is also important. Microsoft Security Essentials and Windows Defender should automatically update, so long as they have a connection to the Internet to receive updates. They should also scan your computer on a regular basis. Other good anti-malware programs should do the same. Scheduled scan settings can be accessed in the settings menu of Microsoft Security Essentials and Windows Defender.

Supplementing Anti-Malware Software

It is strongly discouraged to run multiple anti-malware programs on the same computer as they can conflict with each other, in some cases detecting each other as malicious programs. Often times computers will come preloaded with subscription-based anti-malware programs, such as Norton or McAfee. If such is the case on your computer, and you choose to install and use Microsoft Security Essentials or in the case of Window 8, enable Windows Defender, then the other preloaded, subscription-based anti-malware software should be uninstalled beforehand.

Some people claim that other supplemental anti-malware programs can help protect a computer. I have found that not really to be the case. The only supplemental anti-malware program I've found to

be effective is Malwarebytes' Anti-Malware (MBAM). The free edition of MBAM doesn't provide real-time protection, so it typically won't prevent an infection unless it's used for a preliminary, manual scan of a downloaded program. If MBAM is installed then you should be able to right-click on a file and be presented with an option to scan the file with MBAM. MBAM can be very effective in detecting and removing malware infections that primary anti-malware program may not be able to detect or remove. MBAM seems especially proficient in detecting very common fake anti-malware programs. Thus, MBAM can be handy to have installed on a computer if you know something strange is happening on your computer. In such a case, you could try running MBAM, update it, run a scan, and remove any threats it finds. MBAM can be downloaded from Malwarebytes' website:

http://www.malwarebytes.org/

Extra caution must be exercised when using supplementary anti-malware programs as there are many such programs that are not legitimate. Programs that claim to make Windows faster or clean its "registry" are examples of programs that should be avoided.

Zero-Day Threats

It's important to understand that no anti-malware protection is 100% effective. Anti-malware software has made some impressive advancements over the years, including employing ways of detecting malicious software not just by what the malicious software looks like from a file content perspective, but also by what actions it's performing on your computer. However, malicious hackers are consistently finding new program exploits and developing new clever schemes of infecting computers.

A zero-day threat is malicious software that's so new it hasn't yet been identified by computer security analysts, and hence may not be able to be detected and removed by your anti-malware program, even if you have the latest malware definitions from a software update. For this reason, it's especially important to practice good web browsing habits. As previously stated, an ounce of skepticism is worth a pound of cure. Do not download and install unknown software or click on suspicious website links.

Administrative User Accounts

Administrative user accounts in Windows are user accounts that can install software and make other system-wide changes to the computer. While such accounts may make using the computer a little easier because you aren't bothered to enter a password to install software or perform updates, everyday use on such an account can be dangerous. If you were to get infected while logged in as an administrative user, the infection would likely infect the whole system and potentially damage Windows system files, making infection removal very difficult or impossible without re-installing Windows, which is a very labor intensive task.

Instead of using an administrative user account for everyday use, it's instead recommended to use a limited user account (as they are termed in Windows XP) or standard user account (as they are termed in Windows Vista, 7, and 8). While you may have to log off and back in to perform some tasks (Windows XP) or provide a password for an administrative user account (Windows Vista, 7, and 8), if you were to get infected on a limited/standard user account, the infection would likely just affect that user account and not the whole machine, plus it may be a lot easier to clean-up. Since limited/standard user accounts don't have rights to modify system files, a malicious program is typically very limited in

the amount of damage it can do when run from a limited or standard user account without account elevation (providing an administrative user password in Windows Vista, 7, or 8).

If you are unsure if your everyday-use user accounts are setup as a limited/standard user accounts that can be checked and changed very easily in Control Panel under User Accounts. A good configuration would have all normal-use accounts be set as limited/standard users, especially for high-risk users prone to clicking on things they shouldn't be when browsing the Internet. In addition to those limited/standard user accounts you would also have a single administrative user account with a strong password for cases where hardware (such as a new printer or camera), software, or system updates need to be installed.

OpenDNS Internet Filtering

A company named OpenDNS offers services – some free and ad-based, others subscription-based – for blocking malicious content, among other potentially undesirable content. Their DNS-based Internet filter is relatively easy to setup and is especially nice in that it doesn't require special software on your computer. When you visit a website, the name of the website is translated into a numeric address. That translation is done by a computer on the Internet that's referred to as a "DNS server", or "Domain Name Service" server. By using OpenDNS's server instead of your Internet service provider's DNS server, websites that OpenDNS has deemed to be malicious or contain undesirable content will be blocked. That may not be desirable if you want the Internet completely unfiltered and uncensored, though it can be great if you don't mind filtering and want an extra layer of protection against some known malicious websites. In addition, its easy to undo if you find yourself unable to access websites you know to be safe. More information about their services can be found on their website:

http://www.opendns.com/