Prevent Infection

Protect Your Computer

What is Malware?

Malware is malicious software, typically designed either to give others control of your computer or steal personal information such as passwords, bank accounts, etc.

How Do Computers Get Infected?

If your computer is running not antivirus and not kept updated, malware can install itself *silently, without any action on your part,* as you visit even reputable websites or insert a USB flash drive. Malware can also hide inside items you download, especially “free” music, video, or games. Some malware is distributed via e-mail attachments (never open anything you were not expecting or cannot verify).

How Do I Prevent Infection?

Run an updated Antivirus, do critical updates, and be careful where you click, as detailed below:

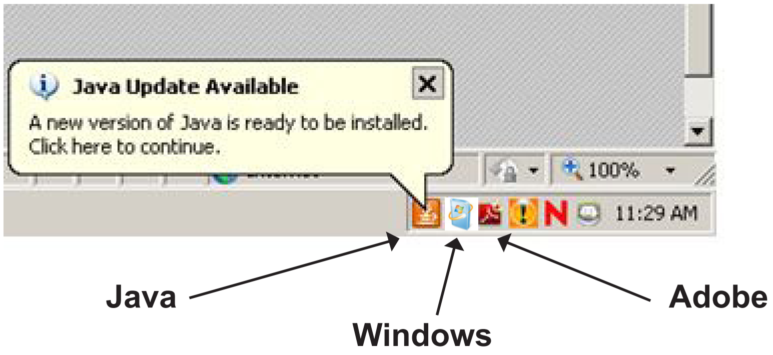
1 Updated Antivirus

There are many reputable antivirus programs available, but none will do the job if they are not kept updated. For home computers, we recommend *Microsoft Security Essentials* because it provides excellent protection, has minimal impact on performance, and is free. See windows.microsoft.com/mse.

Remember, even the best antivirus is similar to a flu shot: you are protected against most known threats, but malware evolves constantly and you will never be protected against all. Antivirus is necessary but just one part of your defense, and if it’s not updated regularly, it’s not protecting you.

2 Update Windows, Java, and Adobe

Malicious code hidden on websites (even reputable sites) can and will probe your computer for vulnerabilities. The most common targets are Windows, Adobe Flash, and Java. If a vulnerable version is found, your computer can be infected silently without any action on your part. Note to Apple users: Macs present a smaller target but are still at risk and need to update. Be on the lookout for icons in the “tray” (lower right-hand corner of the Windows screen) which indicate updates are needed. **Recognize these updates and obey their prompts:**



Java Update Available

A new version of Java is ready to be installed. Click here to continue.

Windows Updates

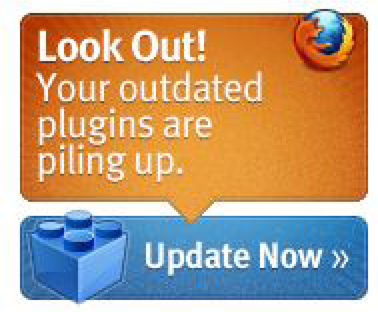
If you see the “updates are available” message in the tray at the lower right of your screen, **follow the prompts to update**. Even better, be proactive and check for updates by clicking START, PROGRAMS, WINDOWS UPDATE.

Adobe Flash and Acrobat Reader

Flash and Reader are frequent targets so it is important to update whenever new versions are released. However, be sure to **uncheck** the optional installs (for example, Google Toolbar) during the update process.

Java--do you even need it?

Outdated versions of Java are the cause of about a third of all infections. If you see the orange “coffee cup” icon in the tray, you need to update Java. As with Adobe, **uncheck the optional installs** if prompted. Better yet, **uninstall Java** to eliminate the threat. Many people can uninstall Java and never miss it (click START, CONTROL PANEL, PROGRAMS AND FEATURES to uninstall). If you need Java later, you’ll be prompted to reinstall it.



Look Out!
Your outdated plugins are piling up.

The plug-in checker at www.mozilla.org/plugincheck/ is a great way to see if Adobe and Flash are up to date in Firefox and Internet Explorer (not as relevant for Chrome since Chrome uses it’s own plug-ins).

3 Careful What You Click!

Think before clicking on any e-mail attachment or link in a message. Remember that downloading “free” music or movies using is very risky behavior since malware can be present in the downloaded files. Generally speaking, the fewer things you install from the Internet, the better.

Frequently Asked Questions

How do I know if my computer is infected? Some malware is easy to spot: the computer will run slowly or throw up constant pop-up windows. More sophisticated malware may give no symptoms at all. Running a “full scan” of your antivirus may detect malware but does **not** prove none is present. Other reputable scanners include MalwareBytes, Combofix, and SuperAntispyware--but even using all of them does not guarantee the computer is clean.

How can I clean or disinfect an infected computer? It is far easier to prevent infection than to cure it. Once infected, the surest way to clean the computer is to back up your documents and perform a reformat or “system recovery” that wipes out all files, good and bad. Use an external drive or online storage to back up your files first.

Shouldn’t I wait until updates are “established” before I install them? Most updates to Windows, Java, and Adobe are released to solve security issues that often are being *actively exploited*; the small risk of updating is far less than the risk of infection.

I have a Mac, so I’m safe, right? Unfortunately, no. Macs are being targeted, too. You still need a good antivirus, should keep your system updated, and be careful what you click.