**Top Ten Ways to Get Infected**

**How your online habits can leave you and your computer at risk.**

Keeping safe online takes more than just installing a few security programs. To protect both you and your computer, here are the top ten bad habits you need to avoid.

**1.** [**Browsing the Web with javascript enabled by default**](http://antivirus.about.com/od/securitytips/a/websecurity.htm)

Today's attackers are more likely to host their malicious files on the web. They may even update those files constantly using automated tools that repackage the binary in an attempt to bypass signature-based scanners. Whether through social engineering or through website exploit, the choice of browser will be of little help. All browsers are equally susceptible to Web-based malware and this includes Firefox, Opera, and the much maligned Internet Explorer. Disabling Javascript on all but the most trusted sites will go a long ways towards safer web browsing.

**2.** [**Using Adobe Reader/Acrobat with default settings**](http://antivirus.about.com/od/securitytips/ht/adobesafety.htm)

Adobe Reader comes pre-installed on most computers. And even if you never use it, just the mere presence can leave your computer at risk. Vulnerabilities in Adobe Reader and Adobe Acrobat are the number one most common infection vector, bar none. Making sure you stay up-to-date with the latest version of Adobe products is imperative, but not foolproof. To use Adobe Reader (and Acrobat) safely, you need to make a [few tweaks to its settings](http://antivirus.about.com/od/securitytips/ht/adobesafety.htm).

**3.** [**Clicking unsolicited links in email or IM**](http://antivirus.about.com/od/emailscams/a/fakelinks.htm)

Malicious or fraudulent links in email and IM are a significant vector for both malware and social engineering attacks. Reading [email in plain text](http://antivirus.about.com/od/securitytips/a/plainttextemail.htm) can help identify potentially malicious or fraudulent links. Your best bet: avoid clicking any link in an email or IM that is received unexpectedly - particularly if you do not know the sender.

**4.** [**Clicking on popups that claim your computer is infected**](http://antivirus.about.com/od/roguescanners/Scanners_to_Avoid.htm)

Rogue scanners are a category of scam software sometimes referred to as scareware. Rogue scanners masquerade as antivirus, antispyware, or other security software, claiming the user's system is infected in order to trick them into paying for a full version. Avoiding infection is easy - don't fall for the bogus claims.

**5.** [**Logging in to an account from a link received in email, IM, or social networking**](http://antivirus.about.com/od/securitytips/ht/koobface.htm)

Never, ever login to an account after being directed there via a link received in an email, IM, or social networking message (i.e. Facebook). If you do follow a link that instructs you to login afterwards, close the page, then open a new page and visit the site using a previously bookmarked or known good link.

**6.** [**Not applying security patches for ALL programs**](http://antivirus.about.com/od/antivirussoftwarereviews/gr/secuniainsp.htm)

Chances are, there are dozens of security vulnerabilities waiting to be exploited on your system. And it's not just Windows patches you need to be concerned with. Adobe Flash, Acrobat Reader, Apple Quicktime, Sun Java and a bevy of other third-party apps typically host security vulnerabilities waiting to be exploited. The free [Secunia Software Inspector](http://antivirus.about.com/od/antivirussoftwarereviews/gr/secuniainsp.htm) helps you quickly discover which programs need patching - and where to get it.

**7.** [**Assuming your antivirus provides 100% protection**](http://antivirus.about.com/od/whatisavirus/g/falsenegative.htm)

So you have antivirus installed and are keeping it up-to-date. That's a great start. But don't believe everything your antivirus does (or rather doesn't) tell you. Even the most current antivirus can easily miss new malware - and attackers routinely release tens of thousands of new malware variants each month. Hence the importance of following all the tips provided on this page.

**8.** [**Not using antivirus software**](http://antivirus.about.com/od/antivirussoftwarereviews/tp/aatpavwin.htm)

Many (probably infected) users mistakenly believe they can avoid malware simply by being 'smart'. They labor under the dangerous misconception that somehow malware always asks permission before it installs itself. The vast majority of today's malware is delivered silently, via the Web, by exploiting vulnerabilities in software. Antivirus software is must-have protection. Of course, out-of-date antivirus is almost as bad as no antivirus software at all. Make sure your antivirus software is configured to automatically check for updates as frequently as the program will allow or a minimum of once per day.

**9.** [**Not using a firewall on your computer**](http://antivirus.about.com/od/antivirussoftwarereviews/Antivirus_Firewall_and_Security_Software_Reviews.htm)

Not using a firewall is akin to leaving your front door wide open on a busy street. There are several free firewall options available today - including the built-in firewall in Windows XP and Vista. Be sure to choose a firewall that offers both inbound and (as importantly) outbound protection.

**10.** [**Falling for phishing or other social engineering scams**](http://antivirus.about.com/od/emailscams/tp/onlinescams.htm)

Just as the Internet makes it easier for legitmate pursuits, it also makes it easier for scammers, con artists, and other online miscreants to carry out their virtual crimes - impacting our real life finances, security, and peace of mind. Scammers often use sad sounding stories or promises of quick riches to hook us into being willing victims to their crimes. Exercising common sense is one of the best ways to avoid online scams. For extra help, consider installing one of the free anti-phishing toolbars

**The above information found at: http://antivirus.about.com/od/securitytips/tp/badsecurityhabits.htm**

**Malware**, short for **malicious software**, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.[[1]](http://en.wikipedia.org/wiki/Malware#cite_note-1) It can appear in the form of [code](http://en.wikipedia.org/wiki/Source_code), [scripts](http://en.wikipedia.org/wiki/Script_%28computing%29), active content, and other software.[[2]](http://en.wikipedia.org/wiki/Malware#cite_note-2) 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.[[3]](http://en.wikipedia.org/wiki/Malware#cite_note-3)

Malware includes [computer viruses](http://en.wikipedia.org/wiki/Computer_virus), [ransomware](http://en.wikipedia.org/wiki/Ransomware_%28malware%29), [worms](http://en.wikipedia.org/wiki/Computer_worm), [trojan horses](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29), [rootkits](http://en.wikipedia.org/wiki/Rootkit), [keyloggers](http://en.wikipedia.org/wiki/Keystroke_logging), [dialers](http://en.wikipedia.org/wiki/Dialer#Fraudulent_dialer), [spyware](http://en.wikipedia.org/wiki/Spyware), [adware](http://en.wikipedia.org/wiki/Adware), malicious [BHOs](http://en.wikipedia.org/wiki/Browser_Helper_Object), [rogue security software](http://en.wikipedia.org/wiki/Rogue_security_software) and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses.[[4]](http://en.wikipedia.org/wiki/Malware#cite_note-4) In [law](http://en.wikipedia.org/wiki/Law), malware is sometimes known as a **computer contaminant**, as in the legal codes of several [U.S.](http://en.wikipedia.org/wiki/United_States) states.[[5]](http://en.wikipedia.org/wiki/Malware#cite_note-5)[[6]](http://en.wikipedia.org/wiki/Malware#cite_note-6) Malware is different from defective software, which is a legitimate software but contains harmful [bugs](http://en.wikipedia.org/wiki/Software_bug) that were not corrected before release. However, some malware is disguised as genuine software, and may come from an official company website in the form of a useful or attractive program which has the harmful malware embedded in it along with additional tracking software that gathers marketing statistics.[[7]](http://en.wikipedia.org/wiki/Malware#cite_note-7)

Software such as [anti-virus](http://en.wikipedia.org/wiki/Anti-virus), anti-malware, and [firewalls](http://en.wikipedia.org/wiki/Firewall_%28computing%29) are relied upon by users at home, small and large organizations around the globe to safeguard against malware attacks which helps in identifying and preventing the further spread of malware in the network.[[8]](http://en.wikipedia.org/wiki/Malware#cite_note-8)**The above information found at: http://en.wikipedia.org/wiki/Malware**