**MALWARE ATTACKS**

Malware, short for malicious software, is any software that gets installed on your computer, phone, or mobile device without your consent. Whether it’s a [keystroke logger](http://www.antivirus.com/security-software/definition/keystroke-logger/index.html) recording your personal information or a [computer worm](http://www.antivirus.com/security-software/definition/computer-worms/index.html) infecting systems, or even [adware](http://www.antivirus.com/security-software/definition/adware/index.html) you didn’t consent, they all have two things in common: they’re all software and they’re all doing bad things which implies software that causes harm due to [bug](http://en.wikipedia.org/wiki/Computer_bug)s or poor design are not classified as malware. It can appear in the form of [executable code](http://en.wikipedia.org/wiki/Executable_code), [scripts](http://en.wikipedia.org/wiki/Script_(computing)), active content or any other software. 'Malware' or ‘Badware’ is a general term used to refer to a variety of forms of hostile or intrusive software. Destructive malware will utilize popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from web sites , virus-infected files downloaded from peer-to-peer connections including [ransomware](http://en.wikipedia.org/wiki/Ransomware_(malware)), [spyware](http://en.wikipedia.org/wiki/Spyware) ,[adware](http://en.wikipedia.org/wiki/Adware) ,[scareware](http://en.wikipedia.org/wiki/Scareware) and many alike. Malware will also seek to exploit existing [vulnerabilities](http://us.norton.com/security_response/vulnerabilities.jsp) on systems making their entry quiet and easy. 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.

ULTERIOR MOTIVE

Today, malware is used by [black hat hackers](http://en.wikipedia.org/wiki/Black-hat_hacking) to steal personal, financial, or business information and sometimes for sabotage (e.g., [Stuxnet](http://en.wikipedia.org/wiki/Stuxnet)). It is broadly used as:

* **Information gatherer:** Government or Corporate websites are guarded to gather information or to disrupt their operation and individuals for information such as personal identification numbers or details, bank or credit card numbers, and passwords are collected.
* **Infectious software:** which turns computers in to "[zombie computers](http://en.wikipedia.org/wiki/Zombie_computer)" which can be used to send [email spam](http://en.wikipedia.org/wiki/Email_spam), to host contraband data such as ‘pirated software’ , to engage in [distributed denial-of-service](http://en.wikipedia.org/wiki/Distributed_denial-of-service) [attacks](http://en.wikipedia.org/wiki/Attack_(computing)) as a form of [extortion](http://en.wikipedia.org/wiki/Extortion) termed as Ransomware or injecting malware laden advertisements into legitimate [online advertising networks](http://en.wikipedia.org/wiki/Advertising_network) and webpages i.e. Malvertising.
* **Spy Agents:** Spyware is an additional hidden tracking functionality that gathers marketing statistics, for example, [Sony rootkit](http://en.wikipedia.org/wiki/Sony_rootkit) is a Trojan embedded into [CDs](http://en.wikipedia.org/wiki/Compact_disc) sold by [Sony](http://en.wikipedia.org/wiki/Sony), which silently installed and concealed itself on purchasers' computers with the intention of preventing illicit copying; it also reported on users' listening habits, and created vulnerabilities that were exploited by unrelated malware.

ROOT CAUSE

“System under attack” may be anything from a single application, through a complete computer and operating system, to a large [network](http://en.wikipedia.org/wiki/Computer_network). Various factors that make a system more vulnerable to malware are:

* **Software Security Defects:** Malware exploits security defects in the design of the operating system, in applications such as older versions of browsers, browsers plugins such as [Adobe Flash Player](http://en.wikipedia.org/wiki/Adobe_Flash_Player#Security) or java which may not automatically update and can be targeted by malware. Another common method of exploitation is [buffer overrun](http://en.wikipedia.org/wiki/Buffer_overrun) where malware may provide data that overflows the buffer with malicious [executable](http://en.wikipedia.org/wiki/Executable) code or data after the end; when this payload is accessed it does what the attacker, not the legitimate software, determines. Secunia PSI is a software that checks PC for vulnerable out-of-date software and attempt to update it.
* **Design defects or manual errors :** Earlier configuring computer using booting devices such as a floppy disk, [CD-ROM](http://en.wikipedia.org/wiki/CD-ROM), DVD-ROM, or USB flash drive was common, for example to install an operating system. Malicious software distributors would trick the user into booting or running from an infected device or medium; for example, a virus could make an infected computer add auto runnable code to any USB stick plugged into it; anyone who then attached the stick to another computing set to autorun from USB would in turn become infected, and also pass on the infection in the same way. Devices can be infected during manufacturing or supply if quality control is inadequate. This form of infection can largely be avoided by setting up computers by default to boot from the internal hard drive. Intentional booting from another device is always possible by pressing certain keys during boot.
* **Homogeneous operating systems:** Most of the computers in a [network](http://en.wikipedia.org/wiki/Computer_network) run the same operating system i.e. [Microsoft Windows](http://en.wikipedia.org/wiki/Microsoft_Windows) or [Mac OS X](http://en.wikipedia.org/wiki/Mac_OS_X) which makes them vulnerable to attacks. However, having a few diverse nodes would deter total shutdown of the [network](http://en.wikipedia.org/wiki/Computer_network), and allow those nodes to help with recovery of the infected nodes. Such separate, functional redundancy could avoid the cost of a total shutdown.

MALWARE SYMPTOMS

If your computer starts to behave in a non-desirable manner it might be experiencing spyware symptoms or have other unwanted software installed. Following can help in detecting malicious software:

* **Pop-up advertisements all the time: P**op-up ads bombards that aren't related to a particular website you're visiting which you may find objectionable or if pop-up ads appear as soon as computer is turn on and you're not even browsing the web, you might have spyware or other unwanted software on your computer.
* **Settings have changed and can't be reverted:** Some unwanted software can change home page or search page settings. Even if you adjust these settings, you might find that they revert back every time you restart your computer.
* **Web browser contains additional components:** Spyware and other unwanted software can add toolbars to your web browser that you don't want or need. Even if you remove these toolbars, they might return each time you restart your computer.
* **Slow Computer:** Spyware and other unwanted software are not designed to be efficient. The resources these programs use to track your activities and deliver advertisements can slow down your computer and errors in the software can make your computer crash. If you notice a sudden increase in the number of times a certain program crashes, or if your computer is slower than normal at performing routine tasks, you may have spyware or other unwanted software on your machine.

MALWARE PROTECTION

**Strengthen your computer's defenses:**

* Install antivirus and antispyware programs from a trusted source. Anti-malware programs scan and monitor your computer for known viruses and spyware. When they find something, they warn you and help you take action. Some of the best malware removal tools are: Spybot Search and Destroy, SUPER AntiSpyware, ComboFix, Malwarebytes' Anti-Malware, HijackThis, Windows Defender (built in to Windows 8)and Microsoft Security Essentials.
* Keep all software up to date. Regularly install updates for all your software and subscribe to automatic updates wherever possible.
* Use strong passwords and keep them secret. Use [password checker](https://www.microsoft.com/security/pc-security/password-checker.aspx) to determine the [strength of your password](http://www.microsoft.com/security/online-privacy/passwords-create.aspx).
* Never turn off your firewall. A firewall puts a protective barrier between your computer and the Internet. Turning it off for even a minute increases the risk that your PC will be infected with malware.
* Use flash drives cautiously. Putting your flash drive in a computer that is infected could corrupt the drive, and ultimately your computer.

**Do not be tricked into downloading malware:** Attackers can enlist your computer by delivering malware in downloads that you think are pictures or movies, or through links that you click in email or instant messages (IM), or on a social network. They usually scare you into clicking a button or link they supply with fake warnings that your computer has a virus which leads to malware infection.

# Watch out for fake virus alerts: Rogue security software, also known as "scareware," is software that appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading alerts, or attempts to lure users into participating in fraudulent transactions. One should not open [spam email messages or click links on suspicious websites](http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx).

# Download safely: User should take caution while surfing or downloading, should keep in mind that he download programs only from trusted websites, read all security warnings, beware of “free” items, use a standard user account instead of an administrator account, don't click links on suspicious websites or in email messages.

REFERENCES:

<http://www.microsoft.com/security/resources/malware-whatis.aspx>

<http://en.wikipedia.org/wiki/Malware>

<http://www.microsoft.com/security/pc-security/malware-protect.aspx>

<http://www.microsoft.com/security/pc-security/malware-remove.aspx>

<http://www.microsoft.com/security/pc-security/antivirus-rogue.aspx>

<http://lifehacker.com/5227896/five-best-malware-removal-tools>