Malware

You Need Malware Protection

Malware can lock up your hardware, steal the passwords for your software, and seriously stress your mental state. To fend off these attacks, you need to fight malware with an antivirus utility or other security software.
Despite the word "virus" in the name, an antivirus utility actually aims to protect against all types of malware. Full scale security suites expand protection to include such things as spam filtering and parental control. Some anti-malware tools work alongside your main protection to provide added security against specific threats, such as ransomware.

The amount and variety of malicious programs out there is enough to make your head spin.
This information by Neil DuPaul will break down the common types of malicious programs and provide a brief description of each.

MALWARE

Malware is short for malicious software, meaning software that can be used to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs. This post will define several of the most common types of malware; adware, bots, bugs, rootkits, spyware, Trojan horses, viruses, and worms.

Adware

Adware (short for advertising supported software) is a type of malware that automatically delivers advertisements. Common examples of adware include pop-up ads on websites and advertisements that are displayed by software. Often times software and applications offer “free” versions that come bundled with adware. Most adware is sponsored or authored by advertisers and serves as a revenue generating tool. While some adware is solely designed to deliver advertisements, it is not uncommon for adware to come bundled with spyware (see below) that is capable of tracking user activity and stealing information. Due to the added capabilities of spyware, **adware/spyware bundles are significantly more dangerous than adware on its own**.

Bot

Bots are software programs created to automatically perform specific operations. While some bots are created for relatively harmless purposes (video gaming, internet auctions, online contests, etc), **it is becoming increasingly common to see bots being used maliciously**. Bots can be used in botnets (collections of computers to be controlled by third parties) for DDoS attacks, as spambots that render advertisements on websites, as web spiders that scrape server data, and for distributing malware disguised as popular search items on download sites. **Websites can guard against bots with CAPTCHA tests that verify users as human**.

Bug

In the context of software, a bug is a flaw producing an undesired outcome. These flaws are usually the result of human error and typically exist in the source code or compilers of a program. Minor bugs only slightly affect a program’s behaviour and as a result can go for long periods of time before being discovered. **More significant bugs can cause crashing or freezing**. **Security bugs** are the most severe type of bugs and can **allow attackers to bypass user authentication, override access privileges, or steal data**. Bugs can be prevented with developer education, quality control, and code analysis tools.

Ransomware

Ransomware is a form of malware that essentially **holds a computer system captive while demanding a ransom**. The malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove the restrictions and regain access to their computer. Ransomware typically spreads like a normal computer worm (see below) **ending up on a computer via a downloaded file or through some other vulnerability in a network service**.

Rootkit

A rootkit is a type of malicious software designed to **remotely access or control a computer without being detected by users or security programs**. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer as part of a botnet. Rootkit prevention, detection, and removal can be difficult due to their stealthy operation. **Because a rootkit continually hides its presence, typical security products are not effective in detecting and removing rootkits**. As a result, rootkit detection relies on manual methods such as monitoring computer behaviour for irregular activity, signature scanning, and storage dump analysis. Organisations and users can protect themselves from rootkits by **regularly patching vulnerabilities in software, applications, and operating systems, updating virus definitions, avoiding suspicious downloads, and performing static analysis scans**.

Spyware

Spyware is a type of malware that functions by **spying on user activity without their knowledge**. These can include **activity monitoring, collecting keystrokes, data harvesting** (account information, logins, financial), and more. Spyware often can **modify security settings of software or browsers to interfering with network connections**. Spyware spreads by exploiting software vulnerabilities, bundling itself with legitimate software, or in Trojans.

Trojan Horse

A Trojan horse, commonly known as a “Trojan,” is a type of malware that **disguises itself as a normal file or program to trick users into downloading and installing malware**. A Trojan can give a malicious party remote access to an infected computer. Once an attacker has access to an infected computer, it is possible for the attacker to **steal data** (logins, financial data, even electronic money), **install more malware, modify files, monitor user activity** (screen watching, keylogging, etc), use the computer in botnets, and anonymise internet activity by the attacker.

Virus

A virus is a form of malware that is capable of copying itself and spreading to other computers. Viruses often **spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs**. Viruses can also spread through script files, documents, and cross-site scripting vulnerabilities in web apps. Viruses can be used to **steal information, harm host computers and networks, create botnets, steal money, render advertisements**, and more.

Worm

Computer worms are among the most common types of malware. They spread over computer networks by exploiting **operating system vulnerabilities**. Worms typically cause harm to their host networks by **consuming bandwidth and overloading web servers**. Computer worms can also contain “payloads” that damage host computers. Payloads are pieces of code written to perform actions on affected computers beyond simply spreading the worm. Payloads are commonly designed to **steal data, delete files, or create botnets**. Computer worms can be classified as a type of computer virus, but there are several characteristics that distinguish computer worms from regular viruses. A major difference is that **computer worms have the ability to self-replicate and spread independently** while viruses rely on human activity to spread (running a program, opening a file, etc). **Worms often spread by sending mass emails with infected attachments to users’ contacts**.

Malware Symptoms

While these types of malware differ greatly in how they spread and infect computers, they all can produce similar symptoms. Computers that are infected with malware can exhibit any of the following symptoms:

- Increased CPU usage
- Slow computer or web browser speeds
- Problems connecting to networks
- Freezing or crashing
- Modified or deleted files
- Appearance of strange files, programs, or desktop icons
- Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs)
- Strange computer behaviour
- Emails/messages being sent automatically and without user’s knowledge (a friend receives a strange email from you that you did not send)
- Complete breakdown of your operating system
- Loss of data

Malware Prevention and Removal

Install and run anti-malware and firewall software. When selecting software, choose a program that offers tools for detecting, quarantining, and removing multiple types of malware. At the minimum, anti-malware software should protect against viruses, spyware, adware, Trojans, and worms. The combination of anti-malware software and a firewall will ensure that all incoming and existing data gets scanned for malware and that malware can be safely removed once detected.

But how does it know?

How does it tell that a program is malicious? The easiest method involves what's called a **signature - a kind of fingerprint that identifies known malicious files**. Early antivirus tools simply checked the numeric hash of entire programs against a blacklist. Malware coders responded to that by making threats polymorphic, so every victim received a slightly different file. And antivirus researchers in turn responded by making signatures more generic, so that all variations on a particular malware strain would still fit the profile.

Isn't it built in?
But, you may ask, doesn't Windows 10 have antivirus built right in? It's true that **Windows Defender** is built into Windows 10, and it gained more responsibilities with the recent Creators Update. If you have no other antivirus, Windows Defender turns on automatically. If you install a third-party antivirus, it goes dormant. The problem is, **independent lab tests and my own hands-on tests have shown that Windows Defender just isn't as effective as third-party alternatives**.

Emergency Malware Removal

There's always the chance that your antivirus might miss a very new, very virulent malware strains. You also may run into trouble when you try to install antivirus protection, because the malware already entrenched on your computer fights back. In either of those cases, you can call on the many free cleanup only tools.

Malwarebytes Anti-Malware is a current favourite. It's not the only choice, though. Sophos, Symantec, and Emsisoft are among the others that offer similar free malware cleaners.

Malware Scan Types

- You can launch a full antivirus scan of your computer at will, to root out any pre-existing malware problems. Most also let you **schedule a regular scan**.
- **But the first line of defence is on-access scanning (runs in the background whilst computer/laptop is on)**.
- Keep software and operating systems up to date with **current vulnerability patches**. These patches are often released to patch bugs or other security flaws that could be exploited by attackers.
- Be **vigilant** when **downloading files, programs, attachments**, etc.
  Downloads that seem strange or are from an unfamiliar source often contain malware.

Spam

Spam is the electronic sending of mass unsolicited messages. The most common medium for spam is email, but it is not uncommon for spammers to use instant messages, texting, blogs, web forums, search engines, and social media. While spam is not actually a type of malware, **it is very common for malware to spread through spamming**. This happens when computers that are infected with viruses, worms, or other malware are used to distribute spam messages containing more malware. **Users can prevent getting spammed by avoiding unfamiliar emails and keeping their email addresses as private as possible**.

It is therefore highly important you protect yourself EVERY DAY, at home.
Install and RUN a malware/spyware protection and registry cleaner EVERY DAY such as:

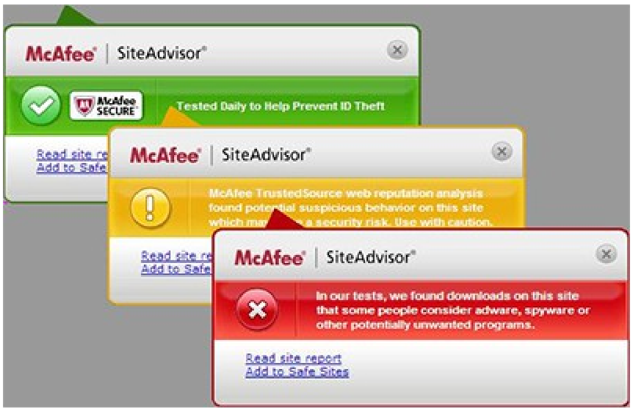
- **https://www.kaspersky.com.au (MAC and Windows)**
- **https://www.mcafee.com/au/index.html (MAC and Windows)**
- **http://www.superantispyware.com/download.html (Windows only)**

AND a CLEANER

- **https://www.ccleaner.com/ccleaner/download (MAC, Windows, & Android)**
They have free versions you can run today/right now! *I suggest purchasing the Pro versions.*

Protect Yourself - Be Smart

McAfee has a fantastic free tool to stop you from clicking on links to websites that may contain malware, viruses, or any kind of phishing scam. Sometimes you can't have this as well a virus program.. depends if they allow it.



Tested Daily to Help Prevent ID Theft

McAfee TrustedSource web reputation analysis found potential suspicious behavior on this site which ma a security risk. Use with caution.

In our tests, we found downloads on this site that some people consider adware, spyware or other potentially unwanted programs.

A green tick says the website has been tested and is safe, a yellow tick means proceed with caution if you *have* to, and a RED TICK advises you to STAY AWAY.

You can download McAfee Site Advisor **http://www.mcafee.com/mcafeewebadvisor** and there is an upgrade to a Professional Version available.

What you can do:

- Most people don't realise a new computer doesn't always come with an excellent virus/malware program. And it may only run for 30 days or not at all unless you do something.

- They also need updating, upgrading and renewing...
  Make sure you have *current* protection (do any upgrade/updates) **AND** they are set to “always on” and “monitoring 24/7”, and check that regularly

- Have something that cleans your browser history/cookies every time you close your browser, like CCleaner

- When downloading anything - watch for, and REMOVE ticks that allow programs to piggy back when you are downloading something you DO want

- Check your “see the programs installed on my computer” area and remove anything you don't use anymore or that you DID NOT download purposely (*be careful – make sure you **know** what you are removing*) Usually found under “control panel” and then “programs and features”

- **DO NOT** click on any attachment in an email when you do not trust or know the SOURCE. Particularly ZIP files. Anything from a “**bank**” should not be asking you to click any link. Google a little of the subject line, heading and see if there is a scam circulating. Otherwise ask your bank

- Delete spam emails as soon as you see them. Most email software/clients allow you to add the email address of annoying spammers to a list and then it can recognise and remove them easily

- EMPTY the trash/spam folders every day. Keep your inboxes neat and empty as possible. Use folders to save emails that you don't need to see any more, but need to keep

- Thunderbird (as opposed to Outlook) has a very easy process to **save your emails offline**, (so if anything happens to them on the server or “out there” you will never lose your emails). Just back them up on your computer as well

- BACK UP YOUR COMPUTER TO AN EXTERNAL DRIVE!

If you want help we can work on this, and set you up to be 99% free from
“I wish I had done this earlier” moments.