# Malware Explanation and Types - Protecting Your PC.

Garry Henwood

## Malware

The term malware refers to software designed and distributed to gain unauthorised access to computers and other connected devices, disrupt their normal operation, gather sensitive or confidential information or spy on the device's user(s).

top tips...

- Ensure you have reputable and appropriate internet security software loaded, updated and switched on at all times on all connected devices.
- Monitor the performance of all devices: if it is substandard for any reason that is not obvious, it may be infected by malware
- Be vigilant of webcams being unexpectedly activated.

## Common types of malware

### Virus

A virus is a file written with the intention of doing harm, or for criminal activity. Some are noticeable to the computer user, but many run in the background, unnoticed by the user. There are many types of virus. A worm for example, can exploit security vulnerabilities to spread itself automatically to other computers through networks. A Trojan horse (or simply 'Trojan') is a program that appears harmless but hides malicious functions. Potentially, a virus could arrive on your device in the form of a Trojan with the ability to replicate itself before moving on to another device (a worm) and also be designed as a piece of spyware.

### Spyware

Spyware is a type of virus that is specifically designed to steal information about your activity on your computer or other device. Spyware writers have a number of different objectives, mainly fraudulent financial gain or identity theft. Spyware can perform a number of illicit functions, from creating pop up advertisements to stealing your bank login details by taking screen shots of the sites you visit and even logging the keys you type (known as a keylogger). Spyware may also be self-replicating. An increasingly common form of spyware is a Remote Access Trojan (RAT), via which a fraudster or other cybercriminal can take over control of infected devices remotely and use it as if he / she were the authorised user. This can include activating webcams and physically spying on users' actions.

### Ransomware

Ransomware is an insidious form of malware which enables cybercriminals to lock down a computer or other device remotely, then charge a ransom to 'unlock' it.

Other types of malware include rootkits, dishonest adware and scareware.

**How devices get infected**

Malware can attack your computers or other devices via the following means:

- Opening infected email attachments such as .exe files.
- Opening infected files from web-based digital file delivery companies (for example HighTail (formerly YouSendIt), Dropbox).
- Visiting corrupt websites, which you may have been directed to via fraudulent links in emails or social media posts.
- Via the internet, undetected by the user (worms are an example of this).
- Macros in application documents (word processing files, spreadsheets etc).
- USB connected devices (such as memory sticks, external hard drives, MP3 players, cameras).
- CDs/DVDs.

**Malware can cause very serious consequences including:**

- Identity Theft.
- Fraud.
- Invasion of personal privacy.
- Theft, deletion and / or corruption of data.
- Non-compliance with data protection rules.
- A slow or unusable computer.

**Internet security software**

It is vital to keep your internet security (anti-virus, anti-malware software up to date in order to provide the most complete protection. Thousands if not millions of new strains of malware are detected every year, to say nothing of the variants of new and existing ones. Each has a set of characteristics or ‘signatures’ that enable internet security software manufacturers to detect them and produce suitable updates.

Most internet security software automatically downloads these updates (sometimes referred to as ‘definitions’) on a regular basis, as long as you are online and have paid your annual subscription (for a paid-for product). This should ensure protection against even the latest malware threats.

The software scans for viruses in a number of different ways:

- It scans incoming emails for attached viruses.
- It monitors files as they are opened or created to make sure they are not infected.
- It performs periodic scans of the files on your computer.

Some internet security software also scans USB connected devices (eg memory sticks, external hard drives, MP3 players), as they are connecting. Some also highlights suspect websites.

Internet security software will *not* protect you against:

- Spam.
- Any kind of fraud or other criminal activity online not initiated by malware.
- A hacker trying break into your computer over the internet.

Internet security software is not effective if it is switched off or not updated with the latest virus signatures.

**Choosing internet security software**

Depending on your budget and whether personal or Business use, there are a number of choices that you can take to decide which internet security software to buy:

- Package or standalone antivirus/antispyware software

Most internet security software vendors sell straightforward programs that only scan for viruses, as well as full security packages that provide other protection including firewall, spam filtering, anti-spyware controls and internet content filters. Antivirus/antispyware packages alone normally cost from £20 and full packages from £30. A package should include everything you need to protect your computers, mobile devices and infrastructure against online threats, and represents a smaller investment than buying each component separately.

Consider internet security software designed to make installation, updating and management easier across multiple devices.

- Free internet security software

There are a number of antivirus/antispyware products that are free – including some for commercial use. In most cases, these 'free' products are no-frills versions of purchasable products which the manufacturer hopes you will upgrade to in the future. The protection factor is likely to be equivalent to the paid-for version, but there may be limited or no technical support and some reduced functionality, for example in scheduling full scans.

- Windows Defender software is included – and enabled by default – in Windows 8, Windows 7 and Windows Vista. The Microsoft product is designed to prevent, remove, and quarantine spyware in Microsoft Windows. It was formerly known as Microsoft AntiSpyware.

Some manufacturers and retailers provide security software bundled with the computer. You do not have to use the security software supplied, but if you decide to keep it, do not forget to subscribe once the free trial period is over so that it stays up to date.

Also note that you should check carefully with vendors' instructions before using one internet security software product with another – as doing so may render both ineffective.

### Where to obtain internet security software

Internet security software is available from vendors' websites, specialist business computing retailers, high street stores and online retailers. When purchasing in store, it is normal to load a disk and then download updates over the internet when prompted. When purchasing online, you will automatically downlaod the latest version incorporating all updates make sure you keep your account details for reinstalling if necessary.

Free internet security software as described above, is also available from some internet service providers (ISPs) and banks such as Rapport. It is also possible to downlaod free software from the internet, but be sure you are using a trustworthy website.

### Virus & spyware protection

Apart from installing internet security software and keeping it updated, we recommend a number of other ways in which to keep your computers, mobile devices and network protected against viruses and spyware. After all, prevention is better than cure.

- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- Be careful with USB connected devices (eg memory sticks, external hard drives, MP3 players) as they are very common carriers of viruses.
- Be careful with CDs/DVDs as they can also contain viruses.
- Do not open any files from web-based digital file delivery companies such as HighTail (formerly YouSendIt) or Dropbox) that have been uploaded from an unknown, suspicious or untrustworthy source.
- Switch on macro protection in Microsoft Office applications like Word and Excel.
- Buy only reputable software from reputable companies.
- When downloading free software, do so with extreme caution.
- Dont be tempted to click on links pertaining to say that you have a virus, these are likely to be malware and should be removed with trusting software.