# What is malware?

Malware, short for "malicious software," is software that is used to harm computer users. It can do things like gather information, impersonate a user, gain access to other computers, or stop a computer from working. It could do this by allowing an attacker to record from a webcam and microphone, disabling anti-virus programs, recording keystrokes, copying emails and other documents, stealing passwords, and more. Most malware is criminal and is often used to obtain banking information or other valuable information. However, it is also used by governments, law enforcement agencies, and even private citizens to spy on users.

# Anti-virus software

You should always use anti-virus software on your computer and your smartphone, which are easily available to buy and download. [Avast](https://www.avast.com) is an easy to use anti-virus program for Windows. [Clam Win](http://www.clamwin.com/) is a good open source alternative. Anti-virus software can be quite effective at combatting cheap, ?non targeted? malware that might be used by criminals against hundreds of targets. However such software is usually ineffective against targeted attacks, such as ones carried out by governments against.

## How can I tell if my computer is compromised?

Malware is very difficult to detect. Scanners such as [Spybot](https://www.safer-networking.org/) or [Malwarebytes](https://www.malwarebytes.org/) can detect and protect against some malware threats and are useful to use.  
While most malware avoids detection by software, it is still sometimes possible to find indicators of it on your computer. For example, services will sometimes send you a warning email if they believe your account has been targeted, you may notice a light indicating that your webcam is turned on when you have not activated it yourself, or your settings have been altered to send copies of your emails to an unfamiliar email address.

# How can attackers use malware to target me?

The most common method of attack is to trick you into installing the malware yourself. There are many ways they try to do this.  
- They may disguise the malware as a link to a website, a document, a software update, or even a program designed to help secure your computer. - You may be targeted via email (which may look as if it?s coming from someone you know), via a message on Skype or Twitter, or even via a link posted to your Facebook page. - You can also infect your computer by connecting infected hardware, like a USB key given to you or found near your office, or a phone connected to charge.

The more targeted the attack the more they?ll try to make it look like something you want to open. For example, in Syria, pro-Assad hackers targeted members of the opposition with malware hidden in fake revolutionary documents and a fake anti-hacking tool. And in Morocco, activists were targeted with malware hidden in a document made to look as if it had been sent by an Al-Jazeera reporter, promising information about a political scandal.

There is also the possibility of someone gaining physical access to your computer to install malware themselves. You can read more about preventing against such attacks in the [Organisational Security ? Office section](umbrella://lesson/office).

# How can I avoid getting infected?

* Always make sure you are running the latest version of your software and downloading the latest security patches. Only the latest updates have the latest protections. It is a common belief that if you are running an unregistered copy of Windows, you cannot or should not accept security updates. This is not true. Always update. [Secunia PSI](https://secunia.com/products/consumer/psi/sys_req/) for Windows is a free tool that will check to make sure your software is up to date.
* Only download software from official sites.
* Only download software from official sites.
* Avoid open opening suspicious attachments (anything from someone you don?t know) or clicking on suspicious links (any links you didn?t request)
* If you are using Gmail, open unusual attachments in Google Drive rather than downloading them.
* Double check the sender?s email address if you get an email with an attachment or link you weren?t expecting, even if the email appears to be written by a friend or colleague. If something seems odd or their tone is unusual, it doesn?t hurt to email the friend to check they sent it and mention it to colleagues.
* Stay alert when browsing websites. Watch for browser windows that appear automatically, and read them carefully. When in doubt, you should close 'pop up windows' by clicking the X in the upper corner, rather than by clicking Cancel.
* Disconnect your computer from the Internet when you are not using it and shut it down completely overnight

# What should I do if I find malware on my computer?

* The first thing you should do if you find malware on your computer is unplug your computer from the Internet and stop using it immediately. Every keystroke you make may be being sent to an attacker.
* Log into a computer you believe is safe and change your passwords; every password that you typed on your computer while it was infected should now be considered to be compromised.
* You may wish to reinstall the operating system (eg Windows, Android, IOS) on your computer in order to remove the malware. This will remove most malware, but some especially sophisticated malware may persist.
* If you can, take your computer to a security expert, who may be able to discover more details about the malware.
* If you have some idea of when your computer was infected, you may reinstall files from before that date. Reinstalling files from after the date of infection may re-infect your computer.

Swipe right for this lesson's checklist

Go to the Advanced lesson for advice on how to protect yourself against targeted malware attacks.

[Go to Advanced Lesson](umbrella://lesson/malware/1)

### RELATED LESSONS

* Office lesson

### FURTHER READING

* [EFF - How do I protect myself against malware](https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware)
* [Security in a Box - Chapter 1, Malware](https://securityinabox.org/chapter-1)