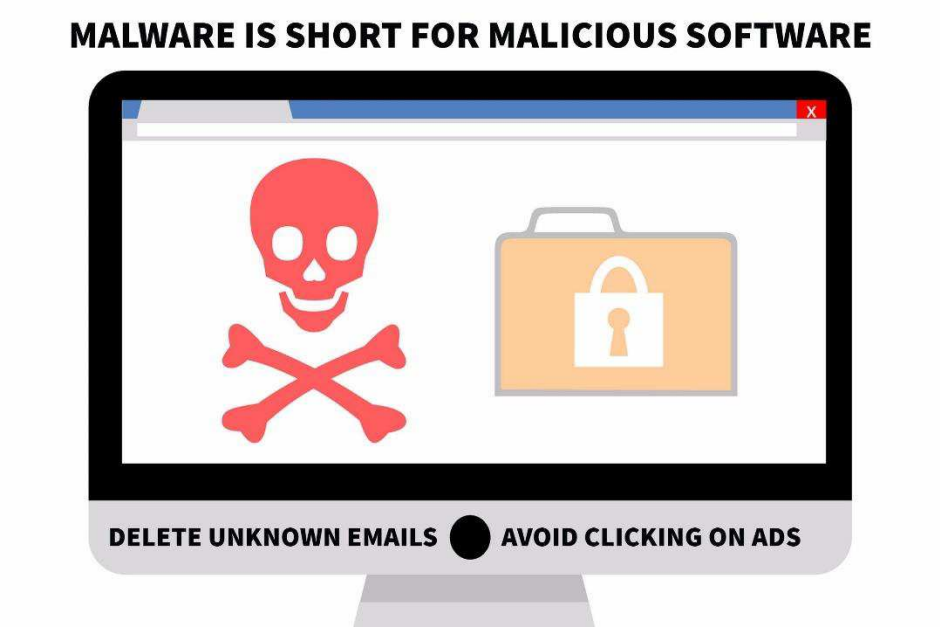

When you hear the term 'malware,' do you want to hide under your desk and cover your ears? Do you feel completely lost hearing this terminology? *Fear not, you are not alone!*

Malware is short for *malicious software*, which refers to a type of computer program designed to infect someone's computer and inflict harm on it, in multiple ways. Malware can infect computers and devices in several ways. It comes in several forms; just a few of which include viruses, worms, Trojans, spyware and more. It's vital you know how to recognise and protect yourself from malware.

Here are the different forms of malware with their meanings, so you can learn more about them:

- Malware – A buzz word for intrusive software, including computer viruses, Trojan horses and adware.
- Adware – Software that automatically downloads or displays advertising banners or pop ups when you are online.
- Spyware – Software that enables you to obtain information about another computer's activities by transmitting data using their hard drive.
- Viruses – Small programs or scripts that can negatively affect the health of your computer. These malicious programs can create files, move files, erase files, consume your computer's memory and cause your computer not to function correctly.
- Worms – A type of virus that replicates itself, but does not alter any files on your machine. However, worms can still create chaos by multiplying so many times that they take up all your computer's available memory or hard disk space. If a worm consumes your memory, your computer will run very slowly and possibly even crash.
- Trojan Horses –Software programs that look like regular programs, such as games and even antivirus programs. Once they are run, these programs can do malicious things to your computer.

The next question is, *"who is creating it, and why?"* Malware today is largely designed by and for professional criminals. These criminals may employ a variety of sophisticated tactics.

In some cases, cybercriminals freeze computer data; making your information inaccessible and then demand a ransom from the users, to get that data back.

One of the many risks that cybercriminals pose to heavy computer users is stealing online banking information, such as banking and credit card accounts / passwords. The criminal hackers who steal this information, may then use it to empty your account or run up fraudulent credit card bills in your name. They may even sell your account information on, where this confidential information fetches a good price.

How do I protect myself against Malware?

- Realise that you are an attractive target to hackers. Don't ever say *"It won't happen to me."*
- Have up to date antivirus software installed on your systems. Without this, you could be in trouble.
- Install security patches. Patching helps to protect your devices and has become extremely important as part of the updating process.
- Be careful with any software you install. Contact your IT provider if you are unsure.
- Delete any unknown emails. Never download or open attachments unless you are sure it's from someone you know. If you receive emails from random people, do not open them.
- Avoid clicking on ads. Especially ads where something is bright and colourful, with the possibility that you can win a prize! Ads have become more sophisticated and interactive so that you'll be tempted to play it like a game.

Please feel free to call our helpful and knowledgeable team on 01843 572600 if you would like any advice about cyber security. You can also email us at hello@365itsupport.co.uk – we are always happy to help and provide advice for your IT requirements.