Malware

What is Malware?

Malware is short for malicious software, and it refers to software programs designed to damage or other harmful/unwanted actions on a computer system. Malware means anything that is harmful to your computer basically.

What are the most common types of Malware?

- **Virus:** Infects program files and/or personal files. These are programs that try to replicate and spread across a computer on a network.
- **Spyware:** Software that collects personal information. These are programs that secretly record what you do on your computer. The majority of spyware is malicious. Its aim is usually to capture passwords, banking credentials and credit card details - and send them over the internet to fraudsters.
- **Worm**: Malware that can replicate itself across a network. A worm is a computer program that copies itself to other computers across the internet. Worms are often used to infect large numbers of broadband-connected computers with remote-control software.
- **Trojan horse:** Malware that looks, and may even operate, as a legitimate program
- **Browser hijacker:** Software that modifies your web browser
- **Rootkit:** Software that gains administrative rights for malicious intent
- **Malvertising:** The use of legitimate online advertising to spread malicious software.

Threats	What can be done to avoid them?
Virus	• Keep your operating system up to date. • Use up to date anti-virus software, Anti-virus software can inspect computer files and email attachments for viruses and remove or quarantine any which are found. • Don’t open an email attachment unless you are expecting it and know the source (many email servers scan emails with anti-virus software on the user's behalf). • Don’t allow other users to use their own memory stick on your system. • Only download files from reputable web sites. • Avoid any software from unreliable sources. • It is good practice to back up your data regularly. If a virus does damage your data, you can restore the damaged files from backup.
Spyware	There are several ways that you can protect yourself from spyware. Firstly, don’t unwittingly install it. Only Download programs and software from reputable software sites and the reviews of download sites can help you decide

which are the safest. Many shareware download sites now test programs submitted to them and offer guarantees that their archives are free of spyware.

Secondly, you can install an anti-spyware tool. Many of these are of high quality, and some are freeware themselves. These tools regularly download updates to stay abreast of newest emerging spyware. Some of them can run in the background all the time, without really slowing down your computer, and they generally do a very good job.

Worm

A good anti-virus program can protect you to some extent, but it's not enough on its own as it's hard to keep it up to date. Many modern worms change hourly and it can take a day or more to create and distribute an anti-virus update.

You also need a firewall to help block the worm's communications, and you should always browse the web with restricted rights - as a 'user', never as an 'administrator'.

But the most effective way to prevent worm infection is to turn off JavaScript for normal web browsing. JavaScript is a powerful tool that makes websites interactive, and it's increasingly relied on by web designers. But it's also the most common entry point that worms use to infect your computer.

So there's a trade-off. Turning off JavaScript for normal web browsing will limit your access to many websites, but it's the best form of protection against worm infection.

Trojan

In computing, a Trojan horse is a program that appears harmless, but is, in fact, malicious. Attackers have long used Trojan horses as a way to trick end users into installing malware.

Typically, the malicious programming is hidden within an innocent-looking email attachment or free program, such as a game. When the user downloads the Trojan horse, the malware that is hidden inside is also downloaded. Once inside the computing device, the malicious code can execute whatever task the attacker designed it to carry out.

- Get an anti-virus scanner of the highest quality and, keep it up to date.
- Install a firewall to prevent hackers from entering the user system.

- Educate users to avoid opening e-mail files, sites, attachments etc.
- In Windows, do not open questionable file extensions such as “exe”, “vbs”, “com”, “bat” and, ensure you can view all file extensions. Windows hides long extensions so the file maybe “xyz.vbs.jpg and, you see only exyz.jpg
- Install an executable server at mail server level as well as a virus scanner on the network.