Types fo malware

Malware is **any code that can be used to steal data, bypass access controls, or cause harm to or compromise a system.**

Knowing what the different types are and how they spread is key to containing and removing them

SPYWARE

- **Designed to track and spy on you, it monitors your online activity and can log every key you press on-your keyboard and capture almost any data**

- it does this by modifying the security settings on your device

ADWARE

- **is often installed with some version of software**

- **is designed to automatically deliver advertisements to a user** - its common that it comes with spyware

BACKDOOR

- **it is used to gain unauthorized access by bypassing the normal   
 authentication procedures to access a system** - it works in background and is difficult to detect

RANSOMWARE

- **it is designet to hold a computer system or the data it contains captive until a payment is made**

- it usually works by encrypting your data so that you cant access it

- it is often distributed by fishing emails

SCAREWARE

- **it used ‘scare’ tactics to trick you into taking a specific action**

- it consists of operating system style windows that pop up to warn you that   
 your system is at risk and need to run a specific program for it to   
 return to normal

ROOTKIT

- **it is designed to modify the operating system to create a backdoor, witch   
 attackers can then use to access your computer remotely**

- they take advantage of software vulnerabilities to gain access to resources   
 that normally shouldn’t be accessible

- they can also modify:   
 system forensics, monitoring tools making them really hard to detect  
 device infected with this has to be wiped

VIRUS

- is a **type of computer program that, when executed, replicates and attaches Itself to other executable files, such as a document by inserting its own code**

- they can be harmless - shows funny img

Destructive - modify or delete data

- they can be programmed to mutate in order to avoid detection.

TROJAN HORSE

- **it carries out malicious operations by masking its true intent**

- it might look legitimate but is, in fact, very dangerous

- **trojans exploit your user privileges and are most often found in img, files,**

**audio files and games**

- they act as a decoy to sneak malicious software past users

WORMS

- **it replicates itself in order to spread from one computer to another**

- **worms can run by then self's unlike a virus**

- **they don’t need user permision and spread very quickly over the network**

Symptoms of malware

- An increase in CPU usage

- PC freezing and/or crashing

- decrease in your web browsing speed

- unexplainable problems with your network connections

- modified or deleted files

- presence of unknown files, programs or desktop icons

- unknown processes running

- programs turning off or reconfiguring themselves

- emails being sent without your knowledge or consent