Malicious Code

A word created by combining parts of two words is called a **portmanteau word**

Malicious code is computer code which is designed to cause problems for a user. It is often called **malware** – a word created by combining **mal**icious and soft**ware**.

Malware refers to a variety of types of hostile or intrusive software. It includes viruses, worms, spyware, adware and Trojans.

- **hostile software** will try to cause problems in the system it infects, such as deleting files or transferring data
- **intrusive software** simply gets in the way, perhaps by installing unwanted software or displaying adverts

All types of malware are a security issue which can be managed by users. Their impacts are often similar: viruses and Trojans, for example, can both have the same effect; the key difference is in the way that they spread.

Computer Viruses

Viruses are malicious software which are designed to harm a user's system. They are usually hidden within other software and infect a system when that software is installed. Viruses modify other software, copying their own code into the software. They can spread rapidly from machine to machine across a network or across the internet, just like illnesses caused by viruses in humans.

The first viruses were developed in the 1970s and 1980s but were effectively harmless experiments. The late 1980s saw the first harmful computer viruses

Viruses are often harmful. For example they might corrupt or delete data on a disk and can make a system unusable.

New viruses develop all the time which is why it is important to update the virus definitions used by anti-virus software on a regular basis.

Trojans

A **Trojan** is a piece of malware which looks like it should be something else. They are usually disguised as legitimate software and might be downloaded from a less secure download service or via a link in an e-mail.

Trojans can be the source of **ransomware** attacks. These are when a system is hijacked and money demanded to allow the user to regain control

When the Trojan is installed it can destroy data, disrupt a system or, most frequently, create a "backdoor" way for a system to be exploited. This can lead to data such as bank account details, passwords or other personal information being accessed.

Trojans are named after the famous wooden Trojan Horse from Greek history which hid soldiers to allow them to get inside the city of Troy. The point of a Trojan is that it allows access to a system through disguise – just like the Greeks and their wooden horse.

Spyware

Spyware creates a "backdoor" to send information about the users system to a hacker. It might send information such as passwords and personal data or could send information about data entered by the user – an infection known as a **keylogger**.

Spyware is generally packaged alongside other software and is installed when that software is installed. It is often hidden within free software or downloads connected to online games such as Minecraft.

Dealing with Malware

Anti-virus software is a program designed to detect, prevent and remove malware.

Firewalls can be used to block malware attempting to download files or transfer data from a network

Originally anti-virus software focussed on detecting viruses, but modern AV programs can deal with a variety of types of malware. They can often detect threats as they occur. It is important to keep anti-virus software up to date and ensure that virus definitions are updated very regularly.

Automatic software updates will also patch vulnerabilities in software, ensuring that malware can spread less easily. If software is not kept up to date, weaknesses can be found and exploited. This can include web browser software and applications such as Flash Player. The issues with Flash got so bad that it is now no longer being updated and many web browsers will warn you before playing a Flash file.

Modern web browsers will often identify web sites which are likely to contain malware threats and spam filters will identify threats in e-mails. Operating systems will generally warn users when they are about to install software as well – in some cases specifically suggesting that there could be a threat if the source of the software is not officially registered.

Educating users of the risks of malware, and in particular of downloading files from dubious websites, is a key strategy to deal with malware.

Ransomware attacks are where hackers install software on a system and then lock it, demanding payment to release the lock. Users can be unable to access any data or computer systems. The NHS was the victim of a major ransomware attack in 2017 and a number of schools, universities and businesses have been the target of attacks.

Activities:

a) Write a definition of the term **malware** [2 marks]
b) Summarise key points about the three types of malware
c) Describe the differences between a virus and a Trojan
d) Research the impacts of recent malware threats, including the use of ransomware
e) Obidos travel runs a network of 7 machines.
    i. Explain why Obidos Travel should be concerned about the spread of malware
    ii. Describe the precautions that OT could take to guard against the risks of malware