Y9 Computing – Autumn 1

Key Term	Definition
Social engineering	humans trying to trick or manipulate other humans.
Shouldering	an attack designed to steal a victim's password or other sensitive data. It involves the attacker watching the victim while they provide sensitive information, for example, over their shoulder.
Phishing	an attack in which the victim receives an email disguised to look as if it has come from a reputable source, in order to trick them into giving up valuable data
Blagging	is an attack in which the perpetrator invents a scenario in order to convince the victim to give them data or money.
Profiling	The act of gathering information about a person , based on their behaviour, choices and habits.
Malware	A generic term given to a group of types of software that are specifically designed to cause harm to a digital device. Mal (malicious) (soft) ware.
Anti-Malware	A type of software to protect your system in real-time against malware attacks or files.
Firewall	Network security device which works live and monitors files and traffic deciding to block or not block files and access, in order to protect the networks
Denial of service attack	This is a cyberattack in which the criminal makes a network resource unavailable to its intended users.This is done by flooding the targeted machine or website with lots of requests in an attempt to overload the system.
Script Kiddies	Script kiddies are hackers (not necessarily kids) who use tools downloaded from the internet that allow them to hack with little technical knowledge.
Penetration testing	Penetration testers (pen testers) are people who are paid to legally hack into computer systems with the sole purpose of helping a company identify weaknesses in their system.

Computer Misuse Act

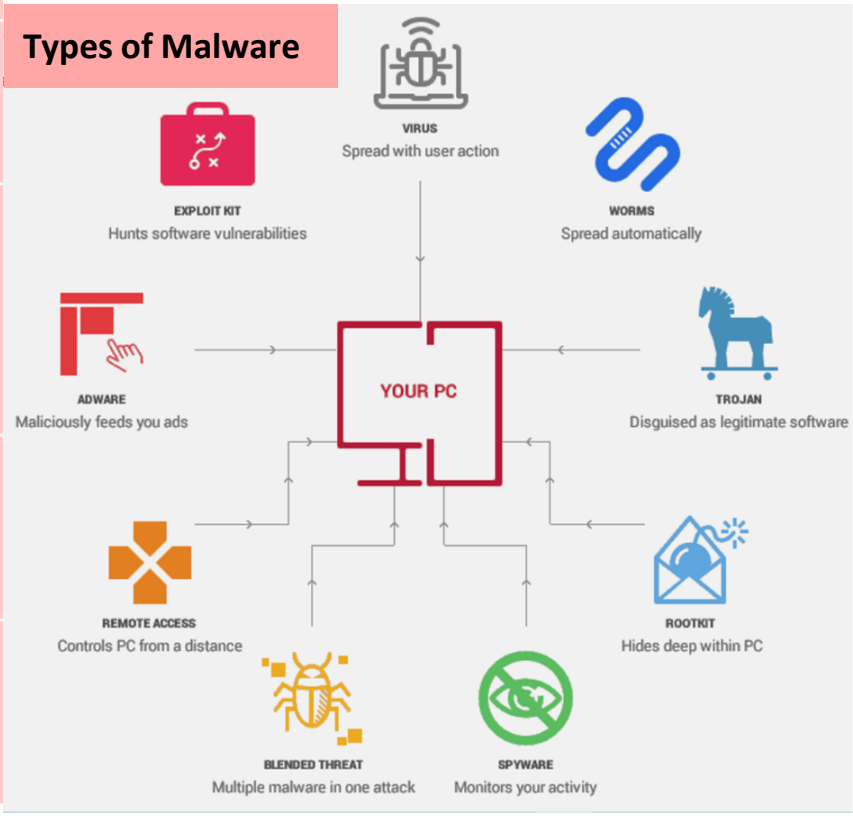
This act covers the **unauthorised access** to a digital device or account. Where there is also **intent to commit further offences**. For example , hacking into a system and stealing data to sell it , is actually two offences. The hacking/unauthorised access breaks the Computer Misuse Act, whilst stealing/selling data breaks the Data protection Act.

Data Protection Act

The Data Protection Act (DPA) is a United Kingdom Act of Parliament which was passed in 1988. It was developed to control how personal or customer information is used by organisations or government bodies.
Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Types of Malware



Hacking

Hacking is the act of gaining access to a system without permission (often electronically) through software. Hacking is broken down into 3 different types of hacker
White hat - Often referred to as an ethical hacker , testing systems for companies and reporting findings.
Grey hat - Skilled developer who may break some laws or ethical standards but without intent.
Black hat - Criminals who break into computer networks with malicious intent to harm or steal.