

**Policies and Laws**

|  |  |
| --- | --- |
| **Network Policy** | A policy that consists of specific settings and principles that employees of a company of organisation must do to use the system. |
| **Computer Misuse Act** | A law that has been designed to prevent unlawful activity on the computer. It is split into 3 parts – Access without permission, intent to do something, and modifying/destroying files. |
| **Copyright, Designs and Patents Act** | A law that protects people’s original work so others cannot change, publish, share or sell it to benefit. This includes assets such as books, music, photographs, videos, games, etc. |
| **Data Protection Act** | A law made up of 8 principles that companies and organisations must follow to keep people’s data secure.  |

**Networks and the Internet**

|  |  |
| --- | --- |
| **Network** | Two or more devices that are connected so they can communicate with one another. |
| **Internet** | A large global network that gives access to information. |
| **Firewall** | A filet feature that monitors traffic coming in and out of a network. It stops things it thinks are a threat coming in.  |

**Types of Attack**

|  |  |
| --- | --- |
| **Brute Force Attack** | An attack that focuses on trial and error methods to match up people’s usernames and passwords in order to access their accounts. There are many different types of brute force attacks that all work in different ways, however all revolve around the idea forcefully accessing accounts  |
| **Data Interception & Theft** | The use of software called packet sniffers that stop data packets when sending messages. The packet sniffers intercept the messages, take the information, and then feedback to the hacker so they can gain personal details. |
| **Denial of Service Attack** | An attack that overloads a system with rapid communications in order to get it to crash and corrupt. This is so it stops businesses and organisations from running as normal, which then result in a loss of profit and reputation due to not being able to satisfy customers. |
| **SQL Injection** | SQL stands for Structured Query Language which is the language used by systems that use databases to store details. SQL can be used to ask questions about the data stored. An SQL injection adds malicious code to corrupt the database. This can cause the system to crash and work similar to a denial of service attack, however an SQL injection also means that the hacker can get into the system to steal stored data.  |

**What you need to be able to do**

* Explain what a network is and know what the threats are linking to the Internet
* Describe how a firewall works and what it does.
* Understand the different types of attacks hackers can use to steal data and corrupt systems and why they do it.
* Define what a network policy is, and understand the different laws linked to using computers.

**Keywords**

|  |  |
| --- | --- |
| Network | Internet |
| Firewall | Force |
| Intercept | Theft |
| Denial | Service |
| Database | Policy |
| Law | Misuse |

**Year 9 Unit 1 – Half Term 2 - Security Systems**