Year 9 Topic 1 – Cybersecurity

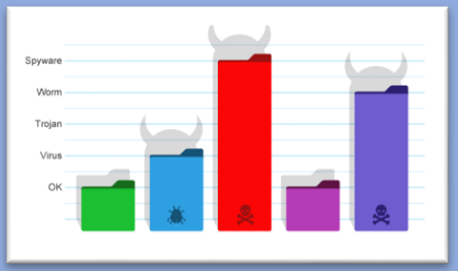
Lesson	Can you?
Lesson 1: You and your data	Explain the difference between data and information Critique online services in relation to data privacy Identify what happens to data entered online Explain the need for the Data Protection Act
Lesson 2: Social engineering	Recognise how human errors pose security risks to data Implement strategies to minimise the risk of data being compromised through human error
Lesson 3: Script kiddies	Define hacking in the context of cyber security Explain how a DDoS attack can impact users Identify strategies to reduce the chance of a brute force attack being successful Explain the need for the Computer Misuse Act
Lesson 4: Rise of the bots	List the common malware threats Examine how different types of malware causes problems Question how malicious bots can have an impact on societal issues
Lesson 5: There's no place like 127.0.0.1	Compare security threats against probability and the potential impact to organisations Explain how networks can be protected from common security threats
Lesson 6: Under Attack	Identify the most effective methods to prevent cyberattacks

Useful websites

- www.threatmap.checkpoint.com
- www.forbusiness.snapchat.com/advertising#targeting
- www.policies.google.com/privacy#infocollect
- www.ncsc.gov.uk
- www.en.wikipedia.org/wiki/Hacktivism
- www.en.wikipedia.org/wiki/2016_Dyn_cyberattack
- www.cps.gov.uk/legal-guidance/computer-misuse
- www.en.wikipedia.org/wiki/Computer_virus
- www.en.wikipedia.org/wiki/Computer_virus#First_examples
- www.us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html
- www.en.wikipedia.org/wiki/Computer_worm
- www.us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html
- www.antivirus.comodo.com/blog/computer-safety/computer-worm-definition
- www.en.wikipedia.org/wiki/Ransomware
- www.malwarebytes.com/ransomware
- www.uk.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

KNOWLEDGE ORGANISER
Key Stage 3 - COMPUTING

Malware is a general term that describes lots of different programs that try to do something unwanted to your computer. Anti-virus software prevents malware from attacking your computer or mobile device. There are free anti-virus applications available:



- A **virus** harms your computer in some way, usually by deleting or altering files and stopping programs from running.
- A **trojan** starts by pretending to be a trusted file, but gives **unauthorised access** to your computer when you run it.
- **Worms** are difficult to get rid of. They copy themselves over networks to **external storage devices**
- **Spyware** collects information from your computer and sends it to someone.
- **Scareware** tricks you into thinking it's software that you need to buy.

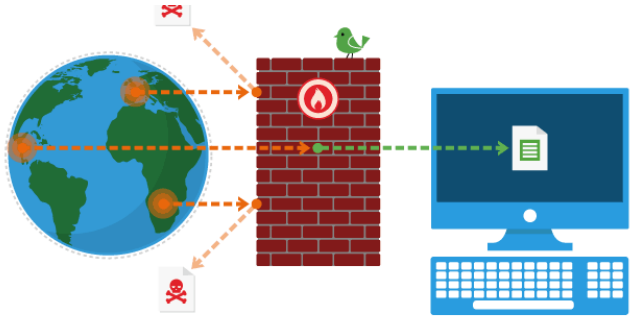
Cyber attacks and **cyber terrorism** are ways of attacking companies and organisations online. There are frequent cyber attacks on the government and businesses in the UK.

Hackers attempt to break into networks to steal private information.

A DoS attack is a deliberate attempt to prevent legitimate users of a network from accessing the services provided by the server or connected systems. The classic DoS attack will come from a single computer sending multiple requests to the server.

Denial of service attacks usually aim to overload servers or systems with requests for data or access to resources like the processor or main memory. Some denial of service attacks also exploit weaknesses, either in the security system or network infrastructure.

A firewall is software that will block unexpected connections coming in to the network. Most operating systems include a firewall.



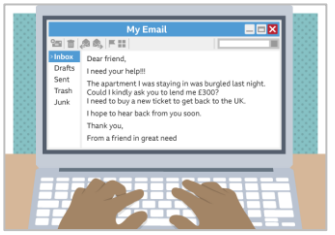
Viruses are written by malicious programmers who wish to cause problems for other computer users.

The primary source of infection these days are **email attachments** followed by **illegal software** and infected files from the **internet**. If you have up to date **anti-virus** software installed this will immediately warn you of any infection. If not, there is usually no evidence of the virus and the user is not usually aware of it until something goes wrong.

A brute force attack goes through every possible combination of a password or encryption key. Modern computers have the processing power to go through combinations of letters, numbers and characters very quickly.

Social engineering is manipulating people into handing over confidential information such as a PIN or password. There are several forms:

- **blagging**
- **phishing**
- **pharming**
- **shouldering**



CHURCH STRETTON SCHOOL