Knowledge Organiser
Spring 1 – Cyber security

Key term	Definition
Cybersecurity	Protecting computers, networks, and data from hackers or viruses.
Hacker	A person who uses computers to access data without permission.
Firewall	A security system that blocks unauthorized access to or from a network.
Antivirus Software	A program that detects and removes viruses and other harmful software from your computer.
Malware	Short for "malicious software" – programs designed to harm or steal data (e.g., viruses, worms, spyware).
Phishing	A scam where someone tries to trick you into giving personal information, often through fake emails or websites.
wo-Factor Authentication (2FA)	A security method that requires two forms of identification to log in (e.g., password + code sent to your phone).
Encryption	A way of scrambling data so only someone with the right key can read it.

Data v Information Data is raw facts and figures. It only becomes information when it has been processed and becomes meaningful

Data is raw facts and figures:

John: 28

Claire: 49

Jade: 40

Ahmed: 45

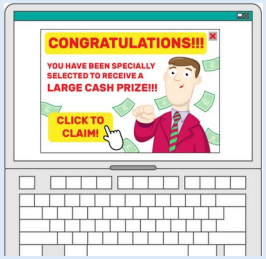
Chloe: 38

Information is created when that data has been processed and becomes meaningful:

These are scores from a test where the pass mark was 35.

John needs to resit the test.

The average score is 40.



There are lots of technical ways to try and keep data safe and secure. **Human error** arguably creates the largest risk of the data being compromised. **Social engineering** is a set of methods used by cybercriminals to deceive individuals into handing over information that they can use for fraudulent purposes. Methods of social engineering are, shoulder surfing, online quizzes, Phishing and blagging.

Methods of protecting data are:-

- Anti-malware
- Firewall
- Password rules
- Auto-updates
- Two-factor authentication
- Biometrics
- CAPTCHA
- Staff training