Knowledge Organiser: Cyber security

Data and information: Data is raw facts and figures. **Information is created when data has been processed and becomes meaningful**. Data does NOT depend on information, but information DOES depend on data. Data is the input and information is the output.

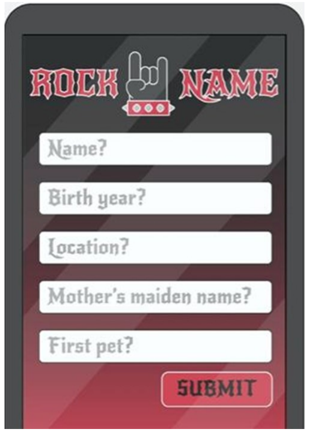
Social engineering: Social engineering is a set of methods used by cybercriminals to deceive individuals into handing over information that they can use for fraudulent purposes. The difference between social engineering and other cybercrimes, is that social engineering is **humans trying to trick or manipulate other humans**.

Shouldering (also known as shoulder surfing) is 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**.

Name generator attacks: These are attacks in which the victim is asked in an app or a social media post to combine a few pieces of information or complete a short quiz to **produce a name**.

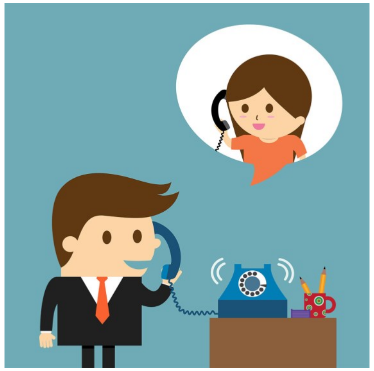
Attackers do this to find out **key pieces of information** that can help them to answer the **security questions** that protect people's



Phishing attack: A phishing attack is 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.

The email usually provides **a link to another website** where the information can be inputted.

Blagging: Blagging (also known as pretexting) is an **attack in which the perpetrator invents a scenario** in order to convince the victim to give them data or money. This attack often requires the attacker to **maintain a conversation** with the victim until they are **persuaded** to give up whatever the attacker asked for



Knowledge Organiser: Cyber security

Hacking : Hacking in the context of cyber security is **gaining unauthorised access to or control of a computer system**.

People may want to hack for the following reasons:

- ethical reasons

- to steal data

- to disrupt services

-for financial gain

- for political reasons (**hacktivism**) or for fun.

Black Hat
Malicious hacker
White Hat
Ethical hacker
Gray Hat
Not malicious, but not always ethical

Computer Misuse Act : protects **personal data held by organisations** from unauthorised access and modification. The act makes the following illegal:

1) Unauthorised **access** to computer material.

2) Unauthorised access to computer materials **with intent** to commit a further crime.

3) Unauthorised **modification** of data.

4) **Making, supplying or obtaining** anything which can be used in computer misuse offences

Script kiddies: Scrip kiddies are hackers (not necessarily kids) who use tools downloaded from the internet that allow them to hack with little technical knowledge.

DOS attack: Denial of Service attack 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**

DDOS : Distributed Denial of Service has the same concept as a DoS attack, but this time it is **multiple computers** making the attacks at the same time. It is a lot **harder to identify who is responsible, as lots of machines are making requests,** many of them because they are infected by malware.

Brute force attack: involves **'guessing'** username and passwords to gain **unauthorized access to a system**. Brute force is a simple attack method and has a **high success rate**. Some attackers use applications and scripts as brute force tools.