# Knowledge Organiser

## Learning Aim B: Cyber Security

Mr Moorcroft

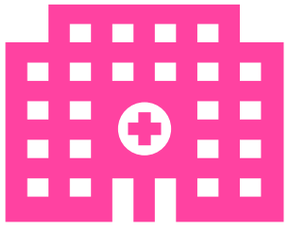
# 01 Why Systems Are Attacked

| Reasons | |
|---|---|
| **Financial Gain/Theft** | When the purpose of an attack is to gain money. A common example is ransomware, which encrypts the user's files until a fee is paid. If the fee is not paid, the files will be deleted. |
| **Fun/Challenge** | Hackers may attack systems for the thrill or sense of personal achievement. They may see more security as an increased challenge. They may also receive recognition from their peers. |
| **Industrial Espionage /Disruption** | When an organisation's intellectual property – e.g. designs, strategies, etc. – are stolen or services are purposely disrupted by a competitor in order to harm the organisation financially. |
| **Personal Grudge** | Some attacks can be personally motivated. Most commonly this is when former or current employees hold a grudge against an organisation, particularly if they feel treated unfairly. |

## Case Study: 'Wanna Cry'

The **'WannaCry'** ransomware attack in 2017 **encrypted** the files of over 200,000 computers worldwide, demanding a ransom paid in **Bitcoin**.

In the UK, this included NHS computer systems, which were running Windows XP and therefore vulnerable.



## Key Terms

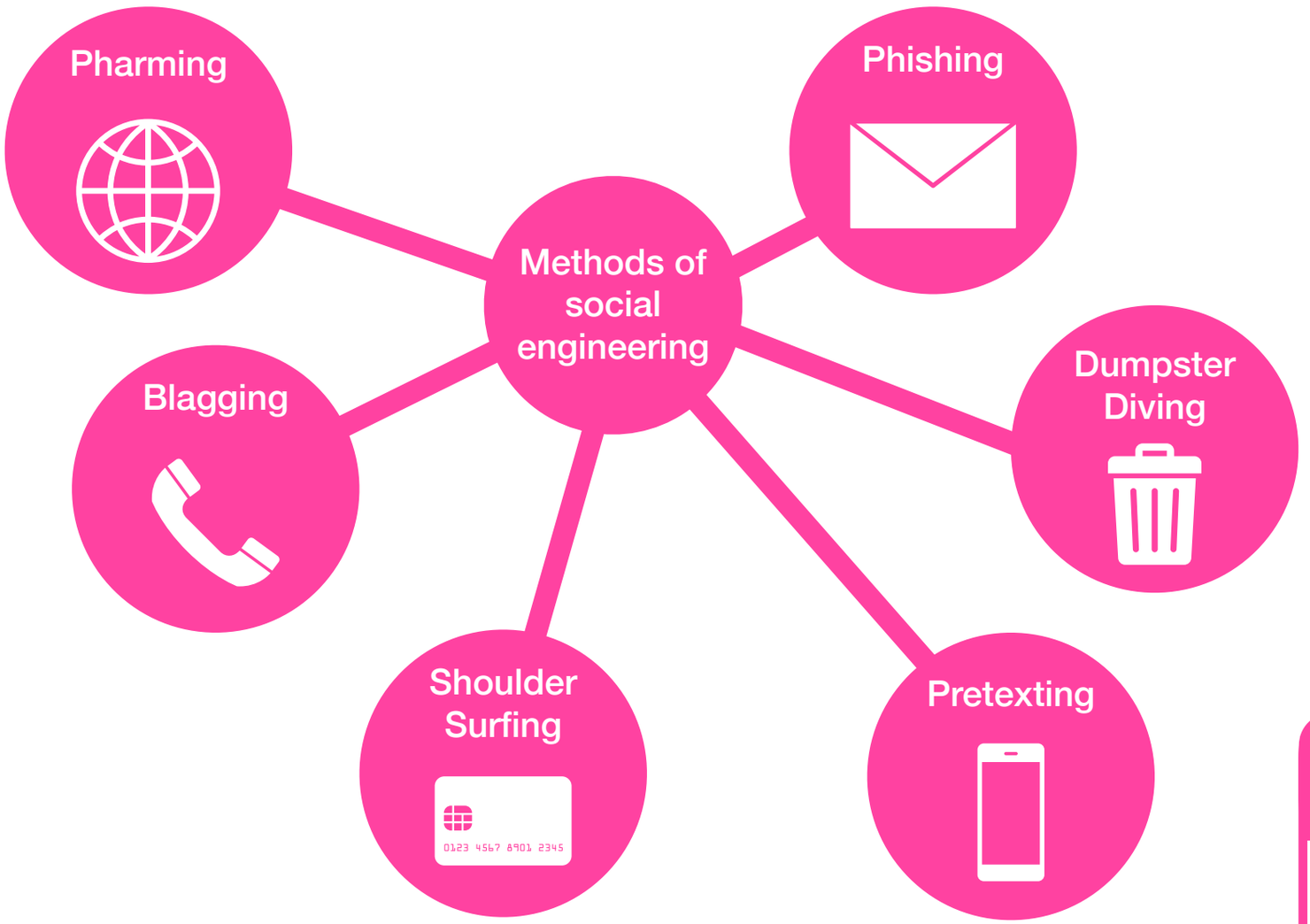
**Intellectual Property** - An idea that you invented that belongs to you. For example, a copyrighted image.

**Ransomware** - A form of malware that encrypts (locks) a user's files until a fee is paid.

**Malware** - Malicious software that is designed to disrupt or damage a computer system.

**Denial of Service (DDoS)** - Floods a computer with requests so it is unable to respond to legitimate requests.

# 02 External Threats




An **external threat** comes from an individual **outside of an organisation**, as opposed to an internal threat which comes from an individual inside the organisation. An external attack is most likely to be for financial gain.

| White Hat Hacking | vs | Black Hat Hacking |
|---|---|---|
| When a hacker is employed by an organisation to test the security of its systems. | | When a hacker unlawfully gains access to a system for their own gain/use. |

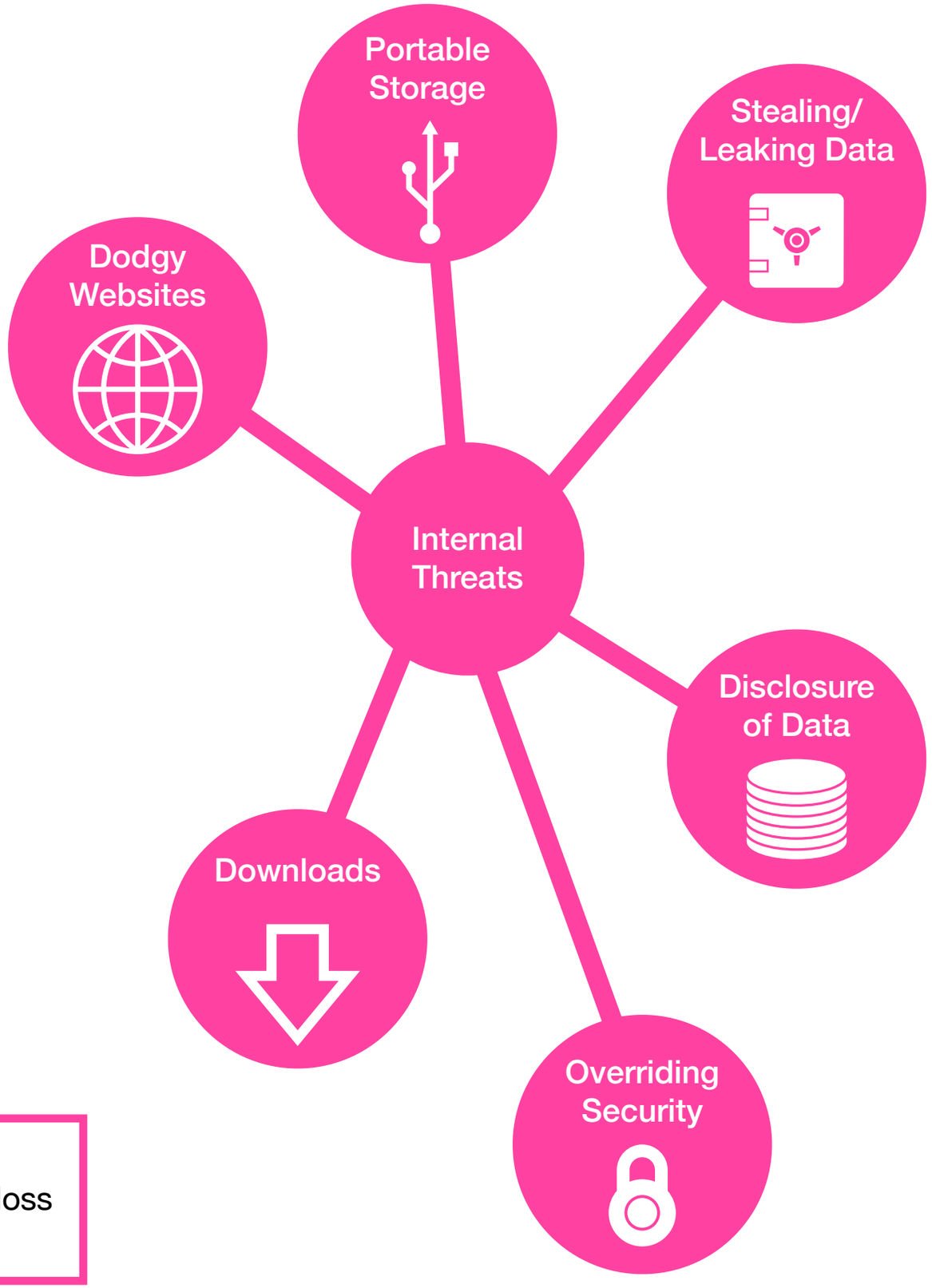
## Man-in-the-Middle Attacks

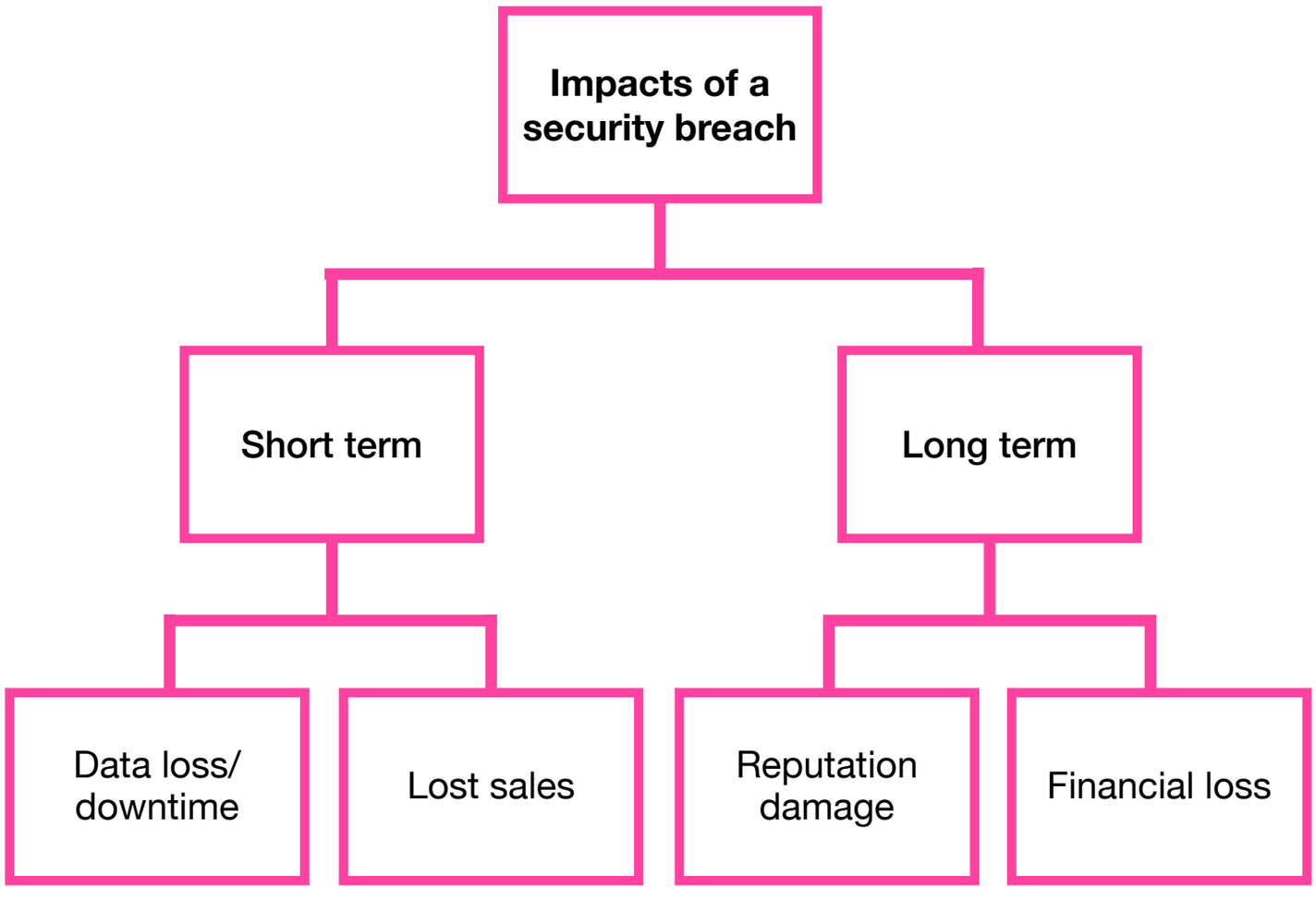
A '**man-in the middle**' cyber attack is where communication between two devices – for example, a user and a web server – **is intercepted and potentially tampered with**.

This type of attack can be prevented by **encrypting data** so it is unusable if stolen (through the **use of a VPN**) or **avoiding** the use of **public (free) Wi-Fi**.

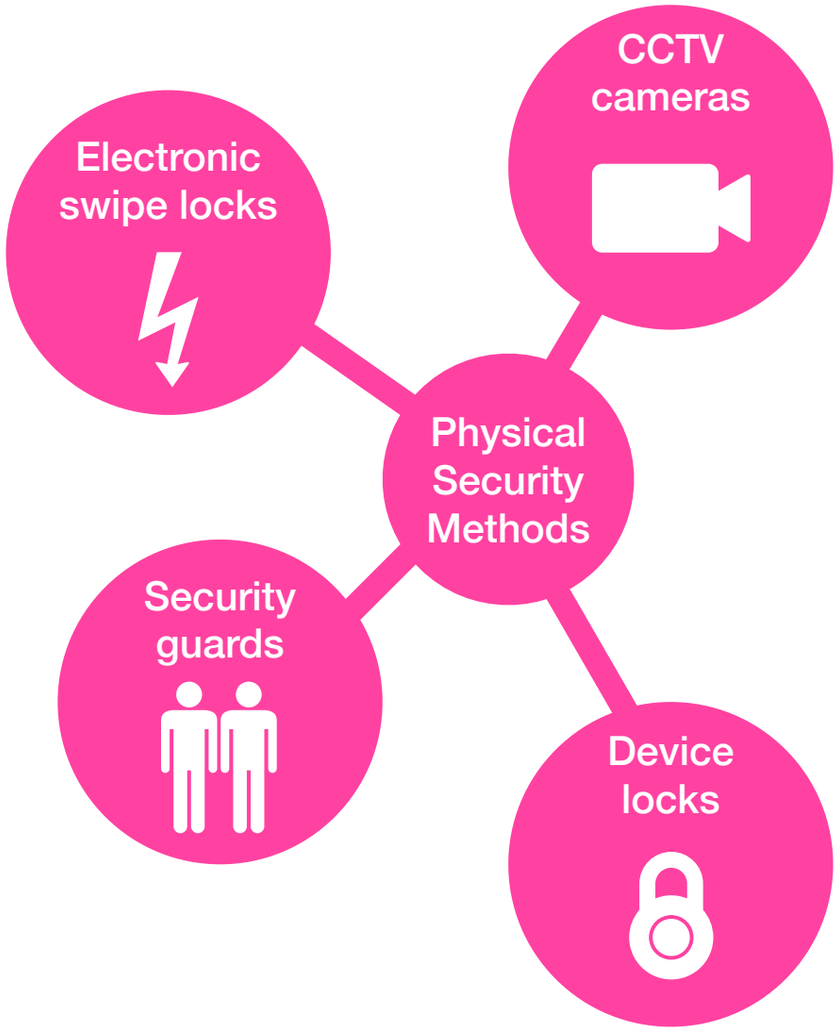
# 03 Internal Threats

Although some internal threats occur because of accidents, it is also possible that an **employee might choose to attack a business** if they feel disgruntled in some way. This may be because they have been let go by the business or passed over for a promotion.



# 04 User Access Restriction




**Two-factor authentication** asks the user to provide a **second form of identification** alongside a password. For example, a six-digit code send to their phone.

| Advantages of Two-Factor | Disadvantages of Two-Factor |
|---|---|
| Adds security. | Some second factors can be lost, e.g. USB. |
| Can use a device the user already owns, e.g. phone. | Slows down access time. |

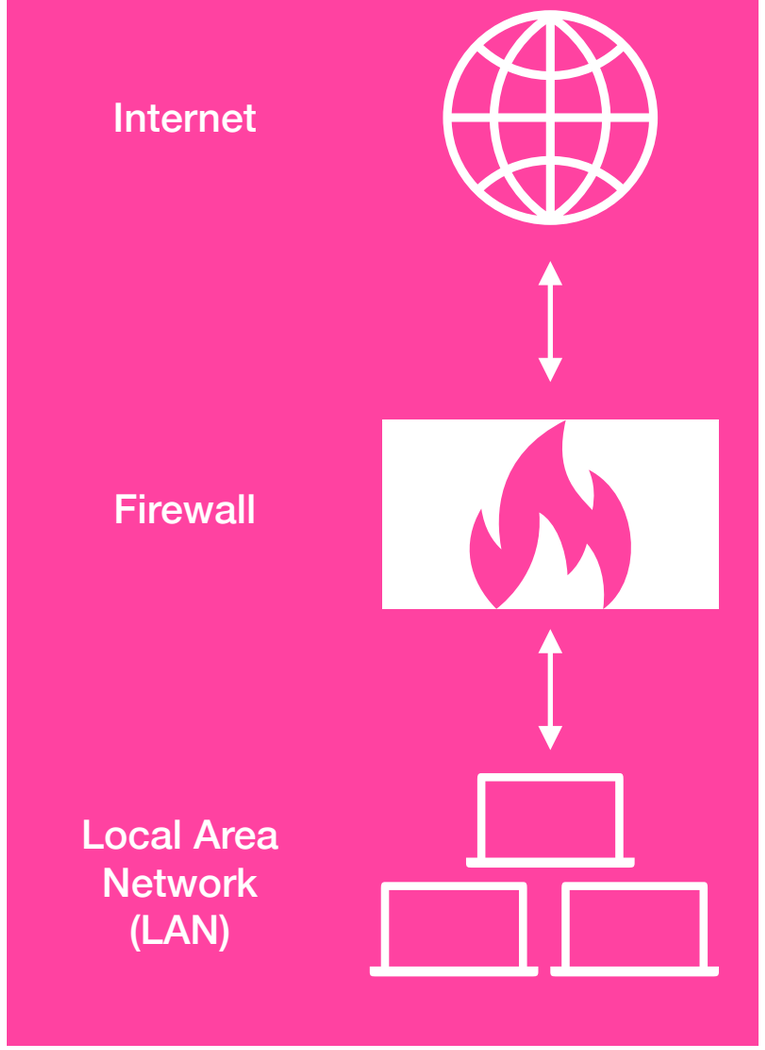
**Biometrics often used by phones:**


| Advantages of Physical Security | Disadvantages of Physical Security |
|---|---|
| Acts as a deterrent. | Often expensive to purchase/ maintain. |
| Prevents access to where files are stored. | Some methods, e.g. CCTV don't prevent theft. |

| Advantages of Biometrics | Disadvantages of Biometrics |
|---|---|
| Don't need to be remembered. | Require specialist hardware. |
| Can't be guessed. | Invades privacy. |

# 05 Firewalls

| Key Terms | |
|---|---|
| **Firewall** | Can be hardware or software based, they use a set of rules that filter suspicious network packets from remote networks. |
| **Local Area Network (LAN)** | A network based in a single geographical location, such as an office or a school. |
| **Access Control List (ACL)** | A list that tells the network which data can be sent and received. |
| **Session cookies** | Data stored by a web browser until it is closed. |
| **Worm** | A small computer program that can spread to other programs. |
| **Trojan** | A type of malware disguised as a legitimate program. |
| **Spyware** | Software that is installed on a device without the user's knowledge with the intention to collect data/information. |

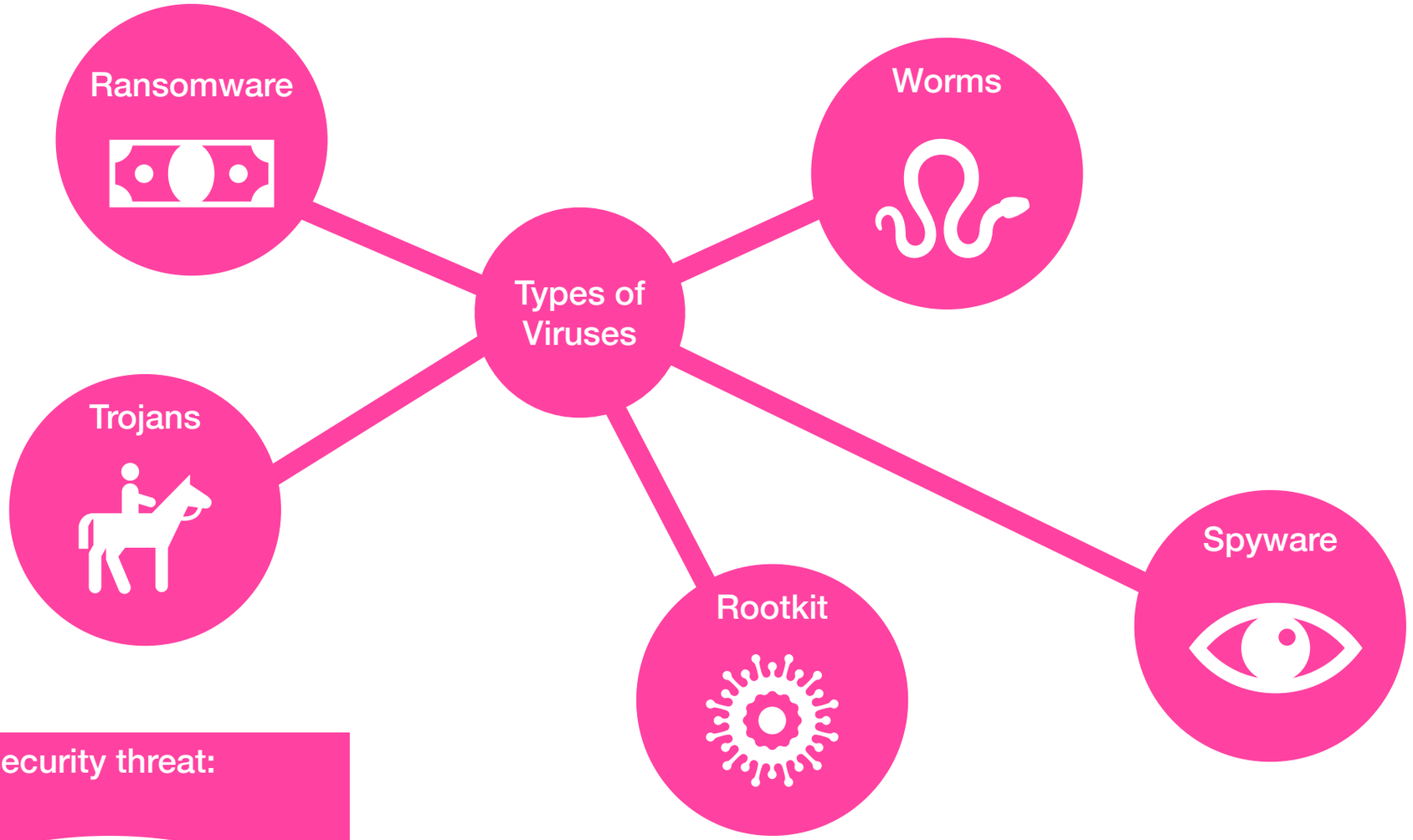



| Advantages of Firewalls | Disadvantages of Firewalls |
|---|---|
| Prevents unauthorised access from hackers. | Can accidentally block legitimate access. |
| Can be used to restrict access to websites. | Uses a lot of memory, slowing performance. |

| Hardware Firewall | vs | Software Firewall |
|---|---|---|
| Sits between an external network and an internal connection - like a LAN and the internet - as a first line of defence. | | On a system - like a computer - to filter network data in and out. Secondary protection, which uses an ACL to block certain data. |

# 06 Anti-Virus Software

**Anti-virus** software monitors a digital system to identify and remove **malicious software** based on what it knows about **viruses** in its database.



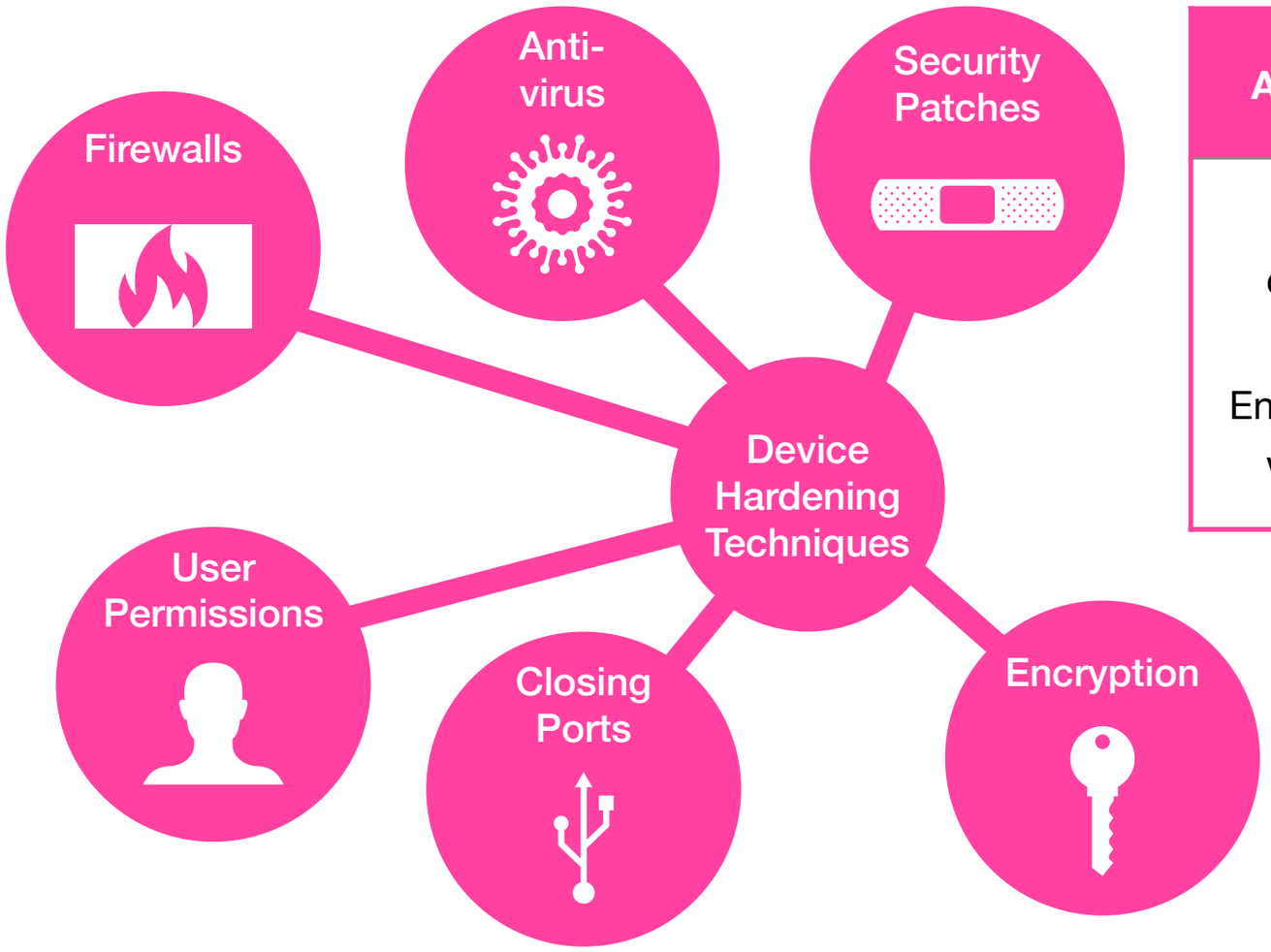

## Software features that pose a security threat:

**Autocomplete** - makes suggestions based on previous inputs, which on a public system could expose other users' inputs.

**Stay-logged-in** - uses cookies to keep a user logged in but could then give subsequent users access to that account.

| Advantages of Anti-Virus Software | Disadvantages of Anti-Virus Software |
|---|---|
| Prevents malicious software from accessing a computer. | Requires constant updates to be effective. |
| Many anti-virus programs are free to download. | Constantly scanning files, which can slow a computer. |

# 07 Device Hardening and Encryption




| Advantages of Encryption | Disadvantages of Encryption |
|---|---|
| Scrambles data so that it cannot be read by others. | Does not prevent data from being stolen in the first place. |
| Ensures organisations comply with data protection laws. | Encrypting a large amount of data can take time. |

| Key Terms | |
|---|---|
| **Vulnerability** | A flaw or weakness in a system design or configuration that allows for access from attackers. |
| **Security Patch** | Additional settings or programs that fix vulnerabilities in operating systems or device firmware. |
| **Privilege** | A set of rules that allows users to use specific components or access data files or folders. |

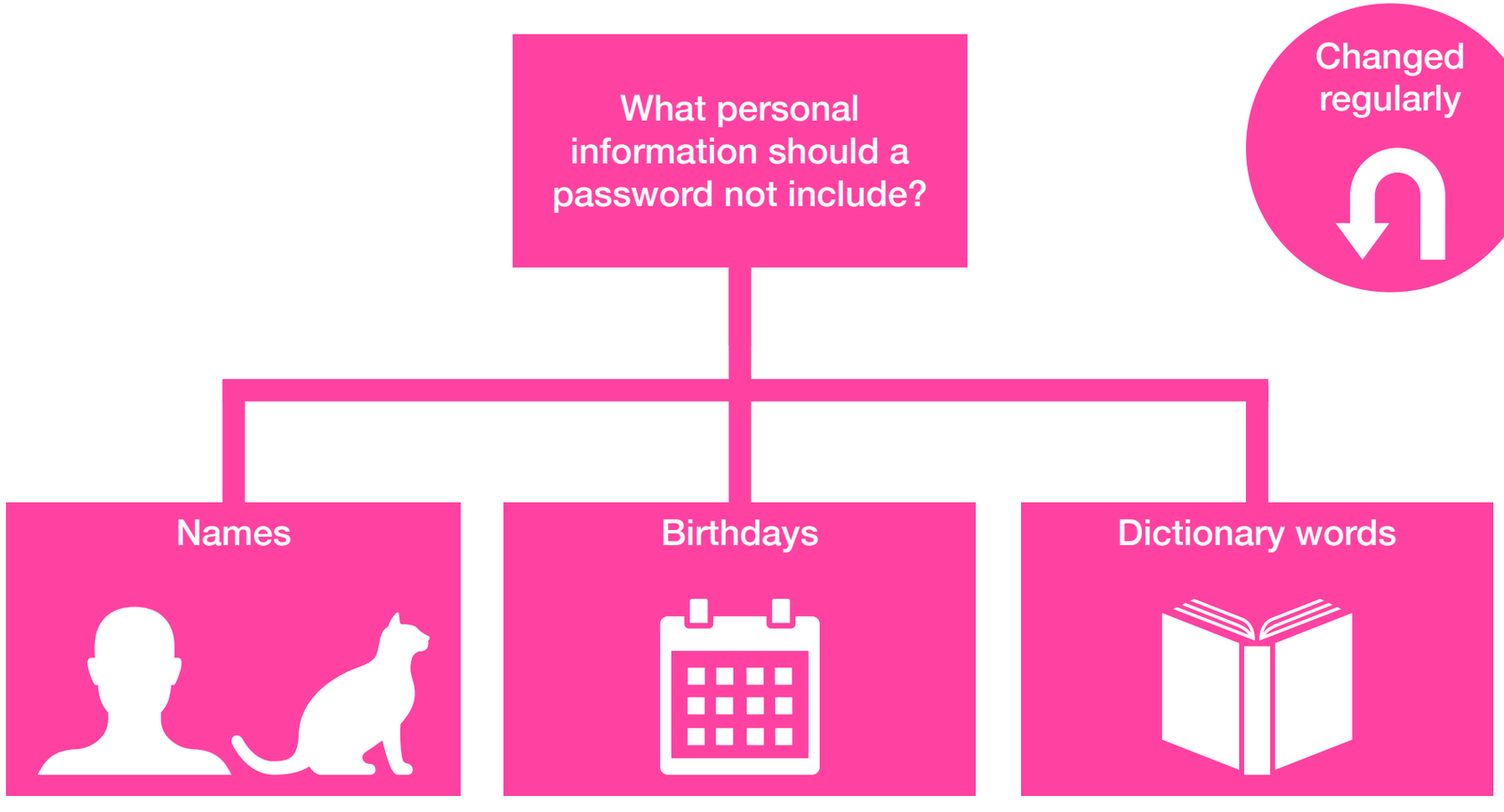
**Encrypted data** is scrambled before it is sent so that it can't be read by anyone else.

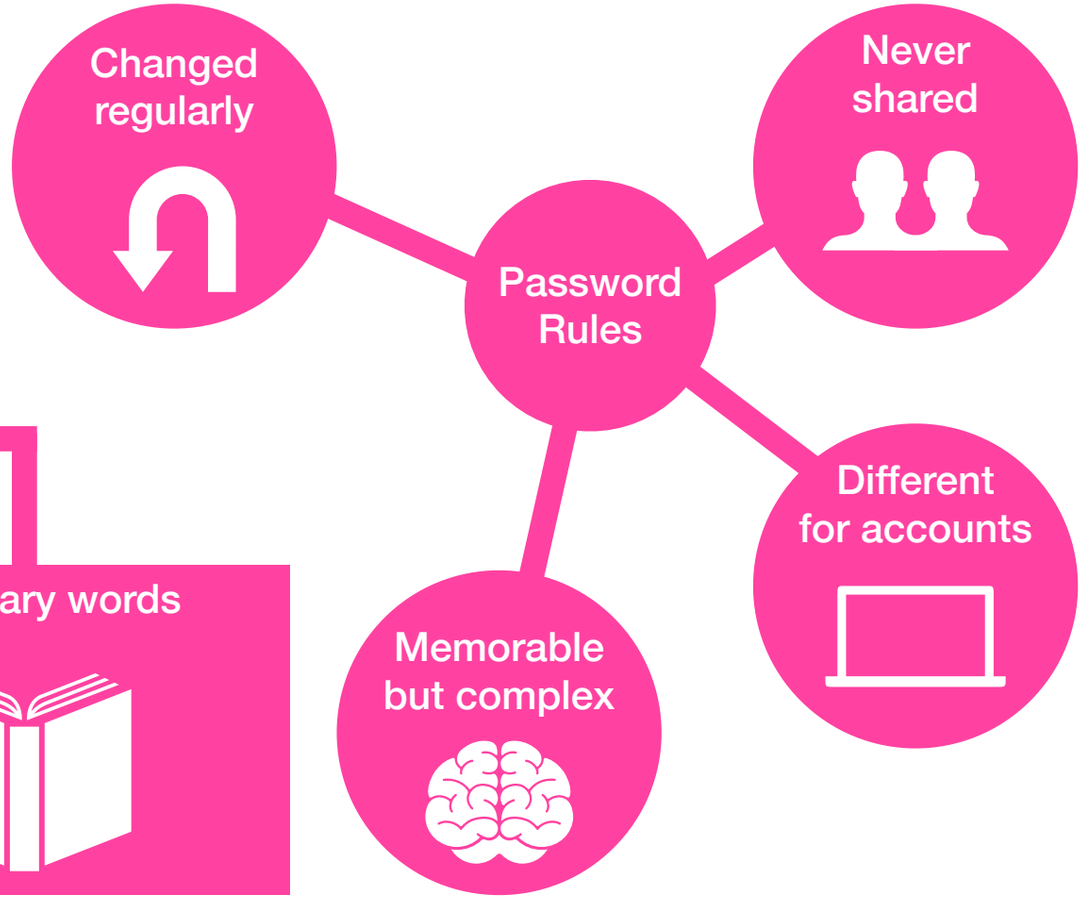
Only the **intended recipient** knows how the data was **scrambled** and therefore how to decrypt (unscramble) it.

# 08 Passwords

| Password Strength | |
|---|---|
| **Weak** | An obvious password using just letters or numbers personal to the user (e.g. PASSWORD or 123456). |
| **Medium** | Uses a combination of letters and numbers but the information is more difficult to guess (e.g. LiverPool5). |
| **Strong** | Makes use of special characters, numbers, upper/lower case letters in a random formation (e.g. A?vEr9gS!). |

**Default passwords** are those that an account is set-up. They should be changed very quickly because they are so **commonly used** and therefore an attacker's first guess.



# 09 Finding Weaknesses

**Ethical hacking** is where an organisation hires someone to to **simulate an attack** on its systems to **find weaknesses**. This is called **penetration testing**.

What vulnerabilities can be found through penetration testing?

- Unpatched operating systems/software

- Data that has not been encrypted

- Bad security practices/ incorrect privileges

| Advantages of Ethical Hacking | Disadvantages of Ethical Hacking |
|---|---|
| You can see if your systems can withstand an attack. | Professionals with such skills are very expensive. |
| Vulnerabilities in system security can be found/fixed. | There is a possibility the ethical hacker could ‘go rogue’. |

| White Hat Hacking | vs | Grey Hat Hacking |
|---|---|---|
| Invited by an organisation to find vulnerabilities/ weaknesses in their systems. | | Attacks a system uninvited but doesn’t do any damage/ steal anything. |

# 10 Security Policies

An **Acceptable Use Policy (AUP)** sets out the rules for how individuals can **use an organisations systems/ network**.

It typically covers use of the internet, use of equipment and software installation.

**How would users gain access to new software?**

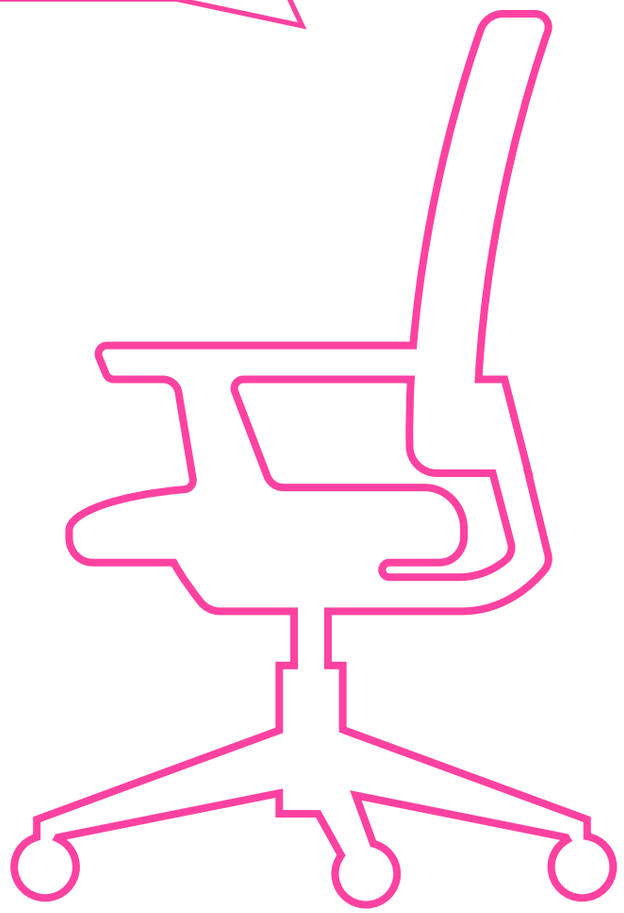
- Contact the IT Helpdesk (administrator) - in writing.
- Choose from an approved list of software.
- Get permission from their manager or superior.
- Be able to justify the need for new software.

## How can an Acceptable Use Policy be enforced?

**Monitoring** - use of computer systems is monitored using either software or CCTV.

**Access rights** - different levels of permissions are set depending on a user's seniority in an organisation.

**Software audit** - a process where all the software on a computer is checked to ensure it is authorised.



# 11 After An Attack

## 1

### Investigation

The organisation should find out the type of attack, how severe it was, how they were affected and when it happened.

## 2

### Respond

The organisation should inform any affected stakeholders (customers, employees, etc.) and the appropriate authorities (e.g. the police).

## 3

### Manage

The organisation should isolate the problem and contain the threat to prevent it doing any further damage.

## 4

### Recover

The organisation should follow its disaster recovery policy, allocating responsibilities and deciding on remedial action.

## 5

### Analyse

The organisation should analyse what went wrong, how it could have been prevented and what lessons have been learned for the future.