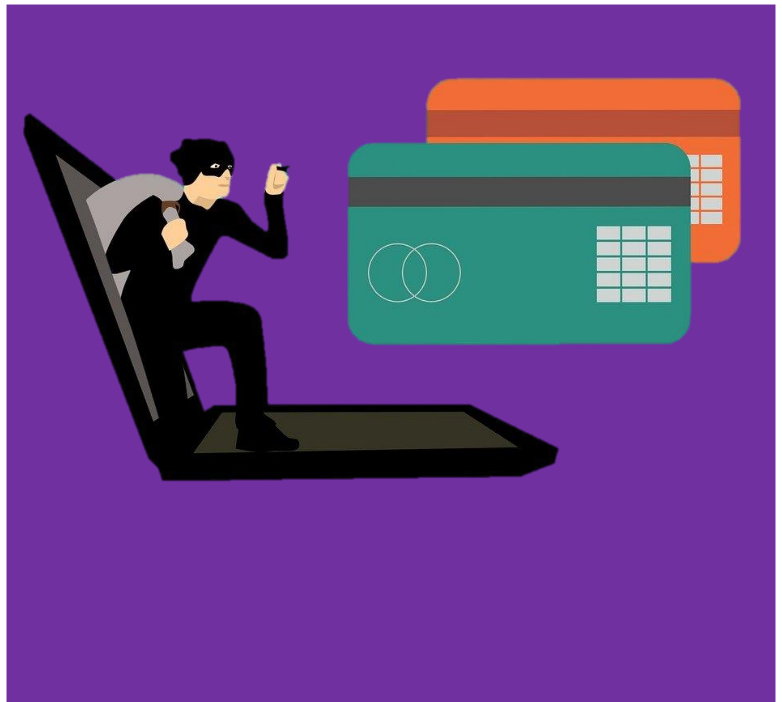
Unpatched or Outdated Software

- Software often contains bugs.
- These can be serious and allow hackers to access parts of the software they should not.
- Software providers release patches, containing code to fix these bugs.
- If these patches aren't installed, hackers can use flaws in the system to gain unauthorised access to the information.
- Old software often is no longer supported by its developers and so will not receive patches.
- This means security flaws can go unfixed for long periods of time or even forever.

Removable Media

- Hackers can use removable media to steal data from systems.
- Removable media can be used to install malware on systems.
- Removable media is small and portable making it easy to steal.
- Organisations will often prevent the use of removable media on their systems.
- Data stored on removable media should be encrypted so that it cannot be easily read if the device is lost or stolen.



Misconfigured Access Rights

- Sometimes users are given access to information or systems they should not have access to.
- Individual user accounts allow access to be restricted to specific users.
- This is not always set up correctly.
- Hackers can use this to steal information or damage systems.

Weak and Default Passwords

- Using easy to guess passwords makes it easier for hackers to access systems.
- Passwords such as password, 1234 or the user's name are the first hackers will try.
- Passwords should contain a combination of lower and upper case characters, numbers and symbols.
- Longer passwords are much harder to guess.
- Many devices and applications have a default password when first setup.
- These passwords are commonly known and available online.
- Hackers will try these passwords first.
- All passwords should be changed to a secure password when devices and software are installed.

Unit 6: Cyber Security

Malware and Malicious Code

- Malware refers to many different forms of hostile, dangerous or intrusive software.
- Anti malware software exists specifically to protect against malware.
- Common sense and caution can reduce the risk of malware.
- Avoiding download untrusted or suspicious programs can reduce the risk.
- Viruses
- A program designed to disrupt or damage a computer system.
- May cause the system to stop functioning or loose data.

Trojans

- Malicious software hidden in what seems to be a normal program.
- Free games or music often contain Trojans.
- Once installed will damage the system or attempt to steal data.

Spyware

- Records activity on a computer system.
- Used to steal personal data.
- A key logger is spyware which records every single key typed

Pharming

- Redirects website traffic to a fake website.
- May involve changing the host files on the victim's computer, or tampering with the DNS system.
- May take advantage of misspent web addresses.

Penetration Testing

- The process of attempting to gain access to a system without knowing usernames, passwords or other normal ways to access it.
- Useful to test systems to identify where weaknesses are.

White-Box Penetration Testing

- Simulates a malicious insider with knowledge of and/or basic credentials for the target system.
- The person performing the test is given some information about how the system works.
- They use this to identify possible holes prior to starting the testing.

Black-Box Penetration Testing

- Simulates an external hacking or cyber warfare attack
- The person performing the test has no information about the system and is not given any credentials.
- They look for any possible weaknesses or flaws using a trial and error approach.

Social Engineering

- Manipulating people to give up confidential information.
- There are many different forms of social engineering.

Blagging (Pretexting)

- Using an invented scenario to engage a specific victim in a way that increases the chance the victim will give out information or perform actions which would be unlikely in ordinary circumstances.
- This often involves researching the target on Facebook or other social media.
- Limiting the amount of personal information posted online helps prevent this.

Shouldering (Shoulder Surfing)

- Watching someone enter person private information over their shoulder.
- This could be watching someone enter their PIN.
- Can be done in person or using hidden cameras.
- Can be prevented by being aware of one's surroundings and being cautions about where sensitive information is entered.
- Screen filters on laptops can help here.

Phishing

- Fraudulently obtaining private information from someone.
- Often uses email and SMS.
- Phishing targets lots of people at the same time, whilst blagging targets a specific individual.
- Phishing emails often contain errors or vague information.

Methods to Detect and Prevent Cyber Security Threats

Biometrics

- Uses things such as fingerprints or facial recognition which are unique to a person's individual biology.
- Much harder to fake or crack than traditional passwords.
- Much more convenient than remembering a password.
- Often used on mobile devices.

Passwords

- A code or word known only by those who should have access to a system.
- The most basic form of protection.

CAPTCHA

- Aims to detect automated attempts to access a system.
- Detects humans from computers
- Asks the user to read a difficult word or identify an image or other task only a person could do easily.
- Stops bots from being able to repeatedly try to access a system to crack it.

Email Confirmation

- Requires a unique code or link sent in an email.
- Means only those with access to a particular email account can access the system.
- Often used to confirm password resets.

Automatic Software Updates

- Installs patches automatically as soon as they are available.
- Prevents patches from being forgotten about.
- Allows patches to be installed more quickly than a human might be able to (e.g. for patches released at night)
- Fixes bugs before they can be exploited.