7 Cyber security threats

1. social engineering techniques
2. malicious code
3. pharming
4. weak and default passwords
5. misconfigured access rights
6. removable media
7. unpatched and/or outdated software

Cyber security threats

1. ~~social engineering techniques~~
2. ~~malicious code~~
3. pharming
4. weak and default passwords
5. misconfigured access rights
6. removable media
7. unpatched and/or outdated software

Threats 1 and 2 are major parts of the syllabus, so leave these for now

Cyber security threats

3. Pharming:

A cyber attack intended to redirect a website's traffic to a fake website

This might be sent as a link in an e-mail which appears to come from a trusted source, found as a link on the internet or linked from a QR code etc…

The fake website then tries to gather information from the user - e.g. by filling in an online form or entering a username and password combination

Cyber security threats

4. Weak and default passwords

Weak passwords are too simple and are easy to guess. For example, sets of very common passwords farewell known (pa55w0rd etc…)

But passwords that are too complex are difficult to remember - so users write them down. Password management software can help

Devices and systems have default passwords (e.g. voicemail, routers) that many users never change, leaving them vulnerable

Cyber security threats

5. Misconfigured access rights

Basic users (e.g. students at school) must only be allowed to do certain tasks on a network or machine. They shouldn’t be able to, for example, install software or access personal data about staff or students

If access rights are misconfigured then users are allowed to do things they shouldn’t be able to. This creates vulnerabilities - data can be accessed, copied, changed or deleted; software being installed can lead to malware

This can also cover access to websites where there may be malware downloaded etc…

Cyber security threats

6. Removable media

Removable media means USB sticks, SD cards, portable hard drives etc…

These can:

a) Introduce malware to systems
b) Be used to copy data and remove it from a site and then be easily lost or stolen

Many organisations now disable USB drives so devices can’t be used. That and the increased use of the Cloud to backup and transfer data means this is probably less of an issue than it was five years ago

Cyber security threats

7. Unpatched and/or Outdated software

Old software is less likely to be secure - e.g. old versions of web browsers; old versions of Operating Systems (Windows 7 for example). There may be vulnerabilities that can be exploited.

Firewalls may not be up to date

Software patches should be automatically updated. These update software and make it less vulnerable

Very old software or OS will no longer get patches released