AQA Computer Science GCSE

3.6 Cyber security

Advanced Notes

This work by PMT Education is licensed under CC BY-NC-ND 4.0

3.6.1 Fundamentals of cyber security

Cyber security consists of the processes, practices and technologies designed to protect networks, computers, programs and data from attack, damage or unauthorised access.

The main purpose of cyber security is:

- To ensure privacy by keeping personal and sensitive information secure.
- To maintain the availability of systems and data so they can be used when needed.
- To protect devices and networks from damage, disruption, or misuse.

3.6.2 Cyber security threats

Cyber security threats

Malicious code (malware)

Malicious code (malware) is an umbrella term used to refer to a variety of forms of hostile or intrusive software. These are covered in more detail in the coming pages.

Social engineering

Social engineering is an umbrella term used for a range of techniques that are used to manipulate people into giving away confidential information. These are covered in more detail in the coming pages.

Pharming

Pharming is a cyber attack intended to redirect a website's traffic to a fake website. A user may accidentally type in a web address incorrectly, and then land on a fake website that is designed to look like the website they were intending on visiting. The owner of this fake website can then collect any data that the user enters, such as their login information or bank details.

Weak and default passwords

When users select their passwords, they may leave them as the default (e.g. `change_me`), allowing hackers to gain access without any effort. Users may also select weak passwords that can be easily cracked - such as ones that only contain a small number of characters, that hackers can use brute force methods to obtain.

Misconfigured access rights

When users are given permission to access more files or systems than they need as part of their role, increasing the risk of data misuse. As a result, staff may be allowed to access areas they are not supposed to, and network admins might not know that secure areas have been breached as no-one has “broken in”.

For example, if a student in a school network is mistakenly given admin rights, they could change important files or access confidential information that should be restricted.

Removable media

Removable media, such as USB sticks or external hard drives, can be used to spread malware or steal data. For example, a USB drive left in a public place might be picked up and plugged into a school computer, unknowingly installing malware that spreads through the network.

Unpatched and/or outdated software

Software is regularly patched to fix known weaknesses and flaws, which can relate to security. Often known, weaknesses / flaws are often published online. Outdated software is no longer supported by its developer, so it might contain security vulnerabilities that haven't been fixed. If patches aren't installed or outdated software is used, then staff or hackers could exploit the known weakness / flaws to gain unauthorised access, potentially even installing malware.

Penetration testing

Penetration testing is the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access. This can be carried out to test the effectiveness of security measures, and find any vulnerabilities / weaknesses that a hacker could exploit, before real attacks happen. These vulnerabilities can then be addressed. There are two main types of penetration test:

White-box penetration tests

Used to simulate an attack from a malicious insider. The person or team testing the system will have knowledge of and possibly basic credentials for the target system.

Black-box penetration tests

Used to simulate an external attack. The person or team testing the system will have no knowledge of any credentials for the target system.

Social engineering

Social engineering is the art of manipulating people so they give up confidential information. Forms of social engineering include:

- **Blagging:** the act of creating and using an invented scenario to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.
- **Phishing:** a technique of fraudulently obtaining private information, often using email or SMS. Typically, the victim will receive a communication designed to look like it has come from a reputable source, such as their bank, which then contains a link to trick them into giving away their personal information, such as login details.
- **Shouldering:** observing a person's private information over their shoulder e.g. cashpoint machine PIN numbers.

To protect against blagging and phishing, users should always be cautious of unexpected phone calls, emails, or messages that ask for confidential details - especially if they create a sense of urgency. Check the source carefully; for example, don't click on links in suspicious emails or texts, and verify the sender's identity through a trusted method. Use strong, unique passwords and avoid discussing private information in public places. When entering PINs or passwords, cover the keypad to prevent shouldering, and check first that you aren't being watched.

Malicious code (malware)

Malicious code (malware) is an umbrella term used to refer to a variety of forms of hostile or intrusive software. Forms of malware include:

- **Computer virus:** A type of malware that attaches itself to a legitimate program or file and spreads when the infected file is opened. It can corrupt or delete data, slow down systems, or even make them unusable.
- **Trojan:** A malicious program that disguises itself as legitimate software. Once installed, it can create backdoors, allowing hackers to control the system, steal data, or install more malware without the user's knowledge.
- **Spyware:** A type of malware that secretly gathers information about a user's activity, such as keystrokes, login details, or browsing habits, and sends this information to the attacker.

To protect against malware, users should install reliable antivirus and anti-malware software and keep it up to date. Software and operating systems should also be regularly updated with the latest security patches. Users should avoid downloading files or software from unknown or untrusted sources, and be cautious when opening email attachments or clicking on unfamiliar links. Backing up important data regularly can also help reduce the damage caused by a malware infection.

3.6.3 Methods to detect and prevent cyber security threats

Biometric measures
Biometric security uses a person's unique physical features to verify their identity. On mobile devices, this commonly includes fingerprint scanners and facial recognition. Because biometric traits are unique to each person and difficult to copy, they provide a strong level of protection. For example, unlocking a phone with a fingerprint ensures that only the authorised user can access it, even if the phone is lost or stolen.

Password systems
Password systems protect accounts and devices by requiring a user to enter a secret word or phrase. A strong password should be long, include a mix of letters, numbers, and symbols, and avoid easily guessed or common words like "password" or personal information such as a name or birthday. It should also be regularly updated. Systems may also include features like account lockouts after too many failed attempts and the requirement to change passwords regularly.

CAPTCHA (or similar)
CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart". It is used on websites to check that a user is human and not a bot. CAPTCHAs often involve identifying distorted text, selecting images, or ticking a checkbox. They help protect online forms and services from automated attacks, such as bots trying to guess passwords or flood a site with spam.

Using email confirmations to confirm a user's identity
Email confirmation is a method used to check that a user has access to the email account they registered with. When signing up for a service or resetting a password, the system sends a link to the user's email. Clicking the link confirms their identity. This adds a layer of security by making sure only the person with access to the registered email can access the account.

Automatic software updates
Automatic software updates help protect a device by ensuring it always has the latest security fixes. Software companies regularly release updates to patch known vulnerabilities that hackers could exploit. Enabling automatic updates means these patches are installed without the user having to remember or do anything manually, keeping the system more secure over time.