Your notes

GCSE Computer Science: revision notes

Cyber security

Contents

1. Malware
2. Social engineering
3. Other threats
4. Protection
5. Encryption
6. Key terms
7. Quick questions
8. What to do next

Malware

- **Malware** is malicious software. A virus attaches itself to files and spreads when they are shared. A worm spreads by itself across networks. A **trojan** pretends to be useful software.
- **Spyware** secretly records what a user does, such as the passwords they type. Ransomware encrypts a victim's files and demands payment to unlock them.

Social engineering

- Social engineering tricks people into giving away information or access. People are often the weakest point in a system.
- **Phishing**: fake emails or messages that look genuine, asking you to click a link or enter your details. **Blagging** (pretexting): making up a story to persuade someone to hand over information. Shouldering (shoulder surfing): watching someone type a PIN or password. Pharming: redirecting users to a fake website.

Other threats

- A **brute-force attack** tries every possible password until one works. A **denial of service** (DoS) attack floods a server with requests so it can't respond. **SQL injection** types SQL code into an input box to read or change a database. Data interception captures data as it travels across a network.
- Other risks: weak or default passwords, wrongly set access rights, removable media (such as USB sticks carrying **malware**) and unpatched (out-of-date) software.

Protection

- Strong passwords, limits on login attempts, CAPTCHA, two-factor authentication and biometrics (such as fingerprints) protect accounts.

- Anti-**malware** software, **firewalls** (which block unauthorised network traffic), automatic updates, encryption (so intercepted data can't be read), user access levels, physical security and backups protect systems and data.
- **Penetration testing**: authorised experts attack a system to find its weaknesses before criminals do. Input validation helps to stop **SQL injection**. Staff training helps people spot social engineering.

Your notes

Encryption

- Encryption scrambles data with a key, so only someone with the key can read it.
- A simple example is the Caesar cipher, which shifts each letter a set number of places along the alphabet: with a shift of 3, CAT becomes FDW. It is easy to crack, so real systems use much stronger methods.

Key terms

Malware	Malicious software, such as viruses, worms, trojans and spyware.
Trojan	Malware that pretends to be useful software.
Spyware	Malware that secretly records what a user does.
Phishing	Fake messages designed to trick people into giving away their details.
Blagging	Making up a story to persuade someone to hand over information or access.
Brute-force attack	Trying every possible password until one works.
Denial of service	Flooding a server with requests so it can't respond to real users.
SQL injection	Typing SQL code into an input box to access or change a database.
Firewall	Hardware or software that blocks unauthorised network traffic.
Penetration testing	Authorised attacks on a system to find its weaknesses.

Quick questions

Cover the answers and test yourself: remembering is what makes it stick.

1. What is phishing?
2. What is a trojan?
3. What does ransomware do?
4. What is shouldering?
5. What is a brute-force attack?
6. What does a firewall do?

7. How can SQL injection be prevented?
8. What is penetration testing?

Answers

1. Fake messages that trick people into giving away their details
2. Malware disguised as useful software
3. Encrypts files and demands payment
4. Watching someone enter a password or PIN
5. Trying every possible password until one works
6. Blocks unauthorised network traffic
7. By validating input before it is used in a query
8. Authorised attacks on a system to find its weaknesses

What to do next

Practise 14 questions on this topic

Try 5 exam questions, with mark schemes

Read the lesson, one step at a time

Free revision for GCSE and KS3 at lycolearn.co.uk. Some notes are for one exam board only, and say so in brackets.

Your notes