Cyber Security Basics

IGCSE Computer Science Revision Sheet

■ **Big Idea:** Cyber security protects computer systems, networks, and data from attacks, damage, and unauthorised access. Understanding the threats — and how to defend against them — is essential for IGCSE Computer Science.

Common Cyber Threats

■ Malware

What it is:
Malicious software designed to damage, disrupt, or gain unauthorised access to a system. Types include viruses, trojans, ransomware, spyware, and worms.

How it works:
Malware is usually delivered through infected downloads, email attachments, or malicious websites. Once installed, it can delete files, steal data, encrypt files for ransom, or give attackers remote control.

How to protect against it:
- Install and update antivirus software regularly.
- Never download files from untrusted sources.
- Keep the operating system and software updated.
- Use a firewall to block unauthorised connections.

EXAM TIP: Malware = malicious software. Types: virus, trojan, ransomware, spyware, worm. Know the difference between them.

■ Phishing

What it is:
A fraudulent attempt to obtain sensitive information — passwords, bank details, or personal data — by pretending to be a trustworthy source.

How it works:
Attackers send fake emails, texts, or messages that appear to be from banks, companies, or known contacts. They contain links to fake websites that steal login credentials or prompt the user to reveal personal information.

How to protect against it:
- Check the sender's email address carefully.
- Never click suspicious links — go directly to the website.
- Enable two-factor authentication (2FA).
- Use email spam filters.

EXAM TIP: Phishing uses fake messages to steal information. Key word: fraudulent. Always explain HOW it tricks users.

■ Brute Force Attack

What it is:
An automated attack that systematically tries every possible password combination until the correct one is found.

How it works:
Software automatically generates and tests thousands of password combinations per second. Short or simple passwords can be cracked in seconds. Longer, complex passwords take significantly longer — sometimes years.

How to protect against it:
- Use long, complex passwords (12+ characters, mix of letters, numbers, symbols).
- Enable account lockout after a set number of failed attempts.
- Use two-factor authentication (2FA).
- Use a password manager.

EXAM TIP: Brute force = tries every password combination. Defence: long complex passwords + account lockout + 2FA.

www.futurelogiceducation.com
hello@futurelogiceducation.com

■ Social Engineering

What it is:
Manipulating people — rather than systems — into revealing sensitive information or performing actions that compromise security.

How it works:
Attackers exploit human psychology — trust, fear, urgency, or authority — to trick employees or users. Examples include impersonating IT support, pretending to be a manager, or creating a fake emergency to bypass security procedures.

How to protect against it:
• Train staff to verify identities before sharing information.
• Never share passwords over phone or email.
• Follow security policies even under pressure.
• Be suspicious of unexpected requests for access or data.

EXAM TIP: Social engineering targets people, not systems. It exploits trust and human psychology — not technical weaknesses.

Teacher note: Students often confuse social engineering with phishing. Clarify: phishing is a type of social engineering delivered digitally. Social engineering is the broader category — it includes in-person manipulation too.

Ways to Stay Secure

■ **Use strong passwords.**
A strong password uses 12+ characters including uppercase, lowercase, numbers, and symbols. Never reuse passwords across accounts.

■ **Enable two-factor authentication (2FA).**
Even if a password is stolen, 2FA requires a second verification step — usually a code sent to your phone — making unauthorised access much harder.

■ **Keep software updated.**
Software updates patch security vulnerabilities. Unpatched systems are easy targets for attackers who exploit known weaknesses.

- **Avoid suspicious links and downloads.**
  Malware and phishing attacks often arrive via links or attachments. If in doubt, do not click — go directly to the official website instead.

- **Use antivirus software.**
  Antivirus software detects and removes known malware. It should be kept updated so it recognises the latest threats.

- **Use a firewall.**
  A firewall monitors and filters incoming and outgoing network traffic, blocking unauthorised connections and suspicious activity.

- **Use encryption.**
  Encryption converts data into ciphertext so that even if data is intercepted, it cannot be read without the decryption key.

EXAM TIP: Examiners want specific measures, not vague answers. "Use a strong password" earns a mark. "Be careful online" does not.

Teacher note: For each security measure, ask students to explain WHY it works, not just what it is. "2FA is used because even if a password is stolen, access still requires a second verification step."

Threat vs Protection — Quick Reference

Threat	How it works	Key Protection
■ **Malware**	Malicious software installed without consent.	Antivirus software, firewall, software updates.
■ **Phishing**	Fake messages trick users into revealing data.	Check sender details, avoid suspicious links, use 2FA.
■ **Brute Force**	Automated tool tries all password combinations.	Strong passwords, account lockout, 2FA.
■ **Social Engineering**	Manipulates people into giving away sensitive data.	Staff training, verify identities, never share passwords.
■ **SQL Injection**	Malicious SQL code inserted into input fields to access databases.	Input validation, prepared statements, limit database permissions.
■ **DDoS Attack**	Overwhelms a server with traffic to make it unavailable.	Firewalls, traffic filtering, DDoS protection services.

KEY FACT: Cyber security = preventing unauthorised access and protecting data. Know the threat, know the defence.

Teacher note: I've added SQL Injection and DDoS to the reference table as bonus content — both appear regularly at higher mark levels even though they are not always explicitly taught at foundation level.

Quick Check Questions

1.	Define cyber security.
2.	State two types of malware.

3.	Explain how a phishing attack works.
4.	Describe what a brute force attack is and how it can be prevented.
5.	Explain why two-factor authentication is more secure than a password alone.
6.	Give two ways an organisation can protect itself from social engineering.

Answers on the next page →

Answer Guide

1.	Cyber security is the protection of computer systems, networks, and data from attacks, damage, and unauthorised access.
2.	Any two of: virus, trojan, ransomware, spyware, worm, adware.
3.	A phishing attack works by sending fake emails or messages that appear to be from a trusted source. They contain links to fraudulent websites or ask the user to reveal personal information such as passwords or bank details.
4.	A brute force attack uses automated software to systematically try every possible password combination until the correct one is found. It can be prevented by using long, complex passwords, enabling account lockout after repeated failed attempts, and using two-factor authentication.
5.	Two-factor authentication is more secure because even if a password is stolen or guessed, a second verification step is required — usually a code sent to the user's phone — therefore an attacker cannot gain access with the password alone.
6.	Any two of: train staff to verify identities before sharing information; enforce a policy of never sharing passwords; make staff aware of common social engineering tactics; require verification for any access requests.

■ **FutureLogic Summary:** Cyber security protects systems, networks, and data. Key threats: Malware, Phishing, Brute Force, Social Engineering. Key defences: antivirus, firewall, strong passwords, 2FA, encryption, software updates, staff training.