Computer Science – Non Negotiables!

Cyber Security

1) Define **cyber security**
    a. **Cyber security** aims to protect networks, data, programs and computers against damage, cyber-attacks and unauthorised access.
2) Explain cyber security methods
    a. **Encryption** – data is scrambled into a code that can only be accessed by someone with the correct key.
    b. **Anti-malware software** – designed to find and stop malware from damaging a network and the devices on it e.g. Firewalls, anti-virus, anti-spyware etc.
    c. **Automatic software updates** – used to patch (fix) any security issues in software.
    d. **User access levels** – controls which parts of a networks certain users can access so lower level users cannot access potentially sensitive information
    e. **MAC address filtering** – checks the unique identification (MAC address) of each device to ensure only allowed devices connect to the network.
    f. **Authentication –** checks that anyone who is trying to access the network is who they say they are.
        i. **Passwords –** these should be strong to ensure they cannot be guess or cracked
        ii. **Biometric measures** – uses scanners to identify people from a part of their body e.g. fingerprint, retina, facial recognition etc.
        iii. **Email confirmation** – an email is sent to the person registering for them to complete the sign up process. It is used to stop people signing up with a fake email address.
        iv. **CAPTCHA** – prevents programs from automatically doing things such as creating user accounts or attempting multiple log in attempts.
3) Name and describe the 4 **social engineering** techniques
    a. Social engineering is where someone is tricked into giving away their personal details. The four methods are:
        i. **Phishing** – sending emails or texts to people claiming to be from a well-known business. **To avoid,** check for poor spelling and grammar, look at the email address, do not click on links if you are unsure.
        ii. **Pharming –** users are directed to a fake version of a website. This usually happens if malware is installed on your device or server. **To avoid,** always check the web address, check for HTTPS and the padlock next to the web address.

iii. **Shouldering** – this is when someone tries to watch someone entering their personal details such a password or PIN number. **To avoid,** always check who is around you.
iv. **Blagging** – when someone makes up a story to try and persuade the victim into giving away personal details. **To avoid,** never give personal details to anyone unless you can 100% verify who they are and that they are someone you trust.

4) Describe the 4 main types of **malware**
    a. **Viruses (including worms)** – can spread to your computer through files. Some viruses can duplicate themselves and slow down a network. Viruses can be destructive and change, corrupt or delete data. **To avoid,** use anti-malware software and keep it up to date.
    b. **Trojan** – these pretend to be something useful so a user will open a file. This the installs a virus on a device. **To avoid,** never open email attachments from people you do not trust.
    c. **Spyware** – this can keep track of what a user is doing by logging what they are typing or by accessing their webcam. **To avoid,** use anti-malware software and keep it up to date.
    d. **Adware** – this makes unwanted adverts pop up on your screen. This is the only non-threatening type of malware. **To avoid**, always read the terms when downloading software as you can agree to installing adware.
5) **Penetration testing** is a way for an organisation to test whether there are any vulnerabilities in their networks.
    a. The two types of penetration testing are white box and black box penetration
    b. White box penetration mimics an insider who potentially wants to access data. The tester is given basic information such as a username and password. This is testing to see how much damage an employee could do and how much data they can access.
    c. Black box penetration mimics an outsider with no knowledge of the organisation. The tester is given either no prior information or very little information such as an IP address. This is testing to see if an outsider can access a network, and if they can, how much damage they can do.