Level 1/2 Vocational

ICT

1.3.1 Risks to information held on computers

Accidental damage

- **System failure:** Mechanical damage, natural disasters (fire or flood) or unexpected power cuts can lead to data loss or damage.
- **Data corruption:** Interruptions to power or software errors can change stored data or program code from its normal state.
- **Human error:** Mistakes such as spilling liquids on hardware, accidentally deleting files or overwriting important data can cause significant problems.

Unintended disclosure by incorrectly assigned access levels

Organisations use access levels to control which parts of a computer system various staff can access and which functions they can use. If a staff member is given the wrong level of access, they may be able to view or modify confidential information, leading to unauthorised disclosure.

Hacking

Unauthorised access to a computer system is referred to as hacking.

- **Black hat hackers:** Individuals who access systems with malicious intent. They might steal data (for example bank details), manipulate information (for example prices or wages) or hold data hostage using ransomware.
- **White hat hackers:** Also known as ethical hackers or penetration testers. These are security experts hired by companies to legally hack their systems to identify and fix weaknesses.
- **Grey hat hackers:** Individuals who access systems without permission, but generally without malicious intent. They may inform organisations of vulnerabilities they find, sometimes expecting a fee for their discovery.

Malicious software

Malicious software, or malware as it is commonly known, is created with the intention of causing harm to a computer system.

- **Viruses:** Programs that replicate themselves on a system by modifying existing software and inserting their own code. They can enter a system through vulnerabilities or by clicking on malicious links.
- **Worms:** A type of virus that infect computers without user knowledge. Worms replicate themselves, consume system resources (slowing performance), and can modify or delete files, or steal data.
- **Trojan Horses (Trojans):** Programs that enter the system disguised as legitimate software. They create a 'backdoor' allowing attackers to control the infected device (a 'zombie computer') in order to steal data or spread more malware.
- **Spyware:** Software that secretly collects data (e.g. login and account details) from a computer system and sends it to a third party without the user's consent.
- **Keylogging:** A form of spyware that records every keystroke typed on a keyboard, allowing cybercriminals to steal passwords and other sensitive information.
- **Ransomware:** Malware that encrypts a user's files, preventing access to them. Cybercriminals then demand a ransom payment in exchange for the decryption key.
- **Distributed Denial of Service (DDoS):** An attack designed to disrupt an organisation's services. The server is overwhelmed with a flood of fake internet requests, causing it to slow down and eventually crash the website or service.

Social engineering

Methods used to trick people into revealing confidential information or performing actions for fraudulent reasons.

- **Phishing:** Fraudulent emails or messages that appear to come from a trustworthy source (for example, a bank). They trick users into clicking malicious links or providing sensitive information. Indicators of phishing include misspellings, email addresses not associated with the legitimate organisation, or hyperlinks that do not lead to the official website.
- **Baiting:** Tempts individuals with an attractive offer (for example, a competition win or a free USB drive found) to entice them into a scam, often leading to the installation of malware.

Emerging threats

As our reliance on the internet and technology grows, new cyber threats constantly emerge. Cybercriminals develop new ways to exploit vulnerabilities, such as ransomware attacks targeting remote workers or new threats related to cryptocurrency.