# Knowledge Organiser: Computer Crime and Cyber Security - Year 8 Computer Science

## Overview

Understanding computer crime and cyber security is essential in today’s digital world. This knowledge organiser explores key topics and concepts that help promote safe and responsible technology use. Each topic will include key knowledge and an activity for you to practice.

## 1. Cyber Crimes

### 1.1 Common Cyber Crimes

* **Definition**: Unauthorised activities conducted via the internet.
* **Examples**:
	+ **Hacking**: Gaining unauthorised access to systems or networks.
	+ **Identity Theft**: Illegally obtaining and using someone else's personal information.
	+ **Online Fraud**: Misleading individuals to gain financial or personal information.
	+ **Cyberbullying**: Using digital platforms to harass or intimidate someone.

### 1.2 Phishing and Spear Phishing

* **Phishing**: A method where cybercriminals trick individuals into revealing personal information by pretending to be a trustworthy source.

**Example**: An email reads, “Dear customer, your account has been compromised. Click here to secure it immediately!” with a suspicious link.

* **Spear Phishing**: A more targeted form of phishing, directing attacks at specific individuals or organisations.
	+ **Example**: An email to a company employee appears to come from the CEO asking for sensitive data.

### Cyber Crimes Activity:

Identify errors in this phishing example: “Dear user, urgent action required! Please confirm your password immediately to avoid suspension or click this link to reset your details: [fakeurl.com].”

## 2. Malware

### 2.1 Types of Malware

* **Worms**: Software that can make copies of itself and spread across networks.
* **Viruses**: Harmful software that can corrupt or delete data on a computer - needs something to start spreading, like an infected file.
* **Trojans**: Seems useful but secretly harms your system or steals information.
* **Adware**: Shows unwanted ads and can slow down your computer.
* **Spyware**: Gathers your information without you knowing and can invade your privacy.

### 2.2 Malware Attacks

* **DDoS (Distributed Denial of Service)**: Attackers overwhelm a server or network with too much traffic, making it crash.
* **Ransomware**: Locks files on your computer and demands money to unlock them.

### Malware Activity:

Research a recent malware attack (such as a ransomware attack) and write a summary including the impact and recovery measures taken. Examples could include the WannaCry attack [WannaCry ransomware cyber-attack: Your questions answered - BBC News](https://www.bbc.co.uk/news/technology-39926855) [Cyber-attack: US and UK blame North Korea for WannaCry - BBC News](https://www.bbc.co.uk/news/world-us-canada-42407488#:~:text=The%20US%20and%20UK%20governments%20have%20said%20North,150%20nations%2C%20causing%20billions%20of%20dollars%20of%20damage.) or the Fylde Coast Academy Trust attack: [Global hacker holds Blackpool schools to ransom, demands £1.2million](https://www.lep.co.uk/news/crime/global-hacker-holds-blackpool-schools-to-ransom-demands-ps12million-4857321)

## 3. Protection Against Malware

### 3.1 Anti-Viruses and Firewalls

* **Anti-Virus**: Software designed to find and remove viruses and malware from your computer.
	+ **Features**: Requires regular updates, offers real-time protection, and has scheduled scanning options.
* **Firewall**: Controls the traffic to and from your computer, keeping out viruses and unwanted access.
	+ **Types**: Can be software-based (program) or hardware-based (physical device).

### Protection Activity:

Explain different methods to stay protected from malware, including how we can use software or change our own behaviour to ensure our devices are secure. Hint: Think how you protect your phone or laptop from other people and what you would do if it became infected.

## 4. Data Theft and Legal Framework

### 4.1 Computer Misuse Act

* **Overview**: Introduced in 1990 to address unauthorised access to computer systems, including hacking.
* **Parts of the Law**:
	+ **Unauthorized Access to Computer Material**
	+ **Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offence**
	+ **Unauthorized Modification of Computer Material**
	+ **Unauthorized Acts with Intent to Impair or Access Data**
* **Penalties**:
	+ **Unauthorized Access**: Maximum fine of £5,000 / 6 months imprisonment
	+ **Unauthorized Access with Intent**: Maximum fine of £5,000 / 5 years imprisonment
	+ **Unauthorized Modification**: Maximum fine of £5,000 / 5 years imprisonment
	+ **Unauthorized Acts**: Maximum fine of £5,000 / 10 years imprisonment

### 4.2 Online Safety Act 2023-24

* **Overview**: Legislation aimed at enhancing protection for users, particularly children, on digital platforms by mandating online safety measures from technology companies.
* **Key Parts of the Law**:
	+ Regulations against fake news and misinformation.
	+ Increased child protection measures on social media platforms.
	+ Parental controls and reporting mechanisms for harmful content.
	+ Strict guidelines for handling user data to ensure privacy.

### Computer Misuse Activity:

Read the following scenarios and identify if a law was broken under the Computer Misuse Act and what the potential penalty would be:

1. An employee accesses a work colleague’s email without permission.
2. A student hacks into the school system to change their grades.
3. A person installs software on a public computer that captures users’ personal data.
4. A coder creates a virus that intentionally deletes files from another user's computer.
5. A group runs a phishing website resembling a popular service to collect users’ logins.
6. A hacker accesses a secured government database to showcase its vulnerabilities.

## 5. Types of Hackers

### 5.1 Hacker Categories

* **White Hat Hackers**: Ethical hackers who test and improve security systems, working with organisations to find weaknesses.
* **Black Hat Hackers**: Cybercriminals who exploit systems for personal gain by stealing information or committing fraud.
* **Grey Hat Hackers**: Operate in between ethical boundaries; they may find security weaknesses without permission but usually without harmful intentions.

### Hacking Activity:

Write a short paragraph explaining the reasons behind the actions of black and grey hat hackers, considering factors like financial gain or ethical dilemmas.

Explain why we need white hat hackers and how they help companies protect systems.

### Additional Activity:

Read the following scenarios and identify which type of hacker (black hat, white hat, or grey hat) corresponds with each situation:

1. A hacker finds a vulnerability in a company's software and reports it to them.
2. A group of individuals gains unauthorized access to a bank's system to steal money and personal data.
3. A person explores a public website, discovering security flaws without permission and showcasing them to the public to raise awareness.

## 6. Ethics in Computing

### 6.1 Defensive Design

* **Definition**: The practice of designing systems with potential misuse in mind to keep users safe.
* **Examples in Software**:
	+ Requiring logins to enhance security before users can access certain functions.
	+ Only allowing the user to upload certain file types.
	+ Only allowing a user to log into 1 account at a time.
* **Examples in Games:**
	+ Guiding players through environments with clear instructions to improve their experience.
	+ Locking buttons during important cutscenes to prevent players from interrupting.

### Defensive Design Activity:

Brainstorm features that could be added to a popular game to enhance security, considering user interactions and potential weaknesses.

## 7. Testing Software

### 7.1 Whitebox and Blackbox Testing

* **Whitebox Testing**: Involves testing a program by looking at its internal workings; testers know how the code works.
* **Blackbox Testing**: Involves testing a program by checking its inputs and outputs without knowing how it operates inside.

### 7.2 Beta Testing

* **Definition**: A phase in software development where a limited number of people are invited to try out a game before its official release.
* **Purpose**: To find bugs and issues that the developers may not have anticipated.
* **Example**: Games often have hundreds or thousands of beta testers who provide feedback and report problems to improve the final product.

### Software Testing Activity:

Create a simple table listing the differences between Whitebox and Blackbox testing, including what you think each method would checks and the benefits of checking this.

## 8. Copyright and Licensing

### 8.1 Copyright Laws

* **Duration**: Copyright usually lasts for 70 years after the creator's death, after which the work can be freely used by anyone.
* **Impact**: Protects the rights of creators, preventing others from using their work without permission.
* **Consequences**: Can lead to fines and penalties for those who infringe on copyright.

### 8.2 Types of Licenses

* **Public Domain**: Works that are free for anyone to use without permission.
* **Creative Commons**: Allows creators to specify how their work can be used and shared according to their preferences.
* **Permission from Creator**: Official agreement allowing use of copyrighted material.
* **Fair Use**: Limited use of copyrighted content for education or critique without needing permission.

### Copyright Activity:

Research a piece of artwork, music, or software and identify what kind of copyright or licensing applies to it.

Example: What sort of copyright licensing applies to Taylor Swifts albums? Why?

## 9. Software Licensing

### 9.1 License Types

* **Single User License**: Allows one person to use the software.
* **Multiple User License**: Covers several users, allowing teams to work together using the same software.
* **Site License**: A type of license that allows software to be used on all computers in a specific location, like a school or office.

### Licensing Activity:

Compile a list of different software products that you use at home and school; consider things like Computer Games or Microsoft Word, Powerpoint. Think of how a school with many Computer Rooms, how does this impact our licensing type?

## 10. E-Waste and Environmental Impact

### 10.1 E-Waste

* **Definition**: Electronic devices that are no longer wanted, which can pollute the environment when not disposed of properly.
* **Impact**: Dangerous materials like lead and mercury from the circuits in e-waste can leak into the environment, harming plants, animals, and humans. Recycling electronics is crucial to protect the planet.

### E-Waste Activity:

Create a poster that educates others about e-waste, its effects on the environment, and ways to recycle and reduce electronic waste.

## 11. Health and Safety Regulations

### 11.1 Computer Usage Risks

* **Eye Strain**: Spending too long looking at screens can lead to discomfort and headaches.
* **RSI (Repetitive Strain Injury)**: Can result from doing the same actions repeatedly, like typing. Good posture and ergonomic equipment can help prevent this.
* **Back Problems**: Prolonged periods of sitting without proper posture can lead to chronic back issues.

### 11.2 Employer Regulations

* Employers must ensure a safe working environment, including providing comfortable workspaces and promoting healthy screen time habits.

### Health and Safety Activity:

Research and write a short report on best practices for maintaining eye health while using computers, including screen breaks and proper lighting.