15. COMPUTER MISUSE

15.1 THE PROBLEM

- Public/media attention is higher on **internet misuse** than general computer misuse.
- **Computer crimes** are a subset of **white-collar crime**, requiring dedicated legislation.
- Before 1990, hacking (unauthorised access) was **not an offence**:
    - Attempts to prosecute by stealing electricity were impractical.
    - Convictions were rare and penalties trivial.
- **Court of Appeal (1988):** upheld appeal of two hackers → triggered quick legislative action.
- **Computer Misuse Act (CMA, 1990):** first legislation to criminalize hacking.
- **Internet and web growth (1990s):** exposed new issues like **Denial-of-Service (DoS) attacks**.
- **Police and Justice Act (PJA, 2006):** amended CMA to address new forms of misuse.
- CMA **does not cover computer fraud**; more general legislation deals with that.

15.2 THE COMPUTER MISUSE ACT 1990 (CMA)

Three main offences under CMA:

1. **Unauthorised access to a computer**
2. **Unauthorised access with intent to commit a serious crime**
3. **Unauthorised modification of computer contents**

Jurisdiction:

- Offences apply if **either the computer or the offender is in the UK**, even if the hacker is overseas.

Section 1: Unauthorised Access

- Definition:
    1. Causes a computer to perform any function to access data/program.
    2. Access is **unauthorised**.
    3. Offender **knows** the access is unauthorised.
- **Key points:**
    - Offence is **intentional**, not accidental.
    - Accessing **unauthorised programs/data**, even if partially authorised, is illegal.
    - **No harm required**; attempting unauthorised access is enough.
- **Penalty:**
    - Originally: fine up to £5,000 or 6 months imprisonment.
    - PJA (2006) increased prison sentence **up to 2 years**.

Section 2: Unauthorised Access with Intent to Commit Further Offence

- Covers **intent to commit a more serious crime** after gaining access.
- Examples:
    - Blackmail using sensitive medical records.
    - Terrorist interference in air traffic control systems.
- **Purpose:**
    - Allows prosecution **before the serious crime is committed**, based on intent.
- **Penalty:**
    - Up to **5 years imprisonment** or **unlimited fine**.

Section 3: Unauthorised Modification of Contents

- Definition:
    1. Any act causing **unauthorised modification** of a computer.
    2. Act performed with **requisite intent and knowledge**.
- **Requisite intent:**
    - To modify contents to:
        1. Impair **operation of a computer**
        2. Prevent/hinder **access to programs or data**
        3. Impair operation of programs or **reliability of data**
- **No specific target required**; intent alone is enough.
- **Examples of offences:**
    - Spreading **viruses, worms, malware**
    - Encrypting company files for **ransom** (ransomware)
    - Concealed **browser redirection**
    - Installing **premium-rate diallers**
- **Penalty:**
    - Originally up to **5 years imprisonment and/or unlimited fine**
    - PJA (2006) increased penalties further

Key Notes on CMA

- CMA is **focused on unauthorised access and modification**, not all computer-related crimes.
- Covers both **attempts and completed offences**.
- **Intent is crucial**; accidental actions are not offences.
- PJA amendments **strengthened CMA** to address modern internet-based threats.

15.5 COMPUTER FRAUD

1. Definition

- **Computer fraud** is the dishonest manipulation of computer systems to:
  - Obtain money, property, or services.
  - Cause financial or other loss.
- Essentially, it applies traditional fraudulent techniques using digital means.

2. Techniques

- Many methods predate computers but have been adapted to technology:
  - **Fictitious employees:** Adding fake staff to payroll systems to siphon funds.
  - **Fake supplier accounts:** Creating bogus suppliers and issuing false invoices.
  - **Spurious invoices:** Using the system to approve fake bills and divert payments.
- **Impact of computers:**
  - Larger-scale fraud becomes possible.
  - Systems are trusted by many, so errors or manipulation are less likely to be questioned.
  - Detection can be more difficult because evidence is digital and not always obvious.

3. Evidence Handling

- Digital evidence is **sensitive and complex**:
  - Requires specialists to collect and preserve properly.
  - Mishandling evidence can lead to wrongful convictions or cases collapsing.
- **Risk:** Blind reliance on computer outputs is dangerous.
  - Errors in software or systems can falsely indicate fraud.