- unauthorised access/hacking (black hat) = ________

- malware (virus, worms, botnet, rootkit, Trojan, ransomware, spyware) = ________________________

- denial of service attacks = ________________________

- phishing (emails, texts, phone calls) = ____________

- Pharming = ________________________________

- social engineering = ___________________________

- shoulder surfing = _____________________________

- 'man-in-the-middle' attacks. = _________________

Impact of security breach

SECURITY BREACH

- ⇒ data loss
- ⇒ damage to public image
- ⇒ financial loss
- ⇒ reduction in productivity
- ⇒ Downtime
- ⇒ legal action

Learning Aim B1 Threats to Data B3 Policy

External Threats = Outside the organisation
Internal Threats = Inside the organisation

Security Policies

Defining responsibilities

Defining security parameters

Disaster recovery policy

Actions to take after an attack

Why systems are attacked

- •fun/c____________________
- •industrial e________________
- •financial g_______
- •personal a___________
- •disruption
- •data/information t________

- unintentional disclosure of data = _______________

- intentional stealing or leaking of information = ____

- users overriding security controls = ______________

- use of portable storage devices = ________________

- downloads from internet = ______________________

- visiting untrustworthy websites = ________________

User access restrictions

Physical security measures (locks)

Passwords

Using correct settings and levels of permitted access

Biometrics

Two-factor authentication (who you are, what you know, what you have).

Explain in the box what each restriction is and how it helps protect data

Procedures for backing up and recovering data

Learning Aim B2 Prevention and management of threats to data

Finding weaknesses

- ethical hacking (white hat, grey hat)
- penetration testing
- analyse system data/behaviours to identify potential risks

and improving system security

Encryption of transmitted data

Firewall (hardware and software)

Software/interface design (obscuring data entry, autocomplete, 'stay logged in'

Anti-virus software

Device hardening

Data level protection

Explain in the box what each protection is and how it helps protect data