

◆ 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

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



## security breach

### Learning Aim B1 Threats to Data B3 Policy

External

Internal

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

- fun/c \_\_\_\_\_
- industrial e \_\_\_\_\_
- financial g \_\_\_\_\_
- personal a \_\_\_\_\_
- disruption
- data/information t \_\_\_\_\_

are attacked

◆ unintentional disclosure of data = \_\_\_\_\_

◆ intentional stealing or leaking of information = \_\_\_\_\_

◆ users overriding security controls = \_\_\_\_\_

◆ use of portable storage devices = \_\_\_\_\_

◆ downloads from internet = \_\_\_\_\_

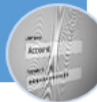
◆ visiting untrustworthy websites = \_\_\_\_\_

# 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