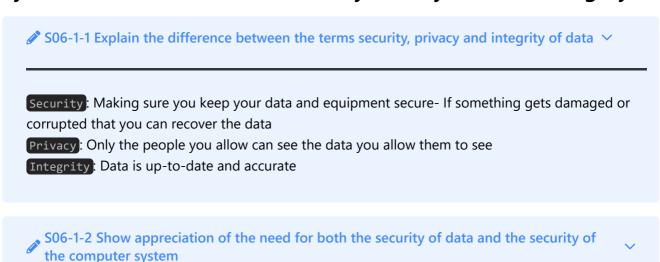
## **Section 06.1 - Data Security**

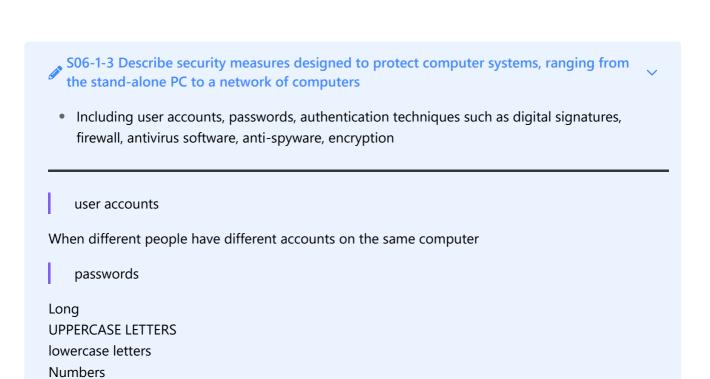
## **Layer 7: Application**

## Syllabus Content Section 06: Security, Privacy and Data Integrity



make sure your data is secure-

- 4 Main things to secure your data:
  - Data backup
  - Disk mirroring
  - Encryption
  - Authorisation



Punctuation symbols (! @ £ \$ % ^ & \* ( ) : , . / " | ) Memorable

authentication techniques such as digital signatures

Remember when we said if Alice uses her private key to encrypt data, then it sucks for making sure the data is secret but its good for knowing the message came from Alice.

 Authorisation: Making sure your data is only accessed by those who you allow User Accounts

Passwords

**Access Rights** 

Read Only files

Digital Signature

firewall

Two types
Software firewall

Hardware firewall

All it does it checks where you are sending data to and who is trying to connect to you It does this by either blocking individual programs or by blocking ports

firewall can control:

- What ports are used if you want to send data
- · What ports are used to receive data
- What programs are fully blocked and cannot send anything.

antivirus software

This checks your computer for malware and removes it or quarantine it Malware = Malicious Software

There are two main types of malware

- 1. Virus
- 2. Spyware

But sometimes, people just use the word malware to describe everything. There are three main ways you can get malware

- 1. Phishing: Fake email sending you to a fake website
- 2. Smishing: Fake SMS text sending you to a fake website
- 3. Pharming: You do everything right and still go to a fake website

anti-spyware

Possibly special-purpose anti-spyware soft ware might be installed. Another option is to install an intrusion detection system that will take as input an audit record of system use and look for examples that do not match expected system activity.

encryption

Symmetric key encryption: one private key is held by both sender and receiver and is used for both encryption and decryption

- Benifit
  - Simple
  - Quick
- Drawback
  - You have to share your key
  - If someone gets your key then they can read everything

Asymmetric key encryption: there is a public key and a private key one of which is used for encryption and the other for decryption

- Benifit
  - Key distribution not necessary
  - Exchange of private keys not necessary
  - Digital signature/message authentication
- Drawback
  - slower because of its longer key lengths
  - not to mention that asymmetric encryption calculations tend to be much more complex than their symmetric counterparts.



 $\nearrow$  S06-1-5 Describe methods that can be used to restrict the risks posed by threats  $\lor$