Protecting Data Techniques

With the impact of the threats like malware and hackers being so significant, it's important that we put things in place to protect ourselves from them.

The best way to protect your data is through implementing simple processes in the use and administration of IT systems. If these are followed then it is unlikely that much harm will befall your data.

	Explanation
File Permissions	File permission means that you can set who can access files and what they can do with them. There are three main file permission types: read-only, read/write and full control.
Access Levels	Access levels control what software, data and services a user can access. The highest level is administrator access.
Backup & Recovery Procedures	Backups involve taking a copy of the data and storing it in a secondary location. This is normally in a different building, called a remote backup. There are three main types of backup: full, incremental & differential.
Passwords	Having a good password is particularly important for protection from hackers. However, choosing a simple password is little protection as a hacker can crack simple passwords in seconds. Guidelines for good password security say that your password should be: • At least 10 characters in length. • Containing uppercase letters, lowercase letters, numbers & symbols.
Physical Access Controls	Physical access controls prevent unauthorised users from gaining access to our IT systems. Examples of physical access controls include access cards, keypad access control, biometric access control & electronic locks.
Digital Certificates	Digital certificates are used to authenticate a user as the owner of a public key so they can use public key encryption. Two key parts of a digital certificate are the signature and the public key.
Protocols	Protocols are a set of rules that defines a method for transmitting data between different devices over a network. Security protocols that are used include SSL and TLS. These allow us to send data securely over the internet using encryption.

Protecting Data Tools

There are a variety of tools we use to protect ourselves from security threats. These, along with the legislation & codes of practice are fundamental in protecting our IT systems.

	Explanation	Implications
Anti-Virus	Is a utility program that is used to prevent malicious software from infecting your computer or detect and remove malicious software that has already infected your computer.	It must be regularly maintained and updated, it doesn't offer complete protection and it can slow performance.
Firewalls	Either a hardware device or a utility program that monitors incoming and outgoing network traffic and blocks any traffic that it deems suspicious.	It can diminish network performance, impair productivity and cannot prevent internal attacks.
Encryption	Is where data is converted into an encoded form so as to prevent unauthorised access. Stored data use symmetric encryption. This uses the same key to both encrypt and decrypt the data. Data during transmission uses asymmetric encryption. This uses different keys to encrypt and decrypt the data.	If you lost the encryption key you cannot recover the data and the sharing of the encryption key can compromise security so it is no use for encrypting data during transmission. An implication of asymmetric encryption is that it can affect the performance of your device during encryption/decryption.
Legislation & Codes of Practice	Legislation has been implemented to protect data and IT systems. These include the Data Protection Act & the Computer Misuse Act. Professional bodies and the Information Commissioner's Office produce codes of practice that are guidelines to help ensure businesses follow best practice and comply with relevant laws.	None.

Pearson BTEC **Level 3 National Extended Certificate in Information Technology**

Unit 1: Information Technology Systems
B Transmitting data
D2 Protecting data

Protecting Data Techniques

With the impact of the threats like malware and hackers being so significant, it's important that we put things in place to protect ourselves from them.

The best way to protect your data is through implementing simple processes in the use and administration of IT systems. If these are followed then it is unlikely that much harm will befall your data.

	Explanation
File Permissions	
Access Levels	
Backup & Recovery Procedures	
Passwords	
Physical Access Controls	
Digital Certificates	
Protocols	

Protecting Data Tools

There are a variety of tools we use to protect ourselves from security threats. These, along with the legislation & codes of practice are fundamental in protecting our IT systems.

	Explanation	Implications
Anti-Virus		
Firewalls		
Encryption		
Legislation & Codes of Practice		