Foxford Learning Plan

YEAR 11

DIT – COMP 3 – Learning Aim B

Cyber Security -Threats to data: Internal Threats to Digital Systems and Data Security

Summer1

Key Vocabulary	
Intellectual Property	An idea that you invented that belongs to you, for example, an image that is copyrighted.
Ransomware	A malicious form of software that is transferred to, and then executed on, a user's machine to damage or disrupt the system or allow unauthorised access to data
Malware	A form of malware, usually infecting unprotected digital systems, occurring when users open malicious email attachments
Denial-of-Service (DoS) attacks	Attack a remote computer by making it unable to respond to legitimate user requests.
Cybersecurity	The combination of policies, procedures, technologies and the actions of individuals to protect from both internal and external threats.
Social Engineering	The act of getting users to share sensitive information through a false pretext (commonly known as 'blagging')
Phishing	A cyberattack that sends spam messages to try and trick people to reply with desired information.
Pharming	A cyberattack that uses malware to direct a user to a fake website that requests information
Network infrastructure	It is a set of physical devices and components that comprise a computer network.
Obscuring data entry	Common technique to solve shoulder surfing when using secure logins in a public place is to obscure the entry of sensitive data e.g. passwords.
Security patches	Additional settings or program codes that fix vulnerabilities in applications, operating systems and device firmware, and are usually downloaded from the manufacturer.
Data Protection Controller	The named person in an organisation who takes responsibility for the safety and security of the organisation's data.
Data Subject	An individual whose personal data is being stored.

Key Skills

Over the course of the topic, I will be able to: -

- Explain why hackers hack the system
- Describe different types of hackers
- Discuss the benefits of securing personal information
- Know the laws that protect individual, organisation and social medial
- Analyse how to choose the right communication technologies
- How to prevent internal and external attack
- Provide advice on prevention and management of threats to data





I will Understand

1. Reasons why systems are attacked
2. How to prevent internal and external attack
3. How technologies have change life of individual and organisations
4. The benefits of securing personal information
5. Prevention and Management of Threats to Data
6. A variety of validation methods and when it is best to apply them
7. The benefits of anti-virus software