Athena
Sixth Form College

DOWNHAM MARKET
ACADEMY

Keywords: Year 10 Computer Science

Topic Title: Network Security and System Software

Introduction to the topic: Understanding of network threats, how to prevent vulnerabilities, Operating Systems and System Software.

Keyword	Definition
Malware	Malicious software. A program designed to cause damage to computer systems, corrupt or change files, steal data, or cause disruption to services.
Phishing	An attack in which the victim receives a message disguised to look like it has come from a reputable source (for example, a bank), in order to trick them into giving up personal information.
Social engineering	Techniques used to trick users into giving away personal information by psychological manipulation.
Brute force attacks	A method of systematically trying all possibilities to find secret information (eg a password or encryption key).
Denial of service attacks	A malicious attempt to overwhelm a server by bombarding it with requests. In a distributed attack, the requests come from a large number of distributed computer systems, typically a botnet.
Data interception and theft	Gaining confidential information by using malicious means, can be digital or physical interception or theft.
SQL injection	Structured Query Language. A declarative language designed for managing data held in a relational database management system. SQL injection is the insertion of malicious SQL code into web forms designed to corrupt, disable websites or spread viruses in addition to stealing information such as credit card numbers, passwords or other sensitive data.
Penetration testing	A method of testing used to discover weaknesses or vulnerabilities in a system that could be exploited by hackers.
Anti-malware software	Software that is used to detect and remove malware.
Firewalls	A system that filters network traffic to protect against unauthorised flows of data in or out of the network.
User access levels	Levels of security on a network – what files, folders and settings a user has access to.

Encryption	The process of applying an encryption algorithm to plaintext to produce cypher text that cannot be understood (without decryption).
Physical security	Physical security measures such as locked door or biometric security
Operating system	System software that manages hardware, software, and resources, and provides services for other software. It will also usually provide an interface for the end user.
Encryption	The process of applying an encryption algorithm to plaintext to produce cypher text that cannot be understood (without decryption).
Defragmentation software	The process of organising file blocks stored on a disk by grouping them into adjacent sectors.
Data compression software	The process of reducing file size by applying a compression algorithm.