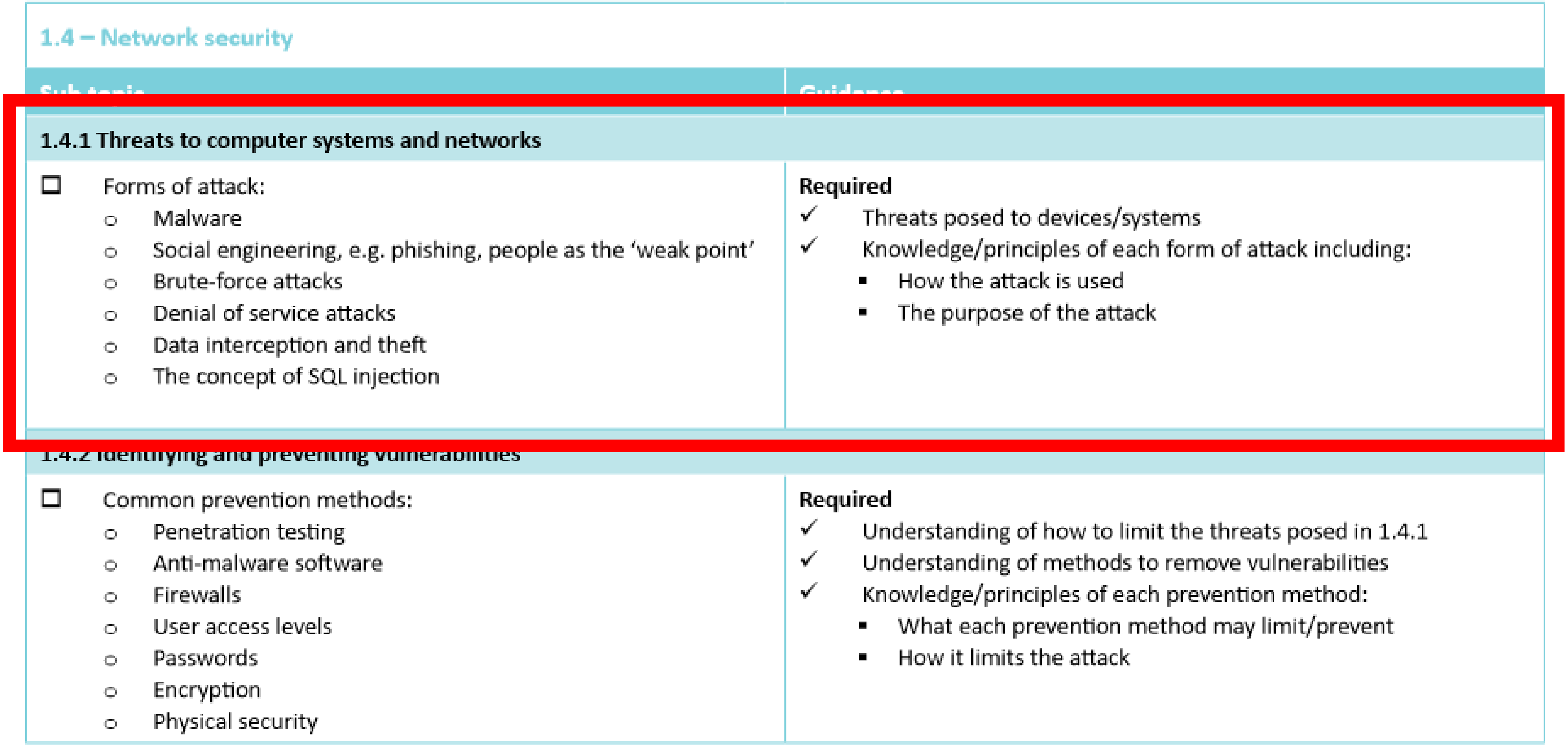
J277 - 1.4 Network Security

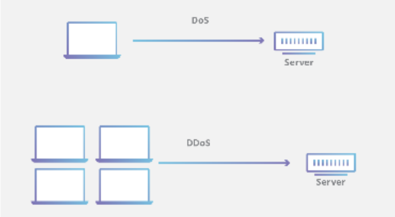
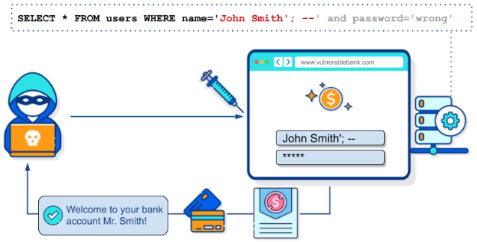


1.4 – Network security

Sub-topic	Guidance
1.4.1 Threats to computer systems and networks	
□ Forms of attack: ○ Malware ○ Social engineering, e.g. phishing, people as the 'weak point' ○ Brute-force attacks ○ Denial of service attacks ○ Data interception and theft ○ The concept of SQL injection	**Required** ✓ Threats posed to devices/systems ✓ Knowledge/principles of each form of attack including: ▪ How the attack is used ▪ The purpose of the attack
1.4.2 Identifying and preventing vulnerabilities	
□ Common prevention methods: ○ Penetration testing ○ Anti-malware software ○ Firewalls ○ User access levels ○ Passwords ○ Encryption ○ Physical security	**Required** ✓ Understanding of how to limit the threats posed in 1.4.1 ✓ Understanding of methods to remove vulnerabilities ✓ Knowledge/principles of each prevention method: ▪ What each prevention method may limit/prevent ▪ How it limits the attack

J277 - 1.4 Network Security

Forms of Attack

	Attack	How it works
	Data interception and theft	Data theft refers to any way sensitive information is compromised, whereas data interception is a specific type of data theft, referring to information that is captured during transmission.
strongdm 0 0 0 0 1 0 0 0 0 2 9 9 9 9 8 9 9 9 9 9 1 2 3 4 5	**Brute- force attack**	A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.
	**Denial of service (DoS)**	These attacks are characterised by an explicit attempt by attackers to prevent legitimate use of a service by flooding it with useless traffic/requests.
 `SELECT * FROM users WHERE name='John Smith'; --' and password='wrong'` John Smith'; -- ***** Welcome to your bank account Mr. Smith!	**SQL Injection**	SQL injection is the placement of malicious code in SQL statements, via web page input

J277 - 1.4 Network Security

Malware

Software designed to damage or disrupt a device or network.

Spyware – Monitors user actions and sends info to the tracker.

Scareware – Tricks users into paying to fix fake problems.

Ransomware - Encrypts files. User pays for decryption key.

Viruses – Attached to other files. Only run or replicate when the file is opened.

Worms – Similar to viruses but self-replicate so spread quickly.

Trojans – Malware disguised as legitimate software. Do not replicate themselves.

Social Engineering

To gain access to networks or sensitive information by using people as a system's weak point.

Telephone –

A person is called by someone pretending to be a friend, colleague or company and is persuaded to disclose confidential information.

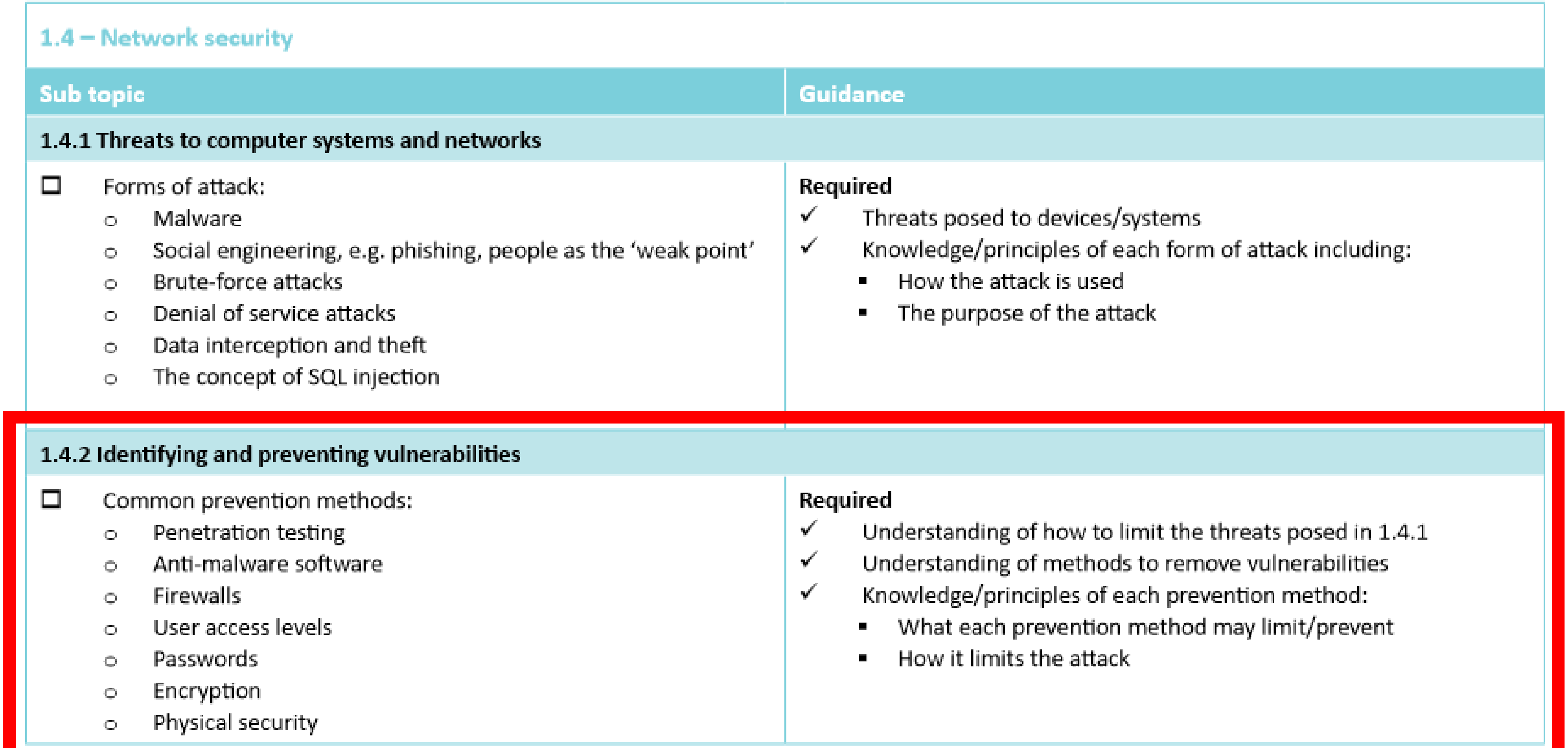
Phishing –

Criminals send emails pretending to be well-known businesses. They contain links to fake website that ask users to update their personal information, which the criminals steal.

People as the weak point –

- Not installing operating system updates.
- not keeping anti-malware up-to-date.
- Not locking doors to server/computer rooms & logging off.
- Leaving printouts with sensitive information lying around.
- Writing passwords down on sticky notes attached to computers.
- Sharing passwords.
- Using easy to guess passwords.
- Not encrypting data on portable media.
- Not having well understood, or poor network policies.
- Not training staff to protect themselves against phishing attacks.

J277 - 1.4 Network Security



1.4 – Network security

Sub topic	Guidance
1.4.1 Threats to computer systems and networks	
□ Forms of attack: ○ Malware ○ Social engineering, e.g. phishing, people as the 'weak point' ○ Brute-force attacks ○ Denial of service attacks ○ Data interception and theft ○ The concept of SQL injection	**Required** ✓ Threats posed to devices/systems ✓ Knowledge/principles of each form of attack including: ▪ How the attack is used ▪ The purpose of the attack
1.4.2 Identifying and preventing vulnerabilities	
□ Common prevention methods: ○ Penetration testing ○ Anti-malware software ○ Firewalls ○ User access levels ○ Passwords ○ Encryption ○ Physical security	**Required** ✓ Understanding of how to limit the threats posed in 1.4.1 ✓ Understanding of methods to remove vulnerabilities ✓ Knowledge/principles of each prevention method: ▪ What each prevention method may limit/prevent ▪ How it limits the attack

J277 - 1.4 Network Security

Network Security Measures

Penetration Testing

Tests performed under a controlled environment by a qualified person.

Checks for current vulnerabilities and explores potential ones in order to expose weaknesses in the system so they cannot be maliciously exploited.

Anti-Malware software

Software with the aim of preventing malware from entering the system.

Examples include viruses, worms and Trojan horses.

Firewalls

Software that performs a ‘barrier’ between a potential attacker and the computer system by examining all the data entering and leaving a network.

Identify threats using a set of security rules, blocking unauthorised access.

User Access Levels

Allows a system administrator to set up a hierarchy of users. Lower level users would have access to limited information and settings.

Higher level users can access the most sensitive data on the system.

J277 - 1.4 Network Security

Network Security Measures

Passwords

A string of characters used to gain access to a service or system, and prevent unauthorised access.

They should be strong and changed regularly to protect against brute-force attacks.

Encryption

Where data is translated into code so that only authorised users, or users with the key can
decrypt it.

Users must need the key in order to decrypt the coded file.

Physical Security

Physical security is used to prevent physical access to devices, and to prevent theft.

Steps may include:

door locks
window locks or bars
intruder alarm systems
CCTV systems
laptop locks security guards