Topic Lesson Plans

Topic: Security

Each Topic starts with an introduction, designed to help introduce the content and encourage students to start to explore more about the topic.

There then follows a Topic Lesson Plan. Topic Lesson Plans are designed to be used by you to deliver the teaching and learning for the topic. Collectively, they should form a small scheme of work with a selection of student activities to bring the topic to life.

Each Topic Lesson Plan includes 3 or 4 activities that are designed to support the learning of the topic to your students, enabling them to develop the Knowledge, Understanding and Skills and provide an opportunity for formative assessment.

The Topic Lesson Plans should be used in conjunction with the following documents:

- Security Introduction PowerPoint
- Security Industry Links
- Links to Assessment

Introduction to the Topic: Security
Computer security is often associated with three core areas; confidentiality, integrity and availability. Every computer is vulnerable to a wide range of security threats, and new threats are emerging all the time. Computers must be protected using a variety of methods to keep them as secure as possible. This unit will examine why information and data are so important, and the implication of a data breach. A cyberattack is any attempt to expose, alter, disable, destroy, steal or gain unauthorised access to or make unauthorised use of an asset. In this lesson plan, we will research the different types of attacks, review specific case studies, and learn how to prevent them.
Introduction to the Topic Lesson Plans
Privacy and confidentiality is the protection of personal information. Confidentiality means keeping information between you and the client, and not telling others, including co-workers, friends, or family. Privacy is one of the primary concerns of ethical computing. However, privacy is not a straightforward concept; it may be interpreted from many different perspectives. There is a thin line between the need to disclose information for the benefit of some individuals and the need to safeguard.

In Information Security, threats can arise in the form of Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

A threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest. Software attacks can take the form of Viruses, Worms, and Trojan Horses (among others). Most people think that malware, virus, worms, bots are all the same things. They are not the same; the main similarity is that they are all malicious programmes designed to behave disruptively.

The term malware is a contraction of 'malicious software'. Put simply; malware is any piece of software that was written with the intent of damaging devices, stealing data, and generally causing problems. Viruses, Trojans, spyware, and ransomware are among the different kinds of malware. In this lesson, you will look at various types of malware and the seriousness of what could happen to the network or organisation.

Topic Lesson Plan No: 1	
Title	**Privacy and Confidentiality**
Aim and objective	Understand the importance of maintaining the privacy and confidentiality of an organisation's information, as well as that of stakeholders Aims: • Explain why data is an essential asset to organisations. • Identify ways in which organisations may lose some of their data. • Discuss different forms of attack on an organisation's data.
How long will this Topic Lesson Plan take to deliver?	90 minutes
What knowledge, understanding and skills will students develop?	8.1.1 Understand the importance of maintaining privacy and confidentiality of an organisation's information 8.1.2 Understand the potential impact on an organisation of failing to maintain privacy and confidentiality 8.2.3 Understand processes and procedures to mitigate threats and ensure security

<table>
<tr><td><b>Self-study activities</b></td><td>N/A</td></tr>
<tr><td colspan="2"><b>Activity 1</b>: Complete the tasks below for the following two organisations:
1. Amazon
2. Local Hospital

• Identify the type of data they would each hold
• Explain the impact of their business if they ‘lost’ some of this data?
• Analyse some of the problems involved in trying to get this data back

<b>Activity 2:</b> Research the difference between data confidentiality and data privacy for an organisation.

What would be the impact on the two organisations above if confidentiality and privacy were breached?

<b>Activity 3:</b> Create a mind map called "Data Loss”.

• Identify different types of data loss
• Import images that represent each type of data loss and add it to the mind map.
• Label each picture/branch to say whether the data loss is accidental or deliberate, natural or human-made, internal or external, criminal or malpractice (some forms of data loss might be more than 1 type).
• Explain the impact of each type of data loss and the problems they might create for an organisation.
• Identify how you can mitigate against each type of data loss.</td></tr>
<tr><td><b>Instructions</b>:</td><td>Start the lesson with a starter activity; find out what the students know. (10 minutes)

Main: work through the activities discussing the main points. Use the links within the Industry Links document. Complete the activities in the order shown. (65 minutes)

Plenary: summarises the lesson objective and aims (15 minutes)</td></tr>
<tr><td><b>Worksheets/ templates</b></td><td>N/A</td></tr>
<tr><td><b>English, maths and digital skills</b></td><td>E2 Present information and ideas.
E3 Create texts for different purposes and audiences.
E4 Summarise information/ideas.
E5 Synthesise information.
M6 Understanding data and risk.
D1 Use digital technology and media effectively.</td></tr>
</table>

Industry Links	https://www.teiss.co.uk/category/threats/

Topic Lesson Plan No: 2	
Title	**Security Risks and Threats**
Aim and objective	Understand potential **technical** threats and vulnerabilities to systems, data and information. • Explain different types of threats. • Give examples • Discuss how system users affect system vulnerability.
How long will this Topic Lesson Plan take to deliver?	120 minutes
What knowledge, understanding and skills will students develop?	8.1.5 Understand potential human threats and vulnerabilities to systems, data and information 8.2.2 Understand the interrelationship between security, identity, confidentiality, integrity, availability, threat, vulnerability and risk management within a business context 8.1.3 Understand potential technical threats and vulnerabilities to systems, data and information 8.1.4 Understand potential physical vulnerabilities to systems, data and information
Self-study activities	NA
Activity 1: What threats do our networks face? Get students to place their answer on sticky notes. Place on the wall and discuss these with the class. **Activity 2**: Ask the students to identify what categories each threat type fits into. **Activity 3:** Explain how to mitigate against these threats and how the solution defends against them.	
Instructions:	Starter activity: find out what the students know. (25 minutes) Main: work through the activities above discussing the

	main points, and referring to recent examples. (70 minutes) Plenary: summarise the lesson objective and aims (25 minutes)
Worksheets/ templates	N/A
English, maths and digital skills	E2 Present information and ideas. E3 Create texts for different purposes and audiences. E4 Summarise information/ideas. E5 Synthesise information. D2 Design, create and edit documents and digital media. D3 Communicate and collaborate.
Industry Links	www.hacksplaining.com/exercises/sql-injection https://www.geeksforgeeks.org/threats-to-information-security/

Topic Lesson Plan No: 3	
Title	**Threats and Mitigation**
Aim and objective	Understand the different threats posed to networks. Aims: • Explain different types of malware. • Give examples of phishing scams. • Discuss how system users affect system vulnerability.
How long will this Topic Lesson Plan take to deliver?	90 minutes
What knowledge, understanding and skills will students develop?	8.2.1 Understand the concept of the CIA (confidentiality, integrity, availability) and how it can be applied to define security aims 8.2.2 Understand the interrelationship between security, identity, confidentiality, integrity, availability, threat, vulnerability and risk management within a business context 8.2.3 Understand processes and procedures to mitigate threats and ensure security

Self-study activities	N/A

Activity 1:

Carry out the below activities for the following types of malware; Worms, Trojan Horses, Viruses, Spyware, Pharming, Adware

- How does a device become infected?
- How it affects your device
- How do you mitigate against it?

Activity 2:

Explain how the following could be used to phish for people's personal and financial details:

1. Someone sends you an e-mail pretending to be from your bank.
2. Someone sets up a website that looks like a legitimate business selling very cheap smartphones.
3. Someone sets up a website that looks exactly like a real business, you know.

Activity 3:

Explain how the following cause security problems for networks:

- Blagging
- Shouldering
- Weak passwords
- Unencrypted USB flash drives
- Taking company laptops off the premises
- Employees using a public hotspot in a cafe
- Lack of training for staff

Activity 4

Research into a recent IT security issue within a large organisation. What happened? What type of attack was used? What was the impact on the company (legal, reputation, sales, etc.)?

Consider how the organisation may have prevented this security breach.

Instructions:	Start the lesson with a starter activity; find out what the students know. (15 minutes) Main: work through the activities discussing the main points, refer to up to date examples. (65 mins) Plenary: summarises the lesson objective and aims (15 mins)
Worksheets/	N/A

templates	
English, maths and digital skills	E2 Present information and ideas. E3 Create texts for different purposes and audiences. E4 Summarise information/ideas. E5 Synthesise information. M6 Understanding data and risk. D1 Use digital technology and media effectively.
Industry Links	https://www.malwarebytes.com/malware/

Introduce the Topic Lesson Plans 4	
Title	**System attacks and prevention mechanisms**
Aim and objective	Understand the different ways in which systems can be attacked. Aims: • Identify different types of attacks on computer systems. • Give examples of how these attacks occur. • Explain the potential impact of different attacks.
How long will this Topic Lesson Plan take to deliver?	90 minutes
What knowledge, understanding and skills will students develop?	8.1.2 Understand the potential impact on an organisation of failing to maintain privacy and confidentiality 8.2.3 Understand processes and procedures to mitigate threats and ensure security
Self-study activities	N/A
Activity 1: • Watch video extract about different methods of attack here: https://www.cisco.com/c/en_uk/products/security/common-cyberattacks.html • Copy and paste the types of attack from the above link. Pair the students off and print out enough copies for each pair. Cut the print outs so you separate the types of attack and the descriptions. Mix these up and ask the students to try and match the correct description to the correct type of attack. **Activity 2:**	

Read the information on the web link about the four types of attack and produce a set of notes to describe how each type of attack occurs.

Activity 3:

Brute Force
https://www.securemac.com/news/members-uk-parliament-emails-hacked-brute-force-attack

Try to find your examples of DoS, and data theft attacks e.g.
https://teiss.co.uk/features/top-five-biggest-cyber-attacks-uk/

Look at the case studies discuss the type of attaching and how it may have been prevented. Discuss what impact this would have and how might it be prevented.

Instructions:	Start the lesson with a starter activity; find out what the students know. (15 minutes) Main: work through the activities discussing the main points, refer to up to date examples. (65 minutes) Plenary: summarises the lesson objective and aims (15 minutes)
Worksheets/ templates	N/A
English, maths and digital skills	E2 Present information and ideas. E4 Summarise information/ideas. E5 Synthesise information. M6 Understanding data and risk. D2 Design, create and edit documents and digital media. D3 Communicate and collaborate.
Industry Links	Video: https://www.youtube.com/watch?v=v6Qgr1wT4uE https://threatmap.checkpoint.com/

Topic Lesson Plan No: 5	
Title	**System Security – physical vulnerabilities**

Aim and objective	Understand potential physical vulnerabilities to systems, data and information
How long will this Topic Lesson Plan take to deliver?	145 minutes
What knowledge, understanding and skills will students develop?	8.1.1 Understand the importance of maintaining privacy and confidentiality of an organisation's information 8.1.2 Understand the potential impact on an organisation of failing to maintain privacy and confidentiality 8.2.3 Understand processes and procedures to mitigate threats and ensure security
Self-study activities	N/A
Activity 1:	
Title	Physical Vulnerabilities
Instructions:	Start with a discussion about physical vulnerabilities. Then discuss what might an intruder (internal or external) do to disrupt or steal from an organisation's network. (10 minutes) Main: In small groups, complete the activities discussing the key points. (120 minutes) Plenary: Summarise the lesson objective and aims (15 minutes)
Worksheets/templates	Perimeter Activity.docx Perimeter Solution.docx
English, maths and digital skills	E2 Present information and ideas. E3 Create texts for different purposes and audiences. E4 Summarise information/ideas. E5 Synthesise information. D2 Design, create and edit documents and digital media. D3 Communicate and collaborate.
Industry Links	http://pathfinder.ara.com/industry-insights/perimeter-security