Computing

GCSE Computer Science – Network Security

Assessment Opportunities	Literacy/Reading opportunities	CEIAG Links
Within every half term, there will be a minimum of 2 low stakes quizzes. These will be automatically marked out of 20. **There will also be a end of unit test which will be based on past exam questions. These questions are then marked and gone through as a class.**	Forms of attack - Network security - OCR - GCSE Computer Science Revision - OCR - BBC Bitesize GCSE Computer Science - 1.4.2 Identifying and preventing vulnerabilities (google.com) Identifying and preventing vulnerabilities - Network security - OCR - GCSE Computer Science Revision - OCR - BBC Bitesize	• Penetration tester • Application analyst • Applications developer • Cyber security analyst • Data analyst • Forensic computer analyst • IT trainer • Machine learning engineer

Curriculum vision:

“Our aim is to deliver a curriculum that is inclusive, relevant and progressive for all learners.”

Topic 1.4 Network security
Lesson 1 - Malware and social engineering

FIRST ASSESSMENT
SUMMER 2022

The big picture

Why is this relevant for the students?

- What computing threats are out there in the world?

Notes: *Use Context Setting task to engage students and create discussion.*

May link to flipped resources if you use flipped learning.

Objectives

What should the students be confident/able to do at the end of the session?

- Explain the different types of malware.
- Discuss a real life malware-related event.
- Understand how phishing operates.
- Discuss how data can be intercepted.

Notes: *These are the core learning that the students should develop during the lesson. This will link to the activities that provide ability to assess the Objectives.*

Engagement

What will make the students want to learn?

- What threats do modern companies face?

Notes: *A short activity that stimulates the students. Ideas taken from big picture activity could be used.*

Keywords

What exam/specification specific words should the students be confident with and need to know?

- Malware
- Viruses
- Worms
- Trojan Horses
- Phishing
- Social Engineering
- Data Interception

Notes: *Multiple Choice Questions will assess these keywords; use the MCQs supplied. You may wish to customise these as needed.*

The sticking points

What activities will the students undertake?

- There are different types of malware
- Phishing extends from email

Notes: *A list of concepts that you want the student to remember by the end of the lesson.*

..

Assessment for Learning

Expected progress:

- Understand types of malware and identify differences.

This is likely to be activities and learning tasks that meet your expectations for the class progress towards the objectives.

Good progress:

- Understand the different types of phishing and how they operate.

This would show a development from basic understanding and be indicative that some students use stretch and challenge material during the lesson.

Exceptional progress:

- Discuss how data can be intercepted.

This would indicate the level of progress if all extension activities have been completed and at 8/9 levels of understanding.

Notes

Differentiation

How will I enable access to each area of learning?

- Task 1 differentiated sheets.
- Task 2 – pair work.
- Task 3 – group research**.**

Notes: *Use of stretch task ideas supplied may support high-end differentiation.*

You will need to modify the resources to meet the needs of your students specifically. You may wish to refer to Departmental or School policies on differentiation methods used within your centre.

Activity 1

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Complete Activity 1 – Table.
- Explain the different types of malware and use resources in order to expand on your answers.

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Activity 2

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Look at the Activity 2 email.
- Identify how you could tell this email may be a phishing email.
- What are the 'tell-tale' signs?

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Activity 3

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Short research, discussion and present findings: **What different ways are there to intercept data?**

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Summary/Plenary

How will I check that students have retained the knowledge?

- What is Phishing?
- Are there different types of phishing? If so, what are they?

Notes: *Use the MCQs to check basic understanding of Keywords and Topics.*

Use the LOR to develop deeper knowledge and allow Peer Assessment and Review. This can be developed to use the LOR ideas as homework etc.

Homework/Flipped Learning

Lesson 2 – Brute force, DDOS and SQL injection

The big picture

Why is this relevant for the students?

- What is a brute-force attack?

Notes: *Use Context Setting task to engage students and create discussion.*

May link to flipped resources if you use flipped learning.

Objectives

What should the students be confident/able to do at the end of the session?

- Understand the meaning of DDOS and brute force attacks.
- Explain the effects of a DDOS attack.
- Explain how to be protected against DDOS attacks.
- Understand the concept of SQL injection.
- Explain how a vulnerability can be exploited.

Notes: *These are the core learning that the students should develop during the lesson. This will link to the activities that provide ability to assess the Objectives.*

Engagement

What will make the students want to learn?

- What DDOS attacks have you heard about in recent years?
- Who was involved?
- Who was affected by the attack (business, clients, customers)?
- Was there a motive around the attack?

Notes: *A short activity that stimulates the students. Ideas taken from big picture activity could be used.*

Keywords

What exam/specification specific words should the students be confident with and need to know?

- Brute force attacks
- DDOS
- Botnet
- Exploit
- SQL injection

Notes: *Multiple Choice Questions will assess these keywords; use the MCQs supplied.*

You may wish to customise these as needed.

The sticking points

What do I want students to remember?

- Botnets are commonly used to perform DDOS attacks.
- SQL injection exploits vulnerabilities with the programming language.
- Vulnerabilities can be exploited.

Notes: *A list of concepts that you want the student to remember by the end of the lesson.*

Assessment for Learning

Expected progress:

- Students to understand the meaning of DDOS and brute force.

This is likely to be activities and learning tasks that meet your expectations for the class progress towards the objectives.

Good progress:

- Students to understand how a botnet is created.

This would show a development from basic understanding and be indicative that some students use stretch and challenge material during the lesson.

Exceptional progress:

- Students to explain vulnerabilities and how they can be exploited.

This would indicate the level of progress if all extension activities have been completed and at 8/9 levels of understanding.

Notes

Differentiation

How will I enable access to each area of learning?

- Answer the following:
  - Explain a recent DDOS attack and discuss the effects on customers and businesses.
  - Research and describe a 'botnet' and explain how they originate.
  - Extension: How can companies protect themselves from DDOS attacks?

Notes: *Use of stretch task ideas supplied may support high-end differentiation.*

You will need to modify the resources to meet the needs of your students specifically. You may wish to refer to Departmental or School policies on differentiation methods used within your centre.

Activity 1

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Complete the worksheet, using https://howsecureismypassword.net/ to consider how vulnerable each system is to a brute force attack.

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Activity 2

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Answer the following :
  - Explain a recent DDOS attack and discuss the effects on customers and businesses.
  - Research and describe a 'botnet' and explain how they originate.
  - Extension: How can companies protect themselves from DDOS attacks?

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs. Reference the Common misconceptions/FAQ guide to support your delivery of the topic.*

Activity 3

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Create an informative leaflet for SQL administrators explaining the importance of protecting against SQL injection and how attackers can exploit vulnerabilities in SQL databases.

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Summary/Plenary

How will I check that students have retained the knowledge?

- Paired quiz – best answer sharing
- What is a DDOS attack?
- What are botnets?
- How does SQL injection work?

Notes: *Use the MCQs to check basic understanding of Keywords and Topics.*

Use the LOR to develop deeper knowledge and allow Peer Assessment and Review. This can be developed to use the LOR ideas as homework etc.

Homework/Flipped Learning

Lesson 3 – Penetration testing, anti-malware and firewalls

The big picture

Why is this relevant for the students?

- Threats to networks are far more prevalent in recent years. How can organisations protect themselves from attack?

Notes: *Use Context Setting task to engage students and create discussion.*

May link to flipped resources if you use flipped learning.

Assessment for Learning

Expected progress:

- Have a basic knowledge of pen testing, anti-malware software and firewalls.

This is likely to be activities and Learning tasks that meet your expectations for the class progress towards the objectives.

Good progress:

- Understand the different types of penetration testers.
- Identify the differing roles of anti-malware and firewall software.

This would show a development from basic understanding and be indicative that some students use stretch and challenge material during the lesson.

Exceptional progress:

- Demonstrate a deep understanding and accurately discuss all of the relevant factors, including the efficacy of preventative tools.

This would indicate the level of progress if all extension activities have been completed and at 8/9 levels of understanding.

Objectives

What should the students be confident/able to do at the end of the session?

- Understand the legalities and consequences of unlawfully intercepting data.
- Understand the concept of penetration testing.
- Understand how security software including anti-malware and firewalls help to protect computer systems.

Notes: *These are the core learning that the students should develop during the lesson. This will link to the activities that provide ability to assess the Objectives.*

The sticking points

What do I want students to remember?

- Penetration testing is carried out to look for vulnerabilities.
- Anti-malware and firewalls both carry out different roles in preventing threats.

Notes: *A list of concepts that you want the student to remember by the end of the lesson.*

Notes

Engagement

What will make the students want to learn?

- What is the 'official title' of the person who is responsible for exploring vulnerabilities of computer systems and reporting of this in an organisation?
- What vulnerabilities may they discover?

Notes: *A short activity that stimulates the students. Ideas taken from big picture activity could be used.*

Keywords

What exam/specification specific words should the students be confident with and need to know?

- Penetration testing
- Anti-malware
- Firewalls

Multiple Choice Questions will assess these keywords; use the MCQs supplied. You may wish to customise these as needed.

Differentiation

How will I enable access to each area of learning?

- Activities 2 and 3 may be found challenging by some students so this is differentiated by task.
- Activity 1 based around research therefore some prompts or pointers may be needed to start some students off.

Notes: *Use of stretch task ideas supplied may support high-end differentiation.*

You will need to modify the resources to meet the needs of your students specifically. You may wish to refer to Departmental or School policies on differentiation methods used within your centre.

Activity 1

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Complete your own research and present the key differences between:
  A white hat hacker | A grey hat hacker | A black hat hacker

- Extension: Discuss the legal implications for each category of hacker.

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs. Reference the Common misconceptions/FAQ guide to support your delivery of the topic.*

Activity 2

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Complete the worksheet to create a flowchart that describes the processes involved in identifying and removing malware from a computer system.

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Activity 3

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Complete the worksheet to identify which vulnerabilities could be addressed using either anti-malware or firewall software.

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Summary/Plenary

How will I check that students have retained the knowledge?

- Develop revision cards using shared resource.
- Check questions and answers by shuffling cards and sharing around to test each other.

Notes: *Use the MCQs to check basic understanding of Keywords and Topics.*

Use the LOR to develop deeper knowledge and allow Peer Assessment and Review. This can be developed to use the LOR ideas as homework etc.

Homework/Flipped Learning

Lesson 4 – User access levels, passwords, encryption and physical security

The big picture

Why is this relevant for the students?

Students to discuss the following:

- What are the benefits of encryption?
- Why should passwords be kept secure?

Notes: *Use Context Setting task to engage students and create discussion.*

May link to flipped resources if you use flipped learning.

Assessment for Learning

Expected progress:

- Understand how to set a secure password.

This is likely to be activities and Learning tasks that meet your expectations for the class progress towards the objectives.

Good progress:

- Understand how a Caesar Cipher works and demonstrate the ability to encrypt and decrypt messages.

This would show a development from basic understanding and be indicative that some students use stretch and challenge material during the lesson.

Exceptional progress:

- Discuss the effects of encryption on organisations such as the Government.

This would indicate the level of progress if all extension activities have been completed and at 8/9 levels of understanding.

Objectives

What should the students be confident/able to do at the end of the session?

- To understand the effects of user access levels on a system.
- To understand how and why passwords must be kept secure and the levels of complexity.
- To learn how encryption can have a negative effect on law enforcement and investigations.
- To understand how encryption works
  To demonstrate a knowledge of a cypher and its' key.

Notes: *These are the core learning that the students should develop during the lesson. This will link to the activities that provide ability to assess the Objectives.*

The sticking points

What do I want students to remember?

- User access levels vary per group, for example administrators will have full access rights
- Students should understand the complexities of a secure password

Notes: *A list of concepts that you want the student to remember by the end of the lesson.*

Engagement

What will make the students want to learn?

- Students will discuss the makings of a secure password.
  Students will build a list of ideas in groups and discuss why passwords should be complex.

Notes: *A short activity that stimulates the students. Ideas taken from big picture activity could be used.*

Keywords

What exam/specification specific words should the students be confident with and need to know?

- User access levels
- Passwords
- Encryption
- Cipher
- Key

Multiple Choice Questions will assess these keywords; use the MCQs supplied. You may wish to customise these as needed.

Notes

Differentiation

How will I enable access to each area of learning?

- Students can research elements of a secure password and or test ideas using an online service.
- Students to complete Caesar Cipher task using different shift keys and phrase lengths varied by ability.

Notes: *Use of stretch task ideas supplied may support high-end differentiation.*

You will need to modify the resources to meet the needs of your students specifically. You may wish to refer to Departmental or School policies on differentiation methods used within your centre.

Activity 1

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Define sets of user access levels for various groups on the worksheet.
- Differentiated by ability on worksheet.

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Activity 2

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Create an infographic to illustrate the importance of secure passwords.

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Activity 3

What tasks will I ask the students to complete to develop their understanding during the lesson?

- Create a Caesar Cipher and demonstrate the ability to encode and decode messages.
- Differentiated by ability.

Notes: *Use the Activities given to develop the students' knowledge of the topic. Each activity may need further differentiation/adaptation for your needs.*

Reference the Common misconceptions/FAQ guide to support your delivery of the topic.

Summary/Plenary

How will I check that students have retained the knowledge?

- Identify as many security features as you can from your own school.
- Identify any extra security features that might be required for a high risk setting such as a police station.

Notes: *Use the MCQs to check basic understanding of Keywords and Topics.*

Use the LOR to develop deeper knowledge and allow Peer Assessment and Review. This can be developed to use the LOR ideas as homework etc.

Homework/Flipped Learning

We value your feedback

We'd like to know your view on the resources we produce. By clicking on the icon above you will help us to ensure that our resources work for you.

Whether you already offer OCR qualifications, are new to OCR, or are considering switching from your current provider/awarding organisation, you can request more information by completing the Expression of Interest form which can be found here: www.ocr.org.uk/expression-of-interest

Looking for a resource? There is now a quick and easy search tool to help find free resources for your qualification: www.ocr.org.uk/i-want-to/find-resources/

OCR Resources: *the small print*

OCR's resources are provided to support the delivery of OCR qualifications, but in no way constitute an endorsed teaching method that is required by the Board, and the decision to use them lies with the individual teacher. Whilst every effort is made to ensure the accuracy of the content, OCR cannot be held responsible for any errors or omissions within these resources.

Our documents are updated over time. Whilst every effort is made to check all documents, there may be contradictions between published support and the specification, therefore please use the information on the latest specification at all times. Where changes are made to specifications these will be indicated within the document, there will be a new version number indicated, and a summary of the changes. If you do notice a discrepancy between the specification and a resource please contact us at: resources.feedback@ocr.org.uk.

Please get in touch if you want to discuss the accessibility of resources we offer to support delivery of our qualifications: resources.feedback@ocr.org.uk