# Unit 1.6 Security Systems

## Low

* Read the definition on Malware and underline the key words in each statement
* Find examples of malware for each type of malware given
* State two things that this malware does

|  |  |  |
| --- | --- | --- |
| **Types of Malware**   * Otherwise known as ‘malicious software’ * Software which can be malicious if damaging to a computer or network | | |
| **Viruses** | **Worms** | **Trojan Horses** |
| * Replicates by reproducing itself * Infects other programs by modifying them * Can also infect other parts of the operating system * Data files, boot sector of hard drive are examples * Concept virus * ILOVEYOU virus | * Replicates by reproducing itself * Does not alter files * Resides in active memory * Takes advantage of parts of an operating system that are not usually visible to the user, for example system files * Morris worm * Blaster worm * Storm worm | * Often disguised as legitimate software * Can allow control of the system and its’ key functions, including: * Deleting data * Blocking data * Modifying data * Copying data * Disrupting the performance of computers or computer networks * Unable to replicate * Can be classified according to the type of actions that can be performed on the computer, examples include exploits, backdoor and rootkit. * OSX/RSPlug Trojan * Klez |

We’d like to know your view on the resources we produce. By clicking on ‘[Like](mailto:resources.feedback@ocr.org.uk?subject=I%20liked%20the%20OCR%20GCSE%20(9-1)%20Computer%20Science,%20Unit%201.6%20Security%20Systems;%20Lesson%201%20–%20Activity%201)’ or ‘[Dislike](mailto:resources.feedback@ocr.org.uk?subject=I%20disliked%20the%20OCR%20GCSE%20(9-1)%20Computer%20Science,%20Unit%201.6%20Security%20Systems;%20Lesson%201%20–%20Activity%201)’ you can help us to ensure that our resources work for you. When the email template pops up please add additional comments if you wish and then just click ‘Send’. Thank you.

If you do not currently offer this OCR qualification but would like to do so, please complete the Expression of Interest Form which can be found here: [www.ocr.org.uk/expression-of-interest](http://www.ocr.org.uk/expression-of-interest)

**OCR Resources**: *the small print*OCR’s resources are provided to support the teaching of OCR specifications, 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.   
© OCR 2017 - This resource may be freely copied and distributed, as long as the OCR logo and this message remain intact and OCR is acknowledged as the originator of this work.

OCR acknowledges the use of the following content: n/a

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](mailto:resources.feedback@ocr.org.uk)

## Medium

* Define what malware is
* Identify the three types of malware and write one type into each column
* Find examples of malware for each type and describe each one and how it works

|  |  |  |
| --- | --- | --- |
| **What is Malware**  Malware, otherwise known as ‘malicious software’, is software which can be damaging to a computer or network. | | |
| **Types of Malware** | | |
| **Viruses** | **Worms** | **Trojan Horses** |
| * Replicates by reproducing itself * Infects other programs by modifying them * Can also infect other parts of the operating system * Data files, boot sector of hard drive are examples * Concept virus * ILOVEYOU virus | * Replicates by reproducing itself * Does not alter files * Resides in active memory * Takes advantage of parts of an operating system that are not usually visible to the user, for example system files * Morris worm * Blaster worm * Storm worm | * Often disguised as legitimate software * Can allow control of the system and its’ key functions, including: * Deleting data * Blocking data * Modifying data * Copying data * Disrupting the performance of computers or computer networks * Unable to replicate * Can be classified according to the type of actions that can be performed on the computer, examples include exploits, backdoor and rootkit. * OSX/RSPlug Trojan * Klez |

1. Locate stories of exploits and reference them to the relevant type of malware.
   1. Summarise the key points you have learnt into a poster informing people about malware

## High

* Define what malware is
* Identify the three types of malware and write one type into each column
* Fine examples of malware for each type and describe each one and how it works

|  |  |  |
| --- | --- | --- |
| **Types of Malware**  **What is Malware**  Malware, otherwise known as ‘malicious software’, is software which can be damaging to a computer or network. | | |
| **Viruses** | **Worms** | **Trojan Horses** |
| * Replicates by reproducing itself * Infects other programs by modifying them * Can also infect other parts of the operating system * Data files, boot sector of hard drive are examples * Concept virus * ILOVEYOU virus | * Replicates by reproducing itself * Does not alter files * Resides in active memory * Takes advantage of parts of an operating system that are not usually visible to the user, for example system files * Morris worm * Blaster worm * Storm worm | * Often disguised as legitimate software * Can allow control of the system and its’ key functions, including: * Deleting data * Blocking data * Modifying data * Copying data * Disrupting the performance of computers or computer networks * Unable to replicate * Can be classified according to the type of actions that can be performed on the computer, examples include exploits, backdoor and rootkit. * OSX/RSPlug Trojan * Klez |

Extension:

1. Locate stories of exploits and reference them to the relevant type of malware.
2. Identify social, moral, legal, cultural issues within these stories
3. Write a short essay on:
   1. “Without hacking there would be less security and the effects of hacking would be worse!” **or**
   2. “There is no perfect virus checker – we are always one step behind in security”