GCSE Computer Science (9-1)

EDULiTO

Security Systems

Topic Tests

Photocopiable Resources

Terms and Conditions of Use

Topic Test - System security

1. (a) What is meant by malware? [1]

……

……

……

(b) Give 3 examples of types of malware and explain how each can be harmful. [6]

Example 1…….

How is this malware harmful?

……

……

……

Example 2…….

How is this malware harmful?

……

……

……

Example 3…….

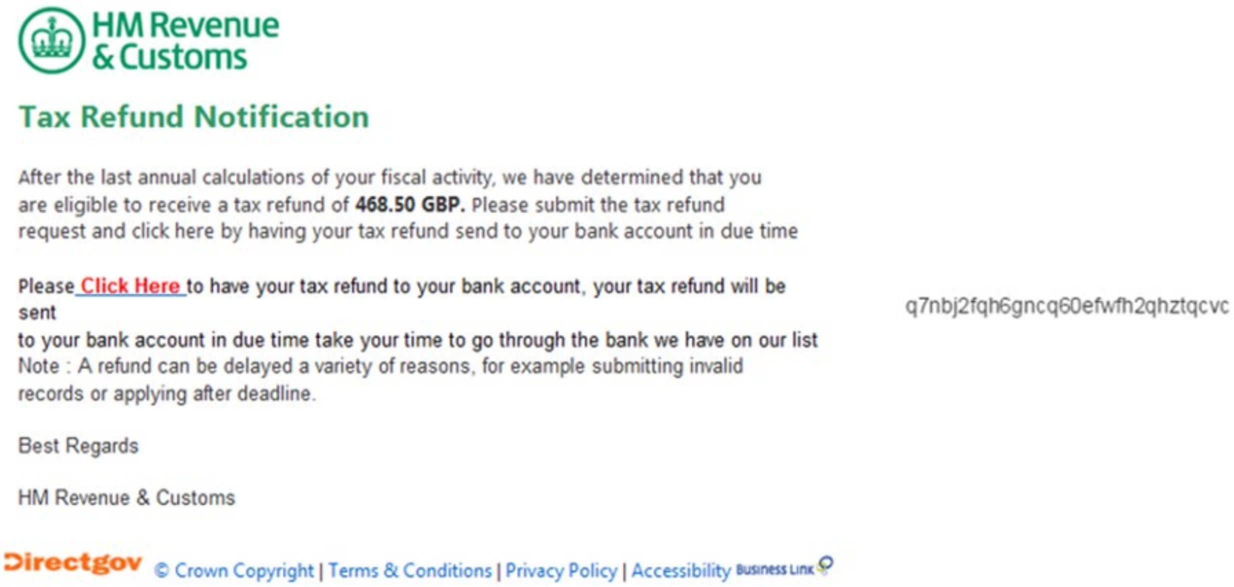
How is this malware harmful?

……

……

……

2. The email below is an example of a phishing attack.



HM Revenue & Customs

Tax Refund Notification

After the last annual calculations of your fiscal activity, we have determined that you are eligible to receive a tax refund of **468.50 GBP.** Please submit the tax refund request and click here by having your tax refund send to your bank account in due time

Please Click Here to have your tax refund to your bank account, your tax refund will be sent to your bank account in due time take your time to go through the bank we have on our list

q7nbj2fqh6gncq60efwfh2qhztqcvc

Note : A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.

Best Regards

HM Revenue & Customs

Directgov © Crown Copyright | Terms & Conditions | Privacy Policy | Accessibility Business Link

List three reasons why it is believed that this is a Phishing attack. [3]

Reason 1

……

……

Reason 2

……

……

Reason 3

……

……

3. (a) Hackers sometimes use social engineering to gain access to network data. What is meant by social engineering? [1]

……

……

(b) Explain how a person would go about carrying out a social engineering attack on a company. [1]

………

………

………

……

(c) What is a brute force attack? [2]

………

………

………

……

(d) What is a denial of service attack and why is it carried out? [2]

………

………

………

……

(e) What is a data interception and theft attack? [2]

………

………

………

……

(f) What is an SQL injection attack? [2]

………

………

………

………

4. (a) Businesses and other organisations usually have an Acceptable Use Policy (AUP). What is an AUP and why do businesses and other organisations feel that it is important to have one? [2]

………

………

………

………

(b) Businesses and other organisations use a variety of techniques to protect their network.

Complete the table by including a description of each technique. [8]

Technique	Description
Penetration testing	
Network forensics	

Network policies	
Anti-malware software	
Firewalls	
User access levels	
Passwords	

Encryption	

Topic Test System security - Mark Scheme

Question Number	Answer	Additional Guidance	Mark
1 a	Malware is short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system. [1]		**1**
1 b	Examples: viruses, worms, Trojan horses, and spyware. Viruses are self-replicating computer programs which install themselves without user consent. They often perform some type of harmful activity on the infected host device. A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Trojan horses do not replicate themselves but they can be just as destructive. One type of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. Spyware is software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.	**1 mark for each example – max 3** **1 mark for each explanation of how it is harmful max 3**	**6**
2	General greeting [1] Link not to expected domain [1] Requests personal information [1] Suggests a sense of urgency. [1]	**Max 3 marks**	**3**
3 a	Psychological manipulation of people into performing actions or divulging confidential information [1]	**Max 1**	**1**
3 b	Pretend you work at a company and get access to the network on a workstation that is already logged in. [1] Gaining network information from existing employees. [1] Gather personal information about a worker and use this to identify their password. [1]	**Max 1**	**1**
3 c	A Brute force attack is a trial and error method [1] used to decode encrypted data such as passwords, through trying every possible combination in sequence [1] until you arrive at the correct password.		**2**
3 d	A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. [1] This could be to extort money or for political reasons. [1]		**2**

3 e	A data interception occurs when packets of data travel across a network, they are susceptible to being read, altered, or "hijacked." [1] Hijacking occurs when a hostile party intercepts network traffic and poses as one of the session endpoints. An attacker can easily read all text traffic. [1]		**2**
3 f	SQL injection attack is used on database applications [1] Malicious SQL statements are inserted into an entry field for execution [1] transmitting the data to the hacker. [1]	Max 2	**2**
4 a	Acceptable Use Policy – This tells company employees how they should behave when using the network. [1] This is a signed agreement that employees are bound by. [1] Ensures that employees follow the network rules supplied by their employer. [1]	Max 2	**2**
4 b	**Penetration testing** Penetration testing is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. [1] **Network forensics** Network forensics relates to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. [1] **Network policies** A network security policy is a document that outlines rules for computer network access. [1] **Anti-malware software** Anti-malware software protects against infections caused by many types of malware. [1] **Firewalls** Firewalls limit access of unauthorised users to your computer and network. [1] **User access levels** Network managers can set up groups of users with different levels of access to the network. [1] **Passwords** A password is a sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user. [1] **Encryption**. Encryption is the conversion of electronic data into another coded form, called cipher text [1], which cannot be easily understood by anyone except authorised users.[1] max 1		**8** **/30**