Cybersecurity	

Threats – sentence(s) on each
 	
Threats – sentence(s) on each
	• the characteristics of different threats to computer systems, including:
	  • malware
	  • phishing
	  • social engineering
	  • brute force attacks
	  • denial of service attacks
	  • data interception and theft
	  • SQL injection
	• different ways of protecting against threats during system design, creation, testing and use, including:
	  • penetration testing
	  • network forensics
	  • anti-malware software
	  • firewalls
	  • user access levels
	  • passwords
	  • double authentication
	  • encryption.

Exam questions

Cybersecurity ensures that computer systems are protected against the threats of criminal activity using electronic data.

(a) Describe the characteristics of the following threats to computer systems:

(i) Malware [2]

.....

.....

.....

.....

(ii) Brute force attacks [2]

.....

.....

.....

.....

(b) Describe the following ways of protecting against threats:

(i) Penetration testing [4]

.....

.....

(ii) Double authentication [3]

.....

.....

.....

.....

.....

14.(a)(i)	Award one mark for each of the following up to a maximum of two marks:
	• software program
	• can perform a variety of different functions such as:
	  • stealing data, encrypting or deleting sensitive data
	  • altering or hijacking core computing functions
	  • monitoring users' computer activity without their permission.

14.(a)(ii)	Award one mark for each of the following up to a maximum of two marks: • a hacking algorithm • tries all possible combinations of lowercase and uppercase characters, numbers and symbols to gain unauthorised access to a computer system.

14.(b)(i)	Award one mark for each of the following up to a maximum of four marks: • the process of testing a computer system, or network, to find vulnerabilities an attacker could exploit • the tests can be automated with software applications or they can be performed manually. Penetration testing strategies include: • targeted testing — testing carried out by the organisation's ITC team and the penetration testing team working together • external testing — to find out if an outside attacker can get in and how far they can get in once they have gained access • internal testing — to estimate how much damage a dissatisfied employee could cause • blind testing — to simulate the actions and procedures of a real attacker by severely limiting the information given to the team performing the test.

14.(b)(ii)	Award one mark for each of the following up to a maximum of three marks: • double authentication is a second layer of security to protect an account or system • users must go through two layers of security before being granted access to an account or system • increases the safety of online accounts by requiring two types of information from the user, such as a password or PIN, an email account, an ATM card or fingerprint, before the user can log in • the first factor is the password; the second factor is the additional item.