Computer Security reading passage

Computer Security

Since the businesses are more and more relying on information and associated information systems (IS) as well as using information technology (IT) a lot changes the problem of computer security over a period of time. Still, there are only small changes occured in the security or safeguards implemented in the information systems. Even identifying the required securities and policies is not able to be done by most of the executives.

A. In the span of July 1991 - July 1996, the internet users from the commercial sector had increased from 33% to 50%. It shows how the internet becomes an important factor for business growth. Generally, the size of the internet approximately doubles each year and the related security incidents have been running in parity. Though the malicious users' percentage is less, the number of failed security incidents is significantly larger since the size of the internet is increased.

B. In network, the morris worm was entered into the Internet which invaded, attacked and replicated itself, in 1998. To fix this problem, Both Email and connectivity has been shut down. But, still, the fixes were to be distributed through Email and so the solution doesn't serve the purpose. Consequently, In 1992, CERT (Computer Emergency Response Team) with the Australian version (AUSCERT) was formed to tackle the worm virus.

C. The problem with Internet security is that malicious incidents are increasing in complexity. The increasing availability of toolkits has become one of the reasons for it. Actually, the toolkits are made for the computer systems designers to guard and develop their sites. But, it turns out to be helpful for those ignorant intruders to execute the intended complex incidents by using many routers and disguises. A US Department of Defence report says that the incidents which have happened are less than 1% but 65% of those are successful. One thing that we should keep in mind is that hackers and intruders don't fit into the geographical, administrative boundaries or time zones. The reason might be they have been geographically dislocated during the attack. Therefore, they must be operating 'off-duty hours'.

D. The key thing to understand here is that system administrators should get it right all the time but the intruder should get it right just once. Evidence will be easier to find for this. In 1997, a Bell Atlantic Network was hacked by the teenager. As a result of his hacking, the computer crashed and 600 homes, a regional airport and emergency services became without telephone communication for six hours. Punishment for this offence is as follows, Two years probation, community service and a fine of US$5,000.

E. From the wake of September 11, Governments started to take sincere action against cyber crimes. It is found that crimes are being connected to national security, which becomes a prime concern for both government officials and the public. The government took action faster. The US Patriot Act was introduced in late 2001. This Act increased the maximum punishment of five to ten years for those who break into computers. Then in

July 2002, the House of Representatives sanctioned the Cyber Security Enhancement Act. If the act of the cyber crime by an offender causes the death of an individual, he will be condemned to life sentence. After the September 11 attacks, the FBI and other government agencies elevated their monitoring of the internet. This becomes the reason for the disappearance of hackers as their act no longer considered as a play or challenge, but terrorism.

F. On the other side, September 11 events caused some ex-hackers to use their broad knowledge, skills and experience to coordinate with the security forces to help the fight against terrorism.

G. Computer viruses and hacking incidents continue even after the punishment threats are increased. Long-time security measures which have been implemented by companies and individuals are not fail-safe. Firewalls are one of the prime IS security measures. It filters the entering data and leaves the corporate IS. Though the firewalls have a number of advantages, it will not be a total cure for all 18 security woes, just an enhancement. It will only offer a false sense of security and just provide a minimal amount of protection against internal attackers. In a nutshell, the corporate world needs to realise that computer security will be an on-going problem and expense.

Computer Security IELTS Reading Questions

Questions 1-7

The reading passage has six paragraphs, **A-G.**

Choose the correct heading for each paragraph from the list of headings below.

Write the correct number, **i-x**, as your answer to each question.

List of Headings

- i. Activities of hackers and intruders
- ii. Importance of Internet
- iii. Computer security and its features
- iv. The Process of Hacking
- v. How Government fight against cyber crimes
- vi. The Morris Worm
- vii. Intruders can easily hack
- viii. How firewall performs
- ix. Ex-hackers and fight against terrorism
- x. Secret of Effective computer security

1. Paragraph A
2. Paragraph B
3. Paragraph C

4. Paragraph D
5. Paragraph E
6. Paragraph F
7. Paragraph G

Questions 8-11

Do the following statements agree with the information given in the reading passage?

Write

- **TRUE**   if the statement agrees with the information
- **FALSE**   if the statement contradicts the information
- **NOT GIVEN** if there is no information on this in the passage

8. The internet size is roughly doubles every year.

9. The toolkits made for the computer programmers to protect their programming.

10. The US patriot act was introduced in early 2001.

11. Polymorphic virus challenges the antivirus to detect the viruses.

Questions 12-14

Answer the questions below.

Choose **NO MORE THAN THREE WORDS** from the passage for each answer.

12. When was the morris worm introduced into the internet?
13. Which act was introduced in late 2001?
14. Which is one of the prime IS security measures?