**4.5.2 Security measures**

**A Study the following six security measures for protecting hardware and software below.**

**1 Control access to hardware and software**

▪ Lock physical locations and equipment.

▪ Install a physical security system.

▪ Monitor access 24 hours a day.

**2 Implement network controls**

▪ Install firewalls to protect networks from external and internal attacks.

▪ Password-protect programs and data with passwords which cannot easily be cracked.

▪ Monitor username and password use — require changes to passwords regularly.

▪ Encrypt data.

▪ Install a callback system.

▪ Use signature verification or biometric security devices to ensure user authorisation.

**3 Protect against natural disasters**

▪ Install uninterruptible power supplies and surge protectors.

**4 Backup data and programs**

▪ Make incremental backups, which are copies of just changes to files, at frequent intervals.

▪ Make full backups, which copy all files, periodically.

▪ To protect files from natural disasters such as fire and flood, as well as from crimes and errors, keep backups in separate locations, in fireproof containers, under lock and key.

**5 Separate and rotate functions**

▪ If functions are separate, then two or more employees would need to conspire to commit a crime.

▪ If functions are rotated, employees would have less time to develop methods to compromise a program or system.

▪ Perform periodic audits.

**6 Protect against viruses**

▪ Use virus protection programs.

▪ Use only vendor-supplied software or public domain or shareware products that are supplied by services that guarantee they are virus-free.

**B Answer the following questions with one or more complete sentences.**

**1 Which of the above security measures do you have in place… …at home?**

*The entrance of our home is looked by a fingerprint reader which opens the door only if the fingerprint matches with the example of the chip.*

*Our network is protected by a firewall.*

*Personally, I save my work on an external hard drive as well as in the cloud.*

…at work?

*Our company uses Office 365 and uses it everywhere. Our work is saved on Microsoft servers.*

*Many of our applications do regularly backups by themselves.*

*Each user must change his password all three months*

**2 Which of these measures are easy to implement and which ones are rather difficult to adopt?**

Easy:

*Install firewalls to protect networks from external and internal attacks.*

*Password-protect programs and data with passwords which cannot easily be cracked.*

*Monitor username and password use — require changes to passwords regularly.*

*Make incremental backups, which are copies of just changes to files, at frequent intervals.*

*Make full backups, which copy all files, periodically.*

*Perform periodic audits.*

*Use virus protection programs.*

*Use only vendor-supplied software or public domain or shareware products that are supplied by services that guarantee they are virus-free.*

Difficult:

*Lock physical locations and equipment.*

*Install a physical security system.*

*Monitor access 24 hours a day.*

*Encrypt data.*

*Install a callback system*

*To protect files from natural disasters such as fire and flood, as well as from crimes and errors, keep backups in separate locations, in fireproof containers, under lock and key.*

*If functions are separate, then two or more employees would need to conspire to commit a crime.*

*If functions are rotated, employees would have less time to develop methods to compromise a program or system*

**3 Find words or phrases among the six security measures which mean…**

a …copies of changes to files made to reduce the risk of loss of data

*Make incremental backups, which are copies of just changes to files, at frequent intervals.*

b …software available for a short time on a free trial basis; if adopted, a fee is payable to the author

*Use only vendor-supplied software or public domain or shareware products that are supplied by services that guarantee they are virus-free.*

c …cannot be disrupted or cut

*Install uninterruptible power supplies and surge protectors.*

d …put at risk

*Monitor access 24 hours a day*

e …deciphered, worked out

*Encrypt data.*

f …protect data by putting it in a form only authorised users can understand

*Install a physical security system.*

g …a combination of hardware and software to protect networks from unauthorised users

*Install firewalls to protect networks from external and internal attacks.*

*Use signature verification or biometric security devices to ensure user authorisation*

h …observe and record systematically

*Monitor access 24 hours a day*

i …measuring physical characteristics such as distance between the eyes

*Use signature verification or biometric security devices to ensure user authorisation.*

j …at regular intervals

*Perform periodic audits.*

*Make full backups, which copy all files, periodically.*

**C How smart cards work. Complete the text with the verbs in the correct form.**

Smart cards prevent unauthorised users from accessing (access) systems and permit authorised users have (have) access to a wide range of facilities. Some computers have smart card readers allow (allow) you to buy (buy) things on the web easily and safely with digital cash. A smart card can also send data to a reader via an antenna coiled (coil) inside the card. When the card comes within range, the reader's radio signal creates (create) a slight current in the antenna causing (cause) the card to broadcast (broadcast) information to the reader which allows (allow) the user, for example, withdraw (withdraw) money from an ATM or get (get) access to a system.

**E Text skimming. People who know how to skim and scan are flexible readers. They read according to their purpose and get the information they need quickly without wasting time. They do not read everything which increases their reading speed. Their skill lies in knowing what specific information to read and which method to use.**

Answer the following questions as quickly as you can by reading the seven text snippets below. Write your answer on the corresponding lines below.

1 Which group hacked into Hotmail? *Hackers Unite*

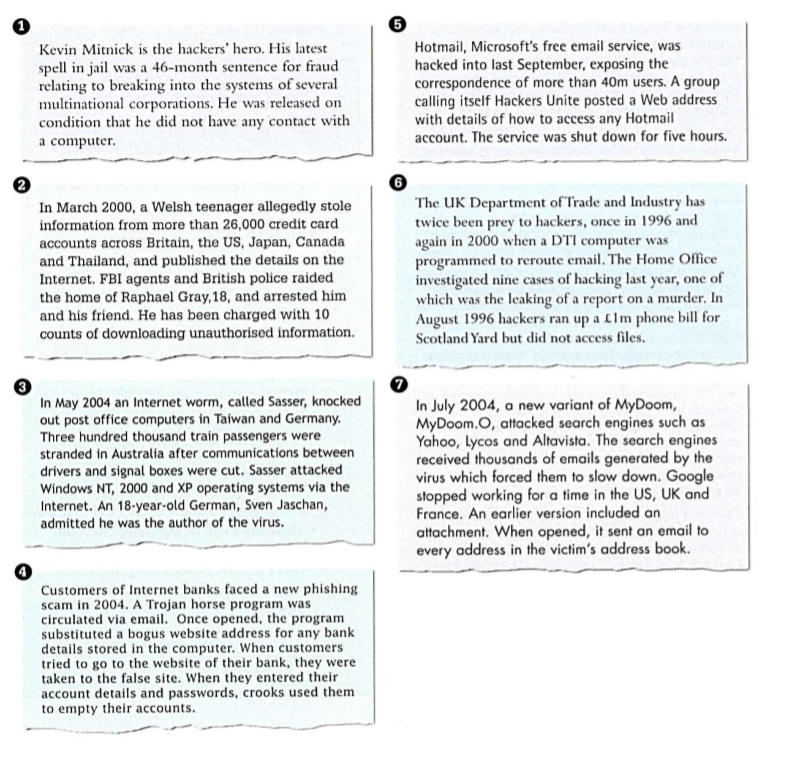
2 What kind of computer crime did internet bank customers face in 2004? *A Trojan horse program was circulated via phishing emails.*

3 Which hacker was sent to jail for fraud? *Kevin Mitnick*

4 What was the effect of the 1996 raid on Scotland Yard? *Hackers ran up a one-million-dollar phone bill for Scotland Yard*

5 Which of the cases reported here involved teenagers? *Case 2 & Case 3*

6 How did MyDoom.0 affect search engines? *MyDoom.0 send thousands of emails to the search engines which forced them to slow down.*



**F Listening**

**a Think about these questions before listening.**

1 How could you hack into a system?

2 How could you stop people from hacking into a system?

**b Listen to part 1 of the recording to check your answers to task A and to find the answers to these questions:**

1 What was Ralph arrested for?

2 What does he do now?

3 Why does he say people are too trusting?

4 What passwords does he suggest for trying to get into a system?

5 What does a firewall do?

6 What is the advantage of a call-back system?

7 To prevent hacking, what sort of passwords should you avoid?

8 What do event logs show?

**c Now listen to part 2 of the recording and find the answers to these questions:**

1 How did Ralph start thinking about computer security?

2 How did he find the most senior ID in the American company's system?

3 According to Ralph, why do people hack?

4 Why did he and his friend hack?

5 How did the police find him?

6 Why does he say companies should use his services?

7 Do hackers know each other?

8 What's the difference between Hollywood hackers and the real world?

9 How risky is credit card use on the internet?

10 What advice does he give for people intending to use credit cards over the internet?

**d Now listen to both parts again to find the answers to these questions:**

1 What evidence did Ralph and his friend leave to show that they had hacked into the American company's system?

2 What is a 'white hat' hacker?

3 What two ways does Ralph give for hacking into a system?

4 What terms does Ralph use to describe someone obsessed by computers?

5 How does he maintain contact with the policeman who arrested him?

6 How does he describe his lack of enthusiasm for the Hollywood hackers?

7 What does he mean by 'It's the retailers who get done'?

8 What's the problem with using smart cards for internet purchases?