1.4 Security

Candidates should be able to:

1.4.1

• show understanding of the need to keep data safe from accidental damage, including corruption and human errors
• show understanding of the need to keep data safe from malicious actions, including unauthorised viewing, deleting, copying and corruption

1.4.2

• show understanding of how data are kept safe when stored and transmitted, including:
○ use of passwords, both entered at a keyboard and biometric
○ use of firewalls, both software and hardware, including proxy servers
○ use of Secure Socket Layer (SSL)
○ use of symmetric encryption (plain text, cypher text and use of a key) showing understanding that increasing the length of a key increases the strength of the encryption

1.4.3

• show understanding of the need to keep online systems safe from attacks including denial of service attacks, phishing, pharming

1.4.4

• describe how the knowledge from 1.4.1, 1.4.2 and 1.4.3 can be applied to real-life scenarios including, for example, online banking, shopping

1.5 Ethics

Candidates should be able to:

• show understanding of computer ethics, including copyright issues and plagiarism
• distinguish between free software, freeware and shareware
• show understanding of the ethical issues raised by the spread of electronic communication and computer systems, including hacking, cracking and production of malware

Network

A computer network is a number of computers linked together to allow them to share resources. Networked computers can share hardware, software and data.

Most computer networks have at least one server. A server is a powerful computer that provides one or more services to a network and its users. For example, file storage and email.

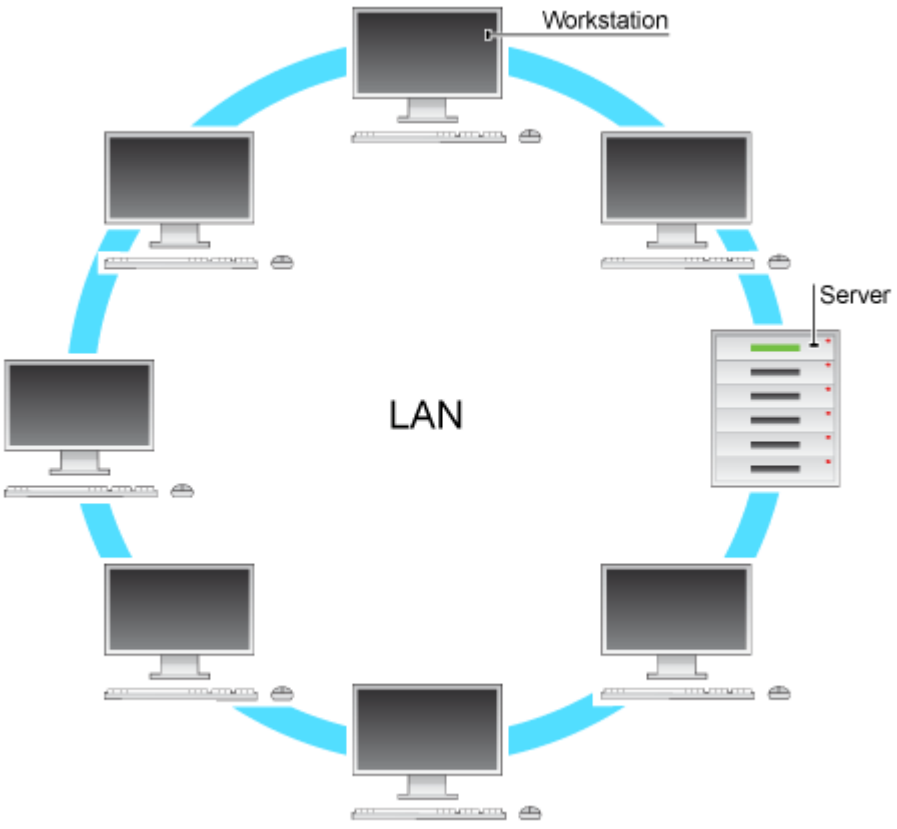
LANs and WANs

There are two main types of network:

1. Local Area Network (LAN)
2. Wide Area Network (WAN)

LAN

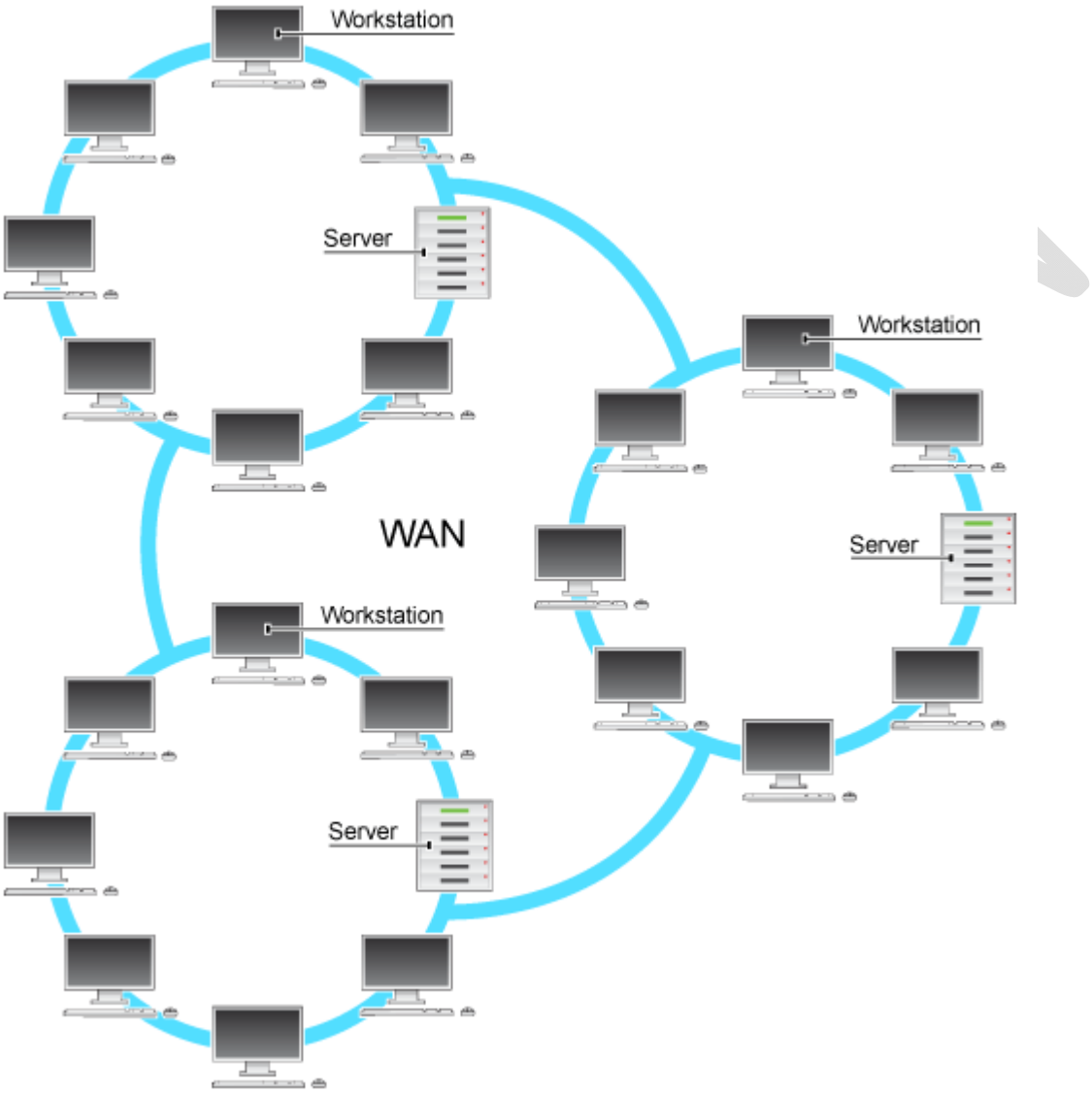
A LAN covers a small area such as one site or building, eg a school or a college.



LAN - Local Area Network

WAN

A **WAN** covers a large geographical area. Most WANs are made from several LANs connected together.



WAN - Wide Area Network

- The Internet is a WAN.
- A network of bank cash dispensers is a WAN.
- A school network is usually a LAN.
- LANs are often connected to WANs, for example a school network could be connected to the Internet.
- WANs can be connected together using the Internet, leased lines or satellite links.

Network & Data Security

As soon as your computer is connected to a network, you have to start thinking about **security** – security of your files, information, etc.

A network allows a person who does to have physical access to your computer (they are not sitting in front of it) to **gain access** all the same. If your computer is connected to a network, other people can connect to your computer.

A person who gains unauthorised access to a computer system is often called a **hacker**.

Preventing Unauthorised Access

There are a number of security measures that you can take to prevent hackers accessing your computer and all of the data stored on it:

Physical Security

The first thing to make sure of is that no unauthorised people can **physically access** (sit down in front of) any of the computers on your network.

For example, by **keeping office doors locked**.

Use a Username and Have a Good Password

The most common way to protect your computer's data is to setup **user accounts** with **usernames** and **passwords**. Anyone not having a username, or not knowing the correct password will be **denied access**.

For this to be effective passwords must be chosen that are **not easy to guess**. Passwords should be a random combination of lowercase letters, uppercase letters and numbers (and symbols if this is allowed):

- 'Weak' passwords: *password, 123456, david, 27dec1992*
- 'Strong' passwords: *s63gRdd1, G66ew$dQ, gdr298783X*

Some computer systems replace the typing of usernames and passwords with other forms of user identification such as **ID cards**, **fingerprint** readers, **voice-print** recognition, etc.

Always Install and Use a Firewall

A firewall is a device, or a piece of software that is placed **between** your computer / LAN and the rest of the network / WAN (where the hackers are!)

You can read about firewalls in the Networking Hardware section.

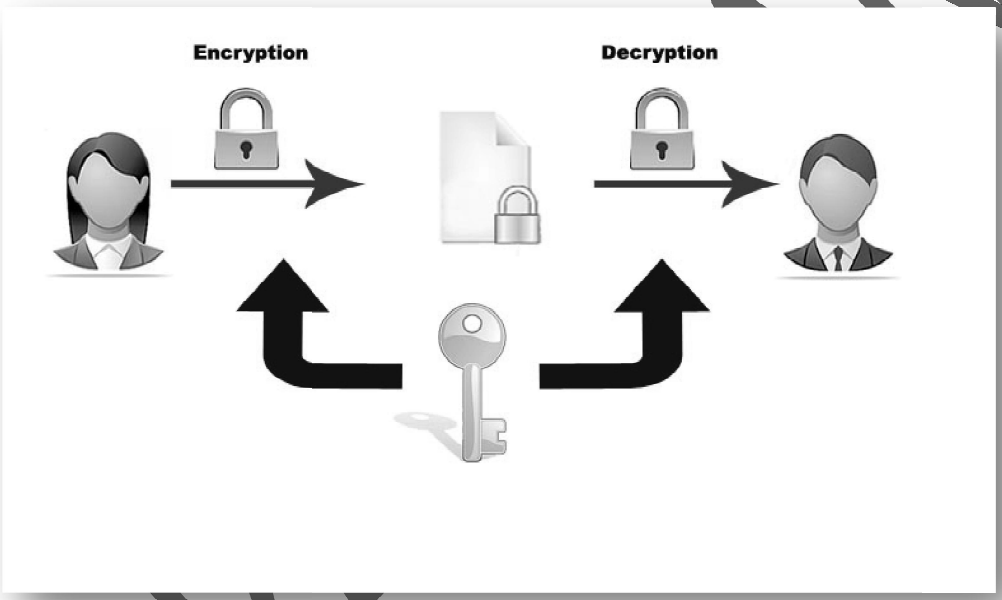
Securing Your Data

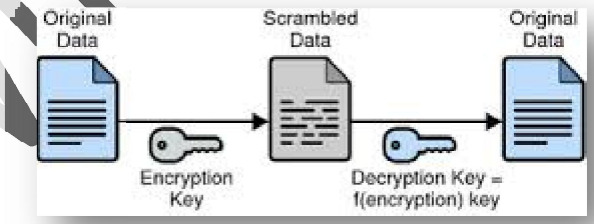
Often we have data that is **private** or **confidential**. This data needs to be protected from being viewed by **unauthorised** people. This is especially true if the data is to be sent via a **public network** such as The **Internet**.

The best way to protect data is to **encrypt** it...

Data Encryption

Encryption is the process of converting information into a form that is meaningless to anyone except holders of a 'key'.





Physical risks

Besides people, there are plenty of other ways that data can be lost or damaged. Here are a few more to think about.

Fire, floods and lightning damage

Although thankfully a rare occurrence, fires and floods do happen. They can cause immense damage and even total destruction of the computer equipment.

If you have been daft enough not to make a back up and store it somewhere other than the office, then it is pretty likely that all of your data is sitting on the now damaged machine and cannot be retrieved.

Theft of equipment

Computers are expensive, attractive items and can be a prime target for thieves.

If your computer is stolen and you haven't made a back up of your data then all of your hard work will end up walking out of the door with the thief.

Scratches on the hard disk

The platters inside a hard disk spin very quickly whilst a 'head' hovers less than a hair's width above them, reading the data.

If you don't shut your machine down properly this head crashes onto the spinning platter causing scratches.

If a scratch occurs just at the point your data is stored, it can be damaged and you might not be able to access it.

Back-ups

It's common sense to make copies of your work, but you would be amazed at how few don't do this.

Whilst you are working, you should remember to save your work every 5 minutes or so. It doesn't take a moment to press the 'save' button.

If you are sensible, you should also save your work as different versions, just in case your work becomes corrupted or you delete something by accident. You can then go back to an earlier version. O.K. you might have lost some work, but you won't have lost it all.

Besides backing up on the system you are using, you should also make a regular back up onto another piece of hardware, preferably something that is removable e.g. removable hard disk, magnetic tape, DVD-RW. This removable back up should be stored off site, so that if there were a fire, flood or theft, you would still be able to get hold of a copy of your data and reinstall it.

Backing up should use the 'grandfather, father, son' method. The daily or 'Son' backups are rotated on a daily basis with one graduating to Father status each week. The weekly or Father backups are rotated on a weekly basis with one graduating to Grandfather status each month.

Physical protection

As you have seen, there are many different ways that you or a business can lose valuable data. With a little bit of planning and thought however, the risks can be reduced or even eliminated.

There are many things you can do to make your equipment more secure:

- Lock the room when not in use

- Use swipe cards or keypads to activate locks

- Bolt computers to the desk

- Use special pens to mark your postcode onto the computer case

- Keep windows shut - especially if on the ground floor. Use bars.

- CCTV video cameras

- In large firms, security guards

Note: in an exam, you would generally only give one example from the list above and then go on to discuss the other methods below.

Unless specifically asked to discuss physical security, don't just list the points from this section.

Software protection

Firewall

A firewall is a program or hardware device that filters the information coming through the Internet connection into your personal computer or into a company's network.

It is set up to allow mainly one way access, i.e. you can go out onto the Internet and access pages, but it checks everything coming back against a set of rules. If the data coming back is from an unauthorised source, then it is blocked.

You may have heard people saying, 'I can't get on that site at school because it's been blocked'; that is the firewall in action.

Software protection

Anti-virus software

This is special software which is used to detect viruses and to limit their damage by removing them.

The software tries to detect viruses before they can get access to your computer. If a virus is detected trying to get through the firewall, the software will give an alert and ask how you want to respond.

It is important that anti-virus software is updated regularly by going to the manufacturers site. Although the software was up-to-date when you bought it, within a few weeks, new viruses will have been released which your software won't know how to detect.

The manufacturers provide downloads to make sure that your software can identify all of the latest threats.

It is also important to run an 'anti-virus' scan regularly, just to make sure that there aren't any viruses lying dormant on your system.

Software protection

User IDs and Passwords

When you log onto your network at school, you have to type in your User ID and Password. This identifies you to the network as an authorised user.

Any sensible company will ensure that staff need a User ID and Password to gain access to the system. This should reduce the risk of outsiders being able to get onto the system and damage data.

People should follow rules when choosing their password:

- passwords should be kept secret at all times

- passwords should not be something that is easy to guess such as pet's name or favourite football team.

- passwords should include text and numbers or symbols

- passwords should be a reasonable length e.g. over 6 characters

- passwords should be changed regularly

Software protection

Audit Log

A very good way of tracing back a problem is for the system to keep an audit log.

This means the computer will record every important event in an 'audit file. It records who saved what and when. Who deleted records or changed them. For example an audit record may look like this:-

User: bigears233

File: TheMostImportantFile.doc

Changed: 3rd January 10:15am

(or Deleted, or Saved).

Data security

Data security is about keeping data safe. Many individuals, small businesses and major companies rely heavily on their computer systems.

If the data on these computer systems is damaged, lost, or stolen, it can lead to disaster.

Key threats to data security

Data may get:

- lost or damaged during a system crash - especially one affecting the hard disk
- corrupted as a result of faulty disks, disk drives, or power failures
- lost by accidentally deleting or overwriting files
- lost or become corrupted by computer viruses
- hacked into by unauthorised users and deleted or altered
- destroyed by natural disasters, acts of terrorism, or war
- deleted or altered by employees wishing to make money or take revenge on their employer

Keeping data secure

Measures that can be taken to keep data secure include:

- making regular backups of files (backup copies should be stored in fireproof safes or in another building)
- protecting yourself against viruses by running anti-virus software
- using a system of passwords so that access to data is restricted
- safe storage of important files stored on removable disks, eg locked away in a fireproof and waterproof safe
- allowing only authorised staff into certain computer areas, eg by controlling entry to these areas by means of ID cards or magnetic swipe cards
- always logging off or turning terminals off and if possible locking them
- avoiding accidental deletion of files by write-protecting disks
- using data encryption techniques to code data so that it makes no apparent sense

Online banking

When you bank online, after you've logged in, you will notice that the http in the address bar has changed to **https**. This indicates that a secure connection between your computer and the bank's computer has been established. Data sent between the two computers is encrypted so that anyone trying to intercept your data will receive meaningless data. The data can only be decrypted into readable data by using a key that is known only to the two computers - yours and the bank's.

Secure Sockets Layer (SSL)

Transport Layer Security (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), are cryptographic protocols designed to provide communications security over a computer network.

Data Protection Act

The **Data Protection Act** 1998 (DPA) is an **Act** of Parliament of the United Kingdom of Great Britain and Northern Ireland which defines UK law on the processing of **data** on identifiable living people. It is the main piece of legislation that governs the **protection** of personal **data** in the UK.

stored electronically is easier to misuse; that software should not be copied without permission; the consequences of software piracy; that hacking can lead to corruption of data, either accidentally or on purpose.

Types of computer misuse

Misuse of computers and communications systems comes in several forms:

Hacking

Hacking is where an unauthorised person uses a network, Internet or modem connection to gain access past security passwords or other security to see data stored on another computer. Hackers sometimes use software hacking tools and often target, for example, particular sites on the Internet.

Data misuse and unauthorised transfer or copying

Copying and illegal transfer of data is very quick and easy using online computers and large storage devices such as hard disks, memory sticks and DVDs. Personal data, company research and written work, such as novels and textbooks, cannot be copied without the copyright holder's permission.

Copying and distributing copyrighted software, music and film

This includes copying music and movies with computer equipment and distributing it on the Internet without the copyright holder's permission. This is a widespread misuse of both computers and the Internet that breaks copyright regulations.

Email and chat room abuses

Internet services such as chat rooms and email have been the subject of many well-publicised cases of impersonation and deception where people who are online pretend to have a different identity. Chat rooms have been used to spread rumours about well known personalities. A growing area of abuse of the Internet is email spam, where millions of emails are sent to advertise both legal and illegal products and services.

Pornography

A lot of indecent material and pornography is available through the Internet and can be stored in electronic form. There have been several cases of material, which is classified as illegal, or which shows illegal acts, being found stored on computers followed by prosecutions for possession of the material.

Identity and financial abuses

This topic includes misuse of stolen or fictional credit card numbers to obtain goods or services on the Internet, and use of computers in financial frauds. These can range from complex well thought out deceptions to simple uses such as printing counterfeit money with colour printers.

Viruses

Viruses are relatively simple programs written by people and designed to cause nuisance or damage to computers or their files.

How to prevent computer misuse

The Computer Misuse Act (1990)

This was passed by Parliament and made three new offences:

1. Accessing computer material without permission, eg looking at someone else's files.
2. Accessing computer material without permission with intent to commit further criminal offences, eg hacking into the bank's computer and wanting to increase the amount in your account.
3. Altering computer data without permission, eg writing a virus to destroy someone else's data, or actually changing the money in an account.

The Data Protection Act

This was introduced to regulate personal data. This helps to provide protection against the abuse of personal information. Find out more about the Data Protection Act.

Copyright law

This provides protection to the owners of the copyright and covers the copying of written, musical, or film works using computers. FAST is the industry body which is against software theft. You can find out more about it in the Copyright section.

There have been cases where laws such as Copyright have been used to crack down on file sharing websites or individuals who store and illegally distribute copyrighted material, eg music. There is a massive problem with many people around the world obtaining copyrighted material illegally.

Close down chat rooms

Some chat rooms have been closed down due to abuses, especially where children are vulnerable. Some have moderators who help to prevent abuses. Advice about sensible use is important; especially to never give personal contact details or arrange meetings without **extreme caution**.

Reduce email spamming

This may be reduced by:

- never replying to anonymous emails
- setting filters on email accounts
- reporting spammers to ISPs, who are beginning to get together to blacklist email abusers
- governments passing laws to punish persistent spammers with heavy fines

Regular backups and security

Just making something illegal or setting up regulations does not stop it happening. Responsible computer users need to take reasonable steps to keep their data safe. This includes regular backups and sufficient security with passwords.

SECURITY AND ETHICS WORKSHEETS

May/June 2004

Q1) (a) State **two** effects of a computer virus.

1.....

.....

2.....

..... [2]

(b) State **two** ways of protecting computers against viruses.

1.....

.....

.....

2.....

.....

..... [2]

May/June 2005

Q2) Data Protection Rules give legal rights to individuals and state that personal data stored on computer systems must be kept secure.

(a) Give one legal right for individuals.

.....

..... [1]

(b) Give one software method of protecting personal data.

.....

..... [1]

(c) Give one hardware method of protecting personal data.

.....

..... [1]

May/June 2006

Q3) Give one effect of hacking.

.....

..... [1]

(b) Give two ways of protecting computer systems against hacking.

.....

..... [2]

May/June 2007

Q4) Computer systems can be affected by viruses.

(a) What is a virus?

.....

..... [1]

(b) Give one effect of a virus.

.....

..... [1]

(c) How can a system be protected from viruses?

.....

..... [1]

(d) Why would backing up data not guard against the effect of a virus?

.....

..... [1]

May/June 2009

Q5) Jon decides to buy a notebook (laptop) computer which he connects to the internet using aWiFi (wireless) broadband connection. Describe four security issues.

1.....

..... [1]

2.....

..... [1]

3.....

..... [1]

4.....

..... [1]

May/June 2010

Q6) A company is concerned about three aspects of the security of data stored in computer files:

- data corruption
- data loss
- illegal access to data

For each of the above, give one reason why it could occur and state one method ofprevention. Your reasons must be different in each case.

Data corruption.....

Reason: .....

..... [1]

Data corruption.....

Prevention: .....

..... [1]

Data loss.....

Reason: .....

..... [1]

Data loss.....

Prevention: .....

..... [1]

Illegal access to
data.....

Reason: .....

..... [1]

Illegal access to
data.....

Prevention: .....

..... [1]

May/June 2010

Q7) Give four features of a Data Protection Act.

.....

..... [1]

.....

..... [1]

.....

..... [1]

.....

..... [1]

Q8) A bank is worried about computer crime.

One of their concerns is online access to customer accounts.

(a) How can a customer's access details be discovered by criminals?

.....

.....

.....

..... [2]

(b) Why would a customer using a credit card for online shopping be more of a security risk than a customer using the same card in a shop?

.....

.....

.....

..... [2]

(c) Describe what measures the bank can take to safeguard customer accounts.

.....

.....

.....

..... [2]

May/June 2011

Q9) A worker at a company has to go through a logon procedure to gain access to her computersystem.

(a) The first thing she has to do is type in a user name and a password.

Why is this done?

.....

.....

..... [2]

(b) The password is typed in twice.
Why is this done?

.....

..... [2]

A menu then appears on her screen. She chooses to connect to the Internet.
(c) Describe two ways her computer system is protected against loss or corruption of filesonce the computer system is connected to the Internet.

.....

.....

..... [2]

(d) The worker leaves her computer system for a 10-minute break.
(i) From a health and safety aspect, why does she need to take a regular break?

.....

.....

..... [2]

(ii) Apart from switching off her machine, how could she ensure her computer system was secure whilst taking her regular break?

.....

.....

..... [2]

May/June 2012

Q10) Describe ways to guard against each of the following Internet security issues. (A differentmethod should be given in each case.)

Viruses.....

.....

hacking.....

.....

spyware.....

.....

phishing.....

.....

tapping into wireless
networks.....

.....

SECURITY AND ETHICS WORKSHEETS

Q1) (a) Any two from e.g.

- memory used up/slows down computer/alters setting/systems failure
- erases files/erases data/corrupts data/data needs restoring
- infects other computers on network
- production loss/financial loss [2]

(b) Any two from

- do not allow outside floppy disks/CD's/DVD's
- use disk free work stations
- download/install and use anti virus software
- scan hard disks regularly
- update the anti virus program regularly
- do not open file attachments from unknown sources/download
- doubtful software from the Internet
- do not use files that come from unknown sources
- buy original software/do not buy pirated software
- use firewalls [2]

Q2) Award 1 mark each:

(a) legal right – right to view/check/change/correct data [1]

(b) software method – checking passwords/codes/fingerprints/

- retina scans/biometric devices
- encryption of data
- firewalls
- install dial back [1]

(c) hardware method – lock keyboard/computer/doors

- use memory sticks/removable drive/external hard
- drive [1]

Q3) (a) One effect from

- fraud/transferring money
- viewing sensitive confidential data
- changing data
- selling data
- virus/logic bomb

- blackmail
- loss of data/file
- misuse + qualification [1]

(b) Two ways from

- passwords/codes
- encryption
- monitoring attempts to access the system/logging use
- lock keyboard/computer/doors
- firewalls
- smart card
- fingerprints/biometrics
- do not read emails from unknown sources
- USB security device [2]

Q4)
(a) program/software/code which replicates itself/copies itself [1]

(b) Any one from:

- loss/damage to computer files/data
- can cause computer to crash/run inefficiently/run abnormally
- attach itself to other files [1]

(c) Any one from:

- use of (up to date) anti-virus software
- don't use disks/CDs/DVDs/memory sticks from unknown sources
- only read/open emails/attachments from known sources
- use of firewalls
- (NOTE: backups, passwords, encryption, don't connect to internet, do not protect against
- viruses) [1]

(d) Any one from:

- wouldn't stop actual computer being infected
- back up files themselves may already have virus attachments
- if computer infected, re-installed files would then also be infected [1]

Q5) any four from:

- hacking into his computer and change/read files
- viruses could be sent
- somebody “tapping into” his WiFi system
- credit card details being stolen
- bogus web sites
- stealing his computer (with security information on hard drive, for example)
- physical eavesdropping in a public place/shoulder surfing
- driving round looking for wi fi access/ WarDriving [4]

Q6) Any three different reasons and associated preventions

(prevention must match reason):

1 mark for reason, 1 mark for prevention

award each point only once

data corruption and data loss

- viruses -use anti virus software, firewalls, no Internet access
- power loss – back-ups, UPS
- malicious damage – back-ups, password protection, controlled access
- computer crash – back-ups, parallel computer (systems)
- damage to CDs/disks – back-ups
- operator error – training / good user interfaces

illegal access

- hacking/unauthorised access – passwords, log-in ids, anti-hacking software
- (physical) lock room/computer
- computer left logged on – log off when not in use, lock computer [6]

Q7)

Any four features from:
– data must be up to date
– data can only be read/used for the purpose for which it was collected
– data must be adequate, relevant and not excessive
– data must be accurate
– data must be destroyed when no longer needed/don’t keep longer than necessary
– data user must register what data stored
– data must be used/collected fairly and lawfully

– data must be held securely
– data must be protected from accidental damage
– only authorised personnel can have access to the data
– fines are imposed for data mis-use
– data should not be passed on to a third party without permission
– a person can view data and have it changed/removed if incorrect
– safe harbour (countries with DPA at least as good) [4]

Q8)

(a) 1 mark each for 2 concerns
OR 1 mark for concern + 1 mark for expansion:
– customer goes online in a public place …..
…… and is overlooked as they enter id/password/PIN
– customer receives emails taking them to a false site …..
….. where they are asked to confirm details by entering them
– customer downloads virus, spyware, …..
….. which logs all key presses including id/password/PIN [2]

(b) Any two points from:

– don't need card number for online transaction/card number already
– online user is anonymous/not visible
– online the customer does not need the card and signature/PIN [2]

(c) Any two points from:
– secure sites using encryption
– use of passwords/PINs/biometrics/advice to change PIN regularly
– no communications with customer requiring personal details
– use of home card readers that generate codes known only to bank and customer
– check with customer at each log on when they were last logged on to the website
– contact customer if unusual transaction/random check
– customer asked to inform bank if intending to use card in another country
– customer asked to inform bank if card lost/stolen
– ensure firewall is in place [2]

Q9) (a) Any one from:
– prevents unauthorised access to files/the computer system
– access to her own directories
– allow authorised access [1]
(b) Any one from:
– verification check
– (double check) password is correct [1]
(c) Any two from:
– firewall
– anti-virus software
– (automatic) backup of data
– auto-save [2]
(d) (i) Any one from:
– repetitive strain injury (RSI) / pain in wrist/fingers
– carpal tunnel syndrome
– headaches/eyestrain/back ache/neck ache [1]
(ii) Any one from:
– "lock" computer system
– automatic screen saver (after short time of inactivity)
– log off from the system
– if computer in an office, lock the office door [1]

Q10)

viruses e.g.
– use anti-virus software // regular virus scans
– don't open/use disks // don't open email attachments from unknown sources
Hacking e.g.
– passwords / user IDs
– firewalls
Spyware e.g.
– anti-spyware software
– delete cookies at end of session
Phishing e.g.
– don't open emails from unknown sources
– don't divulge personal information via email / unsecure website
– ensure that the site viewed has a valid security certificate (SSL)
tapping into wireless networks e.g.
– secured wifi network (protected by passwords)
– encryption / WEP
– no broadcast of network ID [5]