Chapter 8 : Safety

Passwords :

 - too short

 - Easy to guess : Personal information used in password

 -Doesn't contain a mixture of upper case, lowercase, numbers or symbols

Use of strong passwords
Do not use pet names
Do not use personal information
Do not use birthdates
Do not use a password they have used before
Do not use company name

Hard passwords :

Conforms to company rules
Hard to guess
Stop shoulder surfing
Hard to crack

How to manage passwords :

 -Change passwords regularly

 -Use a strong passwords

 - Don't tell anyone else the password

 -Don't write the password down

Explain the need for copyright legislation

It helps to prevent the unauthorised copying of the software
It helps to prevent the unauthorised lending/renting of the software
It gives the author legal protection

Describe four ways that the software houses can help to prevent copyright being broken

A license agreement between the user and the software developer
A unique licence key is used when the software is installed
Software only runs if DVD/CD/Pen Drive is present
Use of a dongle/card plugged into the computer
Holographic sticker which cannot be photocopied shows the product is real
Software built into the program to stop it being copied

Explain what is meant by a virus and how it affects the operation of a computer

A piece of software/malware
Has the ability to replicate itself

Max **two** from:
It corrupts data in the computer
Deletes data in the computer
Fills up memory
Slows the operation of the computer

Explain how key-logging software works.

Records every keystroke on the keyboard
Saves it in a log file
Transmits the log file back to the hackers
Can read a password being typed in
The person is unaware it is happening

Discuss the advantages and disadvantages of social networking rather than email as a means of communication.

Social networking messages can be available to/seen by all
Security settings can restrict who reads/makes the comments
Communication can take place in a (private) chatroom
Comments can be liked/disliked/shared
Don't need to learn email address
Live video/audio calls can be made/streamed
Emails tend to be one to one
Can share live videos
You know who's online
Larger upload size than email

Emails are private between the sender and recipient // more secure
Messages can be alerted as high priority
Attachments can be used
Emails tend to be more formal
Auto reply / forward / reply can be used
In social networking makes a person more prone to cyber predators/trolls

Explain what is meant by Secure Socket Layer (SSL).

Communication protocol
Security technology
Encrypted link between the server and the client

Describe the features that you would look for in a browser to indicate it has a secure connection to a website.

The URL will start with HTTPS
A padlock appears as an icon on the web page
SSL security certificate warning
The background colour of the URL is set to green

Explain what is meant by hacking and the effect it can have on the data or the computer.

Unauthorised access to computer systems   1 mark

Any **one** from: 1 mark
Data on the computer system can be corrupted, edited, deleted, viruses added
Data on the computer system can be copied/stolen/misused
Data on the computer system can be accessed/read

Any **two** from:
HyperText Transfer Protocol Secure
Secure version of HTTP
All data is encrypted
Secure protocol identifier

Any **two** from:
Uniform Resource Locator
A reference/identify to a resource on the WWW/internet
Used as a simple way of addressing a resource

Signs of a virus
She has not much space left on her hard disk even though she had previously
Her computer is performing routine tasks a lot more slowly.
Pop ups keep appearing on her screen at random.
Her friends keep telling her that emails about strange things are being sent by her
Random reboots
Software errors
Recycle bin not working
Computer hanging
Anti-virus stops working

Describe the processes a web browser has to go through to load a web page.
Request made by entering a web address/URL or clicking on a link
Retrieves code from the server/resources downloaded
Interprets the code as a web page/uses page resources to build page
The web page is displayed/renders page to view

HTTP is not secure/HTTPS is secure…
…uses SSL/HTTP does not use SSL
HTTPS transmits data over the internet in an encrypted form/HTTP transmits data over the internet in an unencrypted form
HTTPS requires additional processing power in its servers which could result in slowdown of responses   [2]

Prolonged use of the keyboard
RSI/carpal tunnel syndrome

Any **one** from:
Use a wrist rest
Regular breaks to relax the hands
Stretching exercises
Use of an ergonomically designed keyboard

Looking at a monitor for a long period of time
Eye strain/headache/dry eyes

Any **one** from:
Resting the eyes by looking in the distance
Cutting down on glare
Making sure the screen is at eye level
Use of blue screen technology
Use of flat screen technology

Sitting too long in one position
Back problems/DVT

Any **one** from:
Foot rest
Taking breaks
Ergonomic/adjustable chair

Weak password is easy to guess/strong password is difficult to guess
Weak passwords consist of all letters or all digits or all digits with one letter/all letters with one digit
Weak password is one that has few characters
Strong password uses mixture of upper case letters, digits and punctuation marks
Weak password has repeated characters
Weak password has characters next to each other on a QWERTY keyboard
Weak passwords are ones that are similar to the user name
Weak passwords are passwords that relate to the user

HyperText Transfer Protocol
HTTP is a communication protocol used on the internet to allow communication between two computers (devices)
HTTP is an application protocol/set of rules
HTTP is the foundation of data communication for the World Wide Web   [2]

Image	Safety issues	Minimise the risk
	Tripping over trailing wires/cables	Any **one** from: Use covered cable runs Tie cables to wall Cover cables with carpet Use wireless Organise wires
	Electrocution from spilling drinks	Any **one** from: Do not take drinks/food into computer room Keyboard covers
	Fire from overloaded sockets	Any **one** from: One plug per socket/reduce the load on the socket Use of RCB
	Fire from overheating	Any **one** from: Use of CO_2 fire extinguishers Fans and cooling from open windows/good ventilation

Describe other measures that should be taken to ensure that playing online games is safe for young people.

Be vigilant of others attempting to gain access to your data
Use up to date internet security software…
…antivirus, anti-spyware, firewall
Avoid giving out personal data (**not name**)
e.g. password, home address, email, age, (mobile)phone number
Be aware of addiction e.g. playing for too long
Be aware of hidden costs…
…read terms and conditions
Play authorised games that have a licence/trusted sites
Choose a user name that does not contain personal information
Use strong passwords
Keep the game up to date
Do not use identifiable images

Explain what is meant by encryption of data.

Scrambling of data
Converting data into an unreadable form
Protects sensitive data
Requires an encryption key/decryption key/key to encrypt data
Requires a decryption key/encryption key/public or private keys to decrypt data

Explain what is meant by a digital certificate.

Allows people/organisations/computers to exchange secure information over the internet
Uses a PKI (Public Key Infrastructure)
Unique key used by the sender and receiver

Examples for advantages of social networking
Increase the number of friends worldwide
Send and receive live images instantaneously
Real time information sharing
Common groups can be formed more easily i.e. friends or social grouping and these keep in contact
easier to advertise
…to a larger number of people
easier to publicise events/activities
…music videos
Speed of news increases
Similar interests can contact each other

Examples for disadvantages of social networking
Reduces face to face communication/relationships
Problem with sarcasm increases as it appears as rudeness
Cyber-bullying increases
Grooming increases
Harder to ignore people
Risks of fraud increases
Risks of identity theft increases
Risks of burglary as holiday reporting increases
Time wasting increases
Invasion of privacy increases
Addiction to social networking
Needs the internet
Needs computer/device

Evaluate your own use of computers in terms of health. Include any strategies you have devised.

using the computer for a long period of time can affect my eyes/cause headaches...
...take regular breaks to help with eye strain/headaches

hunching over the computer for a long period of time gives back ache/neck ache...
...Using an ergonomic chair could stop this

Typing for a long period of time or by resting wrists on the table gives RSI...
...therefore a wrist rest/ergonomic keyboard is needed to reduce this.

Eye strain can be caused by looking at the screen too long...
...this is solved by placing a screen filter/using TFT technology

Tripping over loose wires...
...tie them to the walls or under carpet / use cable runs / use wireless

Heavy equipment falling...
...sturdy tables needed / heavy equipment placed in centre of table

Electrocution caused by spilt drinks / food...
...do not take drinks to computer

Fire from overloaded sockets...
...use CO_2 fire extinguisher
...don't use 4 way adapters
...keep the computer room well ventilated

Data monitoring
  Monitoring phone call usage
  Monitoring emails
  Monitoring the time spent on and websites visited
  Monitoring the use of printers / number of copies
  Monitoring where employees log in / log out
  Monitoring when employees log in / log out
  Monitoring failed log ins
  Monitor the amount of storage space used
  Monitoring where they send data to print

Describe the e-safety issues that she should be aware of before she publishes this web page

She should not display pictures of herself in school uniform
She should not display personal details
She should not identify the school
She should make sure the picture is not too revealing
She should use appropriate language
Should not post her email address/contact details
Allow she should be aware of identity theft
Allow she should be aware of online sexual exploitation
Aware that everyone has access to published data

Discuss the advantages and disadvantages of different methods you could use to help minimise the health problems of using the computer.

Advantages
Max **four** marks:
- If the screen is 90 degrees to the window it reduces the glare/eye strain
- If you use a screen filter/blue glasses eye strain is reduced
- If LCD/TFT screens are used then eye strain is reduced
- If my eye is level with the top of the screen it will reduce eye strain/neck ache
- If I take breaks from excessive clicking on the mouse/keyboard this reduces RSI
- Using voice activated systems reduces RSI
- If I use a wrist rest/an ergonomic mouse it will reduce RSI
- If I use an ergonomic chair it will reduce back ache
- If I do not use the computer for long periods of time this will reduce
- RSI/back ache/eye strain/Carpel syndrome/Cubital syndrome/Neck pain/DVT

Disadvantages
Max **four** marks:
- Turning the screen can reduce your ability to see clearly on the screen
- Laptops can be difficult to ensure the screen is 90 degrees as the whole unit needs to be moved
- The cost of safety equipment can be expensive
- Using voice activated systems can be prone to many errors which may increase RSI correcting them
- Users can become over-reliant on equipment
- With laptops/screens it can be difficult to position it so the eye level is at the top of the screen
- Taking breaks every hour can increase the work time

http:// – this is a protocol/transfer protocol/hypertext transfer protocol
www.bbc.com – this is the website address contains domain name, domain type and country code/server
weather – this is the folder name
2193733 – this is the resource or the filename

Moderated and unmoderated forums

A moderated forum is checked/maintained by a moderator/administrator
Moderated forums can reduce freedom of speech/can be biased/Un-moderated forum allows people to post what they like
The moderated forum does not allow inappropriate comments to be posted on the site
Examples of inappropriate language: racist, offensive, swear words, phishing attempts, spam, abusive, unrelated comments – Minimum of 2 examples gains a mark
In a moderated forum those who continually break the rules are banned
Un-moderated tend to be used for spam attacks or phishing attacks
Moderated may be more expensive as they have to appoint a moderator
Posting of moderated comments are delayed as they have to be checked

One from
Both are interactive websites
Both are discussions
Both require networked computers

Electrocution – 1 mark
One from:
No drinks/food allowed in the computer room
Make sure all electrical sockets equipped with RCB/Residual Circuit Breaker
Cover all loose wires
Check the equipment regularly

Fire – 1 mark
One from:
Use a CO_2 fire extinguisher
One plug for one socket
Do not overload sockets
Reduce the need for 4 way adapters

Tripping over trailing cables – 1 mark
One from:
Use cable ducts/place cables under carpet
Fasten cables to the wall
Use wireless
Organise cables

Injuries caused by heavy equipment falling off tables – 1 mark
One from:
Use sturdy tables
Place equipment in the middle of the table

Describe how Sukhjit would recognise a phishing email.

Check the name of sender matches the content of the email
Check any URL link matches the content of the email
Might contain grammar/spelling mistakes
Check plain text
Check the message is not an image
Check if the message is asking for personal information
Might contain unexpected attachments
Urgent/too good to be true
Not address the user by name/generic name used
Might be in your SPAM emails/alerted by service provider

Effects of virus on a computer :
Replicates itself and can fill the computer's memory/hard disc with unwanted
data
Can communicate with other systems
Causes computer to crash
It can delete/corrupt data
Causes the computer operations/system/processes to run slowly/become
unusable
Makes software/OS unusable
Can corrupt/erase contents of hard disc

Reduce risk of viruses
Run up to date anti-virus software/Install anti-virus software
Do not download files/attachments from email addresses that you do not
recognise
Do not download files/games/software from untrusted/unfamiliar website
Scan all emails before opening
Check/scan attachments to emails for viruses
Avoid opening spam emails

Describe four strategies that you could use to minimise the dangers of using social networking sites to
make new friends.

Know how to block and report unwanted users,
Never arrange to meet anyone alone
Always tell an adult first when arranging to meet someone
Always meet in a public place
Avoid inappropriate disclosure of personal data/set privacy settings/Avoid giving email address or
phone number when chatting
Avoid inappropriate disclosure of your own name/Avoid giving your full name
Avoid giving your address
Avoid giving your school name
Avoid displaying a picture in school uniform
Do not display pictures taken at home/Do not display pictures taken of the school with the name
attached/Do not send pictures/videos of yourself to strangers
Ensure that the person you are befriending has very secure privacy settings
Check profiles before contacting people
Verify person's contact details with other trusted people/friends   [4]

Explain the strategies that you could use to protect yourself and your computer whilst using emails.

Never open/download attachments/links from people you do not know…
…as they may contain viruses/allows others to know the email address is live
Never open emails from unknown sources…
…as they may contain viruses
Scan all emails using an up to date anti virus…
…as new viruses are always being created
Keep the number of contacts to a minimum…
…as some viruses send emails to all names in your contacts list
Do not use auto reply to emails…
…allows others to know the email address is live
As the email may be sent to people who should not see it…
…do not use reply all
…check names that you are replying to
When replying always use a subject…
…as people may not open emails without this as they think they are spam
When replying remove extra information that was sent…
…to stop others seeing things they shouldn't
Watch sarcasm as it is not conveyed on the messaging
Use netiquette
Use a spam filter…
…clear SPAM regularly
Do not reply to spam emails…
…as the spammer can see that your email address is live
Do not give personal details in the email
Do not reply to emails from unknown sources

Hacking :

Unauthorised access to computer systems with the intention of causing harm

Two examples from:

Editing files/data
Deleting files/data
Installing viruses
Exposing weaknesses of the system

Describe the measures that should be taken to help protect data from being hacked.

Usernames and strong passwords to stop remote and local logins
Use different passwords for different accounts
Biometric systems to ensure the official user is present
Electronic dongles which only allow login when the dongle is plugged in
Dedicated computers which are the only ones allowed to log in

Describe two advantages of using a web browser rather than a search engine.

If using a web browser, only the URL is needed.
If a URL is typed in a web browser the website is found straight away.
Resource may not be on search engine index yet, therefore cannot be found.
In the search engine the user needs to know what is on the website for the keywords.
Not sharing information with a search engine if you type in a URL

Give three actions that would break copyright.

Making a copy and giving it away to a friend or colleague without permission
Making a copy and lending it without permission
Making a copy and selling it without permission
Making a copy without permission from the author/licence holder
Using a single copy with multiple simultaneous use on a network
Using coding/images from the original copy in your own programs/modifying the original code
Renting out the original copy without permission

Discuss the advantages and disadvantages of using biometric systems rather than more traditional security methods.

Advantages
Biometrics are unique…
…so others cannot sign people in/whereas with password/card systems someone else can sign you in.
Fingerprints/eyes are always with you…
…but a password/card can be lost.
Cannot be forgotten passwords can be forgotten
The user has to be present therefore more secure.
Typing in passwords can lead to errors on data entry…
…biometrics tend to be more reliable.
More difficult to forge…
…passwords can be copied/cards can be stolen.

Disadvantages
Personal liberty infringement…
…fingerprints/biometric must be stored.
Method is slower to enter system than passwords.
Equipment and setup is more expensive than producing cards.
The time taken to set up a store of fingerprints/eye prints can be a long time…
…quicker to set up a database of passwords.
If the finger is damaged/dirty it cannot be read passwords can be more reliable.
If dark glasses are worn retina cannot be read passwords are more reliable
If a voice is not understandable on a voice recognition system may not work.
Facial hair can stop facial recognition passwords are more reliable

A mark can be awarded for a reasoned conclusion
If one side of the argument i.e. all advantages/disadvantages then 3 marks max.
If both sides have been addressed but without expansions/differences then 4 marks max   [6]

Describe three ways in which John could protect his home computer from being infected

Scan the pen-drive as it is inserted into his computer
Use an anti-virus software to scan his computer hard drive
Do not use media from an unknown source
Install/download up-to-date anti-virus software and activate/update anti-virus software/use up-to-date antivirus

Describe what John should do to remove the threat of the computer virus infecting other files
Identify the virus using anti-virus software/scan the file
Option given to delete or quarantine the file
Software quarantines the virus infected file so the virus cannot be activated
Delete the virus/clean/disinfect the file
Check the quarantined file to see if it is safe to open

Smishing

One from:

Never text back to unknown sender
Never respond to any of these types of texts
Never click on any links within the text message
Never give out personal information in a text
Don't allow your mobile phone number to be included in call lists
Blocking unfamiliar texters/numbers

Pharming:

One from:

Use up to date anti-virus/anti-pharming/anti-spyware software
Check address bar for strange web addresses
Keeping DNS servers patched and up to date
Use up to date firewall services on DNS servers

Cookies are sometimes seen as a security threat when in reality they are only a nuisance. Explain, using an example, what cookies are and why they are important to companies.

One from:

A small text file sent/downloaded to a user's web browser when they visit a web site

Two from:

Store information about the visit and are used the next time the user visits the site
Remember the user's details
Remember the user's preferences
Remember items a user bought
Remember passwords
Remember what they searched for
Target products
Offers a tailored experience for users

Describe three strategies that students should use to stay safe when on the World Wide Web.

Only use websites recommended by the teacher
Only use websites ending in .gov, .ac, .org, .edu
Use a learner friendly search engine
Use appropriate search conditions

Describe three strategies that students should use to stay safe when sending and receiving emails.

Only email people already known to you/do not reply to spam emails
Think before opening an email from an unknown person
Never email the school's name
Never use personal details in emails
Never send a picture of the student in school uniform
Only use contact us from a known website
Scan all attachments before downloading them/do not open attachments from unknown people
Check the email address is correct before sending
Check the content of the email before sending

Eye problems/strain
    Take regular breaks/use no-flicker screens/LCD/TFT screens/have eyes tested regularly/turn the brightness down/use blue screen/screen filters/blue glasses
Back pain
    Use ergonomic chairs/use foot rests/regular breaks/sit with good posture/height adjustable chairs
RSI/finger pains
    Ergonomic keyboards/regular breaks/less use of mouse/use trackerballs/wrist rest
RSI/wrist pains
    Hands-free/less use of the mobile phone/wrist rest
Headaches
    Anti-glare screens/matt finish screens/regular breaks/ use no-flicker screens/LCD/TFT screens/have eyes tested regularly/turn the brightness down/use blue screen/screen filters/blue glasses
Deep Vein Thrombosis (DVT)
    Use foot rests/standing up
Neck pain
    Regular breaks/good posture/document holder
Hearing loss/damage
    Turn your headphone volume down

Ffiona wants to communicate with her friend Myfanwy using her mobile phone. Describe four ways she could do this.

Phone call
Text message
Email
Social network site
Blog/microblog
Video call

physical safety is the need to prevent accidents with computers
e-safety is the need to take sensible precautions when using the internet

Explain what is meant by a URL.

A URL is a Uniform Resource Locator
Is the unique address for a file that is accessible on the Internet
It consists of a protocol usually http or https
Then a domain name that identifies a specific computer on the Internet
Then a pathname that specifies the location of a file in that computer.

Describe three methods of minimising the possibility of passwords being misused if intercepted.

Encrypting the password
Ask for memorable information, such as mother's maiden name
Changing passwords very regularly
Use TANs
Only being asked for or providing a limited number of characters from the password
Twin factor authentication

Describe three benefits to customers of using internet banking.

Save travelling expenses
Saves time travelling/queuing
Elderly/disabled people don't have to travel
No embarrassment having to ask for loans face to face
Can bank when banks are closed
Use it anywhere there's an internet connection

Phishing
Fraudster sends an e-mail which appear to be authentic
is sent by a fraudster posing as a bank/organisation
provides a link to a bogus website

Pharming
installing malicious code on a pc or server
user is redirected to bogus website
user accesses websites which look authentic
website belongs to the fraudster/hacker

The bank that Alfonso uses only requires customers to log into their account by inputting a user id and password. Explain why this is not very secure and discuss other ways the bank could identify the customer securely

User id can sometimes be easily guessed
Passwords can be hacked with key logging software
Passwords can be hacked by using random password generators

Four from:
Question is asked such as mother's maiden name/customer's birthplace/date of birth
Question selected can be difficult to answer by hacker.
Answers can be intercepted by hacker
Using a chip and pin reader with bank card to generate a one off transaction code which user enters into online banking
Bank issues a one off transaction code to the user's phone which user enters into online banking
Even if hacker intercepts code is no use to him/her as can only be used once
Inconvenient as have to keep reader and card with you if you want to bank remotely
Using fingerprint scanner to capture digital image of fingerprint
Each fingerprint is virtually unique/ Each retina is unique/ Each iris is virtually unique
Fingerprint scanners can be inaccurate
Fingerprints can alter when people do sustained heavy manual work
Civil liberty issues
Using a retina scanner to detect retina pattern
Cataracts/astigmatism can affect accuracy of reading
Equipment cost is high
Using a digital camera to record image of the iris
High quality images of an iris can be used to 'fool' the system
Biometrics are nearly impossible to forge   [6]