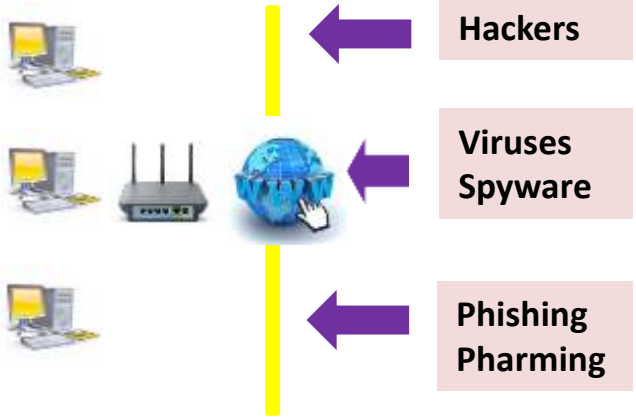
4.2 Network Issues and Communication

- Security issues regarding data transfer
- Network communication

4.2 Network Issues and Communication

Security Issues



How can hackers effect your network and data?

Introduce of viruses & spyware to the Network.

Threat to Data:

- Data could be deleted, edited, corrupted or be replicated.
- Data could be sold or passed on to other people.

Threat to Network:

- Network may have to be shut down to quarantine virus.
- This could stop production and cost an organisation a lot of money.

Should the internet be policed?

Advantages	Disadvantages
• To protect vulnerable users gaining access to undesirable websites. • To prevent illegal material (software, videos) be openly posted and shared by web users. • To bring to justice those users who continually misuse the internet for their personal gain.	• It would be extremely difficult and expensive to police the internet. • Infrastructure including staff and offices would have to be required. • Would be difficult to enforce different rules in different countries. • Could go against freedom of speech.

4.2 Network Issues and Communication

In many countries, hacking of computer systems is an offence.
(a) Explain, using examples, the term hacking.

Exam Question

Hacking is the unauthorised access to computer systems with the intention of causing harm. Hackers could edit, delete and steal data. Hackers could also introduce viruses to a computer network to cause disruption. On the other hand hackers could be employed to expose weaknesses of the system.

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

The use of usernames and strong passwords to stop remote and local logins. Also using different passwords for different accounts would reduce the chance of hacking. Biometric systems could be used to ensure the official user is present.

ICT IGCSE Theory – Revision Presentation

4.2 Network Issues and Communication

User Name & Passwords: Methods of Authentication (Network Security)

Authentication techniques are used to ensure only authorised users are able gain access to a Network via User Names/Passwords, Biometrics, Swipe Cards, TAN, Two Factor authentication etc.

Passwords are a method of authentication.

Disadvantages	Avoiding password interception
• Passwords can be guessed especially if they are simple. • Passwords may be seen by others. • Passwords can be stolen and used by other people. • Spyware could be used to logs key presses to get passwords. • Passwords can be hacked by using password generating software.	• Set strong passwords which include multiple characters such letters and numbers. • Ensure password is regularly changed. • Avoid using the same passwords for all of your accounts. • Install spyware software which will block the installation of any key logging software.

4.2 Network Issues and Communication

User Name & Passwords: Methods of Authentication (Network Security)

Setting a strong Password:

- Use at least 8 characters
- Includes letters and numbers
- Avoid using names or words which could be easily guessed.
- Use upper and lower case letters.

When users log onto to their online accounts they may also be asked for additional information to verify their accounts.

Security Question:

- Users may be asked to answer security questions related to their account.
- Typical questions includes mothers maiden name.

Personal Image:

- QNB (Qatar National Bank) require users to identify an image when they log in on the website for online banking. .
- Users will have to confirm if the image shown is one they selected as their account image.

4.2 Network Issues and Communication

Use examples to describe the difference between a weak password and a strong password?

Exam Question

A weak password is easy to guess and includes few characters and consists of all letters or all digits. A weak password typically relates to the user for example their favourite colour. A strong password is difficult to guess and contains many characters. Also a strong password uses mixture of upper case letters, digits and symbols.

4.2 Network Issues and Communication

Alternatives Methods of Authentication (Network Security)

Device		Overview/Advantages
Biometrics • Finger Prints • Retina Scan • Iris Scans • Face Scans • Vocal Recognition		• Biometrics use unique data. • Only the person with the biometric features can access the network. • Can not copy/replicate biometric data
Magnetic Swipe Cards		• Swipe cards are used to gain access to the system by swiping the card into the reader. • Swipe cards are quite easy to use and update. • Could also be used to gain entry into a room (hotel room).
Transaction authentication number (TAN)		• TAN is used by online banking services. • User will insert their bank card into the TAN reader which will then provide a code which will need to be entered to complete a transaction.
Two factor authentication		• Two Factor Authentication involves the user typing in their password and then typing in a code. • The code is sent to the registered phone number of the account as a text. • If an unauthorised attempt is made to log into an account then the text message will alert the user.

4.2 Network Issues and Communication

Describe alternative methods of authentication apart from a user ID and password that a bank could use to improve the security of online transactions?

Key Words: Biometrics, security questions, Two factor authentication, TAN

Exam Question

The bank only using a user id and a password as their sole method of authentication could be potentially risky. Passwords can easily be guessed or hacked by key logging software. In addition passwords can be generated by using password generator. To improve security customers could be asked to answer a personal security question liked to their account to identify themselves to the bank. They could also be requested select an image to verify their account. Since biometric data is unique to the individual it could be used to provide a more secure login as data cannot be copied. In addition the bank could request for a TAN (Transaction authentication number) when customer to complete a transaction. Finally two factor authentication could be implemented which would require the user to enter a code which would have been sent to their mobile number as part of the login process.

4.2 Network Issues and Communication

Biometric methods are increasingly being used to authorise user access to computer systems. Explain, giving examples why biometric methods are considered to be a more secure method of authorising access to a network than using ID and passwords.

Exam Question

Biometric methods are more secure method of authentication because it contains unique data which not be copied, guessed, overseen or stolen like passwords. Only the person with the unique biometrics features can gain access to the network whereas any one with the password would be able to gain access. Finger prints, retina scans, facial characteristics and voice recognition can be used to identify individuals to a network.

Explain, using examples, what is meant by authentication techniques.

Authentication techniques are a method of identifying yourself to a system. An example is using a password and user ID.

4.2 Network Issues and Communication

Security issues regarding data transfer: Viruses & Spyware

A computer virus is a piece of programming code/software which can install and replicate it self on to a computer system without the user's permission. A computer virus can cause the following problems.

1. Causes the computer to crash – become slower
2. Sometimes files can be deleted – leads to computer malfunction.
3. Data files can be copied by the hacker or the files could be corrupted.
4. Could stop production until the virus has been quarantined.

Spyware gathers data from computers without the user knowing. Spyware could monitor key presses to gain personal information or passwords. This information would be sent back to the hacker.

Installing anti virus and spyware software and the use of a firewall is not enough to keep your computer safe. You also need to pay attention to the following points.

- Do not download any files from untrusted sources including email attachments.
- Do not install illegal software onto your computer.
- Do not click on links from unknown websites.
- Do not connect storage devices (e.g. USB) from unknown sources.
- Ensure virus software is up to date and virus definitions are regularly updated.

4.2 Network Issues and Communication

John is working on a school History project and saves his work. He is told by one of his teachers that the school network has been infected by a computer virus.
(a) Explain what is meant by a computer virus and give examples of how a computer virus can affect a computer.

Exam Question

A virus is a piece of software/program code that infects a computer by attaching itself to files. A computer virus has the ability to replicate itself. The virus can cause the computer to crash or shut down. It can delete and corrupt files on the computer. Computer operations, files or software can become unstable or unresponsive.

John copies his History project from the school network onto his home computer using a pen drive. There are many ways his home computer can become infected by a computer virus. 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 anti-virus software to scan the computer hard drive on regular occasions. Also John needs to ensure he does not use media from an unknown source or downloads attachments from unknown email addresses. The anti-virus software should be regularly updated to protect against the latest threats.

4.2 Network Issues and Communication

Security issues regarding data transfer: Firewall

Prevents computer accessing undesirable/unauthorised sites

Helps to prevent malware (viruses) getting into computer/from the internet

Keeps a list of undesirable sites/IP addresses
Keeps a list of acceptable sites/IP addresses

Monitors and controls incoming and outgoing data traffic.

Prevents unauthorised computers using the internet accessing the computer

Warns you regarding threats/allows you to accept/reject downloaded programs

4.2 Network Issues and Communication

The organisation has a computer network which is connected to the internet. The router contains a firewall. Explain why a firewall is needed?

Exam Question

The firewall is needed for network security. It controls the incoming and outgoing network traffic.

A firewall establishes a barrier between a trusted, secure internal network and the Internet. In addition it logs incoming and outgoing traffic and stops malicious traffic. Furthermore it prevents computers connecting to unwanted sites. Also the firewall prevents untrusted/unrecognised computers accessing data on the system.

4.2 Network Issues and Communication

Encryption

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

1. Data is scrambled up (Data is Encrypted).

2. If the data is intercepted it then it prevents people from understanding and reading the data.

3. The person with the key is able to Decrypt and understand the data.

Disadvantages

- Data can still be deleted from system
- Criminals can use encryption to keep incriminating material secure

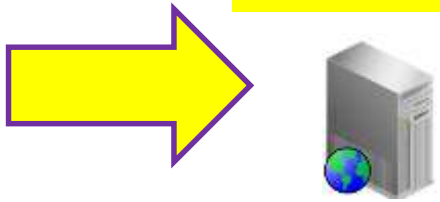
4.2 Network Issues and Communication

Describe the process of encryption and give an example?
Key Words: Data, Scrambled, key, decrypted, online transaction?

Exam Question

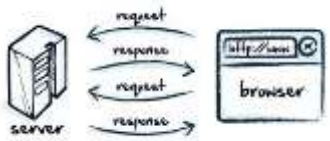
When using online banking data will be encrypted. When the user logs on to a secure website they will enter personal details into the webpage. The information will then be encrypted (scrambled) so if the information was to be intercepted it would be meaningless for them. Once the bank receives the information they will be able to decrypt the information using a key and convert it into a form which can be understood.

4.2 Network Issues and Communication



Can be used to **monitor** Internet usage

Can **block** certain sites



Server passes on **requests** to the Internet
Passes the requested web pages to individual computers

Can **cache/store** the webpages

Can act as a **buffer** (between Internet and LAN)

Can act as a **web server**

4.2 Network Issues and Communication

Security issues regarding data transfer: Data Protection Act

Data protection Act applies to paper based or electronic forms of data stored on a computer. The data protection act is to protect rights of the individual who the data is obtained from.

Web based business such as Amazon or Ebay store sensitive data about customers including payment details. They would have to abide by the data protection act to keep the data secure.

Principles of the Data Protection Act

1. Data must be fairly and lawfully processed.
2. Data can only be processed for the stated purpose.
3. Data must be adequate, relevant and not excessive.
4. Data must be accurate.
5. Data must not be kept longer than necessary.
6. Data must be processed in accordance with the data subject rights.
7. Data must be kept secure.
8. Data must not be transferred to another country unless they have adequate protection.

4.2 Network Issues and Communication

Most data protection acts include the principle that data should be stored securely. List four other principles of a typical data protection act.

Exam Question

- Information must be processed fairly and lawfully
- Information collected must be processed for limited purposes
- Information collected must be adequate, relevant and not excessive
- Information collected must be accurate and up to date
- Information must not be held for longer than is necessary
- Information must be processed in accordance with the individual's rights
- Information should not be transferred outside the area of the Act unless adequate levels of protection exist.

4.2 Network Issues and Communication

Network communication

Type of Communication	Overview/Advantages	Disadvantage
Physical Faxing	• Requires a fax machine and a telephone line. • Number of the recipient dialled before the document is copied and sent. • Physical documents are printed and can be signed.	• Anyone can access faxed documents. • The fax may be out of paper or ink (toner). • No notification of fax received.
Email Communication	• Can send multiple attachments. • Can send to multiple recipients in one message. • Emails can be received instantly and accessed on many platforms including tablets and phones.	• Email attachments may include viruses. • May receive spam (unwanted mail). • May receive phishing (scam) emails to obtain personal data.
Electronic Faxing	• Electronic Fax is sent via a internet connection. • No need to buy a fax machine, ink or paper. • Electronic Fax documents are sent to an email which will ensure the correct person will receive the fax – less chance of document being intercepted. • Electronic Fax's can also be sent directly to a fax machine. • Send fax's from any location with an internet connection. • No additional cost to send fax over internet network.	

4.2 Network Issues and Communication

Network communication

Advantages and Disadvantages of using email compared with faxing

	Fax	Email
Advantages	• Documents can be signed which are legally accepted. • Physical copies of documents can be sent and automatically printed.	• Emails are password protected so less likely chance of data being intercepted. • Emails can be received instantly. • Attachments can be edited and sent back. • Can send to many recipients at the same time.
Disadvantages	• Data is more likely to be intercepted once it is printed from the fax machine. • There could be delays in receiving the fax due to a busy telephone line or lack of paper or ink. • Fax can only be received during office hours. • Not everyone has a fax machine.	• Cant be used when documents need to be signed. • Viruses can be download from attachments. • Unwanted emails could be received (Phishing/Spam).

4.2 Network Issues and Communication

Describe the advantages and disadvantages of using email compared with faxing?

Exam Question

Email can be received on many different platforms (PC, Laptop, Smart phone) instantly. In contrast a fax will only be received once it has been printed. If the fax machine is offline or there is a problem with the printing (lack of ink or paper) then the fax will not be received. Also a fax can only be received if the recipient has a fax machine and during office hours. In addition the fax can be intercepted by anyone close to the fax machine. On the other hand email is password protected which would ensure the security of the email. The main advantage of an email is that a message can be sent to many recipients and attachments can be added. Nevertheless unwanted emails could be received and viruses could be downloaded from attachments. The main advantage of a fax is that you receive a physical copy of the document and signed copies can be legally accepted.

4.2 Network Issues and Communication

Describe two similarities between physical faxing and electronic faxing.

Exam Question

Physical faxing and electronic faxing both involve you being assigned a fax (phone) number and the user of a phone line. Both can involve use of a hard copy original.

Describe three differences between physical faxing and electronic faxing.

Physical faxing requires purchase of a fax machine. Electronic faxing requires the use or purchase of a computer. Physical faxes can be picked up by anyone however electronic faxing goes straight to your email address. With a Physical fax the phone line could be busy or engaged. In addition Physical faxes must have paper and the fax machine could can get paper jams. Electronic fax is quicker to arrive than physical since it goes direct to your email.

4.2 Network Issues and Communication

Network communication

Type of Communication		Overview	Hardware
Video Conferencing		• Video conferencing uses both **video** and **sound** using an **internet connection**. • It can be used to have business meeting when people are in different locations.	• Web Camera • Screen/Monitor • Speaker • Microphone
Advantages	• No **need to travel** to have meetings which would cut down on **travelling costs** (including flights and hotel) and **travelling time**. • Video conference can be **held at short notice**. • Facilitates **long distance learning** – students can access live lectures without travelling.		
Disadvantages	• **Technical problems** with the internet or hardware could effect the quality of the video conference. • **Set up costs** to purchase hardware/software and to provide relevant training to staff. • **Lack of personal contact** you would have if it was a face to face meeting. • **Different time zones** could make it difficult to find to find a suitable time to have a meeting. • Not possible to **sign documents**.		

4.2 Network Issues and Communication

Describe the advantages and disadvantages of video conferencing?

Exam Question

Video conferencing can be held at short notice without the need to travel. As a result travelling time and expenses would be saved. However set up costs to buy equipment could initially be expensive. Also staff would require training on to use the technology. In addition during the video conference there could be technical problems which could affect the quality of the sound and video. Video conferencing could also facilitate long distance learning nevertheless the different time zones could be an issue when arranging a meeting. Moreover the lack of personal contact could it make it more difficult to understand the tone and context of the conversation. Furthermore it would not be possible to sign documents.

4.2 Network Issues and Communication

Describe three drawbacks of setting up and using video-conferencing?

Exam Question

Power cuts could lead to parts of the video-conference shutting down. Also a Lip sync problems/time lag could means that the picture is not running at the same speed as the sound. Some participants may be video-conferencing outside of work hours due to time zones. In addition it would be expensive to purchase the hardware and software required. Furthermore the quality of the video conference would be dependent on a reliable internet access. Staff would also have to be trained and this could be additional expense for the company. Moreover documents will not be able to be signed and physical objects cannot be examined.

4.2 Network Issues and Communication

Network communication

Type of Communication		Overview	Hardware
Audio-Conferencing		Audio conference can be done over the telephone network or using a computer making use of VOIP. 1. The organiser of the phone conference is given a unique Pin which can be shared participants. 2. For Participants to join they have to dial the conference phone number. 3. Then they would have to enter a PIN.	• Telephone VOIP • Microphone • Speakers
Web-Conferencing		• Web conference can be done using internet connection. • It is very similar to video conference as participants can hear audio and see a live video stream. • Participants can join the web conference by clicking on the supplied link from the organiser. • Participants can join and leave the web conference at any time. • Instant messaging (IM) feature is available to communicate with other participants. • Participants can be given permission to speak and can share content such as images, video or presentations.	• Same as video conferencing. • Keyboard could be use for IM.

4.2 Network Issues and Communication

Network communication

Set up an Audio-Conferencing

1. Contact Audio Conference Provider
2. Phone number and Pin is provided for the Organiser and the Participants
3. Conference details emailed to participants
4. Organiser calls the number and enters the PIN
5. Participants call the number and their PIN.

Set up an Web-Conferencing

1. Contact Web Conference Provider
2. Web link and Pin is provided for the Organiser and the Participants
3. Conference details emailed to participants
4. Organiser starts the conference.
5. Participants can join by accessing the web link and entering their PIN.

4.2 Network Issues and Communication

The directors of a multi-national car company need to communicate with each other. They have decided that the best way to do this is through web-conferencing.
(a) Describe web-conferencing and how it could be used in this scenario.

Exam Question

Web Conferencing allows for real time collaboration and communication. Multiple users are connected to the internet and see the same screen at all times in their web browsers. The web conference allows users to instant message each other details of the car. VOIP could allow users to discuss the car range. Full motion video can be used to show the car being test driven.

4.2 Network Issues and Communication

There are several ways in which members of an organisation can organise meetings. These include video-, audio- or web-conferencing.
(a) An organisation is planning an important meeting with the Directors of the three main offices.

They are going to set up an audio-conference. Describe the process of setting up this type of conference.

Exam Question

To set up an audio conference a provider would have to be contacted. The conference provider would provide a phone number and a PIN for the organiser and participants. The ograniser would then email the details of the conference to all participants including the phone number and PIN. At the start of the conference organiser calls the provided number and types in his PIN. Then each participant dials the number and enters the PIN.