



# GCSE ICT

## INSIDE THIS DOCUMENT

<b>Online Services</b>	<b>2</b>
<b>Online Storage</b>	<b>2</b>
<b>File Compression</b>	<b>4</b>
<b>Collaborative Working</b>	<b>6</b>
<b>VLEs</b>	<b>7</b>
<b>Ubiquitous Computing</b>	<b>9</b>
<b>Online Communication</b>	<b>10</b>

## Intro to the Unit

This unit provides an introduction to the modern online world. We will base the course around your current knowledge and build on it to investigate a range of different services including email, online data storage, collaboration software, blogging and social networking. The internet and web of tomorrow will be even more powerful, more connected, more intuitive and a more important part of our lives, whether that is through smart devices, cloud based systems or simply just integration between different technology and systems that we already use in our day to day lives. This unit will give you a better knowledge of how the online world is impacting our lives and the challenges that brings.



## Investigating Online Services and Online Communication

How do websites work? How do emails reach your computer? How does the use of computer applications affect your daily life? This unit provides an introduction to the modern online world. Starting with your own experiences, you will extend your knowledge of online services and investigate the technology and software that supports them. You will learn more about a range of services including email, online data storage, collaborative software, search engines and blogging.

This unit will help you understand the main technologies and processes behind the internet and investigate how they come together to let you view websites and send

information across the world. The internet and web of tomorrow will be even more powerful, more connected, more intuitive and a more important part of our lives.

This will result in an internet of services, objects and infrastructure (ubiquitous computing) which will radically change our lives. For example, smart appliances will be able to talk to each other, clothes will monitor our health and retailers will access social media to gain insight into shoppers' preferences.

You will explore a range of digital devices, such as smart phones and digital music players and consider the technology that enables these devices to share and exchange information.

This technology has created new concerns regarding

security and privacy. You will investigate these concerns and consider how users should behave online to safeguard themselves and respect others.



# Online Services

What do you use the internet for? It is likely much more than you may initially realise. Examples could be:

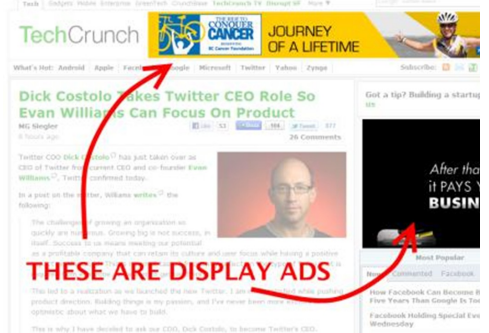
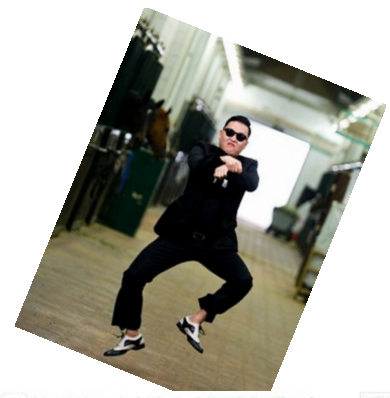
- communication (email, instant messaging, newsgroups, social networking, online conferencing, blogs)
- real-time information (train timetables, news services, traffic reports, flight status updates, weather)
- commerce (internet banking, online auction websites, retail sales, publishing)
- government (online tax returns, e-voting, applications for services/grants, revenue collection)
- education (online learning/training)

- virtual learning environments (VLEs)
- business (video conferencing, collaborative working, business networks)
- entertainment (multi-user games, radio players)
- download services (music, film, upgrades, software).

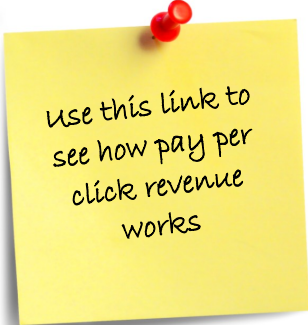
These services may often be free to you, but they cost a lot of money to develop and run and someone has to pay for that!

Did you know that the estimated cost for running the YouTube servers to deliver 1 billion views of "Gangnam Style" was \$297,000. By putting adverts before the video and on the page it was shown on, the estimated revenue for YouTube was \$348,000!

These sums are money are generated



by "Pay per Click" advertising. Whenever you click on a advert, the company who the advert is for pays a small amount of money to the company who is hosting (displaying) the advert. All of those small amounts of money build up to large amounts of money!



Use this link to see how pay per click revenue works

<http://www.youtube.com/watch?v=op4gt37dGuc>



# Online Storage

Do you have a webmail account like Gmail or Hotmail? Do you have a Facebook account? It is likely that the answer is yes to both of these. Have you ever thought about where all that data is stored?? On your computer? On a server in the local town? On a server on the other side of the world?

When it comes to online storage, it doesn't really matter where it is stored. As long as you can gain access to it, it can be anywhere on the internet (in the cloud) and you would be able to access it!



Use this link to see how online storage works

<http://www.youtube.com/watch?v=-bn6UTm9xno>



## Advantages and Disadvantages of online and offline storage



Online Storage	
Amount of Data that can be stored	Between about 500Mb and 100GB
Different Devices that it can be accessed from	Any (with appropriate software)
Where can it be accessed from?	Anywhere (as long as you have an internet connection)
Speed of access	Dependent on the speed of your internet connection
Can backups be run automatically?	Yes, but needs specialist software
Cost	Free to about £70/year
Is it secure?	In theory yes, but lots of sites on the internet have been hacked + you are trusting someone else with your data

Offline Storage	
Amount of Data that can be stored	1GB to 4TB
Different Devices that it can be accessed from	Any with a USB or network connection
Where can it be accessed from?	Generally have to be physically connected to it
Speed of access	Very fast
Can backups be run automatically?	Yes, but needs specialist software
Cost	£2 up to £700 (one off cost)
Is it secure?	Yes, but memory sticks etc can be lost

Search on internet for "Online data storage services".

List out the following information for at least 5 different BIG companies that offer online storage

Company Name	Different amounts of storage that you can have	Cost	Special Features

Discuss in a small group what methods of storage you use on a regular basis.

These could be memory sticks, drop box, your laptop, your phone. List out whether they are online or offline (i.e. on the internet or something physical you have like a memory stick etc).

Write notes on what you think about the different methods? What problems have you had with them? Where have they been useful?

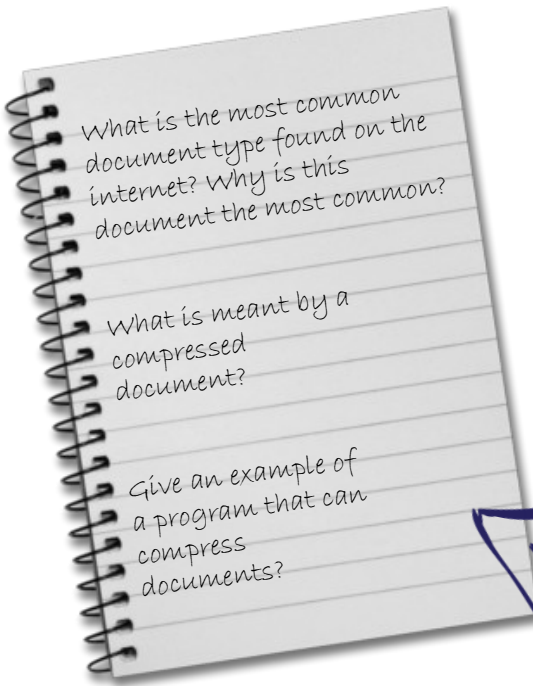
Remember that although you may not have an online storage account like dropbox, you could well be using online storage with something like Facebook to store pictures. What are the advantage and disadvantage of that? You can share the photo with people, but how do you know who has access to them? Perhaps you have an online account with Playstation or Xbox.

What information is stored there about you? How much personal information? How secure are those systems? How much data did Playstation lose in a recent hack?

*discussion*



# Online Storage— Continued



**POSSIBLE EXAM QUESTIONS**



## Online Storage & Compression

Join up the boxes to show whether the facts shown below are advantages or disadvantages for either online storage (like Google Docs) or offline storage (like a memory stick or external hard disk).

- Can store between about 500MB and 100GB
- Can be used for backing up your documents automatically (assuming you have got the correct software installed to do it)
- Can be accessed from anywhere where you can get an internet connection
- Might get hacked or someone steals your data
- Very cheap – a lot of the drives are free or given away
- Needs to be physically connected to the machine
- LOTS of storage space – up to 4TB!
- Can get lost or broken
- Can work with different machines
- Very fast – much faster than using the internet

Advantage	Online Storage
Disadvantage	

Advantage	Offline Storage
Disadvantage	

Do you have a webmail account like Gmail or Hotmail? Do you have a Facebook account? It is likely that the answer is yes to both of these. Have you ever thought about where all that data is stored?? On your computer? On a server in the local town? On a





## LZW compression

Most compression programs use a method of dictionary compression by grouping words together.

The system for arranging dictionaries varies, but it could be as simple as a numbered list. When we go through Kennedy's famous words, we pick out the words that are repeated and put them into the numbered index. Then, we simply write the number instead of writing out the whole word.

Word	Word Index
Ask	1
What	2
Your	3
Country	4
Can	5
Do	6
For	7
You	8

Our sentence now reads: "1 not 2 3 4 5 6 7 8 -- 1 2 8 5 6 7 3 4"

So now, if you know the dictionary index, you can reconstruct the file! This is what the expansion program on your computer does when it expands a downloaded file.

But how much space have we actually saved with this system? "1 not 2 3 4 5 6 7 8 -- 1 2 8 5 6 7 3 4" is certainly shorter than "Ask not what your country can do for you; ask what you can do for your country;" but keep in mind that we need to save the dictionary itself along with the file.

In an actual compression scheme, figuring out the various file requirements would be fairly complicated; but for our purposes, let's go back to the idea that every character and every space takes up one unit of memory. We already saw that the full phrase takes up 79 units. Our compressed sentence (including spaces) takes up 37 units, and the dictionary (words and numbers) also takes up 37 units. This gives us a file size of 74, so we haven't reduced the file size by very much.

But this is only one sentence! You can imagine that if the compression program worked through the rest of Kennedy's speech, it would find these words and others repeated many more times.

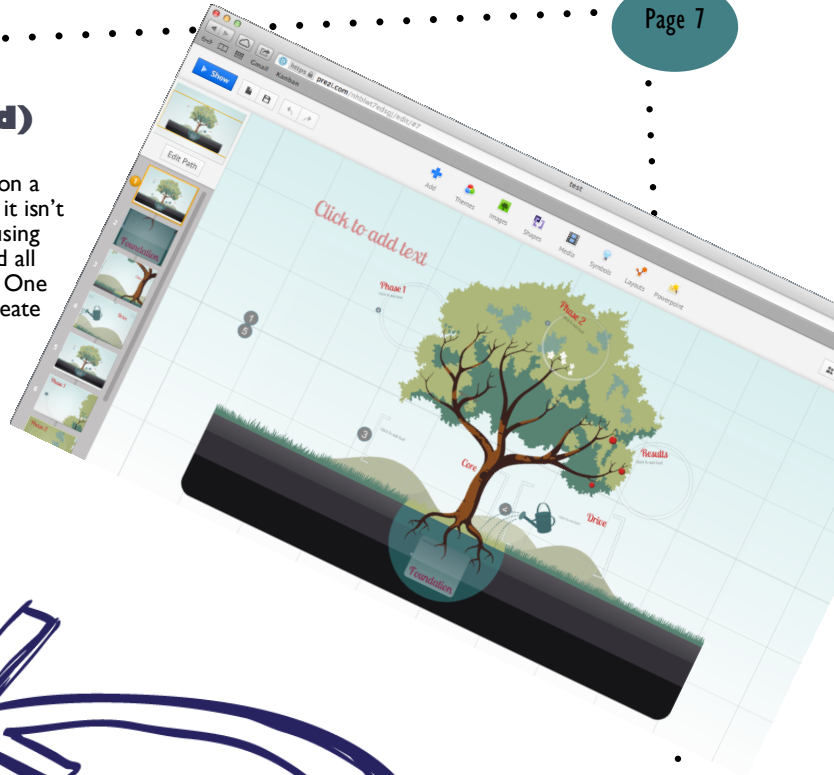
## Collaborative Working

One of the benefits of working online is that it is possible to work collaboratively. Digital files can be quickly and easily sent from one person to another (or to multiple people) at the click of a button. The question you should ask though is: Is working collaboratively easier and better online?

Advantages and disadvantages of working collaboratively online	Advantages and disadvantages of working collaboratively offline
Quick to send work to people in different locations	All need to be in the same place if you want to all work on the same thing at once
Share and modify assets and ideas quickly via digital files	Potentially more flexible to discuss and rough out ideas
Make modifications quickly individually	Slow if you are relying on the post
Difficult to know who has the latest version if you are communicating by email	Slower to include some assets like photos and videos
Everyone has to have access to the same files and programs	Software/hardware issues aren't so much of a problem when you have a pencil and some paper!
Data can be lost easily if mistakes are made	Other than in the post, work generally isn't lost

## Collaborative working (continued)

Not everything is better online—trying to work with colleagues on a document which is being emailed around is very difficult because it isn't clear who has the latest version. But there are solutions to this using cloud based technology—essentially doing the same as you would all sitting around a piece of paper, but working in the cloud instead. One prime example is "Prezi", where people can work together to create presentations online. The documents are shared all the time, therefore as different people make changes to the presentation, those changes are automatically updated for anyone else who is



## POSSIBLE EXAM QUESTIONS



Look at the Keywords: **Explain, Compare**. These tell you what sort of answer the question is after.

If you are not sure what some of these things are in these questions, you need to be looking them up to find out!

## Collaborative Working & VLEs

VLE stands for "Virtual Learning Environment". It is essentially a website, but the main difference is that documents, assets and resources placed on it can be shared between different groups of people so that they can work collaboratively on those documents. Unlike the shared drive at school, which you can access, but not save back to, a VLE allows you and your group to work with documents which your teacher has assigned to your class and where applicable, save work back to the VLE, have group discussions, and work collaboratively. One of the advantages of these systems is that they are cloud based, therefore you can access them from anywhere on the internet. They aren't the only for of collaborative working. Others which you should be aware of are:

- Contemporary social media including web logs (blogs), wikis and podcasting
- Document and resource management systems such as Microsoft Sharepoint
- Social networking websites to share information and build online communities

Use the box below to find out what these things are and who uses them generally

What they are	Typical Users

## Collaborative working (continued)

Working online, however brings with it a number of new key terms which you will need to know what they mean

Term	Meaning
Netiquette	The correct or acceptable way of communicating on the Internet.
Online Profile	An online identity, internet identity, or internet persona that an Internet user establishes in online communities and websites. This does not necessarily have to reflect their real world profile
Network of Friends	A collection of friends, both on and offline who are interconnection. Friends of friends and friends who know each other through other friends and interests
Virtual World	A virtual world is an online community that takes the form of a computer-based simulated environment through which users can interact with one another and use and create objects.
Online Chat	Online chat may refer to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly.
Chatroom	A site on the internet where a number of users can communicate in real time (typically one dedicated to a particular topic)

Working collaboratively online brings with it a number of different challenges and questions which you should consider in your revision for the exam. Find out what some of these things are and what impact they have on online communication

What are the advantages of using social networking websites for communication?

Is Instant Messaging used any more, (like MSN) or has it taken a different form like BBM or Facebook messenger? What are the advantages of these systems?

What is the role of a client and a server in order to support instant messaging? Why do we need them?

What are the benefits of real time communication over the internet? For example live video, voice over IP (VoIP) or web meeting / conferencing software. How do these work?



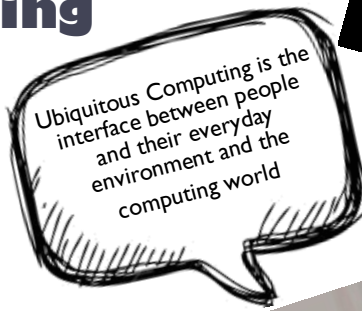
# Ubiquitous Computing

Ubiquitous means:

**“existing or being everywhere at the same time”**

**“Constantly encountered”**

**“Widespread”**

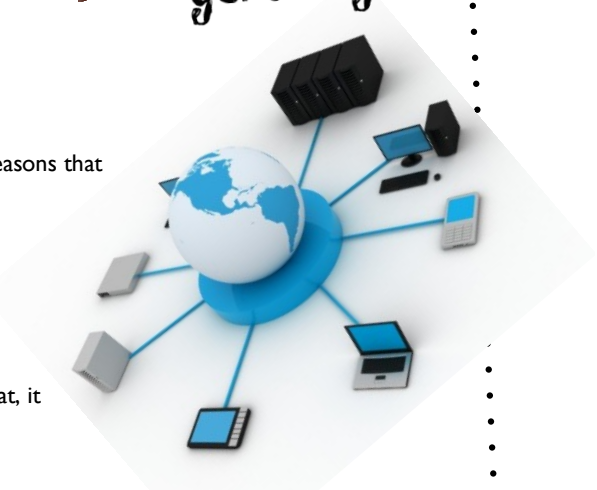


Ubiquitous computing means technology which is everywhere and we use it all of the time. Ask yourself these questions:

- What technology do you use every single day?
- What technology could you not do without in your life? (why....?)
- Is your ubiquitous technology networkable?
- It is likely to enable you to be global and local at the same time?
- Social and personal at the same time?
- Public and private at the same time?
- In control of what is going on around you?
- Do lots of other people also use this technology for the same purposes and reasons that you do?



If you find that there is technology which you use every day and couldn't be without, then it is likely to be ubiquitous. If it allows you to answer "yes" to the later questions, then it is most definitely. Keep a log over the period of a week to see what technology you use, how long you use it for and where you are when you are using it. You will quickly see that there is so much technology influencing our lives that we sometimes don't even know it. The ubiquity of computers has become so great, it has become "normal"



Day	Technology used	How long was the technology used for?	Where were you when the technology was used?
Monday			
Tuesday			
Wednesday			
Thursday			
Friday			
Saturday			
Sunday			

# Online Communication

There are lots of different ways that people can communicate online with each other—it is very likely that you have used multiple methods just today! Social Networking, instant messengers, text messaging, VoIP systems. What do they do and what are the advantages and disadvantages of them though?

## Contemporary Social Media

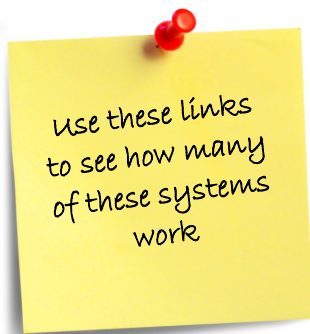
Contemporary Social Media is a form of online communication where people (users) can generate their own content. It enables them to be able to publish and access information on topics that they are interested in. This is often done using web logs (blogs), wikis and podcasting

## Virtual Learning Environments

These are online spaces where people can work as a team on shared documents. Resources can be stored here which others can access, works on and submit back. Some people just use them for storing resources, but it is possible to do much more, including interaction, voting, testing, discussion, communicating and learning.

## Social Networking Websites

These are websites where people can share information, build communities and stay in touch with people online. Information, photos, comments and stories can be published and shared with groups of people enabling them to keep in touch with each other and socialise.—Examples include Facebook, Twitter, MySpace, Bebo etc.



System	Link
How Blogs work (in plain English!)	<a href="http://www.youtube.com/watch?v=XY5acLmS3RQ">http://www.youtube.com/watch?v=XY5acLmS3RQ</a>
How Podcasting works (in plain English!)	<a href="http://www.youtube.com/watch?v=j7V-CBgpsml">http://www.youtube.com/watch?v=j7V-CBgpsml</a>
How Social Media works (in plain English!)	<a href="http://www.youtube.com/watch?v=MplOCIXljPE">http://www.youtube.com/watch?v=MplOCIXljPE</a>
How Twitter works (in plain English!)	<a href="http://www.youtube.com/watch?v=jGbLWQYJ6iM">http://www.youtube.com/watch?v=jGbLWQYJ6iM</a>
How Wikis work (in plain English!)	<a href="http://www.youtube.com/watch?v=-dnL00TdmLY">http://www.youtube.com/watch?v=-dnL00TdmLY</a>
What is Augmented Reality?	<a href="http://www.youtube.com/watch?v=D-A1I4Jn6EY">http://www.youtube.com/watch?v=D-A1I4Jn6EY</a>



All this technology is great, but is it great all of the time? Some people don't really think about the implications of socializing and communicating online. Messages or any form of communication online can be very public—a message go travel around the world very quickly. Additionally anything put onto the internet is generally there for ever, even if you delete it, it will have been backed up somewhere! Something can come back to cause issues in the future!



A woman was fired from her job after writing very abusive comments on Facebook about her boss. Unfortunately she forgot that she had added her boss as one of her friends!



A juror in the UK was dismissed after she disclosed sensitive case information on her Facebook profile, MSN reports. "I don't know which way to go, so I'm holding a poll" the juror wrote, asking her Facebook friends to weigh in on the



Virgin Atlantic took disciplinary action against 13 crew members who participated in a Facebook discussion that "criticised [Virgin's] safety standards and insulted passengers," The individuals "posted messages on Facebook referring to passengers as "chavs" and making jokes about faulty engines," explains the Guardian, adding that they also "joked that planes were full of cockroaches and claimed the airline's jet engines were replaced four times in one year."



Teen Police Commissioner needs to resign because of her apparently racist tweets from several years previous!



# Advantages, Disadvantages and Risks of Contemporary Social Media

Use lines to join up the advantages, disadvantages and risks

Can reach a large number of people in a short period of time

Information can be public and you have little control of what people say or comment

Generally free to create and post information

Audience “volunteers” information about themselves and their interests which means you can target them accurately

Brand hi-jacking and viruses can be introduced if general public is allowed too much control

Easy to reach your target audience

Can become viral

Can take a long time to keep up to date

People can unsubscribe if it is not kept up to date

Advantages

Disadvantages

Risks



# Advantages, Disadvantages and Risks of Virtual Learning Environments

Use lines to join up the advantages, disadvantages and risks

Enables "Social" learning online

Homework can be set and handed in online

Non technical teacher of student may have problems using it

In internet in school or at home isn't working, you can't use the VLE

Revise and work at your own pace

Reduces face to face contact with people which is important to help build social skills

Makes it very easy to work customise resources for disabled pupils

Can take a long time to develop resources for it!

Advantages

Disadvantages

Risks

# Advantages, Disadvantages and Risks of Social Networking Websites

Use lines to join up the advantages, disadvantages and risks

Keep in touch with people around the world

Generally free

Build a network of contacts and interact with lots of people at the same time

Identity fraud and theft

Can be used to spread malicious humour and false information

Quick and easy to update from most devices and many systems have the ability to interact with social networking sites

You can find information and people who have similar interests

Can store text, messages, photos and videos on almost any topic you like

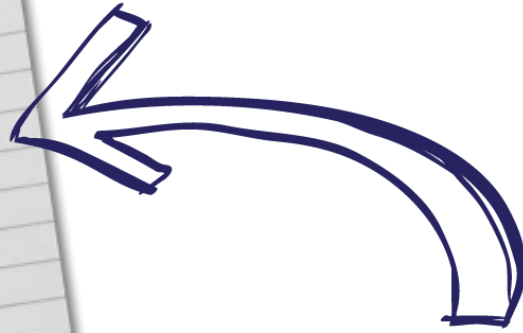
People can stalk you if you post too much information about yourself online

Advantages

Disadvantages

Risks

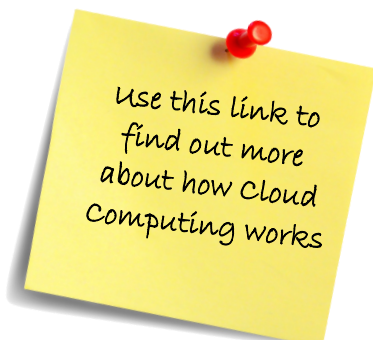
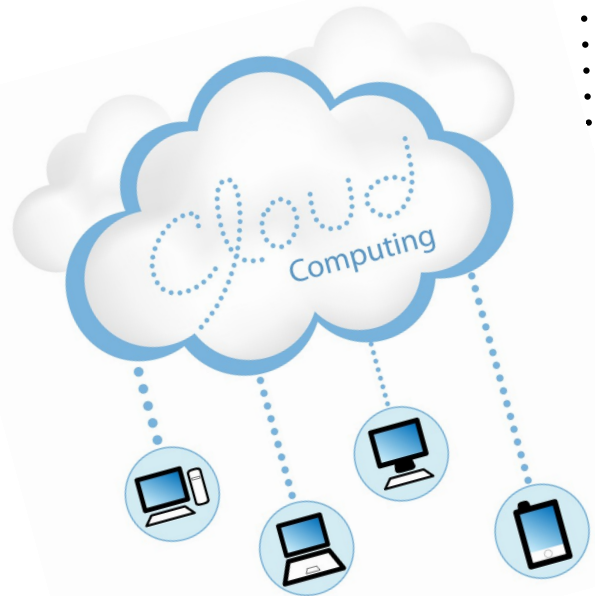
## POSSIBLE EXAM QUESTIONS



These are mostly “knowledge” questions—do you know something or not? But look there are also secondary questions which ask you to explain. This means you need to know how stuff actually works in order to pass the exam

## Cloud Computing

Although there are a number of different definitions of “Cloud Computing”, the basic definition of it is using a network of remote servers hosted on the internet to store, manage and process data rather than a local machine. This used to just mean “keeping your files online”, but as technology improves, cloud computing has developed to include actually being able to use programs online—i.e. although you are viewing the work on the screen in front of you, a lot of the processing and the actual program itself is running on a server on the internet somewhere. The advantage is that you can work collaboratively very easily (remembering back to the Prezi system from the earlier page but additionally it means you can work from any location that has an internet connection. The disadvantages of cloud storage, however are that you are completely dependant on your service provider to ensure that your data is safe and secure (with the amount of cases of hacking we have at the moment, do you know your data is secure!). In order to get to your cloud storage, you data has be transmitted over a public network (the internet). While the transmission is encrypted to make it secure, how do you know this for sure? Finally, what happens if you NEED that data and your service provider is down, or the connection to it is broken? Cloud storage is potentially good, but there are some significant issues to overcome.



<http://www.howstuffworks.com/cloud-computing/cloud-computing.htm>

# How the Internet works

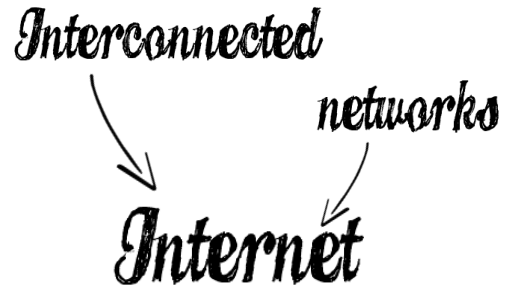
The internet is huge! It is estimated that there are about 46million webservers on the internet in 2013. Forbes.com estimated in January 2013 there were 8.7 billion devices attached to the internet around the world.

Servers which track Google to see how many pages it is indexing, estimate that it currently has 4.1 billion pages in its records.

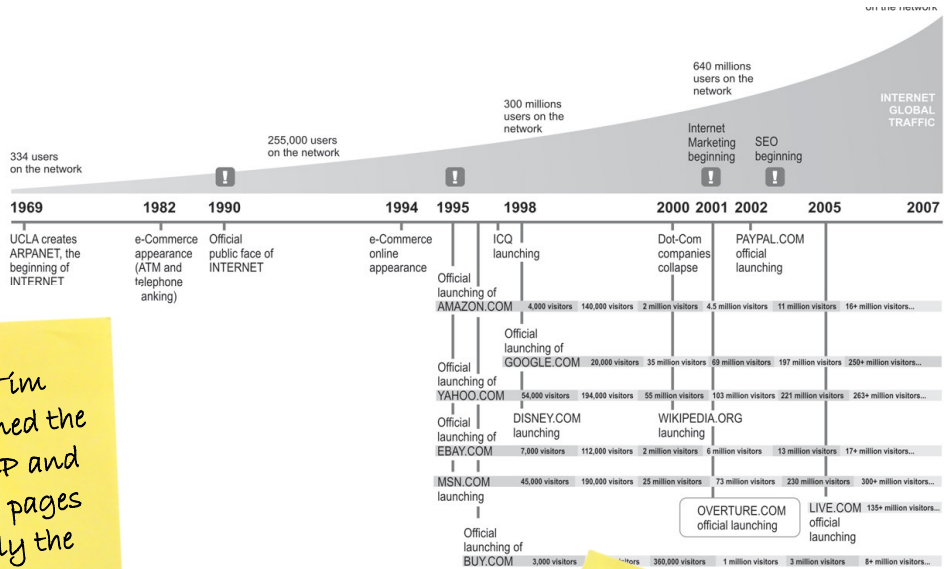
The concept was first invented in 1969 by the American army as a way of linking computers together so that should there be a nuclear war, the army bosses could still communicate with each other even if they were in

deep underground bunkers in mountains across the country.

The Internet is a VERY large collection of interconnected networks. When you combine these words it makes the word "Internet". Like a maze, it is all of the different computer networks around the world all linked together. The advantage of this is that no single person, company or country owns the whole network (they only own bits of it), so it is very difficult to stop or switch off. Equally because it is "interconnected", this means there are lots of different routes around it. If one route is broken or blocked for some reason, data can simply take a different route!



The graph below show the tracking of approx. numbers of people using the Internet since it was first thought up in 1969. Then only 334 people used it. Now it is billions. Remember the "Internet" is just the network over which all the data is sent. The WWW is simply just part of that!



In 1989 Sir Tim Berners-Lee joined the concepts of TCP and hyperlinking pages and suddenly the WWW was born

[http://www.bbc.co.uk/schools/gcsebitesize/ict/datacomm/0internet\\_act.shtml](http://www.bbc.co.uk/schools/gcsebitesize/ict/datacomm/0internet_act.shtml)

Use this link to find out more about how the internet works!

Use this link to see real time statistics of how many pages Google and other search engines are currently indexing!

<http://www.worldwidewebsite.com/>



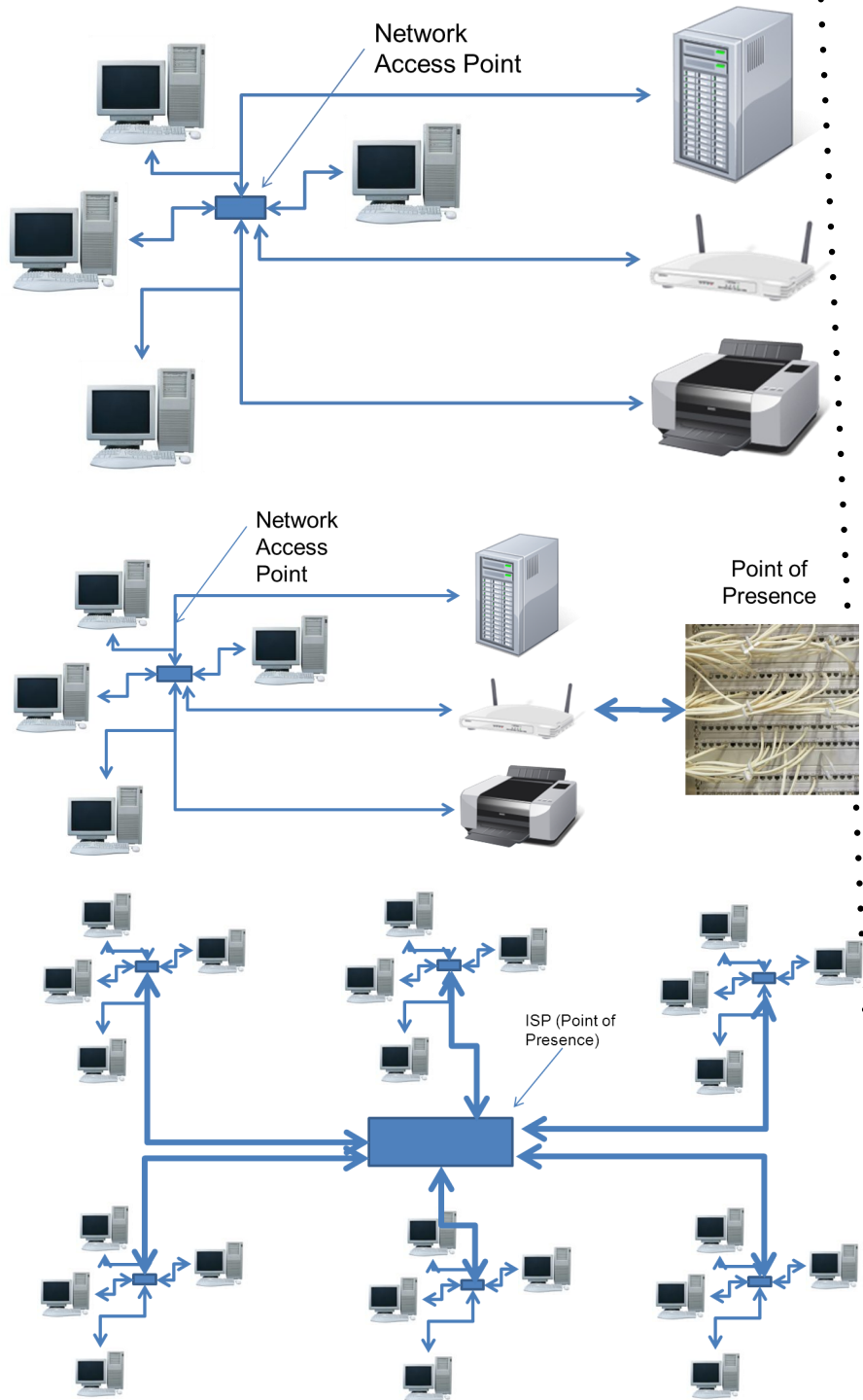
You probably have a network at home. It could just be a PC and a laptop which can both connect to the internet at the same time. Or it might be much more with smart phones, games consoles, smart TVs and media players all connected and able to surf the internet at the same time. If you think about how many devices you have at home which can connect to the internet and then multiple that up by the number of houses in your street and then multiple that by the number of streets in your town—now you can start to see why there is an estimated 8.7 billion devices attached to the internet around the world!

For a network to work, though it needs to have a “Network Access Point”. This is simply the box which all of the devices on your network are connected to. The connections, however, might be via a wire or wireless depending on the device

In turn that “Network Access Point” needs to have a route out to the outside world (the internet). Exactly what route this takes is variable depending on your setup, but typically if you use BT Internet or Virgin, the “route out” will be your modem which will be the inter-connection between your home network and the network of your Internet Service Provider (ISP).

Your ISP is your connection with the internet—they are your **“Point of Presence”**

Taking the assumption that everyone in your street all use the same ISP (for example BT), you can see here that all of the small home networks all connect into one ISP which provides them all with a point of presence—a way out onto the internet.



*Use these links to find out more about how different networks work!*

<http://computer.howstuffworks.com/internet/basics/internet.htm>

<http://www.howstuffworks.com/wireless-network.htm>

<http://www.howstuffworks.com/home-network.htm>

# Section 9: How the Internet works

But if everyone in your street and town are all connecting to the same ISP, what happens if that ISP goes wrong for some reason??

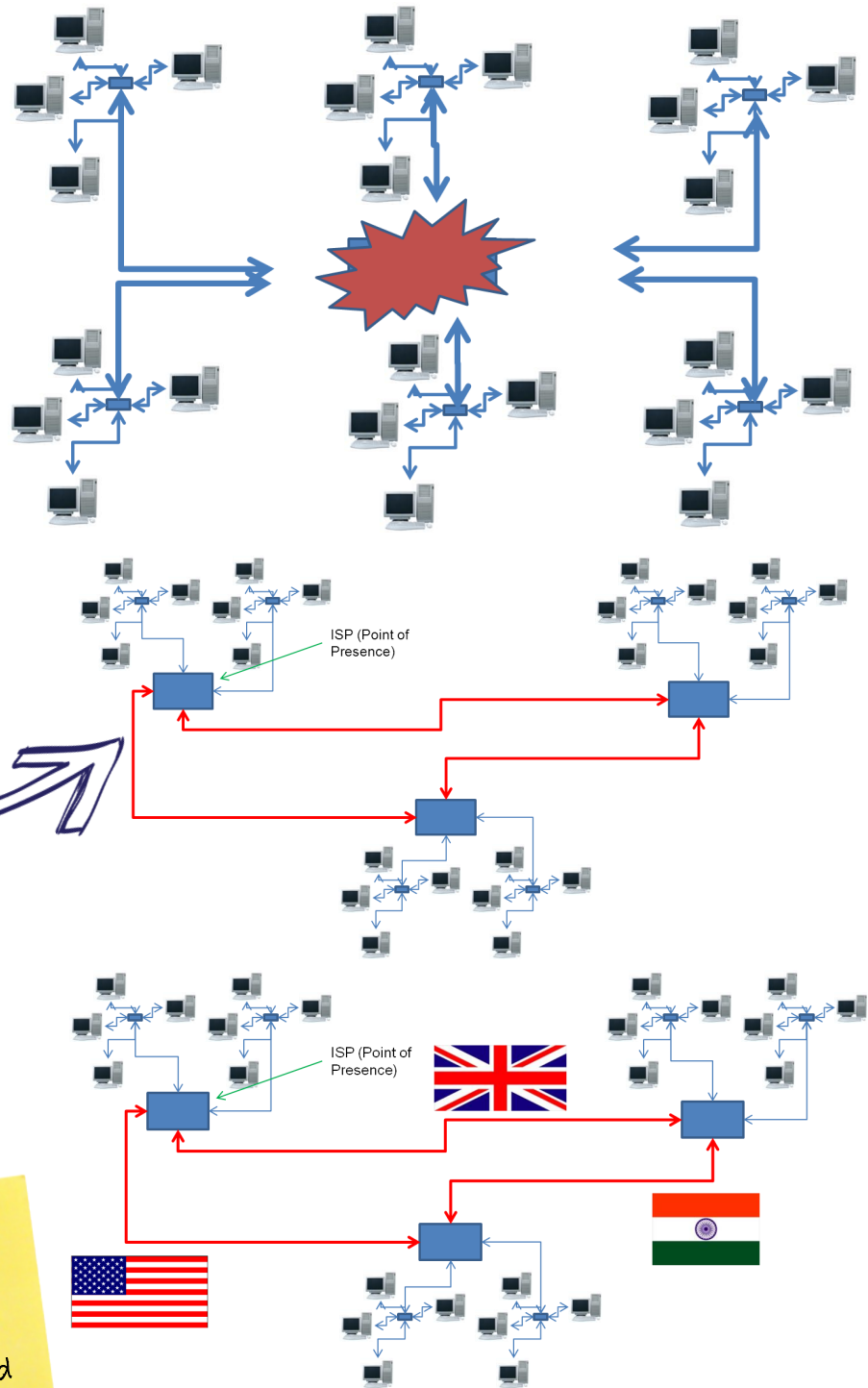
The answer is that no-one in your street or town can connect to the internet—you have suffered from the problem of having a single point of failure.

The internet has ways of overcoming this very problem because all of the networks are, by their very name, interconnected—i.e. Connected in several places. There is little you can do if your ISP goes wrong, but as you can see below, all of the ISPs and other network providers are connected by multiple routes. If one of them goes down for some reason the data travelling from one network to another (for example from your house to a website and back again), can simply take another route.

Even when you use the internet, as the data packets are travelling to and from your PC they can each take different routes to get to their destination!



All of those different networks between you and the destination machine which you are trying to get to (the server) are potentially in different countries around the world. No single country owns the internet and if governments attempt to get involved in the freedom of data travelling across those networks, then the data can simply just take a different route!



Want to see all the networks you go through to get to a destination? Click on the start menu and type in: cmd and then press enter. This will load up a DOS prompt. Type in: tracert www.bbc.co.uk and you will see all the network hops which your request is going through

```

C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\kitz>tracert www.bbc.co.uk

Tracing route to www.bbc.net.uk [212.58.224.113]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  Router
  1  23 ms  24 ms  25 ms  lo1.plusnet.pth-ag2.plus.net [195.166.128.61]
  2  25 ms  23 ms  23 ms  ge1-2.vlan3.pth-gw4.plus.net [212.159.1.31]
  3  25 ms  26 ms  26 ms  ge1-1-8-23.ptn-gw1.plus.net [195.166.129.222]
  4  25 ms  25 ms  23 ms  rt-linx-b.chdo.bbc.co.uk [195.66.226.103]
  5  27 ms  26 ms  26 ms  www13.chdo.bbc.co.uk [212.58.224.113]

Trace complete.

C:\Documents and Settings\kitz>_
    
```



## POSSIBLE EXAM QUESTIONS



What is an ISP (point of presence)?

What is a web browser, why do we need them?

What is a network access point?

Explain what is a domain name?

Explain what a firewall is and why we need them

What equipment do we need in order to connect to the internet?

## What are protocols and what do they do?

If everyone you met spoke a different language to you, you probably wouldn't really get very far. You might understand bits of what people were saying, but may not get everything from everyone. The internet is a little bit the same. There are hundreds of different manufacturers out there, ranging from Apple to Microsoft, to CISCO to IBM to Dell to Sun to pretty much anything in between. Add on top of that, all of these different manufacturers are running different Operating Systems (the software which runs on a computer/device which fundamentally makes it work) and you have the potential to replicate this idea of everyone speaking foreign languages, but in terms of computers all talking different languages.

So how do we overcome this? The answer is simple—you use a "Protocol", a set of agreed commands and language to communicate those commands. As long as the two (or more) different systems communicate with each other using an agreed protocol, then it doesn't matter what language they speak or what Operating System or hardware they are running. They are all using an agreed protocol.

Don't know what this is on about? Think about websites—they all start with **HTTP**. This stands for **Hyper Text Transfer Protocol** (the protocol invented by Sir Tim Berners-Lee). It is the protocol which allows client PCs (regardless of their operating system or web browser they are using) to all communicate using an agreed set of common commands and instructions!



# PROTOCOL

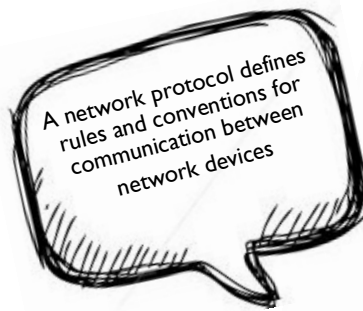


ANDROID



## Protocols: Continued

It is important that you know what the different protocols are and what they are used for. There are thousands out there, depending on the systems which need to communicate and what they need to communicate about. Here are the technical details of the main ones



# HTTP



Hypertext Transfer Protocol – used by web servers and web browser to deliver web pages and web content. Uses port 80. This can be made secure by using the HTTPS protocol which is a secure, **encrypted** version. This is generally used for sites where you have to log in like online banking, social networking and any site which involves money transfer

# FTP



File Transfer Protocol – used to communicate between PCs and servers for uploading/downloading data/files from one machine to another (more reliable than other protocols). It is often used for uploading web pages to a web server. On advantage of it over HTTP is that if the connection is interrupted, it can continue from where it left off when the connection is re-established. A downside, however is that it needs specialist software to run. Uses port 21.

# POP3



Post Office Protocol – used by email clients to connect to servers to RECEIVE emails. Uses port 110.

# SMTP



Simple Mail Transfer Protocol – use by email clients to connect to servers to SEND emails. Uses port 25.



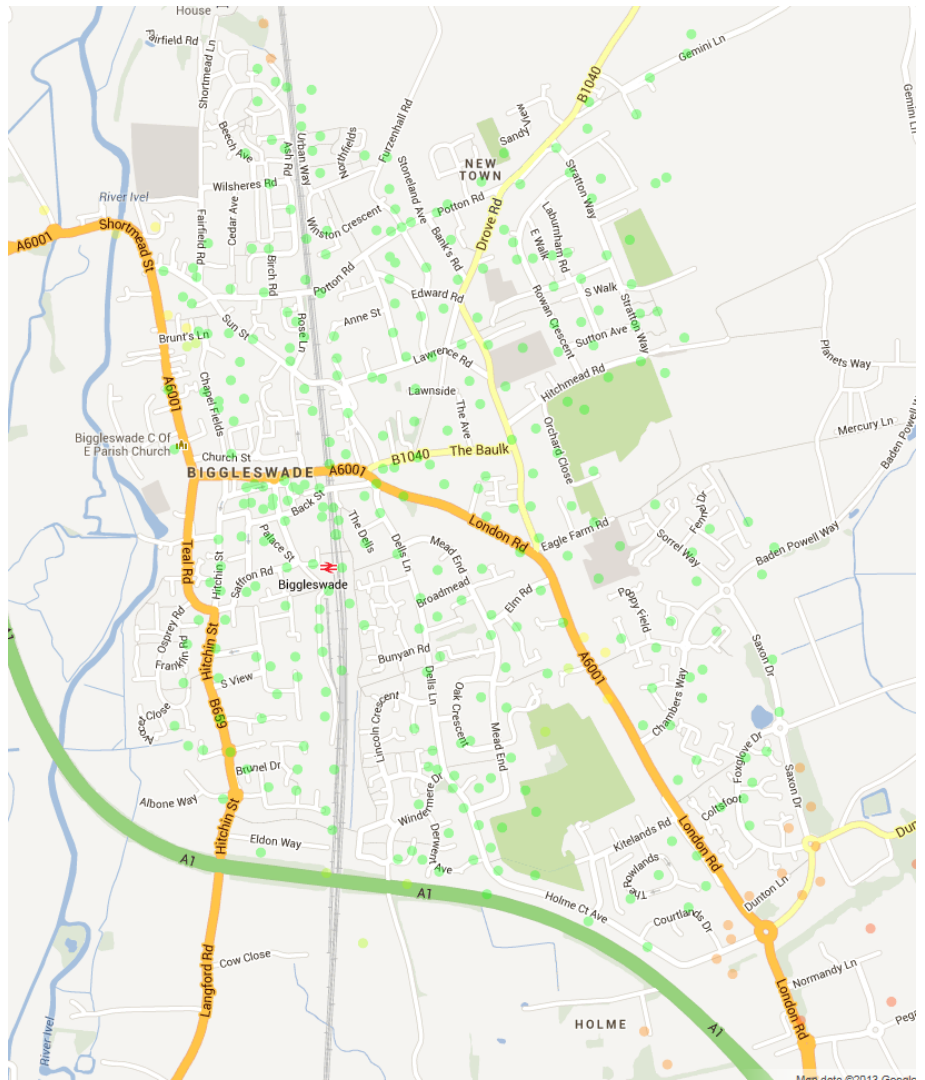
# Transmission Rates

With all of this data being sent from one machine to another all around the world, you may then wonder why the content you are looking at on the internet can stutter and lag. Surely it is just electricity going down a wire? Why does it need to be so complicated??

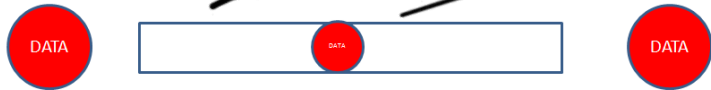
The answer is because it IS complicated and moving that much data around and getting it to the right place takes a lot of processing power, a lot of very complex networking equipment and a huge amount of electrical engineering. To be successful in a networking job, it is very useful to have a solid grounding in network technologies, network programming (primarily CISCO), network configuration and electronic engineering. You also have to be good at maths—a lot of configuration involves calculations. The speed of this data moving around is called your “Transmission Rate”. It is the speed at which data can be moved (transmitted) from one machine to another. How fast the transmission rate is measured typically in “megabits per second” (Mbps). This is your “bandwidth” - how much data can be transmitted over your connection every second.

The speed of your internet connection (your bandwidth) is very dependant on your ISP, the type of connection you have (fibre or copper) and how far away from the exchange you live. This picture shows the approximate connection speeds around Biggleswade. The majority of the town is quick (16Mbps and above), but some areas such as those at the top of Shortmead Street (near the river Ivel) and around Dunton Lane near B&Q are slower (between 4 and 16Mbps per second). This is mostly likely because there are no fibre optic cables in these areas and they are further away from the telephone exchange.

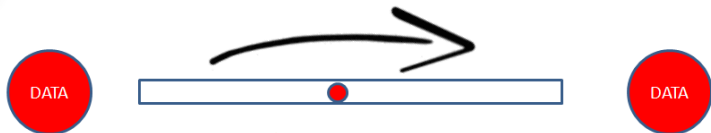
One way of thinking about the bandwidth of a connection is that it is a little bit like trying to squeeze a foam ball down a pipe. The foam ball represents a web page coming from a web server (using the HTTP protocol). In terms of the amount of data, the page is the same regardless of how fast your connection is. If you are trying to transmit that data through a slower connection (like trying to squeeze the ball down a smaller pipe), then it takes longer to get through. Your type of connection and therefore your bandwidth is exactly the same. The higher the transmission rate, the more data can be sent along it per second.



- Fibre Connection (Virgin Media, BT Infinity etc)



- DSL Connection (Normal BT Broadband)

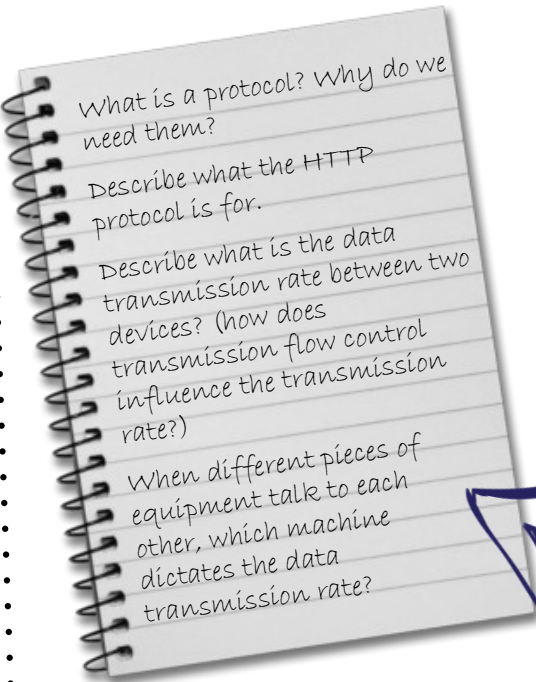


Use this link to put in your postcode and see the estimated broadband speeds where you live

<http://maps.thinkbroadband.com/>

<http://www.thinkbroadband.com/guide/howitworks/>

[http://www.youtube.com/watch?v=7\\_LPdttKXPc](http://www.youtube.com/watch?v=7_LPdttKXPc)



**POSSIBLE EXAM QUESTIONS**

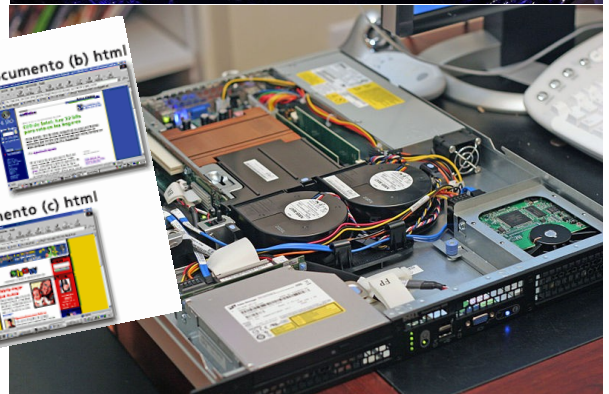


## Understanding the concepts, functions and impact of the worldwide web

The worldwide web is a collection of information, stored on computers connected to the internet. The pages which contain this information are linked together using hyperlinks. This concept of hyperlinking between documents was invented by Sir Tim Berners-Lee while he was working at CERN in 1989. His idea, research and invention became the Worldwide Web as we know it today.

To make it work you need a web server, a web client (like Internet Explorer or Google Chrome) and a connection between the two. The purpose of a web server is to store and deliver web pages to the requests of web clients using the Hypertext Transfer Protocol (HTTP). This means that they store and deliver HTML documents (the actual web pages themselves) to your PC together with all of the associated content (i.e. pictures, sound, videos and interactive stuff)

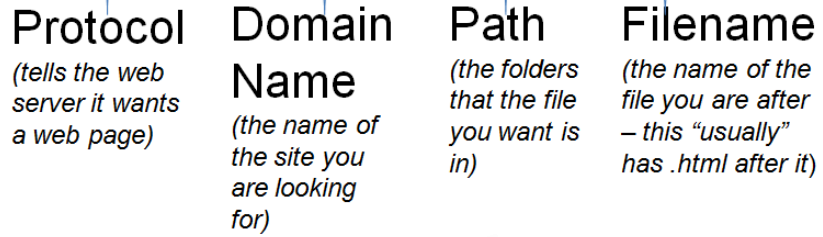
Web pages themselves use a hyperlinks to connect one page with another. A page will have multiple links on it which connect it with other pages either within the same website or to other websites. This mesh structure of different interconnected pages is what forms websites. The links allow you to see how one piece of information is connected/related to another which is what makes websites and the Worldwide Web so powerful.



## Uniform Resource Locators (URLs)

When you type in a website address into your web browser (for example Internet Explorer or Google Chrome), you are building up a structure of different components which are needed in order to uniquely identify the page or piece of content you are after and also tell the webserver how you would that information delivered. Although you may not always need to type in every part of the address, and sometimes you are just clicking on a link, therefore don't need to type any of it! But your web browser will use the whole URL to be able to tell the

– <http://en.wikipedia.org/wiki/Biggleswade>



webserver what information is it after. **The protocol** serves two purposes. Firstly it tells all of the pieces of network equipment between you and the webserver (remember page 4 showing a trace route) that your machine needs to make a connection to port 80 on the webserver. The HTTP bit also tells the webserver what sort of content it is expected to deliver back to you (i.e. a HTML file—a web page).

The **Domain Name** is the name of the site you are looking for in a human readable form. Computers like numbers not names, but if you had to remember the

**DOMAIN**

unique number for every website in the world you wouldn't be able to do it. When you type in the domain name, the networking equipment between you and the webserver translate that into a number which they can use. It is essentially the address of the webserver.

Once you have got to the webserver you are after **the path** tells the server what folder to look in to find the file you are after.

**The filename** on the end is simply the actual name of the file you are after. Typically this needs “.html” after it, but most servers are clever enough to put this in if you don't

**FILENAME**

**PROTOCOL**



*get it right*

**PATH**

## The main features of HyperText Markup Language (HTML)

HTML stands for HyperText Markup Language. It is the way that webpages are laid out. It is handled by the HTTP protocol. A HTML page is made up from a collection of tags which are used to tell the web browser to do different things when the page is displayed.

The <HTML> tag at the start tells the web browser that it is about to receive from HTML content. Everything inbetween the <HTML> tag (the open tag) and the </HTML> tag (the close tag) is HTML content. The <HEAD> tag tells the browser that everything within the that tag is information for the heading of the page. Logically therefore, the <BODY> tag tells the browser that everything within the open and close <BODY> tags is the main body of the page.

Different tags perform different functions. Examples shown here are:

**<h1>** - This changes the size of the text to be a heading

**<a href>** - This makes a hyperlink

**<img src>** - This tells the browser to find the file that is in the quotes and display it as a picture

```
<html>
<head>
  <title>Welcome to My Website</title>
</head>
<body>
  Welcome to My website
</body>
</html>
```

```
<html>
<head>
  <title>Welcome to My Website</title>
</head>
<body>
  <h1>Welcome to My website</h1>
  <hr />
  <font color=red>This text is in red</font>
  <a href=http://www.google.com/>go to google</a>
  
  <p>This text will be my first paragraph. I can
  add more later</p>
</body>
</html>
```



Use this link to learn more detail about how URLs work

<http://www.youtube.com/watch?v=SMxx9XEF6m0>

To see a list of different HTML tags, use this link. Be aware though, there are LOADS!

<http://www.w3schools.com/tags/>

## Internet Browsers and Search Engines



There are lots of different web browsers out there, depending on your device and your operating system. Although they may each look slightly different and operate in a slightly different way, their role and purpose is the same for all of them. They are there to translate the HTML content (code) which is being delivered by the webserver and display that content as a webpage on your screen for you to view. As you interact with that page (clicking on buttons, rolling over links etc), your web browser is transmitting those actions back to the webserver so that it can respond to your requests.



Search engines are available to help you to find the content you are looking for on the internet. With billions of pages out there and more being made every second, it would be impossible to keep track of it all.

Search engines help us to find content by keeping an index of lots of pages out on the internet. Their role is to keep this index up to date and use it to deliver relevant results to internet searches to help users find the content they are after quickly and efficiently.

<http://www.youtube.com/watch?v=KyCYoGusqs>

Use this link to find out more about how Google works

Use this link to set some amazing stats about how big the internet really is!

<http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/>

# Understand the purpose, concepts, processes and implications of email

Consider the world without email for a moment. According to the Office of National Statistics 56% of the UK population have broadband internet and they estimate 70% of the UK use email at least once a week. That's 44 million people!

*discussion*

Questions you could ask yourselves and those around you:

- What are the benefits over old / other methods of communication?
- What are the advantages and disadvantages?

But email does not just mean someone sending an electronic letter from one person to another—there are a number of different ways of doing it. Below is a table showing three different methods

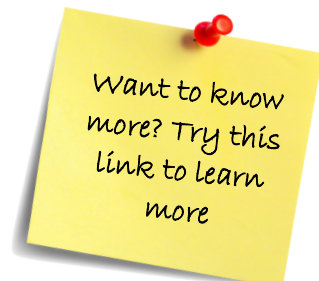


Webmail	Email Client	Push Email
Examples include Gmail, Yahoo Mail, Hotmail	Examples include Outlook, Apple Mail, Thunderbird	Blackberry email
Messages can be accessed from various computers or mobile devices at different locations, using different web browsers. Files can be attached to email and sent to one person or multiple people with ease.	Mail can be read offline (you don't have to be connected to the internet to read email which has already been downloaded). Files can be attached to email and sent to one person or multiple people with ease.	The email is pushed to the phone rather than the usual method of email where the client has to go to ask for the email to be downloaded. This means you get the email faster and don't use as much data in your plan "asking" for email that isn't there yet.
Some kind of backup is usually provided by the server.	Files don't need to be redownloaded when you need them	
With limited bandwidth, access to long messages can be lengthy, unless the client keeps a local cache.	Searches are faster because you are searching local files on your computer rather than on a server	
There may be privacy concerns, since messages staying on the server at all times have more chances to be casually accessed by IT personnel, unless end-to-end encryption is used	If you are not near the machine they are on you can't gain access to them	
	Backup is the responsibility of the person who has the machine where the emails are stored	

When you click "Send" your email software (either an email client or webmail), converts the message into the email format and then attempts to connect with the SMTP server at your ISP (look on page 6 for protocols). The SMTP server will talk to the Domain Server at your ISP to get the address of the domain you are trying to send your email to. Remember from page 9 that the Domain is the human readable name of the server. A Domain Name System (DNS) server translates that name into a number which is the actual address of the server. Once the SMTP server at your ISP knows the address of the server you are wanting to send your email to, it will connect to it across the internet (going through whatever hops are needed to get there) and deliver the email. The receiving email server will look at the email alias (the bit before the @ symbol) and based on that will store the email ready for the recipient. Next time the recipient connects to the internet and tries to read his email, the newly received message is automatically downloaded.

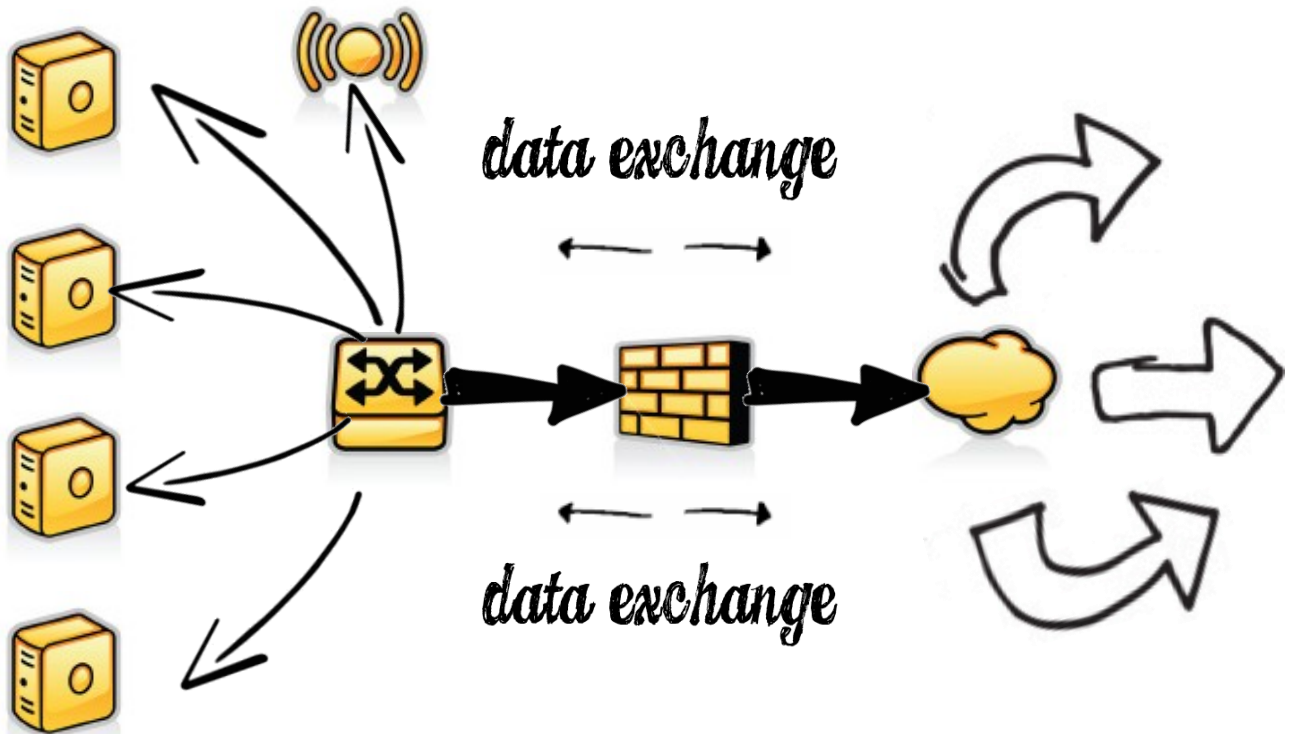
So next time you send an email, remember that your message has gone through at least 3 servers to get to you, and probably a whole host of other kit in between!

<http://computer.howstuffworks.com/e-mail-messaging/email.htm>





# Understand the concepts, processes and implications of data exchange and compare different methods



Data exchange is simply the passing of data between computers in a network, including the internet (which if you remember is simply just interconnected other networks). In downloading this document, you have exchanged data between a server and your PC. How this happens, however isn't just a case of plugging it and hey-presto, it is more complex than that. Data can be transmitted in different ways and different devices use different modes for doing it. As you would expect, there are also different types of hardware and software involved depending on what type of transmission you actually want. Below is a table which describes the main types of transmission mode used by different devices

Transmission Mode	Digital Devices that use it	Advantages and disadvantages
Simplex	Commercial Radio and TV Baby Monitors Wireless Microphones Radio Controlled Models Surveillance Cameras GPS	Simplex transmission means that the data exchange is <b>ONE WAY ONLY</b> . A good example of this is typically any system where the data is broadcasted, but there is no way of knowing whether or not it has been received. This reduces the data rate and is simpler to do because you only have to worry about one route of transmission. A disadvantage, however is that it is not interactive. For some systems, like GPS, however it doesn't have to be.
Half Duplex	Walkie-Talkies Very old modems	Although the transmission is two way, <b>ONLY ONE DIRECTION AT A TIME</b> . A good example of this is a walkie-talkie where you need to wait for one person to stop talking before you can. Modems used to work like this. This allows interactivity, but is slow because one device has to wait for the other one to finish before it can start transmitting
Duplex	Telephones (including Mobile Phones) Computer Networking Printers	Duplex (or Full Duplex) allows transmission in <b>BOTH DIRECTIONS AT THE SAME TIME</b> . This is much faster because devices don't have to wait for each other before they start transmitting. It also reduces data collisions. It is more complicated, but modern technology is much more advanced and typically doesn't really have any problems with this sort of concept any more.

### Real-time communication

As the bandwidth increases to people's homes and businesses, we become more reliant on the internet for different tasks and for communication. One of the uses of real-time communications is Voice over IP (VoIP). One of the best known suppliers for this sort of service is Skype (though now they additionally handle video conferencing over IP also). To be able to use VoIP services you need several pieces of equipment and software.

You need to have a computer or VoIP phone which is capable of connecting to a VoIP service. This can either be done through dedicated hardware like a phone, or it can be software running on a PC, laptop or even a smart phone.

You then need a modem, or some other method of communicating with the internet. This is because VoIP is over IP (internet protocol). It needs the internet in order to make the communication possible.

Finally you need a service provider who can offer you VoIP services. It may be that if you are using Skype etc you don't need this—the whole lot is handled by your laptop, but if you are wanting to connect your VoIP phone so it can make calls to normal landlines, you need to have a dedicated service than can offer this sort of thing.



LAPTOP



VOIP PHONE



SERVICE PROVIDER

MODEM



Video and sound, however takes up a lot of bandwidth because it needs a lot of data per second to work. As you saw on page 7, the greater your bandwidth, the more data you can transmit per second. VoIP calls and video conferencing calls need more bandwidth because they use more bits per second. In order to make this work we need to compress the data so that it can be transmitted more quickly over the network.

This is done using CODECS.

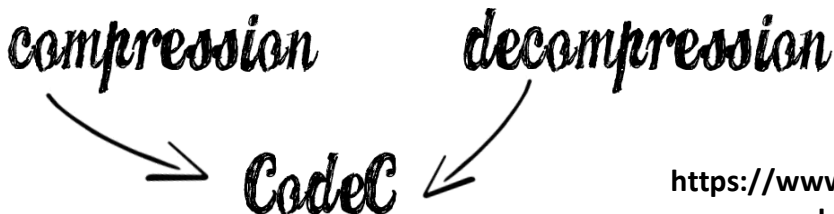


If we take an average 360p image (roughly average to the default size use for YouTube videos), that is 480 pixels across by 360 pixels down. This makes 172,800 pixels for one picture (width x height). At full colour (24 bit), that makes 518,400 bytes ([number of pixels x number of bits per pixel] / 8). This is 506KB or roughly half a megabyte. At a fairly average 15 frames a second this would make a whopping 7.5Megabytes per second. You would need a 60 to 100 Mbit fibre connection to be able to deliver that much data! The answer is to compress it with a codec so that the amount of bandwidth needed is much smaller. Codec is a mixture of the words "Compression" and "Decompression". They work by removing unnecessary data before transmission. Examples could be frequencies the human ear can't hear or cutting out background noise so it doesn't need to be transmitted. There are a number of different codec out there and which one you used depends on how much compression you want vs the quality of the sound. Typically the harder you compress your transmission, the smaller the bandwidth requirement, but also the lower the quality of the sound.

480



360



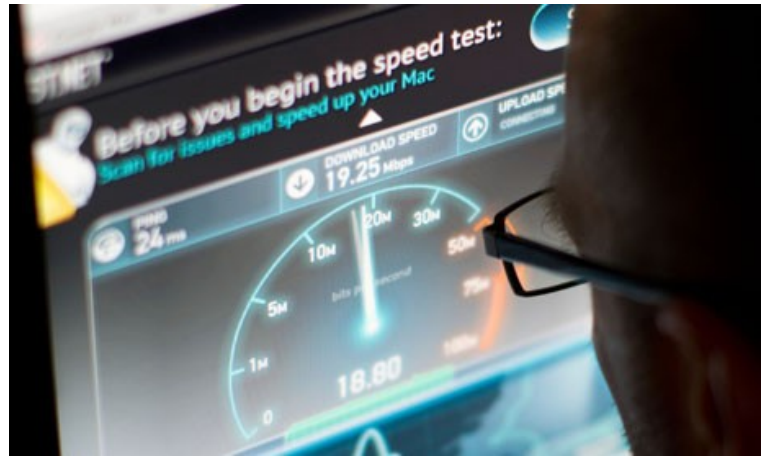
Want to know more? Try this link:

[https://www.youtube.com/watch?v=bFmWRcTn\\_D0](https://www.youtube.com/watch?v=bFmWRcTn_D0)

## Comparing methods of transmission

Whether you are wanting to watch online movies, or download the latest games, it is fair to say that in today's modern world we all want decent fast broadband. To achieve this you need to have the right kit, the right cables and (sadly) live in the right place.

Below is a table which shows the characteristics of different transmission methods



Transmission Method	Transmission Mode	Approx Bandwidth and Effective Range
Fibre Optic	Full duplex	Typically up to about 100Mb/sec. Fibre Optic cables typically can go many miles before they slow down the connection. This is currently the best type of connection to have.
Wireless (infra red)	Full duplex for networking. Simplex for remote controls	Short range—typically only a few meters. Infrared needs to have line of sight (ie. No obstructions like walls etc in the way). Depending on the type of IR connection the bandwidth is roughly between about 115Kb per second and 4Mb per second
Wireless (WiFi)	Full duplex	Wifi has reasonable range, depending on the version you are running. It will pass through walls etc and typically will go about 20 meters (though you can get more powerful aerials). Bandwidth is very much dependant on the distance between your device and the wireless router + also what is between you and it. Speeds ranging from 50Mbits per second up to 150Mbits per second are normal.
Wireless (Microwave)	Full duplex	These are usually used for specialist needs. Microwave links can go 30 to 40 miles, but the need line of sight—i.e. Nothing in the way. Although they can be used to transmit data, they typically are used for radio and TV
Wireless (Satellite)	Full duplex	As the name suggests you are using satellites for your internet connection! On average these have a bandwidth of about 18Mbits per second. One of the main problems with satellite networking, however is latency—the time it takes for the signal to get somewhere. This is because you are going via space!
Copper (normal wires)	Full duplex	Normal ADSL broadband runs on normal telephone wires. It is hugely influenced by the distance between you and the telephone exchange. Speeds can range from less than 1MBit per second up to about 20 Mbits per second.



<http://www.thinkbroadband.com/guide/fibre-broadband.html>

<http://news.bbc.co.uk/1/hi/technology/8068598.stm>



Identify the transmission mode and describe the features of that mode for the following devices: Mobile Phone and a Printer

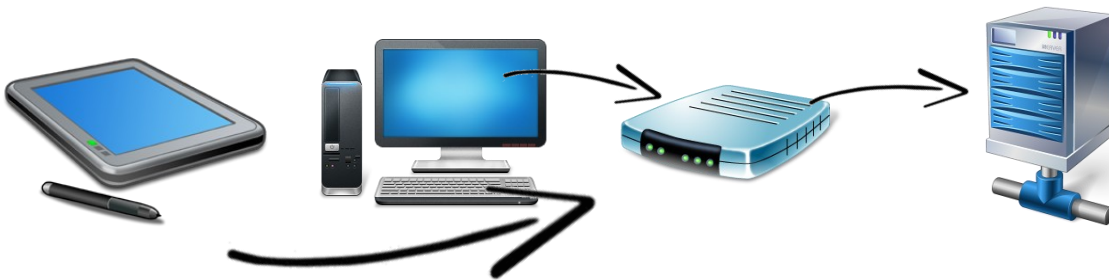
What are the advantages of Fibre Optic broadband over normal phone dial up such as ADSL?

What does CODEC stand for and why do we need them?

## POSSIBLE EXAM QUESTIONS

## Understand the concepts, structures and implications of networking

What kit do you need to make a network at home actually work. Believe it or not, it is actually fairly simple. You need a networkable device (like a PC, smart phone or tablet computer), a modern or router (a network access point) and a service provider to give you a point of presence on the internet.



But this is just the hardware, there is still a lot of processing which goes on between you and the webserver which you are surfing the internet. Much of this processing used to be done by the servers, but as computers become more powerful and web browsers have more features added to them, the amount of processing the servers have to do is changing.

### client side processing

This is where scripts are processed by the computer / device which is displaying the page. Examples of this could be error checking, for example confirming that someone has entered information correctly, plus handling of local data like game or browser settings. The advantage of client side processing is that it doesn't place as much load on the web server

### server side processing

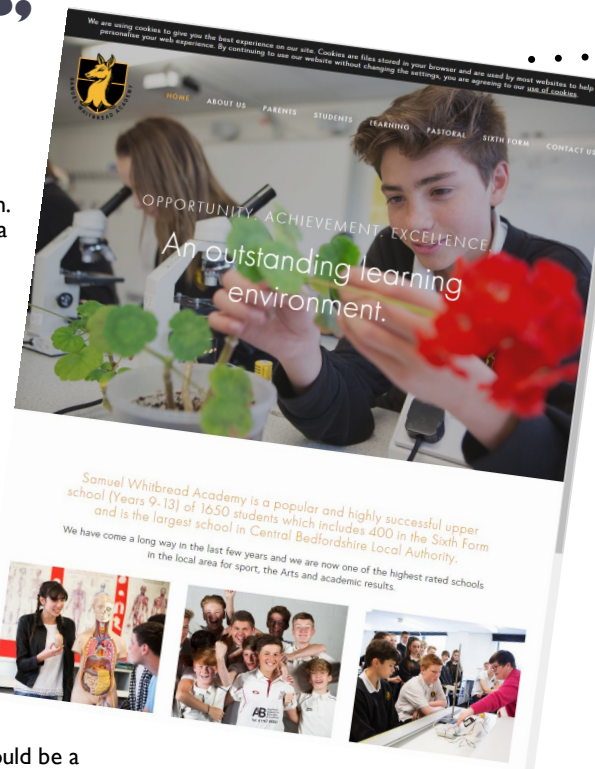
This is where information (either from the web browser or elsewhere) is processed by the server and used to make a decision / choice of some sort. Examples include log in scripts to confirm that you are who you say you are. The advantage of server side processing is it can be easily upgraded by the

get it right



# Understanding the concepts, processes and implications of data storage.

- Many websites which require heavy server side processing are usually database driven.
- Web pages are not stored as traditional HTML files, but as information / data within a database. As the web browser requests pages (using the HTTP protocol), the pages are build dynamically by the database and delivered to the browser. This is exactly how the school website works.
- The database behind these sites needs a Database Management System (DBMS) in order to be able to work efficiently and store all of the data required for the website to work.
- These databases can often be accessed through a web browser which simply means that although as the user you are clicking on hyperlinks within the administration pages of a site (using the HTTP protocol), in the background your web browser is translating those requests into something more useful for the DBMS server to be able to use and work with.
- Typically the online database which these systems use follows a structure which is something similar to what is shown below:



*fields*

A field contains a single piece of data. That could be a number, some text, even a video. It is a single piece of data. In order for the computer to work on it though, it needs to know what data type it is.

*data types*

The data type tells the computer what sort of data it is looking at in the database. Examples could be number, text, website address etc. Knowing what data type a specific piece of data is means the computer can work efficiently with it.

*records*

Once all the fields about a data subject have been completed, this data is saved together as a record. For example, if all the fields contained information about a person like "name", "address", "date of birth", when all of this information was combined together it would form a record—all the information about one person, one data subject.

*tables*

Combine all of those records together (for example one for each student in a class) and you would have a table. A table is all of the records in a particular category.

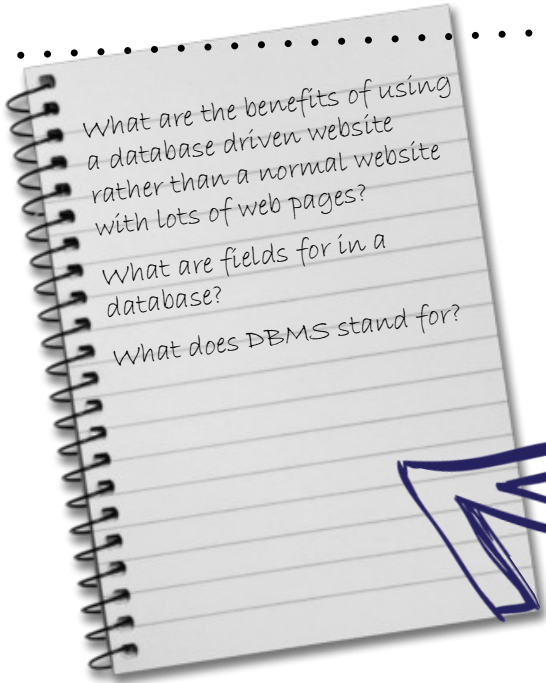
*relationships*

This shows the connection / relationship between data in two different records or tables or even between multiple database. Keeping these up to date are what makes database driven websites so much more powerful.

[http://www.teach-ict.com/gcse\\_new/databases/terminology/miniweb/index.htm](http://www.teach-ict.com/gcse_new/databases/terminology/miniweb/index.htm)

Use this link to find out more about how databases work!





**POSSIBLE EXAM QUESTIONS**



**Practice exam**

A large rectangular area with a black border, containing ten horizontal dotted lines for writing answers.

# Types of Threats to Data

In years gone by, the main danger to people was through weapons. In the modern world, there is a new danger—a cyber threat. As a data subject, you are worth money. Your name, address, phone number, email address—it is all valuable information to someone. For some people it is useful so that they can contact you to try to trick you in a scam, but for others, data can be used for very sophisticated identity fraud, stealing money and goods without you even noticing it is happening.

This section gives details of some of those threats and different things you can do to avoid becoming a victim.



## opportunistic threat

Use this link to see the top five threats to data currently

<http://www.bbc.co.uk/news/technology-17846185>

As the name suggest, this is the threat that comes from someone who finds a computer unattended that has been logged in to a system. You may have experienced this when your friends write something stupid as a Facebook status when they find you logged in on a PC, but imagine a more serious system like a bank or medical database—with that sort of information about someone it would be very easy to commit crime.

## computer virus

Typically these are small programs which are self replicating and can copy themselves from one computer to another. The damage they do can vary from virus to virus. Some just cause mischief, like changing settings, but others can steal information, sending it to another computer somewhere to be collected, used and sold on.

# malware



Malware is malicious software—software which is hostile, intrusive or annoying. Examples of this include Trojan Horses (software which appears to be ok, but in reality is allowing access to your system without you realising it, spyware, and adware. It might be that the malware is just collecting information about you to deliver targeted adverts, but how do you know that it isn't collecting more information about to send to a hacker somewhere??

# phishing



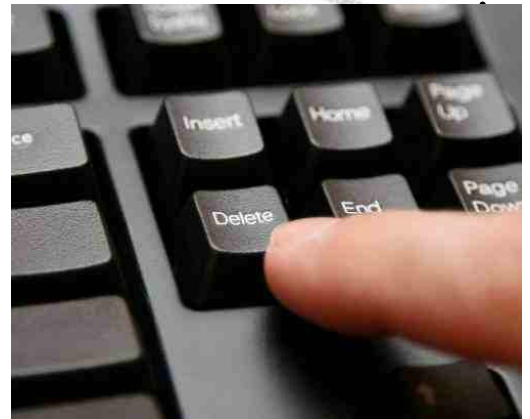
This type of threat is much simpler and relies on tricking the human to give the information rather than using sophisticated code to find it. A typical method is that you receive an email which appears to come from a legitimate source, warning you of a problem and asking for your password or financial details. The user enters those details, which are then sent to a different computer somewhere to be collected and used!



# accidental damage



We've all done it! You click the wrong button and delete your work, you don't save your work and the computer crashes or there is a power cut. That sinking feeling that you have just lost a lot of data and it is YOUR fault. It doesn't always have to be your fault though—fire, flood, theft, all of these involve potential loss of data, therefore accidental damage is just as serious as the other "more sophisticated" methods.



# discussion

In small groups, research some examples of high profile companies who have had their systems hacked. Answer the following questions:

- Why do you think that company was targeted?
- What do you think were the intentions of the hackers?
- How did the company respond to the attack?
- Do you think it is possible to create a secure network that will never be hacked? If so, how would you go about creating this?



<http://www.heavy.com/tech/2013/03/a-timeline-of-companies-that-have-been-hacked-in-2013/>



# Importance of Security

In 2012 it was estimated that the UK received up to 1000 cyber attacks every hour! It is likely this will have gone up since then. With the rise of the influence of the internet, the importance of security online is more than ever before. Below are cases which highlight this.

<http://www.thisismoney.co.uk/money/saving/article-2096060/Hackers-crack-new-online-banking-security-putting-25m-people-risk.html>

Any organisation which trades online (banks being a prime example), rely on a reputation for being secure. If this reputation is damaged, people might be put off from using those organisations. The link above shows how even the "secure pin" devices have been cracked. Is nothing secure?!!

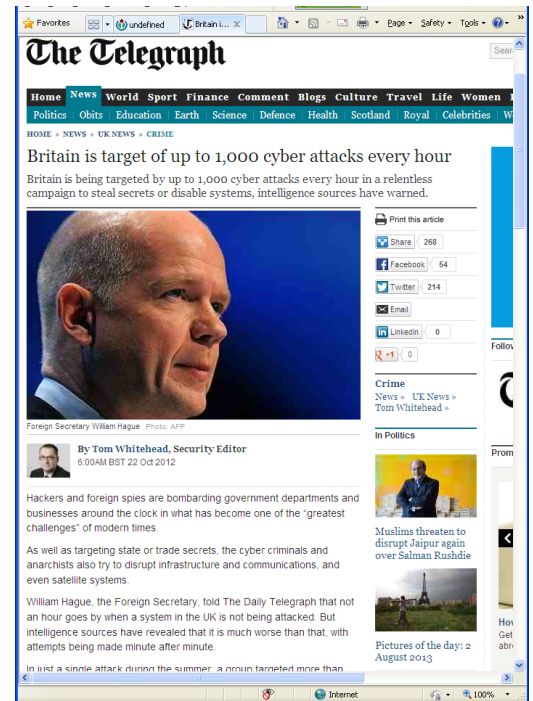
<http://edition.cnn.com/2013/07/19/opinion/hayden-snowden-impact>

When an organisation's secrets are spread to the competition, then advantages which that organisation has are lost. Big technology companies rely on secretive work to remain ahead of their competition. How would Apple feel if Google knew what the new iPhone specifications were going to be? On a wider scale though, the link above explains what Edward Snowden did in mid 2013, releasing a considerable number of US government secrets. The impact was considerable embarrassment for a number of big countries (including the UK) and also admission by a number of big internet companies that they have been involved in government requests for information about people.

<http://www.bbc.co.uk/programmes/b006mg74/features/consumer-advice-identity-fraud>

As more and more information is stored online about people, so the danger of what happens if that information is stolen, becomes much greater. Identity theft is when someone poses as you. This can be in order to gain financially, or to steal, commit fraud, or gain access to systems which they wouldn't normally have access to. The problem comes when you suddenly find that you are in trouble for what they have done. Use the link above to see a program by the BBC Watchdog team all about the problems of identity theft.

Any company which collects and stores information about people in the UK must sign up to the Data Protection Act. This is run by the "Information Commissioner's Office (ICO). Signing up to the act places a legal obligation on a company to store, transmit and use peoples' data safely, securely and responsibly. You would think that this is common sense, but you only need to type in "company fined by ICO" into Google and you will find hundreds of cases where companies have been fined by the Information Commissioner's Office for NOT keeping data secure or for using it inappropriately or illegally—it is happening ALL the time. Every time you receive a random phone call, text or email offering you free compensation for an accident you didn't have, it is quite likely because your details have been sold on, given away or stolen.



<https://www.youtube.com/watch?v=WDUS6-LSdPs>



get it right



This is what the Data Protection Act (1998) covers. It would be good to remember these

Data Must be:

- Fairly and lawfully processed - i.e. only used for legal purposes
- Processed for limited purposes - i.e. only used for what the data subject wanted
- Adequate, relevant and not excessive - i.e. only relevant information is stored
- Processed in accordance with your rights
- Accurate
- Not kept for longer than necessary
- Not transferred abroad without adequate protection
- Kept secure

Remember to read the question and think "what is this asking for?". You NEED to be able to understand the exam question before you can correctly answer it

A business requires its staff to use strong passwords.  
Give an example of a strong password and explain why it is strong.

Give examples of work sort of information phishing attacks usually try to steal.

You are setting up a new business with 5 employees. What measures do you need to take into account to ensure the integrity of the data in your company?

**POSSIBLE EXAM QUESTIONS**



# Preventative and Remedial Actions

Now that you have seen a number of the dangers and threats to your data, the next, most obvious question is: How can you make your data more secure and limit the amount of damage which can be done.



Most attacks on data is via electronic means - i.e. across a network. A physical barrier is simply a physical way of stopping that from happening. This could be as simple as switching the computer off when it is not in use, or locking it away (this is a good example when if you are talking about laptops and tablet PCs or phones). It could also mean putting the computer somewhere which reduces the possibility from damage from fire, flood, electrical interference. Did you know that one of the physical barriers at school takes advantage of the size of the school. The servers where all your work is stored are located at one end of school, but the backup tapes which back up all your work each night are at the opposite end. Obviously the backups are taken off site to ensure safety, but it would be highly unlikely that a fire could destroy the whole school, so this physical barrier between the servers and the backup system ensures data is safe.

## physical barrier



Passwords are a sequence of characters (numbers, symbols and letters) which only you should know. A password will allow you access to your data, but not others. It is important to think about your password to make it strong. Your boyfriend or girlfriend's name would be way too easy.

## password control



Some tips on how to make a strong password. These would be easy things to remember for the exam!



passwords should be at least 8 characters

They should use a combination of lower and upper case letters

They should include numbers and symbols!

They should be hard to guess—not an easy combination like abc123 or the favourite we see in ICT lessons: "qwertyuiop"

Make sure it isn't just your name with a number after it!

Avoid words from the dictionary—a computer can guess these in seconds by trial and error



You are subject to this almost all the time, but without realising it! Different people within an organisation have different levels of access to data. For example a network administrator will have more access to different data than a normal user. In the same way at school you have access to your home drive and the shared drive, but not to the teacher drives. Restricting access means that you don't have access to data which you shouldn't be able to see, edit or delete. Don't be all paranoid about it though, it works both ways. Normal teachers don't have access to your home drives - they have to ask to view files and data there. Again, this stops them accidentally deleting your work which if you remember was one of the main causes of loss of data!

This is software which is designed to intercept (i.e. find) viruses before they enter your computer system. Anti-virus software monitors your network activity (internet browsing and general use of a network), files and email to look for suspicious files and application activity. If it sees something it doesn't like, it can isolate it in a quarantine or stop it from running. In some cases it can remove and repair files. It is very important to have anti-virus software and keep it up to date because new viruses come out all the time. Remember that on page 2 and 3 you saw that viruses and malware were two different things. Equally, there is specific software for intercepting viruses and specific software for intercepting malware - don't assume they are the same thing!

If all goes wrong and your data is lost, then having a backup is useful so that you can get your files and data back again. There are several different ways of doing this including onto CD/DVD or memory stick - basically anything where you can make a copy of your file(s). Companies use magnetic tape drives and whole server systems to backup their data because a CD or DVD wouldn't hold enough data. You can also backup your data across a network or even the internet using services like Dropbox, SkyDrive and Google Drive. (see page 2 of the "Learning Aim A" revision guide for more details on Online Storage.)

It is important that your backup tapes are not in the same place as the original data (i.e. the computer itself). This is the "physical barrier", explained on page 6. Many types of backup exist including:

- Full backup - where ALL the data on a drive or folder is backed up. This is great because it means you have everything backed up, but depending on how much data you have, this can take a while
- Incremental backup - where only the files or data which has changed since the last backup was made. This is good because it is much faster - you are only backing up the changes, but is bad because it means that to recover a file you potentially need to have more than one tape in order to get all of the bits you need.

Ever wondered how Google backups up all of it's data? The answer is by using huge tape drive systems with robotic arms which move the tapes around inside.

It is estimated that the Google Earth Maps alone use up about 20,500 terabytes of data and that the servers around the world process about 24 petabytes of data each day! Backing up data is VITAL!

<https://www.google.com/about/datacenters/inside/>

<https://www.youtube.com/watch?v=avP5d16wEp0>

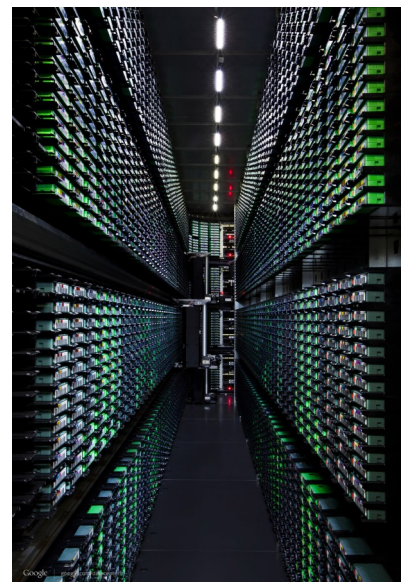
# access levels



# anti virus software

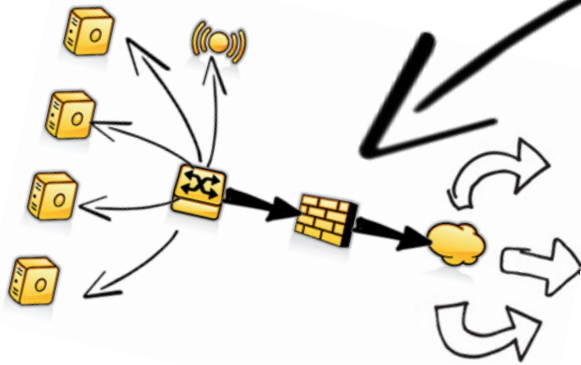


# backup and recovery



A piece of software or hardware which monitors all network traffic which is arriving and leaving your computer. All of your emails, internet browsing traffic, streaming videos and audio. A firewall can be used to control what applications and services have access in and out of your computer and hopefully should stop unwanted or harmful traffic. There are different firewalls in different places which serve different purposes. For example at school, the computers have software firewalls to stop unwanted traffic from one machine to another. There is the school firewall which can be used to stop unwanted in-bound traffic and control outbound traffic, for example what websites you can go to. There is also a county firewall which can also block what websites ALL the schools in Bedfordshire can go to. The objective is to keep people safe and prevent problems from dodgy sites. The firewall also works hand in hand with the access levels which you read about on page 7.

firewalls ...



This shows a hardware firewall. All network traffic has to go through it, so it can monitor everything from all the computers

When data is encrypted, it is turned into code which you need a specific key to unlock. An algorithm (essentially a really complex maths equation), sometimes also called a cipher, is used to encode / encrypt the data before it is transmitted (either over a network or by file on a memory stick / CD etc). If anything else tries to read that data without the cipher, then it will just appear as garbage. The machine which is meant to receive the data will have the correct cipher and uses this to decode / decrypt the data so it can be read. This is useful as a preventative measure to stop files and data from being intercepted during transmission and the information being stolen.

encryption



## Personal Safety

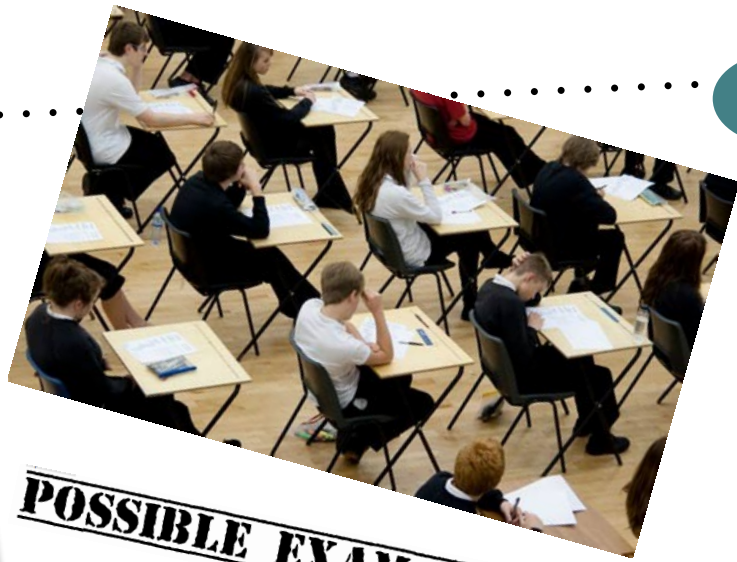
Think about how much personal information you reveal about yourself on social networks and via instant messaging systems. It is all too easy to give away information which could threaten your safety, security or reputation. The most obvious threat is from people who might not be who they claim to be. How much information you reveal about yourself, however can also have an impact on you when you didn't expect it. Remember that employers often look at Social Networking sites to see someone's background - what if that information isn't correct? Do you really want that photo of you to be available for everyone to see? Check your personal settings, you might find that the default settings are not as secure as you would like them to be. Think about what information you put online about yourself - if you put your pet's name on a social networking website, could someone then guess your password?

Identity Theft: When someone steals your personal details in order to use them to open bank accounts, get loans or passports etc in your name

get it right







Give three examples of threats to computer systems.

Give the methods that you can use to reduce the threats which you lists in question 1

How can you help to prevent identity theft when using social networking sites?

## **POSSIBLE EXAM QUESTIONS**



## **Practice exam**

A large rectangular area with a black border, containing multiple horizontal dotted lines for writing, intended for the student to answer the practice exam questions.

Use this page to write your own notes



