

Contents

		Page
Networking	Cloud Computing	3
	Public Cloud	3
	Private	4
	Hybrid	5
	Cloud-based Services	5
	Advantages of Cloud-based Services	5
	Disadvantages of Cloud-based Services	6
	Web Hosting	6 – 7
	Types of Hosting	7
	Trends: Networking and Connectivity	8
Security Risks	Introduction	9
	Spyware	9
	Phishing	9 – 10
	Keylogging	10
	Online Fraud	10
	Identify Theft	11
	DOS Attacks	11 – 12
	DDOS Attacks	12 - 13
Security Precautions	Introduction	14
	Encryption	14
	Public and Private Key Encryption	14
	Digital Certificates	15
	Digital Signatures	16
	Server-side Validation of Online Form Data	17 – 18
	How Does Server-side Validation Work?	19
	Biometrics in Industry	20
Economic Impact	Economic Implications: Introduction	21 – 22
	Competitive Advantage	22 – 23
	Global Marketplace	23 – 24
	Business Costs	24 – 25
	Scalability and Maintainability	26 – 27
Social Impact	Social Implications: Introduction	27
	Censorship	28
	Freedom of Speech	28
	Privacy	29 – 31
	Encryption	32 – 33
	Global Citizenship	34
	Online Communities	34

Cloud Computing

Cloud computing is a term used to describe the provision of services for data storage, applications and collaboration through an online system, accessed over a network. Cloud services will not work unless network access is available, but as network access has become more common and more reliable, cloud computing has become more popular.

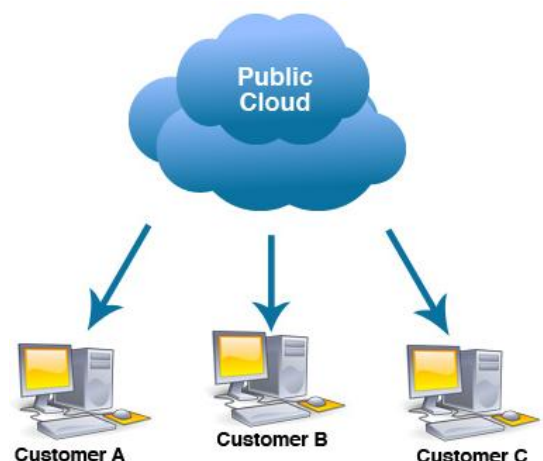
Cloud computing services are available from any location that is on the network. This makes access to cloud services very flexible. It also means that local storage does not have to be used to store data, as it can be stored "in the cloud" (i.e. on the servers of the company providing the cloud service).



Behind the cloud services, companies maintain servers that are set up to provide services to each user. This setup can be highly complex, as servers are spread around the world and requests are balanced out between servers to handle high volumes of traffic. Cloud servers hold large volumes of data and must also make sure this data is up to date at all locations. Cloud computing architecture allows companies to design a system that can scale from handling hundreds of users to millions, without redesigning their applications.

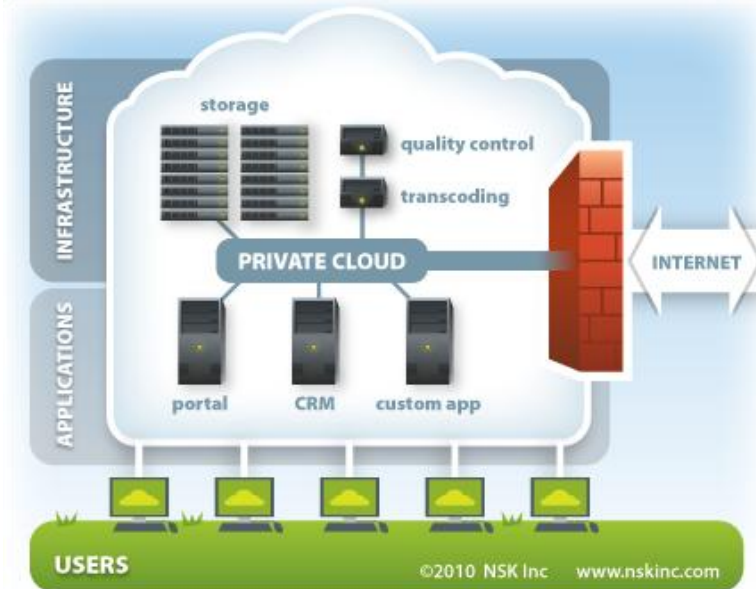
Public Cloud

Public cloud services are available for any user to log in and use. Access to data in the cloud is still controlled (users cannot see each other's files, for example) but access from the Internet makes this a more open approach than a private network. Whilst security issues caused by the possibility of uninvited users can be important in a public cloud service, companies that use public cloud services can be reassured that the providers are providing the same level of security to all parts of their service, which may mean an effective level of security for each organisation using the services. For this reason, public cloud providers like Amazon and Google, who provide cloud services through their own servers, are popular with businesses.



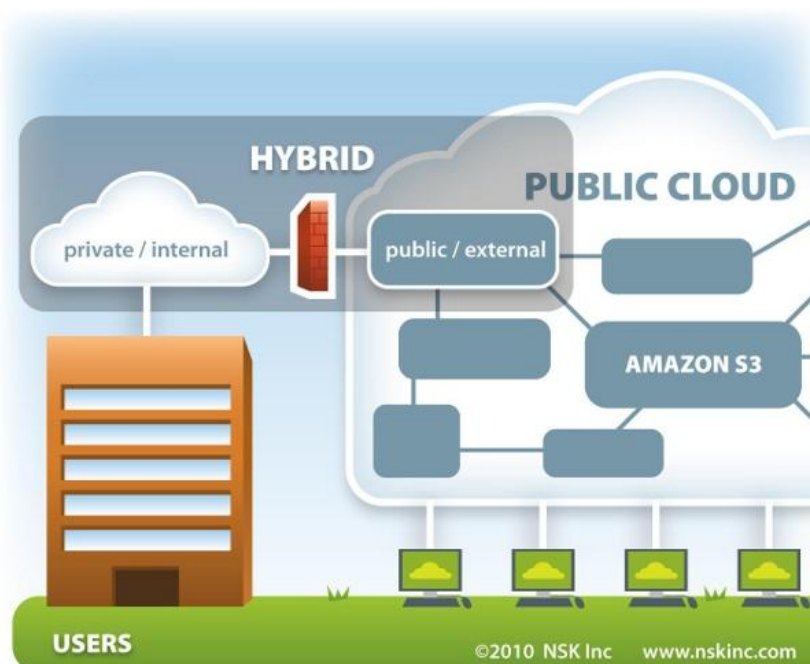
Private Cloud

Private cloud services are privately, self-hosted servers which can be accessed from anywhere within an organisation. This allows widespread sharing of documents and communication without user accounts being accessible from a public cloud provider. A private cloud will be expensive to set up, as a company must set up its own data centre operations to maintain servers for the cloud services to run on.



Hybrid Cloud

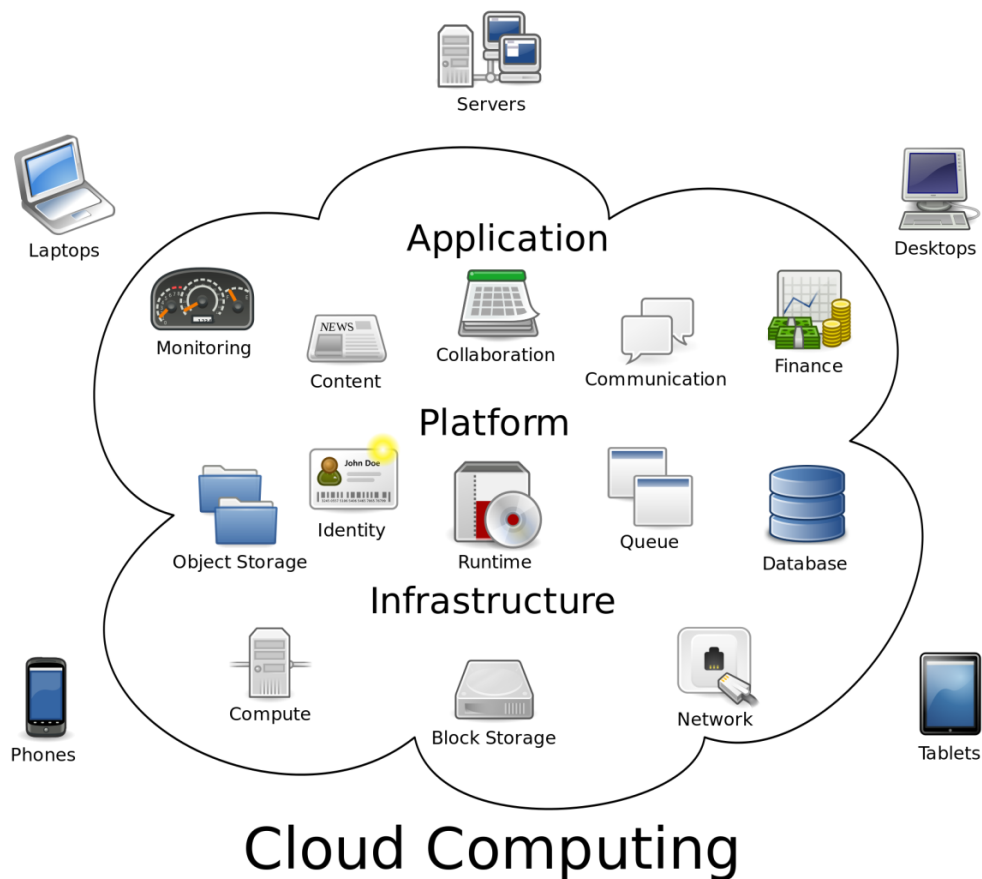
Hybrid cloud services combine publicly accessible services provided by external companies with privately hosted services. An example of a hybrid cloud would be a company that provides web-based email using a major external provider such as Microsoft or Google, but has access to an internal, private file server that is hosted securely onsite in an office, rather than on the servers of an external provider. This means that the company has minimal hardware and maintenance costs but can have most of the benefits of cloud-based services available to users.



Cloud-based Services

Cloud-based services come in many forms, just as applications for computers do. Cloud-based services include applications, services or resources made available to users on demand via the Internet from the servers of a cloud computing provider. For example:

- **Storage services** such as Google Drive, OneDrive, Dropbox or iCloud can be used to store media files and documents, accessible from any computer.
- **Application services** such as Office365 and Google documents allow users to create and edit documents through a web browser, storing or downloading the final version.
- **Infrastructure** - providing scalable computing power in the form of "virtual machine" servers. The RAM, CPU and backing storage of the servers can be changed and servers can be copied easily. The user can run any services or software on the machines.
- **Platform** - a pre-set application for building a website or online program that can be customised and set up to produce a software solution. Instead of an application like a word processor, a platform would be an installation of Drupal, a content management system, or a program running on Google's App Engine, a platform for running code on Google's servers.



Advantages of Cloud-based Services

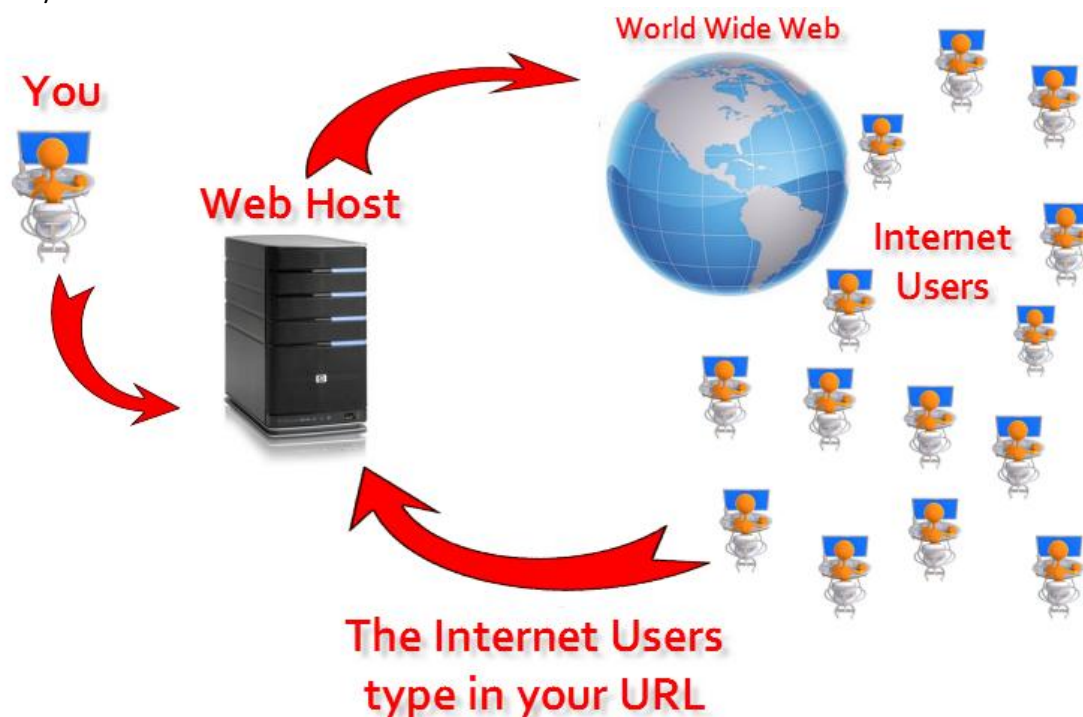
- Cloud-based services are accessible from anywhere.
- Cloud-based services can expand storage and processing resources automatically (the provider will always have extra capacity!)
- Security across the service will be strong, as the company providing the service specialises in making it secure.
- Less hardware and management of hardware takes place in each company that uses cloud-based computing

Disadvantages of Cloud-based services

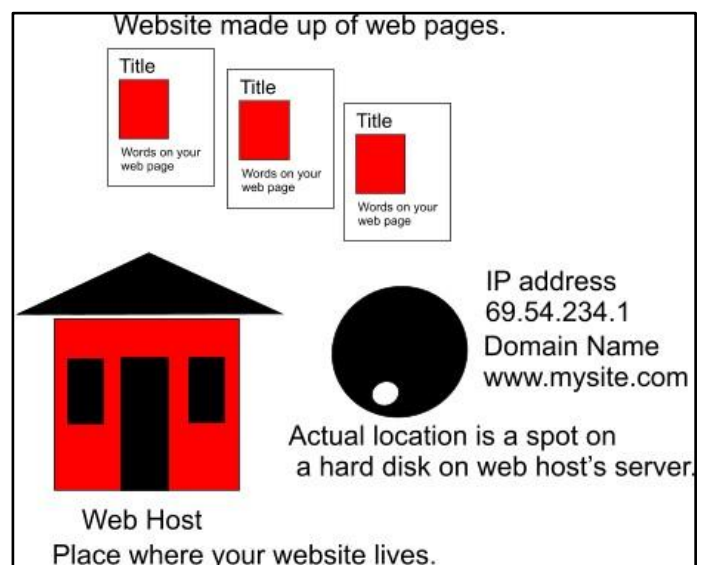
- Network must be available for cloud services to operate
- Network bandwidth must be sufficient for data transfer between the client computer and the cloud service
- Security is taken out of the hands of the company and placed in the hands of the provider
- The legality of storing personal data in different areas of the world (or not knowing its exact location) can be problematic.

Web Hosting

Web hosting is online storage provided to users who wish to publish web pages online. A web host runs a web server, which allows pages to be publicly viewable, and provides the user with access to write/amend the files on the website.



Web hosting is usually accessed from a domain name which must be purchased and pointed to the web hosting provider. A web host will provide a user with storage space on their server. Any page put within the public area of the storage space will be accessible from the website's address.



What is hosting?



Types of Hosting

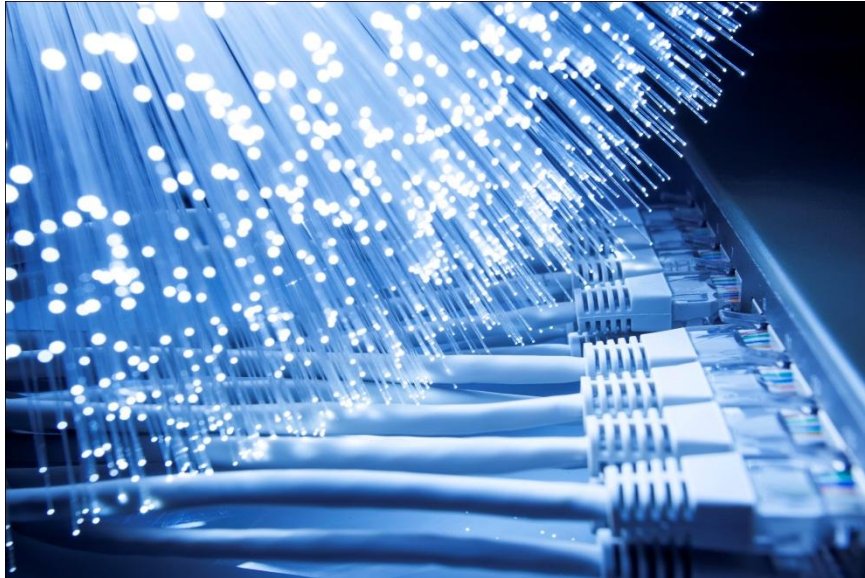
- **Shared Hosting** is a single user account on a web server. Shared hosting servers can have thousands of separate accounts which allow the web host to cut costs as each website shares the hardware and running costs. Shared hosting can be free (often because the web host will add adverts to the web pages) or for a small fee. Shared hosting is secure (no user can access another user's files) but is more susceptible to hacking, because of the number of accounts on one server.
- **Dedicated Hosting** will give a user the resources of a full server. This can be very expensive, as the user is paying for the hardware and running costs of a computer hosted in a data centre. Dedicated hosting is very secure as only one user has access to the server and the resources aren't shared.
- **Virtual Private Servers** are a cheaper form of dedicated host, where several virtual machines are run on one server. This means each account has its own "private" computer with full access, but the resources of one server are divided up amongst them. This is secure, but if one of the virtual machines crashes the computer, other virtual machines may be affected.
- **Self-hosting** can be achieved by connecting a computer to a home router. The computer can act as a web server if the firewall of the router is set to allow public web traffic (HTTP port 80) to access the computer. The computer would need to remain on for 24 hour access, and this could generate costs both through use of electricity and bandwidth on the network of the ISP.



Trends: Networking and Connectivity

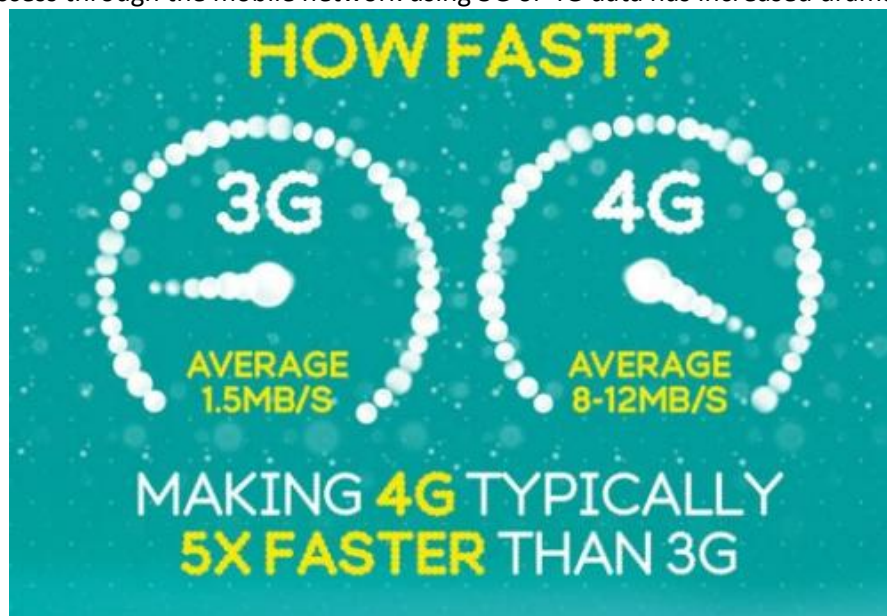
Although developments in the area of networking are taking place all the time, the general trends include:

- Broadband connections are now available in the majority of UK household.
- Internet connection speeds have increased. Broadband connections are commonplace and the average speed of UK broadband in 2014 was 18.7Mbps. The average speed in 2008 was 3.8 Mbps.



Broadband Communications

- Internet access through the mobile network using 3G or 4G data has increased dramatically.



Mobile Networks

- The cost of download has reduced. Communications companies are willing to provide "unlimited" data to many users, or set data limits of several gigabytes per month.
- Increasing amounts of data is stored online in cloud services, including photos and documents.
- More devices are Internet-enabled, including smartphones, cars, GPS devices, televisions, DVD players and even domestic lighting systems, fridges and central heating controls.

Security Risks

Computer networks are essential feature of modern life. However, those same networks also support a range of fraudulent and criminal activities. Descriptions of these several criminal activities are described in the following pages.

Spyware

- Spyware is software that aids in gathering information about a person or organisation without their knowledge and that may send such information to another entity without the consumer's consent, or that gains control over a computer without the consumer's knowledge.
- This can include monitoring browser behaviour or collecting keyed in data.



Phishing

Phishing is a common form of Internet fraud. It is carried out by providing an interface that looks familiar, which is used to gather data and send that data to a third party. Phishing relies on users' inability to notice that the message or website is not coming from a reliable source. It can be difficult for users to spot a fraudulent website because many phishing attacks use advanced techniques to fool the user.

The basic idea behind a phishing website is to collect information using an HTML form. Typically, the web form will ask for information that is used to access a secure website such as a bank or email account. The input to the form will be passed to a server-side script that will email or store the data for the criminal. As long as the website looks legitimate, many users will not hesitate to provide the details.

This is an example of a typical "phishing" e-mail. The bank here is fictional, but a real phishing attempt would claim to be from an actual bank the customer belongs to. Notice how the email tries to establish authenticity by using the bank's logo and providing what appears to be link to a website the customer has visited many times before. When inspected closely, the URL for the website is often a sequence of digits that represent the IP address of the criminal's server or the URL for a spoof website. Phishing emails often originate from overseas and may include spelling mistakes or make reference to 'Dear valued customer' rather than using personal details.



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Avoiding Phishing Attacks

Simple rules can be applied to avoid phishing attacks:

- Do not respond to calls, emails or web pages asking for personal details when you have not requested a password change or support.
- Use a spam filter on email - this will remove many previously detected phishing attacks.
- Know your source - check the address of the website. If it seems suspicious, report it.
- Check security - is the site secured using SSL encryption? If so, read the digital certificate carefully to see if the site is legitimate.



Keylogging



Keylogging is a technique used to steal data by logging keystrokes on a keyboard. This is carried out without the user being aware of the process, so that the data can be sent a criminal third party.

Keylogging is often used to steal personal details such as logins or credit card numbers.

Online Fraud

Online fraud is the use of networks to steal information and commit crimes, most often involving identity theft. Online fraud can be used to fool people into handing over money or personal details through a variety of methods including viruses or spyware to gain information about a user, or simply trick them into giving out details using a phishing scam. Online fraudsters will use data to hijack accounts. Other fraud involves manipulating a target through online dating or offers of "get rich quick" schemes in order for them to pass funds to the fraudster.

To protect against online fraud, users should be vigilant. The best protection for online fraud is common sense, and an understanding of the technologies behind the Internet.



Identity Theft

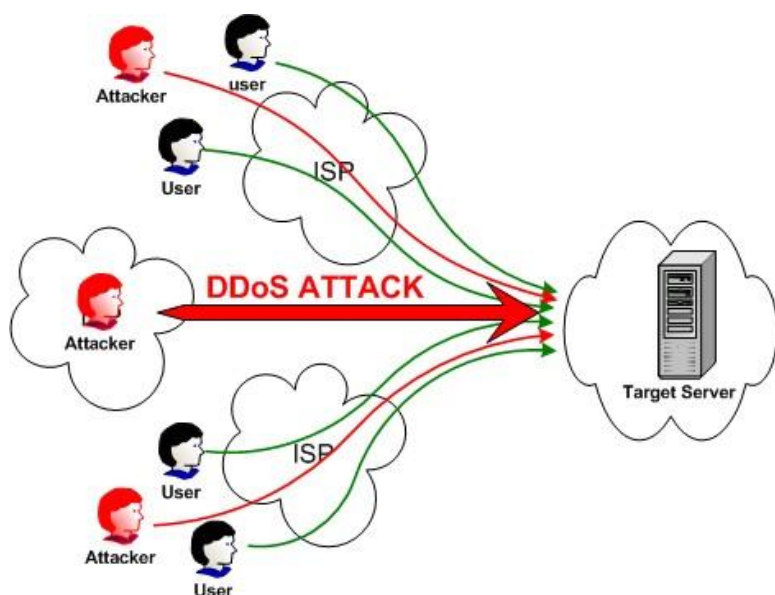
Identity theft is a crime. Criminals take a person's personal details and use them to steal money. Tell-tale signs of identity theft include money being removed from accounts, or receiving letters and emails about new accounts that have been opened.

Over 1.8 million people in the UK have been affected by identity theft, with an average loss of £1000. A significant proportion of identity theft is carried out online.



DOS (Denial of Service) Attacks

- Denial of Service attacks attempts to shut down a server by targeting it with traffic. If the traffic overwhelms the server, it will become unavailable to ordinary users.
- Denial of service attacks can use security vulnerabilities or simply flood the server with a large number of requests.
- Since large organisations like Amazon, Google and Microsoft would have more resources than any single attacking computer, many DOS attacks are distributed amongst a large number of attacking computers. This is called a Distributed Denial of Service Attack.
- Often DOS attacks utilise the resources of infected host computers. These hijacked computers are then controlled remotely and are instructed to attack a server. This is known as a bot-net.
- Firewalls can prevent some traffic from entering the system but cannot protect against attacks that look like "real" web traffic. Anti-virus software can prevent exploits being used to access the server.



A Denial of Service attack is a common form of Internet attack. It does not need to be carried out by an expert hacker | anyone with a simple program can carry out an attack. This is because a DOS attack is caused by sending an overwhelming volume of traffic to a single point on a network. This stops the device from working because:

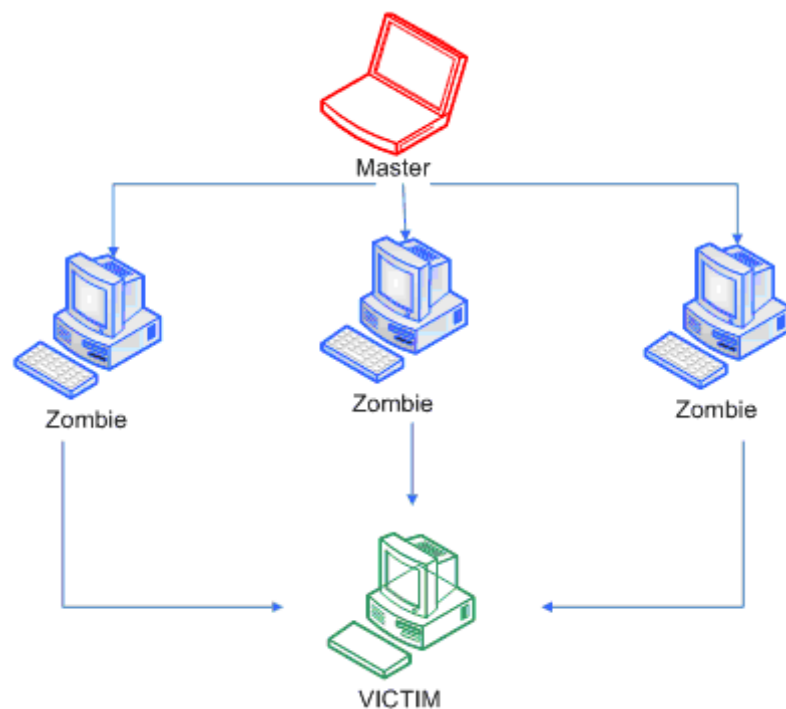
- The buffer of the server which deals with incoming information will be fill with requests and therefore unable to receive any more
- The server cannot serve requested files or data at the rate they are requested
- The processor in the server may be utilised 100% of the time simply trying to deal with data requests which means that other critical processes and applications find it difficult to get time allocated to them

The Ping of Death

An early version of DOS was to use the ping command, which sends a packet of data to a networked computer, and measures the time the computer takes to respond. The Ping of Death is a large packet (several thousand kilobytes) sent repeatedly to a target computer. This will ultimately overrun the buffers of the computer, preventing it from communicating. Most operating systems have patched this problem to deal with this security vulnerability.

Distributed Denial of Service (DDOS Attacks)

It is possible for a large number of computers to combine in an attack on one computer on a network. This is carried out using an array of computers all targeting the same computer manually or automatically.



Distributed Denial of Service Attack

Computers can be used without the user knowing, if a virus has managed to install a **botnet**. A botnet is a piece of software that can be used to carry out a task on a computer, but is remotely controlled: whenever the master computer issues a command, all computers in the botnet will obey the instruction.



Anonymous

The hacker group Anonymous regularly uses the DDOS technique to take down the websites and services of organisations. This has included the FBI and the Church of Scientology. The group uses a program called the Low Orbit Ion Cannon to carry out the attacks. This acts like a botnet, but in this case, the users of the attacking computers have chosen to take part.

Security Precautions

Users of any online system must take precautions to ensure the privacy of their computing devices and security of any data that they send across the Internet. Basic security precautions include:

- Firewall
- Password
- Anti-virus software
- Security suite

In addition to these basic security techniques, a number of specialist methods can be used. Several of these are describe in the following pages.

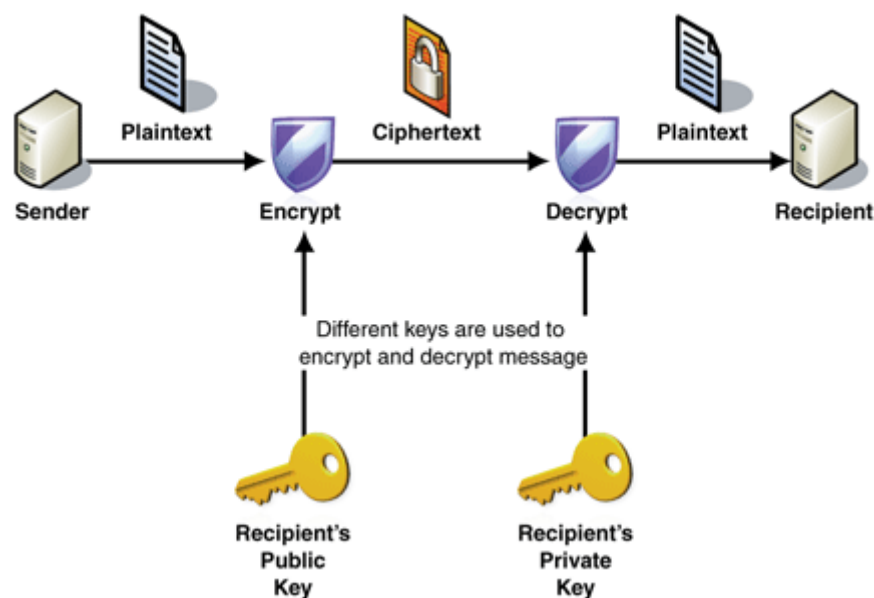
Encryption

Encryption means encoding information using a mathematical formula, so that it cannot be read without being decoded. This means the data can be transmitted across a network safely, as long as only the sender and receiver know how to descramble the data: on the web, the HTTPS protocol is used to send encrypted data.

Encrypted data should also be used when data is sensitive: all banking websites use encryption. Encryption can also be used on hard drives and other storage devices to make sure that the data can only be read by a user who has permission.

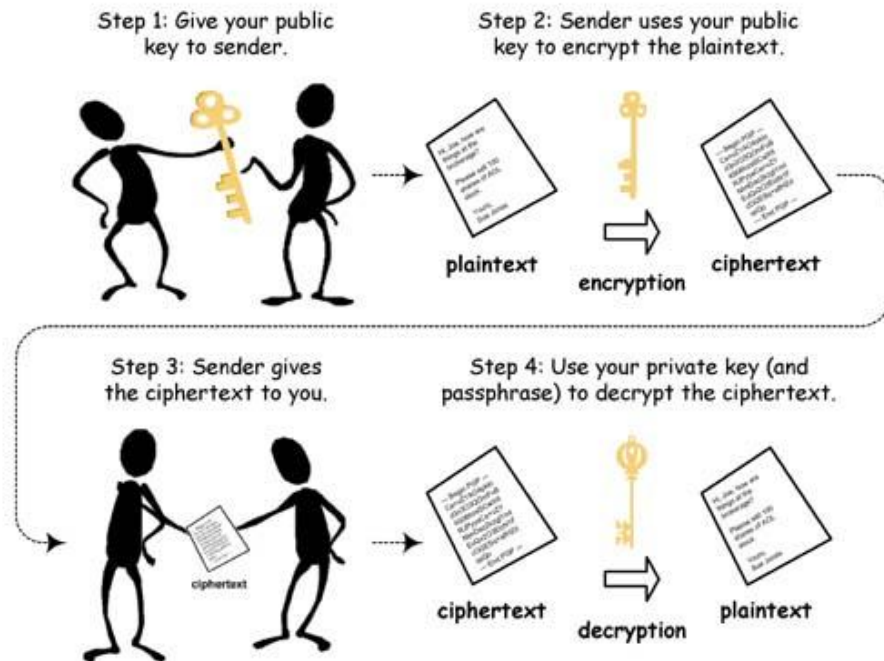


Modern encryption systems use two different keys (or codes) to encrypt data. These keys are known as a **public and private key** (this is also known as **asymmetric encryption**). Older encryption systems are far simpler than this (also known as symmetric encryption) and use the same key to both encrypt and decrypt a message.



Public/Private Key Encryption

Private/Public key encryption uses a pair of keys, one private and one public. The public key and the encryption algorithm are kept in the open, freely usable by anyone. This means that anyone can use the public key to encrypt a message that is then sent to the owner of the private key; the private key is kept hidden by the owner and is used to decrypt any encrypted message received.



Digital Certificates

In the same way that a driver's license or a passport can be used to prove the identity of its owner, a **digital certificate** provides a means of proving the identity of an online business which wants to participate in electronic transactions.

A digital certificate is a document provided by a company known as a Certifying Authority (CA). Before issuing a digital certificate, the CA first checks details of the online business using public records. A digital certificate is then issued by the CA and signed with the CA's private key. The certificate typically contains information about the business to help verify their credentials:

- Owner's public key
- Owner's name
- Expiration date of the public
- Name of the CA that issued the digital certificate
- Serial number of the digital certificate
- **Digital signature** of the CA



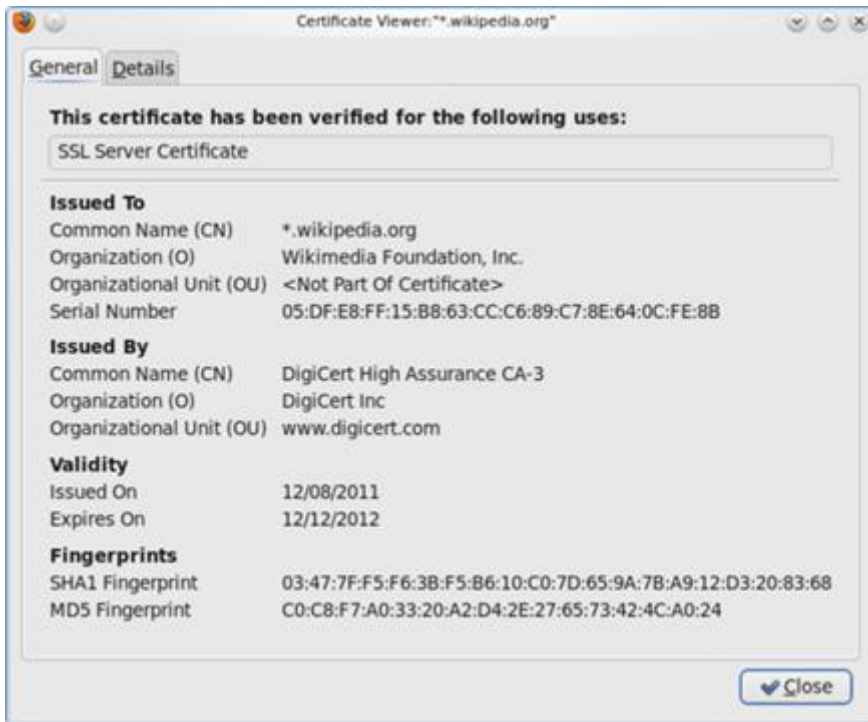
A message encrypted with the digital certificate's public key *can only* be decrypted using the private key held by the online business. When the digital certificate is sent to a user, the user can be confident that the server belongs to a genuine business and can connect their computer to the server safely and securely.

Digital Signatures

A **digital signature** is added to the digital certificate and can be used to check that a certificate is accurate and has not been changed in any way since it was issued. Browsers have a collection of

trusted CA public keys installed. When a new digital certificate is received, it can be compared with the list known to the browser to check the validity of the certificate.

A digital signature is a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic: users know who created the document and know that it has not been altered in any way since it was created.

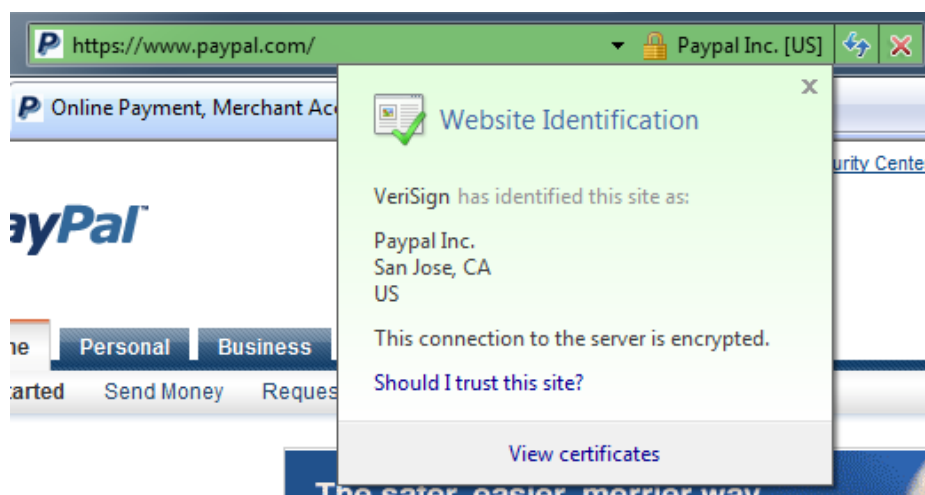


A digital certificate

HTTPS

You may be familiar with the HTTPS protocol used when transmitting financial details. You will also be familiar with the lock icon in your browser which is visible when you are logged into a website or about to buy something from a website using the HTTPS secure protocol. The lock icon indicates that the website is backed by a digital certificate and is a genuine website and is not a fake set up by criminals.

The image below shows PayPal as viewed in Internet Explorer. The lock icon and green background of the address bar let the user know that this website is backed by a digital certificate. Clicking on the lock provides additional detail about the certificate.



Server-side Validation of Online Form Data

An HTML form is used to gather details from users of a website. The HTML `<form>` and `<input>` tags are used to create the structure of the form and provide the form components used to enter the details required. Once the details have been entered, they are submitted to a web server for processing.



Online forms created using HTML

Client-side Validation

Some of the validation of the form data can be carried out using client-side script. For example, JavaScript can be used to make sure that none of the mandatory details are missing. **Client-side validation** of form data is useful since it means that the details can be checked **before** they are transmitted across the Internet. There are, however, occasions when validation of form data **must** be carried out using server-side script.

Server-side Validation

When a customer tries to login to a secure page, a client-side script can be used to make sure that a username and password has been entered. Once those details have been submitted to the web server, a server-side script must be used to check that the password is correct. It wouldn't be possible to perform this validation using a client-side script because that could lead to a breach in security of the website. If JavaScript code was used on the client-side to check whether a user had entered a valid password, it would be easy for a user to manipulate by turning off JavaScript or using developer tools to change the contents of variables.

Form Processing

The following HTML script:

```
<html>
<head>
  <title>Example of a simple form using HTML tags</title>
</head>

<body>
<form name="simple form" method="POST" action="process_details.php">

<table>
<tr><td colspan="2">Checkboxes</td></tr>
<tr>
  <td><input type="checkbox" name="transport">I have a bike</td>
  <td><input type="checkbox" name="transport">I have a car</td>
</tr>

<tr style="height:15px"><td colspan="2"></td></tr>

<tr><td colspan="2">Radio Buttons</td></tr>
<tr>
  <td><input type="radio" name="gender">Male</td>
  <td><input type="radio" name="gender">Female</td>
</tr>

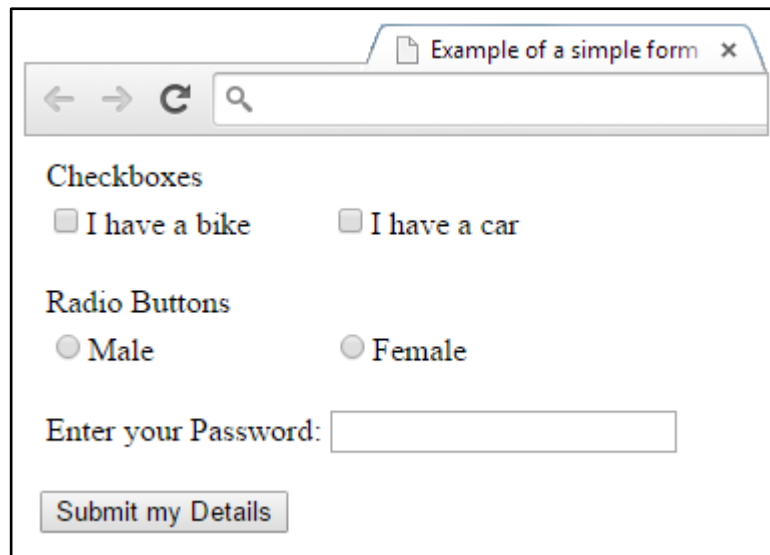
<tr style="height:15px"><td colspan="2"></td></tr>
<tr>
  <td>Enter your Password:</td>
  <td><input type="password" name="password"></td>
</tr>
</table>

<p><input type="submit" name="submit" value="Submit my Details"></p>

</form>
</body>

</html>
```

produces the form shown below:



How Does Server side Validation Work?

The diagram below will help explain how server side validation works for security purposes. The example below explains how server side validation works with Facebook. The same process applies to online banking, Amazon, YouTube, Twitter and any other website that a username or password.

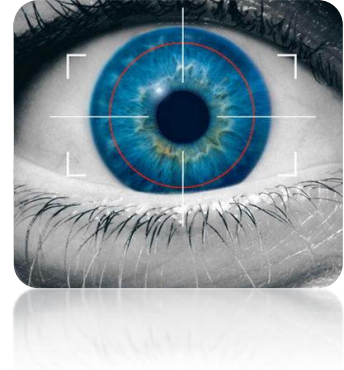
1. You go onto Facebook and type in your username and password into the form and click submit/login.
2. Your login information is sent to Facebook's server so they can check to make sure it is you.
3. Facebook's server then accesses Facebook's database. This is the place where Facebook stores all its user information such as logins info, contact details, passwords etc.
4. The database then will search for that certain username and password to check if it is valid.
5. If the username and password are found the server then sends you the HTML files to access your account. If the combination is incorrect you will be asked to re-enter your login details.



- Server-side validation is used to check data submitted to a website using HTML forms.
- Server-side validation can check the contents of a field to make sure the data is sensible, using range checks, length checks, presence checks, type checks and address checking (looking for a valid email address).
- More importantly, server-side validation is used to make sure that there are no security risks.

Biometrics in Industry

- Biometrics is the use of physical data, such as the unique imprint of a hand or retina, to authenticate users.
- Biometric data is very secure because it is extremely hard to forge or replicate.
- Companies can use biometric scanners to make sure that only current employees can gain access to a system, and that a password cannot be compromised.
- Biometric data is also used by companies for user experiences such as voice recognition and face recognition.
- Biometric data is widely used by immigration authorities on entry to a country. For example, fingerprint and face data is captured from all visitors entering the USA.



Biometrics is becoming increasingly popular in industry. Keeping the right people out and letting the right people in remains the main reason for the use of biometrics. Employers looking for better ways to provide for security and restrict access to specific areas in the workplace, and to be able to know which individuals were present in specific workplace areas at any given time are making use of biometric technology. Fingerprint / palm recognition, face recognition, voice recognition and retina scanning are all used by businesses to restrict who can access restricted areas.



This sort of technology is also becoming increasingly popular on mobile devices. One example of this is the iPhone using a fingerprint scanner called Touch ID. The fingerprint scanner will use your fingerprint to uniquely identify the owner of the phone and unlock it. It can also be used to purchase Apps, music and movies from the iTunes store.

Economic Impact of E-commerce

Lots of traditional businesses have been badly disrupted by the Internet, but it has also empowered many others. This is especially the case among small and medium-sized enterprises, where the Internet is enabling big gains in productivity and transforming localised markets into global ones.

In the late 1990s most major UK companies were seeking to develop an Internet presence, because those without this means of communication would rapidly fall behind competitors with an Internet presence. Since 1997, there has been a dramatic increase in the percentage of the population online in the UK. The successful organisation of the future will communicate through traditional and modern electronic means. Existing and potential customers will be able to access both well laid out High Street stores or showrooms and exciting, easy to navigate websites.

A recent study for Google by the Boston Consulting Group says Britain is now the biggest e-commerce market in the world in per capita terms and the second largest online advertising market.

Value of internet economy by country

Index, geometric mean = 100

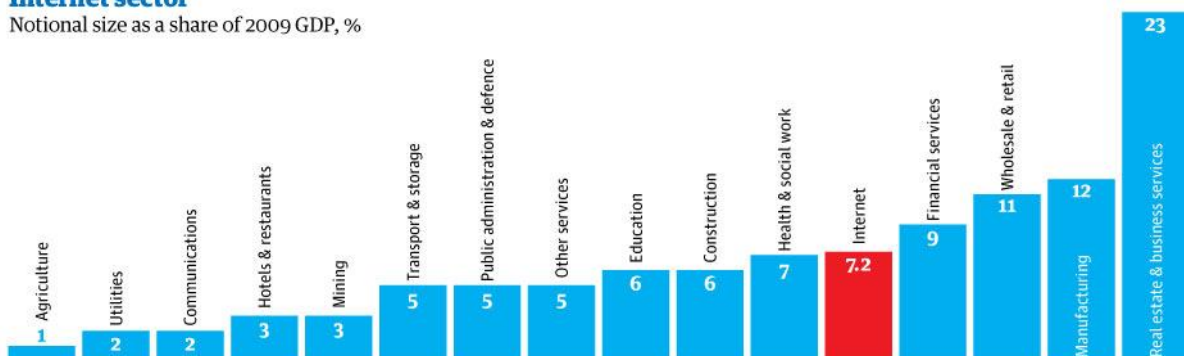
Expenditure: online sales and online advertising



One of the key conclusions of the BCG report is the estimate that, in 2009, the internet business made £100 billion in the UK. That is 7.2 % of the 2009 economy. But that number is less significant than the role that the Internet plays in driving innovation and generating sales for U.K. businesses and in providing benefits to consumers.

Internet sector

Notional size as a share of 2009 GDP, %



Reduced Costs for Consumers

Lots of commodities that would once have cost you a lot now comes largely free. From Google and Facebook, to Wikipedia, GPS and the time and money saved by shopping online — these things are largely immeasurable as far as the official statistics are concerned, yet they are undoubtedly useful and are an increasingly important enabler of economic advancement.

Consider the traditional music industry, which used to involve, finding, recording and marketing new acts, and then cleaning up through copyrighted CD sales.

For decades, the model worked well — at least for the record producers and a small, elite of popular artists. Then along came digital downloads, legal or otherwise. These have destroyed the old music company stranglehold on distribution, and in so doing made previously quite pricey music either far less expensive or completely free. The pound value of music consumption has declined but the volume of music consumption has risen exponentially.

In a similar way, the traditional business model used in the newspaper industry has been badly undermined by the Internet, but news demand and consumption has never been higher.

The public is consuming these products in ever greater quantities. Digital delivery has marginalised distribution costs, so that once developed, a product can be made available to multiple users at zero cost.

Competitive Advantage

Any advantage that a firm has over its competitors, allowing the business to generate greater sales or margins and/or retain more customers than its competition is referred to as competitive advantage. In any company, information technology allows companies to gain competitive advantage by reducing costs, increasing their product range, providing after sales support and exploiting changes in competitive scope.

Competitive advantages give a company an edge over its rivals and an ability to generate greater value for the firm and its shareholders. Information technology increases a company's ability to coordinate its activities regionally, nationally, and globally. It can unlock the power of broader geographic scope to create competitive advantage.

Competitive advantage in terms of cost is a firm's ability to produce a good or service at a lower cost than its competitors, which gives the firm the ability sell its goods or services at a lower price than its competition or to generate a larger margin on sales. Competitive advantage is also created when a firm's products or services differ from its competitors and are seen as better than a competitor's products by customers.



The suppliers can monitor the consumers' buying habits and interests so that they can tailor their offer suit to consumers' needs and keep the on-going relationship with them.

Competitive Advantage: Use of Social Media and the Internet of Things

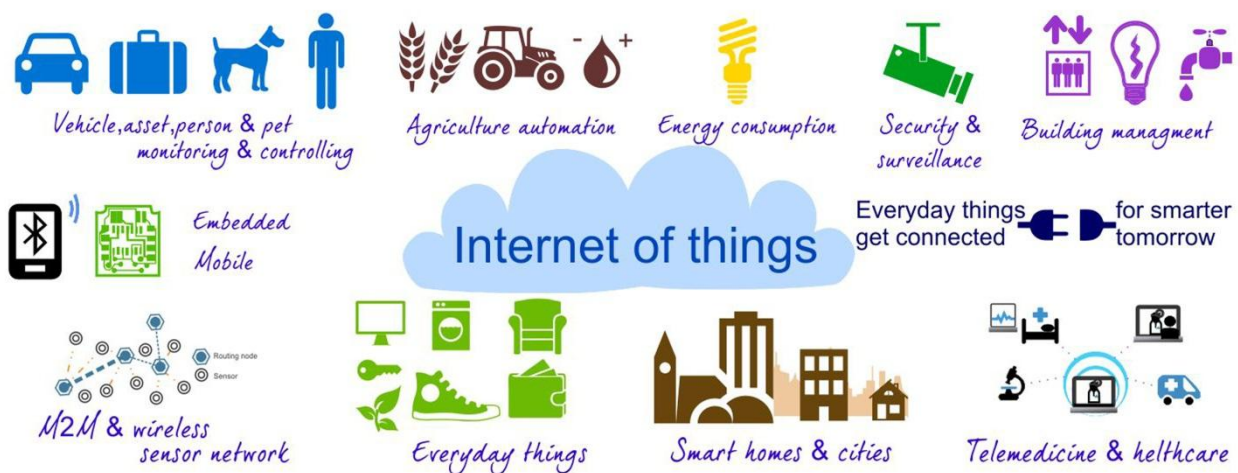
No matter what organisation you run or belong to, one priority should be blatantly clear: your



customer service needs to evolve. A key tool that can help evolve customer service is social media. Social media grants companies the opportunity to have one-on-one conversations with customers and potential customers. By listening, we can find out what's off-putting about a service, frustrating about a product or missing from an experience altogether. Over half of consumers now use social media to directly reach out to companies to report satisfaction, problems and ask questions.

In today's world of cutting-edge technology, we can listen even further. We can do that by connecting products, or maybe more widely recognised, by utilising the Internet of Things. While many have talked about the Internet of Things, few have identified it as a way to better customer experiences—where it really has the opportunity to shine.

By “listening” to products and enabling them to tell the service team when they're having problems, it's very possible to avoid the need for a customer to pick up the phone at all. It sounds very futuristic, but it's very possible to connect products into business processes now.



Let's use hot tubs as a connected product example. First, the hot tubs are equipped with sensors that capture data such as temperature, humidity and pH. Through a dashboard, the company can compare sensor data to social data. They can look at social sentiment compared to sensor readings and drill in where there may be problems. The system also lets the company monitor their product 24/7—at any time they can check on the product's status and performance. They can drill down to each specific hot tub, understanding its exact situation at all times. The data is so specific that they can look at a map of the wiring on a hot tub and identify and troubleshoot issues remotely, before the customer notices. When there is an issue that must be solved by a technician, it's the organisation letting the consumer know—instead of the frustrated consumer calling into the organisation. The hot tub owner can sit back, relax and feel confident that they're getting the maximum quality out of their product with uninterrupted service

Global Marketplace

E-commerce is the buying and selling of products or services over electronic systems such as the Internet. Using the Internet to sell to international consumers is a very low risk business strategy for companies to use for developing an international customer base. Companies do not have to tie up huge financial investments through franchising, direct investment or brick-and-mortar stores overseas. The combination of global marketing with an Internet distribution method allows many companies to try their hand at reaching growing target markets overseas.

Going global is even easier than it has been in the past. Small entrepreneurs can market their product overseas from their living room, while large corporations have access to consumers across the world 24 hours a day by using the Internet. The Internet and the increasing growth of technology make it easy to reach consumers with websites.

Global Marketing: Advantages

The Internet and new technologies have allowed companies to easily expand to overseas markets; a business can target a global audience, compared to the local audience attracted by a local store. It also provides a tremendous database for the company to use to build their customer base.



Fluid pricing is when process are increased or decreased quickly depending on circumstances. For example, when selling airline tickets, as more are sold and fewer are available, the tickets can become more expensive as demand rises. Alternatively, when selling products like holidays, as the departure dates draw closer, the prices can be reduced to ensure that all places are sold. Use of fluid pricing allows online businesses to quickly react to changing circumstances that wouldn't be possible for traditional High Street stores.

The biggest advantage is the ability to reach huge, growing target markets to increase market share and profits. Countries such as India and China have a developing middle class with a large disposable income. The market is ripe for American companies to promote their products and services for long-term growth opportunities. It is very easy to customise websites for each international country, which can reflect local customs, currency and advertising messages.

Global Marketing: Disadvantages

Along with advantages, there are also disadvantages and issues for companies who use E-commerce.



Legal Issues: Sales in a particular country will be bound by the Consumer legislation of that country. To ensure that all trade is lawful, businesses must be aware of the laws that apply and what rights consumers have.

Consumer Trust and Security Issues: The main concern of consumers is that their financial details will not be safe and that businesses will store them in an insecure way. Any business that wants to trade effectively online must make use of secure payment systems and invest in secure systems to store customer details.

Consumer Trust: Consumers also worry about whether the company they are trading with is a legitimate business. Any successful online business must work hard to gain the trust of consumers by incorporating features such as rating and feedback systems, personal recommendations and suggested purchases that are based on previous sales. An online business can monitor the buying habits and interests of their consumers so that they can then tailor their offer suit to consumers' needs. This allows the business to establish trust in their brand and maintain on-going relationships with consumers.

Lack of Human Contact: Some customers are put off from purchasing online because they cannot speak to anyone from the business. Many customers prefer face-to-face contact. For this reason, some online businesses have developed online avatars to provide a human-like interface to their websites. Others businesses make use of instant messaging to provide a service to online customers. This service can be used to provide help and advice about products and make suggestions.

Product Description Problems: Customers worry that product descriptions may not be accurate. This is especially difficult with colour options as some computers display colours differently. The quality of the image used on the site can also be a problem.

Business Costs

E-commerce can give a lot of benefits to business organisations, especially in term of cost reduction and reaching global market.

Business costs include:

- Start-up costs
- Running costs
- Staffing costs
- Investment costs



Start-up Costs

Compared to setting up a traditional store, the start-up costs of a website are relatively low. Since the overhead costs to build the physical store front may be avoided by companies who use e-commerce as their business operation, this is a great incentive for business owners.

The business, however, will have to consider the start-up costs associated with the hardware and software systems that will be needed to support an e-commerce business.

Running Costs

With e-commerce, suppliers can reduce costs to manage their stock because they can automate the stock management using web-based management systems. This method can help reduce their running costs.

E-commerce can reduce advertising costs because it is easier to update the advertisement using software technology.

Since an online business doesn't need expensive premises on the High Street, rental costs are reduced along with the running costs associated with heating and lighting.

Any online business must take account of web hosting costs and broadband costs,

Staffing Costs

Staffing costs can be reduced with e-commerce because the sellers can automate their online store fronts and thereby reduce the number of staff needed to support the business.

Since there is no store to be staffed, trading can be carried out at any time of the day or night, in all different times zones of the world. This provides the option to offer 24 hour shopping, 7 days a week, at minimum additional cost.

Investment Costs

Investment in research and development, internally-created software and certain other intangibles such as intellectual property rights are costs that must be covered by any online business.

Businesses who offer a global marketplace must develop software to translate between languages, to make communication with international customers easier to implement. There is also a need for software that provides currency conversions.



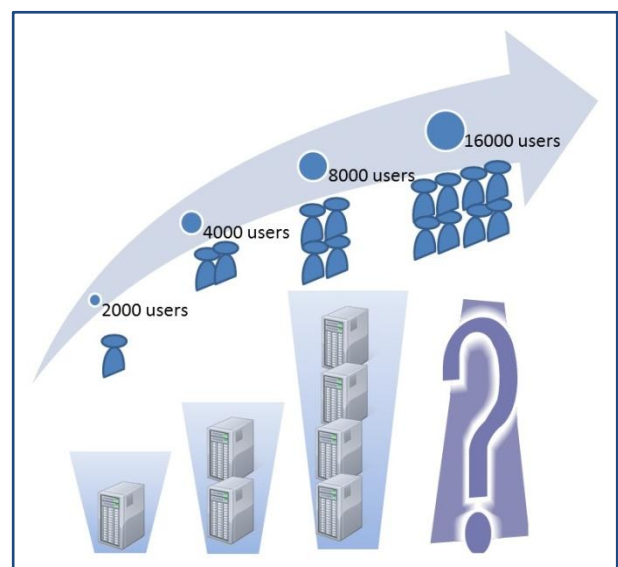
<http://education-portal.com/academy/lesson/internet-and-global-marketing-ecommerce-on-an-international-scale.html>

Scalability and Maintainability

Scalability refers to the ease with which the size of something can be changed (increased or decreased) according to need. In the case of e-commerce, the term scalability usually corresponds to the hardware, software, and network infrastructures used to keep websites and related systems up and running. Having scalable systems and applications is important for companies because it means that valuable resources and investments won't be lost when it is necessary to **maintain** the systems or make changes to them.

From a technological standpoint, scalability can involve very simple actions like adding memory to a PC or server, increasing the number of nodes on a computer network, or adding new or more sophisticated features to an e-commerce website. However, it often involves a company's entire e-commerce architecture, which consists of many different technology elements.

During e-commerce, companies rely on databases to store and present information about products (including prices, sizes, colours, and options), customers (including names, addresses, preferences, and credit card numbers), content that appears on dynamic web pages, and more. Servers are



another important piece of the puzzle. Finally, networks of workstation computers for staff, connected by miles of cabling and network hardware components, also play central roles. In an ideal world, it would be possible for a company to add, replace, or take away different pieces from this constellation without negatively impacting the entire system.

Unfortunately, such is not always the case. When companies find themselves in a position to grow, there are often hurdles that must be overcome first. Among these hurdles are old "legacy" systems that are still very important to the company's operations, but which were not designed for e-commerce. Although there are ways to connect legacy systems to e-commerce software, high volumes of transactions can present problems. Rather than establishing individual patches for many legacy systems, one possible solution to a challenge like this would be to replicate essential data from all legacy systems involved in e-commerce and place it into a special database called a data warehouse, which is compatible with the web and e-commerce. This warehouse could then be scaled more easily, depending on the company's needs.

Two keys to scalability are modularity and replication. For example, a software application can be divided into different smaller sections or modules, each corresponding to a different function or area of e-commerce. One module might be devoted to a program's user interface while another deals exclusively with the data being accessed. Successful e-commerce applications keep these modules separated and require little interaction between them. This allows each layer to be more easily modified without affecting other system areas. If necessary, more memory or processing power can be devoted to one level of an application, but not to others.

Replication also is important. When companies create a component for one area of their e-commerce operation, such as programming instructions that deal with accepting special promotional discounts, a good strategy is to then re-use this code in other applications or areas of the site, rather than re-creating it from scratch every time.



Social Impact

The Internet is changing the way we work, socialise, create and share information, and organise the flow of people, ideas, and things around the globe. The Internet accounted for 21% of the growth in mature economies over the past 5 years. In that time, we went from a few thousand students accessing Facebook to more than 800 million users around the world, including many leading firms, who regularly update their pages and share content.



Censorship

Internet censorship is the control or suppression of what can be accessed, published, or viewed on the Internet. It may be carried out by governments or by private organisations at the behest of government, regulators, or on their own initiative. Individuals and organisations may engage in self-censorship for moral, religious, or business reasons, or out of fear of legal or other consequences.

The extent of Internet censorship varies on a country-to-country basis. While most democratic countries have moderate Internet censorship, other countries go as far as to limit the access of information such as news and suppress discussion among citizens. Internet censorship also occurs in response to or in anticipation of events such as elections, protests, and riots. Other areas of censorship include copyrights, defamation, harassment, and obscene material.

A widely publicized example of Internet censorship is the "Great Firewall of China". The system blocks content by preventing IP addresses from being routed and consists of standard firewall and proxy servers at the Internet gateways. The system also selectively engages in DNS poisoning when particular sites are requested. The government does not appear to be systematically examining Internet content, as this appears to be technically impractical. Internet censorship in the People's Republic of China is conducted under a wide variety of laws and administrative regulations. In accordance with these laws, more than sixty Internet regulations have been made and censorship systems are vigorously implemented by provincial branches of state-owned ISPs, business companies, and organisations.

**MORE THAN
1/3 OF THE
WORLD'S
INTERNET
ACCESS IS
CENSORED**

Freedom of Speech

Freedom of speech is the political right to communicate one's opinions and ideas. Freedom of speech is understood to be fundamental in a democracy and includes any act of seeking, receiving and imparting information or ideas, regardless of the medium used, including the Internet.

**Freedom of
Speech is Not
a Licence to
abuse. It is a
responsibility.**

Governments restrict speech with varying limitations. Common limitations on speech include libel, slander, obscenity, hate speech, incitement, classified information, copyright violation, trade secrets, right to privacy, public security and public order. The term "offense principle" is also used to expand the range of free speech limitations to prohibit forms of expression where they are considered offensive to society, special interest groups or individuals.

The right to freedom of expression is recognised as a human right under article 19 of the Universal Declaration of Human Rights and recognised in international human rights law in the International Covenant on Civil and Political Rights (ICCPR). Article 19 of the ICCPR states that "everyone shall have the right to hold opinions without interference" and "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". Article 19 additionally states that the exercise of these rights carries "special duties and responsibilities" and may "therefore be subject to certain restrictions" when necessary "for respect of the rights or reputation of others" or "for the protection of national security or of public order (order public), or of public health or morals".

Privacy

Internet privacy involves storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Privacy has been a concern of many people from the beginnings of large scale computer sharing.



Privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behaviour on a website. PII refers to any information that can be used to identify an individual. For example, age and physical address alone could identify who an individual is without explicitly disclosing their name, as these two factors are unique enough to typically identify a specific person.

People with only a casual concern for Internet privacy do not require total anonymity. Internet users may protect their privacy through controlled disclosure of personal information. The revelation of IP addresses, non-personally-identifiable profiling, and similar information might become acceptable trade-offs for the convenience that users could otherwise lose using the workarounds needed to suppress such details rigorously. On the other hand, some people desire much stronger privacy. In that case, they may try to achieve Internet anonymity to ensure privacy — use of the Internet without giving any third parties the ability to link the Internet activities to personally-identifiable information of the Internet user. In order to keep their information private, people need to be careful with what they submit to and look at online. When filling out forms and buying merchandise, that becomes tracked and because the information was not private, companies are now sending Internet users spam and advertising on similar products.

Posting things on the Internet can be harmful or in danger of malicious attack. Some information posted on the Internet is permanent, depending on the terms of service, and privacy policies of particular services offered online. This can include comments written on blogs, pictures, and Internet sites, such as Facebook and Twitter. It is absorbed into cyberspace and once it is posted, anyone can potentially find it and access it. Some employers may research a potential employee by searching online for the details of their online behaviours, possibly affecting the outcome of the success of the candidate.

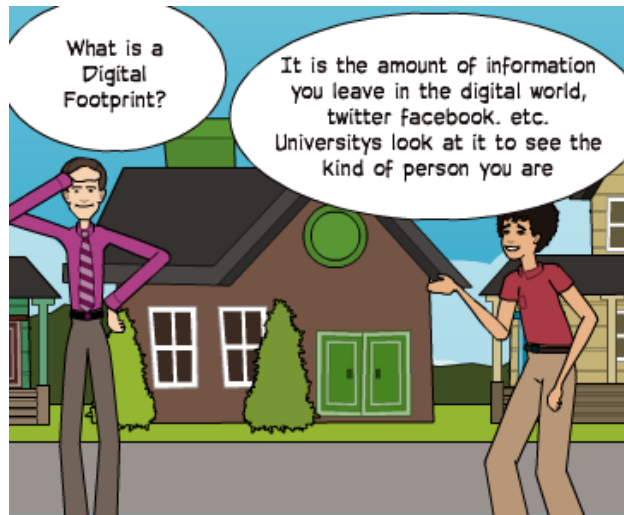


There are a number of pointers that helps an individual Internet user protect their privacy and anonymity and thereby avoid possible identity theft and other cyber-attacks. Preventing or limiting the usage of Social Security numbers online, being wary and respectful of emails including spam messages, being mindful of personal financial details, creating and managing strong passwords, and intelligent web-browsing behaviours are recommended.

Risks to Internet Privacy

Companies are hired to watch what Internet sites people visit, and then use the information, for instance by sending advertising based on one's browsing history. There are many ways in which people can divulge their personal information, for instance by use of "social media" and by sending bank and credit card information to various websites. Moreover, directly observed behaviour, such as browsing logs, search queries, or contents of the Facebook profile can be automatically processed to infer potentially more intrusive details about an individual, such as sexual orientation, political and religious views, race, substance use, intelligence, and personality.

Those concerned about Internet privacy often cite a number of privacy risks — events that can compromise privacy — which may be encountered through Internet use. These range from the gathering of statistics on users to more malicious acts such as the spreading of spyware and the exploitation of various forms of bugs (software faults).



Several social networking sites try to protect the personal information of their subscribers. On Facebook, for example, privacy settings are available to all registered users: they can block certain individuals from seeing their profile, they can choose their "friends", and they can limit who has access to one's pictures and videos. Privacy settings are also available on other social networking sites such as Google Plus and Twitter. The user can apply such settings when providing personal information on the Internet.

Children and adolescents often use the Internet (including social media) in ways which risk their privacy: a cause for growing concern among parents. Young people also may not realise that all their information and browsing can and may be tracked while visiting a particular site, and that it is up to them to protect their own privacy. For example:

- Twitter threats include shortened links that lead one to potentially harmful places
- threats in their e-mail inbox include email scams and attachments that get them to install malware and disclose personal information
- threats on Torrent sites include malware hiding in video, music, and software downloads
- smartphone threats include geo-location, meaning that one's phone can detect where they are and post it online for all to see

Users can protect themselves by updating virus protection, using security settings, downloading patches, installing a firewall, screening e-mail, shutting down spyware, controlling cookies, using encryption, fending off browser hijackers, and blocking pop-ups.

HTTP Cookies

An HTTP cookie is data stored on a user's computer that assists in automated access to websites or web features. It may also be used for user-tracking by storing special usage history data in a cookie, and such cookies—for example, those used by Google Analytics are called tracking cookies. Cookies are a common concern in the field of Internet privacy. Although website developers most commonly use cookies for legitimate technical purposes, cases of abuse do occur. In 2009, researchers noted that social networking profiles could be connected to cookies, allowing the social networking profile to be connected to browsing habits.

The original developers of cookies intended that only the website that originally distributed cookies to users could retrieve them, therefore returning only data already possessed by the website. However, in practice programmers can circumvent this restriction. Possible consequences include:

- the placing of a personally-identifiable tag in a browser to facilitate web profiling, or,
- use of cross-site scripting or other techniques to steal information from a user's cookies.



Cookies do have benefits that many people may not know. One benefit is that for frequently visited websites that requires a password, cookies make it possible for users to avoid having to sign in every time. Unfortunately, one of the most common ways of theft is hackers taking one's user name and password that a cookie saves. A cookie can also track a user's preferences and show them websites that might interest them. Cookies make more websites free to use without any type of payment. Such websites make a profit by selling their space to advertisers. These ads, which are personalised to a user's likes, can often freeze the user's computer or cause annoyance.

Cookies are mostly harmless except for third-party cookies. These cookies are not made by the website itself, but by web banner advertising companies. These third-party cookies are so dangerous because they take the same information that regular cookies do, such as browsing habits and frequently visited websites, but then they give out this information to other companies.

In past years, most computer users were not completely aware of cookies, but recently, users have become conscious of possible detrimental effects of Internet cookies: a recent study done has shown that 58% of users have at least once, deleted cookies from their computer, and that 39% of users delete cookies from their computer every month. Since cookies are advertisers' main way of targeting potential customers, and some customers are deleting cookies, some advertisers started to use persistent Flash cookies and zombie cookies, but modern browsers and anti-malware software can now block or detect and remove such cookies.

In the past, websites have not generally made the user explicitly aware of the storing of cookies, however since tracking cookies, and especially third-party tracking cookies, are commonly used as ways to compile long-term records of individuals' browsing histories, European and US law makers took action in 2011 to force businesses to alert users to the use made of cookies on their websites.

Encryption

SSL uses public-key encryption to exchange a session key between the client and server; this session key is used to encrypt the http transaction (both request and response). Each transaction uses a different session key so that if someone manages to decrypt a transaction, that does not mean that they've found the server's secret key; if they want to decrypt another transaction, they'll need to spend as much time and effort on the second transaction as they did on the first.

When we use the Internet, we're not always just clicking around and passively taking in information, such as reading news articles or blog posts -- a great deal of our time online involves sending others our own information. Ordering something over the Internet, whether it's a book, a CD or anything else from an online vendor, or signing up for an online account, requires entering in a good deal of sensitive personal information. A typical transaction might include not only our names, e-mail addresses and physical address and phone number, but also passwords and personal identification numbers (PINs).

The incredible growth of the Internet has excited businesses and consumers alike with its promise of changing the way we live and work. It's extremely easy to buy and sell goods all over the world while sitting in front of a laptop. But security is a major concern on the Internet, especially when you're using it to send sensitive information between parties.

Information security is provided on computers and over the Internet by a variety of methods. But the most popular forms of security all rely on encryption, the process of encoding information in such a way that only the person (or computer) with the key can decode it.

Computer encryption is based on the science of cryptography, which has been used as long as humans have wanted to keep information secret. Before the digital age, the biggest users of cryptography were governments, particularly for military purposes.

Types of Encryption

Symmetric Keys

- ◆ Encryption and decryption use the **same key**.



Asymmetric keys

- ◆ Encryption and decryption use different keys, a **public key** and a **private key**.



Symmetric-Key Encryption

In symmetric-key encryption, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message.

Public Key Encryption

Also known as asymmetric-key encryption, public-key encryption uses two different keys at once -- a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. Although a message sent from one computer to another won't be secure since the public key used for encryption is published and available to anyone, anyone who picks it up can't read it without the private key. The key pair is based on prime numbers (numbers that only have divisors of itself and one, such as 2, 3, 5, 7, 11 and so on) of long length. This makes the system extremely secure, because there is essentially an infinite number of prime numbers available, meaning there are nearly infinite possibilities for keys.

A popular implementation of public-key encryption is the **Secure Sockets Layer (SSL)**. Originally developed by Netscape, SSL is an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information.

In your browser, you can tell when you are using a secure protocol in a couple of different ways. You will notice that the "http" in the address line is replaced with "https," and you should see a small padlock in the status bar at the bottom of the browser window. When you're accessing sensitive information, such as an online bank account or a payment transfer service, chances are you'll see this type of format change and know your information will most likely pass along securely.

Once your browser requests a secure page and adds the "s" onto "http," the browser sends out the public key and the certificate, checking three things:

- 1) that the certificate comes from a trusted party;
- 2) that the certificate is currently valid; and
- 3) that the certificate has a relationship with the site from which it's coming.



Global Citizenship

A global citizen is someone who identifies with being part of an emerging world community and whose actions contribute to building this community's values and practices. The term global citizenship typically defines a person who places their identity with a "global community" above their identity as a citizen of a particular nation or place. The idea is that one's identity transcends geography or political borders and that the planetary human community is interdependent and whole; humankind is essentially one.

Historically human beings always have organised themselves into groups and communities based on shared identity. Such identity gets forged in response to a variety of human needs - economic, political, religious, and social. As group identities grow stronger, those who hold them organise into communities, articulate shared values, and build governance structures that reflect their beliefs.



Today the forces of global engagement are helping some people identify themselves as global citizens, meaning that they have a sense of belonging to a world community. This growing global identity in large part is made possible by the forces of modern information, communication, and transportation technologies. In increasing ways these technologies are strengthening our ability to connect to the rest of the world: through the internet; through participation in the global economy; through the ways in which world-wide environmental factors play havoc with our lives; through the empathy we feel when we see pictures of humanitarian disasters, civil conflicts and wars in other countries; or through the ease with which we can travel and visit other parts of the world.

Those who see ourselves as global citizens are not abandoning other identities; such as allegiances to our countries, ethnicities, and political beliefs. These traditional identities give meaning to our lives and will continue to help shape who we are. However, as a result of living in a globalised world, we find we have an added layer of responsibility. We have concern and a share of responsibility for what is happening to the planet as a whole, and we are members of a world-wide community of people who share this concern.

Online Communities

An online community is a virtual community whose members interact with each other primarily via the Internet. Those who wish to be a part of an online community usually have to become a member via a specific site and necessarily need an internet connection. An online community can also act as



an information system where members can post, comment on discussions, give advice or collaborate. Online communities have become a very popular way for people to interact, who have either known each other in real life or met online. The most common forms people communicate through are chat rooms, forums, e-mail lists or discussion boards. Most people rely on social networking sites to communicate with one another but there are many other examples of online communities. People also join online communities through video games, blogs and virtual worlds.