Website Production

Assignment 2

Unit 28

George Hotten

Website Technologies

Technology	Description	Example
WWW	The World Wide Web is the information system where documents and resources can be stored and accessed by URLs.	www.wikipedia.org – thousands of pages of information about different topics.
ISP	An Internet Service Provider is a company that provides access to the internet.	Virgin Media, Sky and BT.
Domain Name	A domain name is a combination of words used to form a URL. These are meant to be memorable so people can easily access the domain's website.	google.com
Domain Name Register	A company that sells you a domain name and registers it with ICANN.	Namecheap, GoDaddy.
Web Hosting	Web hosting is often found on a server using a service to serve HTML files to a browser.	NGINX or Apache2.
Server	Physical or in the cloud, servers are powerful computers whose primary purpose is to provide services such as web hosting.	AWS, Google Cloud.
HTTP	Hyper Text Transfer Protocol – a protocol used by browsers to request HTML documents from a server	N/A
HTTPS	HTTP but all data sent between the browser and the server is encrypted using end-to-end encryption.	N/A
TCP/IP	Transmission Control Protocol is that standard that allows for devices to communicate over a network via packets, whilst the Internet Protocol is the method for sending the data.	N/A
SMTP	Simple Mail Transfer Protocol is used to send emails to an email server.	Sending an email using Gmail or Outlook.
FTP	File Transfer Protocol is used to transfer files between two devices.	A program such as Filezilla or WinSCP.
Database	A database is storage of data in a structure defined by the	MySQL, MongoDB.

	user. This can hold as much data as they want and whatever data they want.	
Cookies	Cookies are small pieces of information sent to your browser by a website to help it retain information about you	This can be used for advertising, logon data, etc.
Proxy	A proxy acts as a gateway between you and the internet. Instead of connecting directly to the website, this is done via the proxy.	VPNs such as Surfshark or NordVPN.
DNS	A Domain Name Server is a service used to resolve URLs such as google.com into a IP the computer can understand such as 8.8.8.8	google.com would resolve to 172.217.169.78

Client-Side Web Performance

Computer Hardware

If your computer has outdated and slow hardware, it won't be able to process the web requests fast enough and it won't be able to load the website in a timely fashion. Having better hardware will allow for your computer to process the web response faster so it can display the page to you in lightning speed.
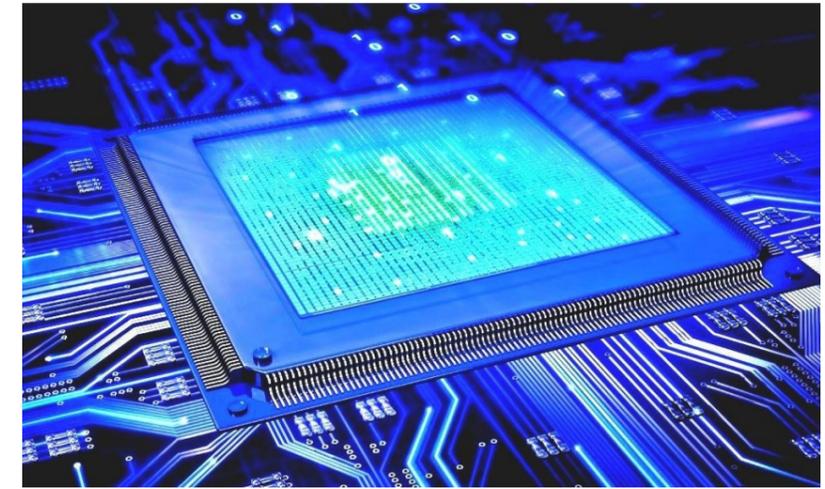
Browser Caching

Modern day web browsers are able to cache webpages, meaning they save a copy in their local storage and when requested, they load that cache instead of making a new request to the server. This allows for drastically faster load times as the website is being loaded directly from your storage. Caches have a TTL (Time to Live) meaning they expire after a certain amount of time to ensure you still get the most up-to-date version of the website.

Internet Speed

If you have slow internet, web documents will take longer to download from the server, meaning loading times will increase and you will be sat waiting for longer, ruining the experience of the website.
Having faster internet means your computer can send and receive data quicker and load it so much faster, keeping up with the snappy expectations users have of the internet.

Browser Limitations

Older web browsers aren't able to utilise the modern solutions modern browsers can today, such as multithreading. Multithreading allows the browser to use multiple threads, sometimes even multiple cores when processing web requests. This allows for parallel task execution, meaning that multiple tasks can be executed at the same time to drastically decrease load time. Make sure you are using a modern browser such as Chrome or Firefox and that they're on the latest version!

Server-Side Web Performance

Excess Traffic

If the server is being overwhelmed with web requests, it may stop replying to requests as it is simply unable to handle any more. This means many users will not be able to access the resource they are requesting. To combat this, web masters can add more servers and add load balancing software such as NGINX to allow the load to be distributed across multiple servers.
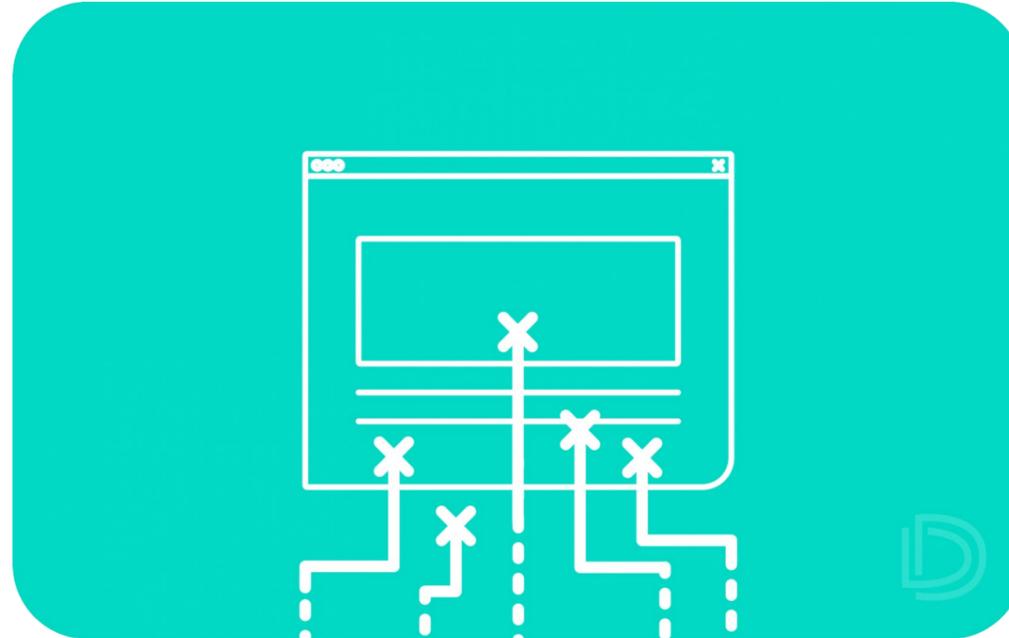
Bandwidth

If the server your resource is running on has a low amount of bandwidth, it will limit the amount of requests it can receive and respond to. If your bandwidth is low, requests from users may not be fulfilled or even acknowledged. This can make it seem like the web server is not functional and hinder the user experience.
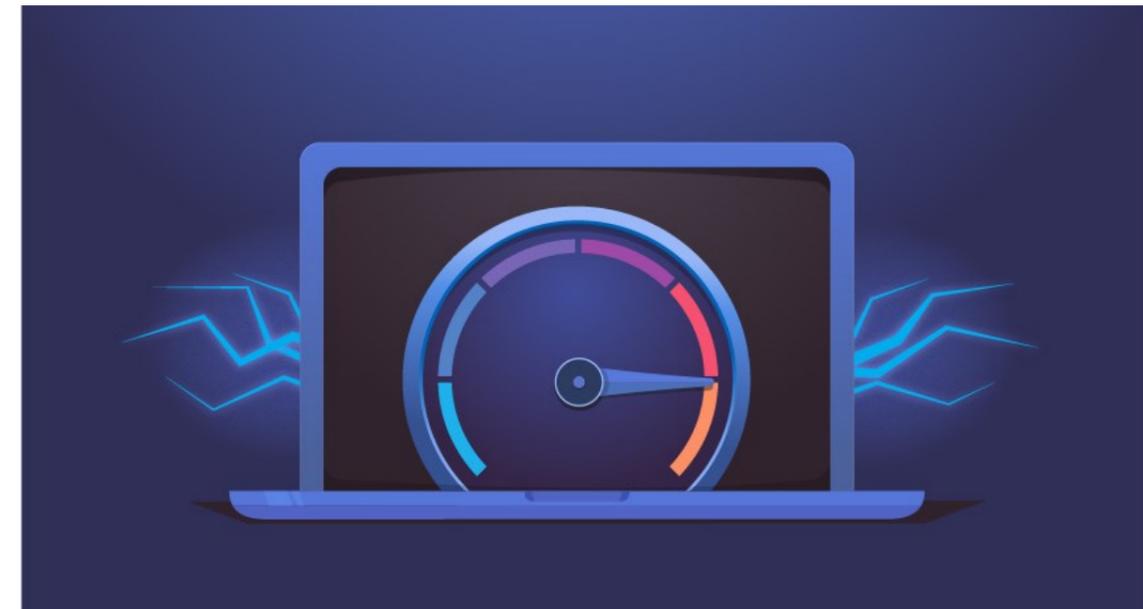
Databases

Depending on the purpose of the resource the user is trying to access, a database may be required. It is important that a modern and fast database is used to avoid drastically increasing load times, especially if the database contains large sums of data. Ways to increase the speed of a database is to store it on faster storage mediums, such as NVMe drives or in system memory if you have enough of it.

SECURITY THREATS, PREVENTIONS AND LAWS

BY GEORGE HOTTEN
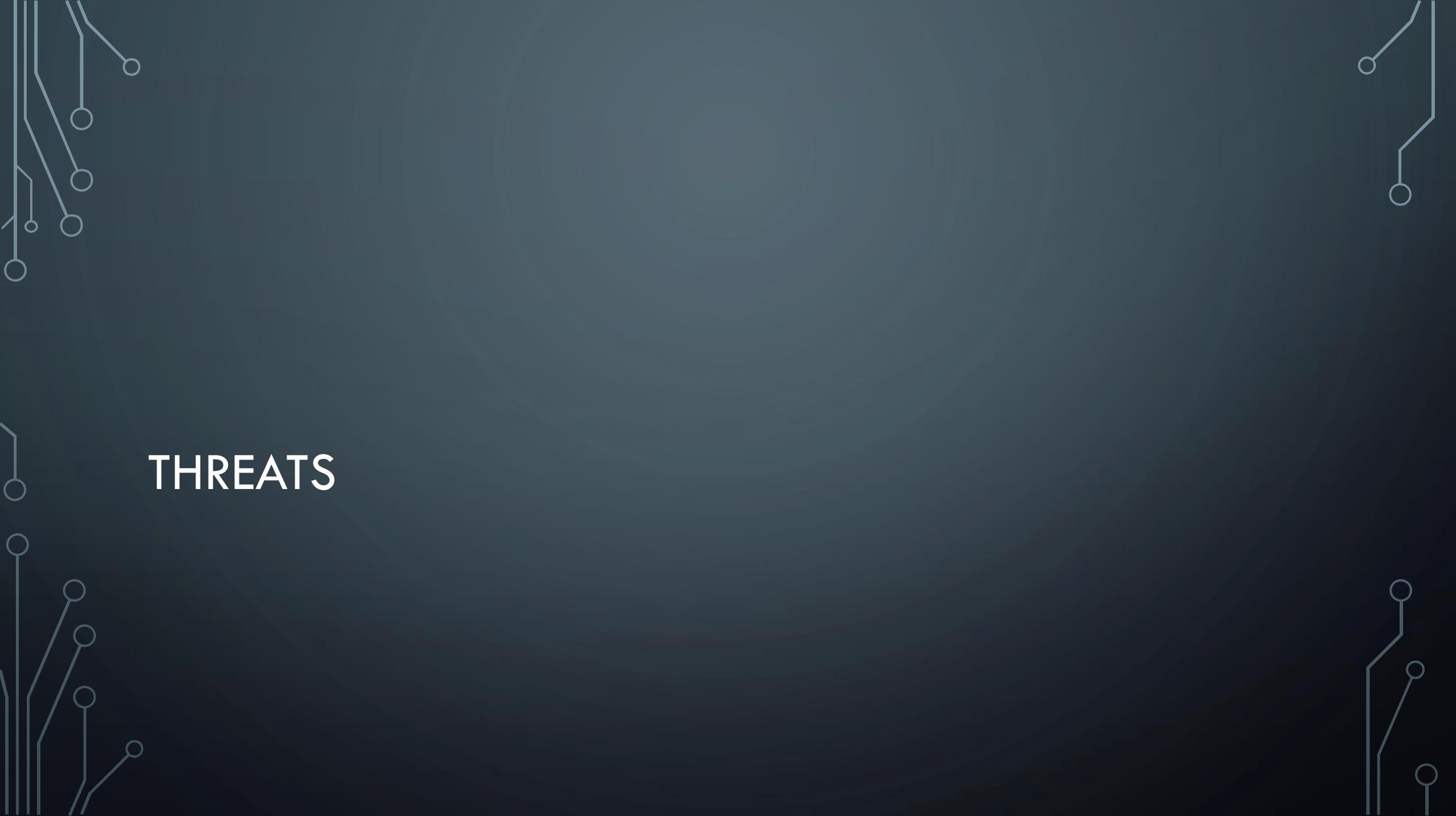
THREATS

VIRUS

Viruses are self-replicating software that causes either damage to a computer system or steal data. The virus is often baked into software such as pirated games, emails and downloaded files.

TROJAN

A trojan is a type of malware that disguises itself as another application, and once executed causes havoc on the system. It can often provide a 'back door' into the system for hackers to use later to steal data or do further damage.

WORM

A virus that duplicates itself and spreads itself throughout a network using open network shares, email or Internet Relay Chat.

IDENTIFY THEFT

Identity theft is where a fraudster has so much information on a person, they can impersonate them to the point where it is hard to tell the difference. People often do this to steal from a person or receive benefits from that person.

DATA SNIFFING

Data sniffing is where, usually on a Wi-Fi network, hackers intercept packets being sent across a network. These packets can contain data that is being sent and received from a web server, including information such as banking details or logon information.
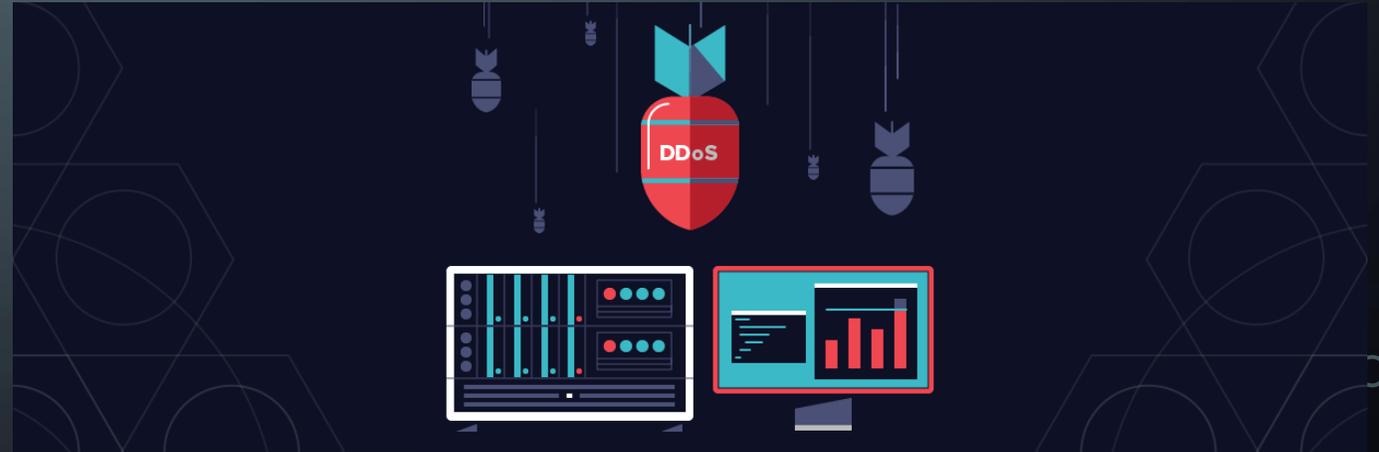
DENIAL OF SERVICE

Denial of Service is where a web server is flooded with requests from a specific machine or a group of zombie machines. The number of requests overloads the server causing them to crash or take a very long time to respond to requests.

PREVENTIONS

VIRUSES

To mitigate the risk of infecting their network with a virus, businesses should install proper anti-virus software on all their servers and machines. To stay up to date with the latest malware, this software should be regularly updated. It is also recommended to give the employees training on being safe on the internet to further lower the risk of a malware attack happening.

SECURE SOCKET LAYER

An SSL is a cryptographic protocol that secures packets sent over the internet. This means both the client and server must be authenticated before they can read any data sent. This is often done through RSA certificates.

PASSWORD PROTECTION

To mitigate the risk of a user's account getting hacked via brute force, businesses should implement a strong password policy. For example: contain both upper case and lowercase, letters and numbers, symbols and use more than 8 characters. They should also implement an attempt limit. If there are too many failed attempts, the account should be locked, and the user should be sent an email advising them about the attack.

FIREWALL

Using a firewall allows you to filter the requests that enter your network, meaning that any malicious requests can be blocked. This also applies to stopping DoS attacks as the firewall can filter large number of requests sent from the same person within a short amount of time. However, using a firewall can also hinder performance as it must scan every request that enters the network to check for threats. This may slow the server's response time down; however, in the long run it would be worth it as it prevents attacks, and the reduced performance margin will only be minor.

LAWS

DATA PROTECTION ACT

This act governs how companies must store and protect sensitive data. This applies to paper and electronically stored data. The 8 acts are:

- Fair and lawful
- Purposes
- Adequacy
- Accuracy
- Retention
- Rights
- Security
- International transfers

This ensures that all data the company holds on its employees is held securely and is collected within reason – for example only having the data they need and only keeping it while they need it. This means their employee's data is safe and it does not invade their privacy.

COPYRIGHT, DESIGN AND PATENTS ACT

This act protects the work you have created. For example, work such as code, music, writing, and arts are all protected under this law. The content of websites is also protected under copyright. For example, the company's website and any digital material they create can be licensed and protected from anyone attempting to steal their work.

DISABILITY DISCRIMINATION ACT

This act protects people with a disability from being treated less favourably than other people due to their disability. Businesses must accommodate for people with a disability by providing extra help such as ramps for wheelchair users. This act also covers discrimination by association, which is where you are discriminated against by being connected to someone with a disability.

Web Communications

Internet Service Providers

Internet Service Providers are the companies that provide you access to the internet. By paying a monthly fee, they give you access to their hardware (such as a router which allows you to access the internet), a connection to the internet, along with other services such as TV (which is sometimes included in your plan). Some examples of ISPs include the following:

Web Hosting Services

Web Hosting Services are companies that you can rent compute power from to host your website. For example, companies such as Contabo allow you to rent a Virtual Private Server (aka a virtual machine) where you can host your services. These companies also allow you to rent dedicated servers or a bare-metal server for much more powerful computing power.
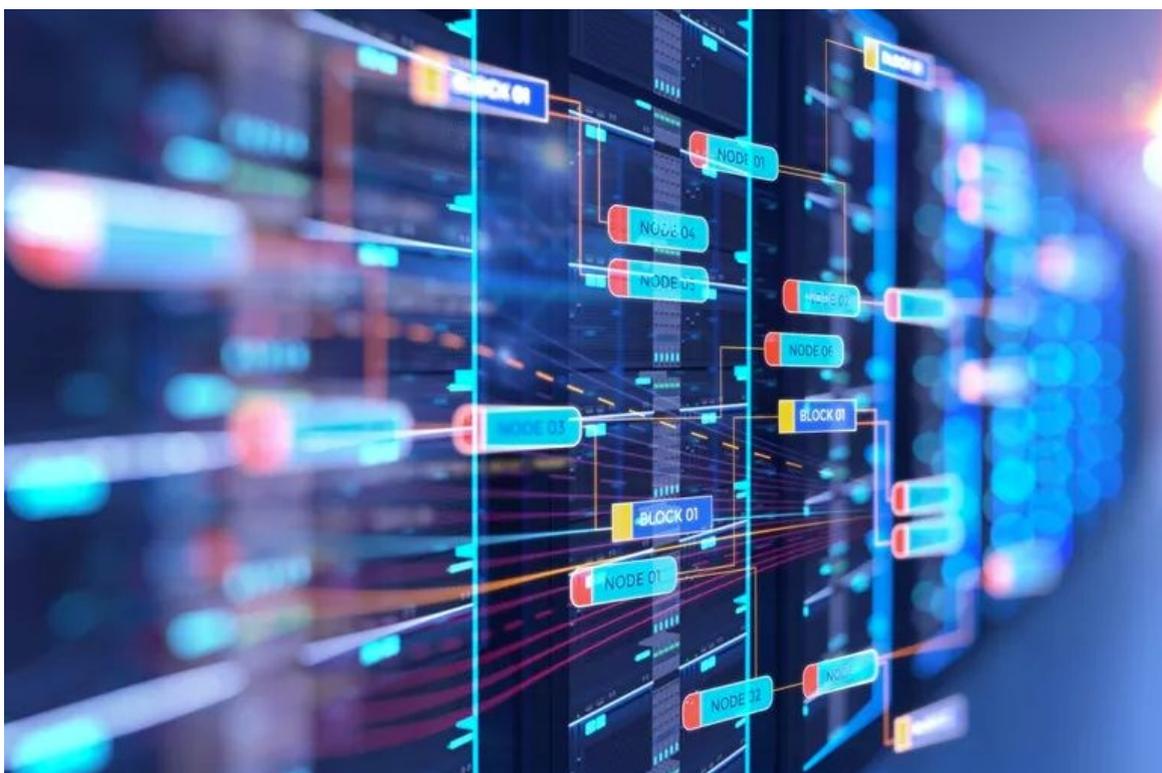
Domain Structure

The Domain structure is setup with 3 levels. Third-level, second-level and top-level domain. A completed domain name is known as a fully qualified domain name (FQND).

An example of this is:

Third-level domain	Second-level domain	Top-level-domain
en	.wikipedia	.org

The top level domains are managed by Network Information Centres who allocate second-level domains. Second-level domains can be freely chosen by the public, providing not already taken. Third-level domains are considered sub-domains and can be freely set by the owner of the second-level domain. They are usually used for services such as mail, imap, smtp, etc.

Domain Name Registrars

A Domain Name Registrar is a company that sells domain names. You get to choose from a wide list of different top-level domains such as .uk, .com, .dev and second-level domains which can be whatever the user desires as long as it is not already registered. They also tend to operate Domain Name Systems which browsers can access to see what domain points to what IP.
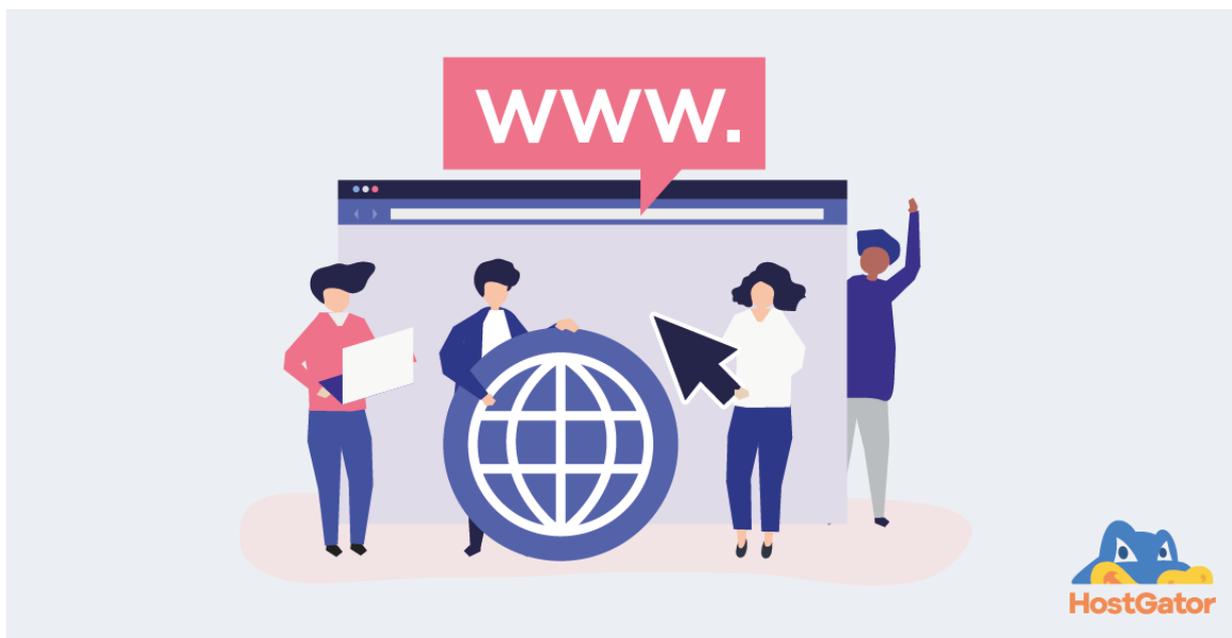
World Wide Web

The World Wide Web is a information retrieval service that allows users to access a vast library of resources and documents which can be accessed using URLs and domains. The WWW works in a client-server format. This means that the client requests resources from the server and the server replies.

Web 2.0

Web 2.0 is a representation of a shift in how the internet is used. Compared to Web 1.0, it has more user-generated content than ever before, along with better usability for end-users.

Web 1.0 describes the first stage of the internet, where most of the pages were statically generated and was only used by a small amount of people. Web 2.0 now has dynamic HTML and is used by millions of people around the world, with billions of lines of information easily accessible with a quick Google search.

TCP/IP Model

The TCP/IP model is the representation of how devices communicate on the internet. The model considers of 4 layers:

TCP/IP	Purpose & Example
Application	Responsible for high-level protocols such as HTTP and deals with the representation of data. Only applications that require communication are considered part of this layer. Other examples of protocols are DHCP or POP3.
Transport	Responsible for the data flow and error correction whilst it is being sent over a network. This is done via the TCP or UDP protocol.
Internet	Responsible for the transmission of data between two networks. An example device is a router. Data at this layer is considered a packet.
Network Interface	Defines how data should be sent physically through a network and is responsible for the transmission of data between devices on the same network. Example devices are switches and cables. Data here is considered a frame before it is turned into binary.

TCP/IP Model Continued

Web applications interact at the Application layer, using protocols such as HTTP and IMAP. Inside the layer, there are 3 sub-layers: Application (Layer 7), Presentation (Layer 6), Session (Layer 5).

At layer 5, the transmission between the client and the server is controlled to ensure data is transmitted successfully, as fast as possible and without wasting any resources.

At layer 6, data received from the internet is de-encrypted and de-compressed ready to be sent to the browser at Layer 7.

At Layer 7, web browsers translate the data received from the internet and display it on the user's display.