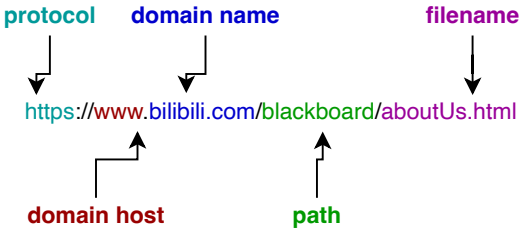
IGCSE 05 The Internet and its uses(1)

Internet	World Wide Web
Users can send and receive **emails**.	A collection of multimedia web pages and other information on **websites**.
Allows **online chatting** (via text, audio and video).	http(s) protocols are written using **hypertext mark-up language(HTML)**.
Makes use of transmission protocols **(TCP)** and internet	**Uniform resource locators(URL)** are used to specify the location of web pages.
A worldwide collection of interconnected networks and devices.	Web resources are accessed by **web browsers**
	WWW uses the internet to access information from web servers.

URLs(Uniform resource locators):
text address used to access websites



http and https
http: Hypertext transfer protocol (http) is a set of rules that must be obeyed when transferring files across the internet.
https: http with secure

Web browsers
Browsers interpret (translate) HTML from websites and show the results of the translation (either as a website page or play multimedia).
web browsers functions:
1. a **home page** and **address bar**
2. the ability to store favourite websites and web pages (**bookmarks**)
3. keeping a history of websites visited (**user history**)
4. the ability to allow the user to **navigate forwards and backwards** through a website
5. allowing many web pages to be open at the same time by using **multiple tabs**
6. making use of **cookies**
7. using **hyperlinks** to navigate between websites
8. data stored as a **cache**
9. make use of JavaScript.

DNS
domain name server (DNS) is used to find the IP address from the domain name in the URL typed into the browser window.

How web pages are located, retrieved and displayed:
1. The user opens their browser and types in the URL and the browser **asks the DNS server for the IP address of the website**.
2. if DNS server can't find in its database or its cache, so it sends out a request to DNS server
3. The DNS server finds the URL and can map it to this IP address is sent back to the DNS server which now puts this IP address and associated URL into its **cache/database**.
4. This IP address is then sent back to the user's computer.
5. The computer now **sets up a communication** with the website server and the required pages are downloaded. The computer's browser interprets the HTML, which is used to structure content, and then **displays the information** on the user's computer.Cookies are small files or code stored on a user's computer

Cookies
Cookies are small files or code **stored on a user's computer**. Cookies are **sent by a web server** to the browser on a user's computer.

Cookies functions:
1. saving personal details
2. tracking user preferences
3. holding items in an online shopping cart
4. storing login details

Session cookie features:
1. Stored **temporarily** on the user's computer.
2. Once the browser is closed, the website session ends and the cookie is deleted.

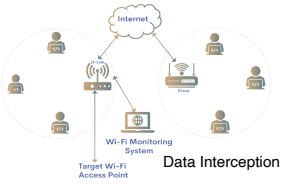
Persistent cookie features
1. Remember user's log in details.
2. Cookies are **stored on user's hard drive** until **expiry date** reached or user deletes them.
3. Remain in operation even after browser closed or website session terminated.

Digital currency
Digital currency exists purely in a digital format and has **no physical form** unlike fiat currency
Cryptocurrency is a type of digital currency that overcomes **security** and **confidentiality** issues.

Blockchaining
1. **decentralised database**: when a new transaction takes place, all networked computers in the system get a copy of the transaction, removing security risks such as **hacking**.
2. **block**: contains **data**, **a new hash value**, **a previous hash value** pointing to the preceding block.
3. **proof-of-work**: used to prevent high speed number crunching from altering all of the block hash values by a cybercriminal.

cryptocurrency uses:
1. smart contracts
2. in research – for example, development of new drugs
3. in politics
4. in many areas of education.

CyberSecurity threats
1. brute force attacks
2. data interception
3. distributed denial of service (DDoS) attacks
4. hacking
5. malware
6. phishing
7. pharming
8. social engineering.



Data Interception

Brute Force attacks:
Brute Force attacks is a method where all combinations of letters, numbers and other symbols are tried to generate passwords. **longer**, **more complex**, **passwords** make the task of the cybercriminal much harder

Data Interception:
Data interception is the stealing of data by tapping into a network.
packet sniffers: all data packets on a network and read the data being moved across the networks.
War driving(access point mapping): intercepts Wi-Fi (wireless) signals.

Security Threats (Hacking)
Hacking: the act of gaining illegal **access to a computer system without the user's permission**.

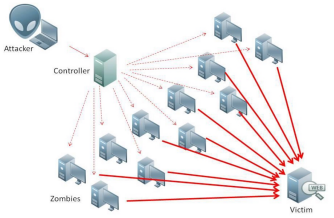
Hacking Threads:
1. identity theft or gaining of personal information
2. data can be deleted, passed on, changed or corrupted.

Prevents:
1. firewalls
2. change strong password
3. anti-hacking software

DDoS(Distributed Denial of Service attack)
DoS(Denial of Service attack): attempt at **preventing users from accessing part of a network**, notably an internet server.

Prevent:
1. using an up-to-date malware checker
2. setting up a firewall
3. applying email filters

What happen in DoS:
1. Many requests are sent from a computer
2. Requests are sent to the webserver
3. The webserver becomes flooded with traffic
4. The webserver cannot handle the requests / fails
5. he website can no longer be accessed
6. Attack maybe distributed



DDos attack

DoS signs:
1. slow network **performance**
2. **inability** to access certain website
3. large amounts of **spam email**

Security Threats (Malware)
Viruses – programs (or program code) that can **replicate/copy themselves** with the intention of **deleting or corrupting files, or causing the computer to malfunction**. They need an active host program on the target computer or an operating system that has already been infected before they can run. virus often **sent as email attachments**, **reside on infected websites** or on **infected software downloaded** to the user's computer.
Worms – these are types of standalone viruses that can **replicate themselves** with the intention of **spreading to other computers**; they often networks to search out computers with weak security that are prone to such attacks
Trojan horses – these are malicious programs often disguised as legitimate software; they **replace all or part of the legitimate software** with the intent of carrying out some harm to the user's computer system
Spyware – software that **gathers information by monitoring**, for example, all the activity on a user's computer; the gathered information is then **sent back to the person who sent the software** (sometimes spyware monitors key presses and is then referred to as key logging software)
Adware – software that floods a user's computer with unwanted advertising; usually in the form of pop-ups but can frequently appear in the browser address window redirecting the browser to a fake website which contains the promotional adverts
Ransomware – programs that **encrypt the data on a user's computer**; a decryption key is sent back to the user once they pay a sum of money (a ransom); they are often sent via a Trojan horse or by social engineering

IGCSE 05 The Internet and its uses(2)

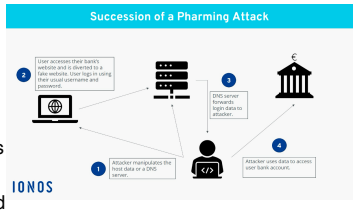
Phishing occurs when a cybercriminal sends out **legitimate-looking emails** to users. The emails may contain links or attachments that, when initiated, **take the user to a fake website**; or they may **trick the user into responding with personal data**

Pharming is malicious code installed on a user's computer or on an infected website. The code **redirects the user's browser to a fake website** without the user's knowledge.

Phishing

Phishing and Pharming Similarity:
1. Both are designed to **steal personal data**
2. They both **pose as a real company**/ perso

Phishing and Pharming Differences:
1. Pharming uses **malicious code installed on hard drive**
2. Phishing is **in form of an email**
3. phishing requires use to follow a link / open an attachment



Pharming

Prevent phishing attacks:
1. be aware of new phishing scams
2. not to click on any emails links
3. run anti-phishing toolbars on browsers
4. always look out for https
5. ensure up-to-date browser. run a good firewall

Prevent pharming attacks:
1. use **anti-virus software**
2. **modern browser** alert user
3. **check the spelling** of websites
4. use of **https**

Social engineering

Social engineering occurs when a cybercriminal creates a social situation that can lead to a potential victim 'dropping their guard'.

Instant messaging: Malicious links

Scareware: pop-up message with virus

Emails/phishing scams: opens a link in the email, redirects their browser to a fake website

Baiting: malware-infected memory stick

Phone calls: download some special software

Keep data safe from security threats

Access level:
user accounts control a user's rights, different levels of access for different people.

Anti-malware

Anti-virus: must be **kept thoroughly up to date** and should run in the background to maintain their ability to **guard against being infected** by such malware

Anti-virus features:
1. **check** software or files **before run**
2. **compares** a possible vires against a **known database**
3. carry out heuristic checking
4. allow user to automatically or decision to delete
5. needs to be kept up to data
6. full system check

Anti-spyware: detects and removes spyware programs installed illegally on a user's computer system,

Anti-spyware Feature:
1. detect and remove spyware
2. prevent a user from downloading spyware
3. encrypt files
4. encryption of keyboard
5. block access to a user's webcam
6. scans for signs that user's personal information has been stolen

Authentication: refers to the ability of a user to prove who they are.
Passwords and user names:
Passwords are used to restrict access to data or systems. They should be hard to crack and changed frequently to retain any real level of security.
Biometrics: Biometrics relies on certain unique characteristics of human beings

Two-step verification

Two-step verification is used as a method of authentication where **two different types of authentication** are needed to identify someone

Automatic software updates

Automatic updates of software keep a device secure. The updates will contain patches that could include updated virus checkers, software improvements and bug fixes.

Check spelling and tone of communication and of URL links

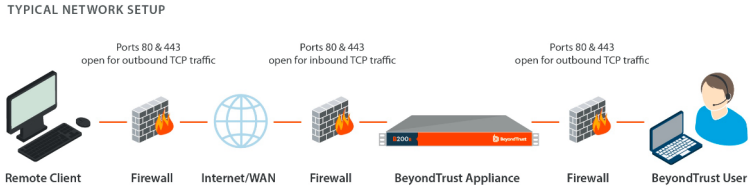
actions when receive an email:
1. Look out for suspicious links
2. Check the spelling in the email itself and any links
3. Check the tone of the message and language used
4. Check email addresses

Biometric technique	Benefits	Drawbacks
fingerprint scans	it is one of the most developed biometric techniques Very **easy to use** relatively small storage requirements for the biometric data created	for some people it is **very intrusive**, since it is still related to criminal identification it can make **mistakes** if the skin is dirty or damaged
retina scans	very **high accuracy** there is no known way to replicate a person's retina	it is **very intrusive** it can be relatively **slow** to verify retina scan with stored scans very **expensive** to install and set up
face recognition	**non-intrusive** method relatively **inexpensive** technology	it can **be affected** by changes in lighting, the person's hair, change in age, and if the person is wearing glasses
voice recognition	**non-intrusive** method verification takes less than 5 seconds relatively **inexpensive** technology	a person's voice can be **easily recorded** and used for unauthorised access **low accuracy** an illness such as a cold can change a person's voice, making absolute identification difficult or impossible

Keep data safe from security threats (Firewall)

Firewall Task:
1. **Monitors traffic** coming into and out of the computer
2. **Checks** that the traffic meat any criteria
3. **Blocks** any traffic that does not meet the criteria
4. Allows a set **blacklist**
5. Can **close certain ports**

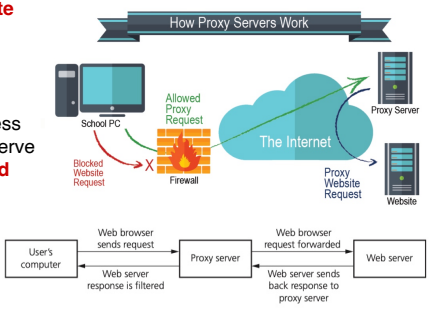
Firewall Feature:
1. can help **prevent hacking**
2. can **set criteria**
3. can **monitor** incoming and outgoing traffic
4. can check whether traffic meets
5. can **rejects** any traffic that does not meet



Keep data safe from security threats (Proxy Server)

Proxy Servers: act as an **intermediate** between the user and a web server

Proxy Server Features:
1. allow internet traffic to be filtered.
2. keeps users' **ip address secret**
3. **block** request from certain IP address
4. **prevents direct access** to a web serve
5. attack hits the **proxy server instead**
6. can also act as firewalls



Privacy settings

Privacy settings are controls available on web browsers, social networks and other websites; they are designed to limit who can access and see a user's personal profile (data)

Privacy settings Features:
1. **'do not track' setting**: stops collecting browsing data
2. check to see if the payment methods have been stored on websites
3. privacy options (**browsing history, storing cookies**)
4. advertising opt-outs preventing unsolicited adverts from websites
5. preventing **apps sharing your location**.

SSL(Secure Sockets Layer): a type of protocol - a set of rules used by computers to communicate with each other across a network

SSL certificate: a form of **digital certificate** which is used to **authenticate a website**.

SSL used:
1. online banking
2. online shopping
3. sending and receiving emails
4. using cloud storage facilities
5. used in instant messaging
6. social network