5 The Internet & Its Uses

5.1 The Internet & The World-Wide Web

The **internet** is the infrastructure that allows networks & devices to connect to each other.

The **world-wide web** is the collection of websites & web pages accessed using the **internet.**

A **URL (Uniform Resource Locator)** is a text-based address for a **web page**

- **HTTP (Hypertext Transfer Protocol)** – the **protocol** (set of rules) used for transferring data on the internet
- **HTTPS (Hypertext Transfer Protocol Secure)** – secure version of HTTP that uses **encryption (SSL)** to protect data transferred

protocol://domain/web page or file name
https://www.example.com/index.html

Web Browser

The main purpose of a **web browser** is to render **HTML (hypertext markup language)** and display **web pages**

Functions

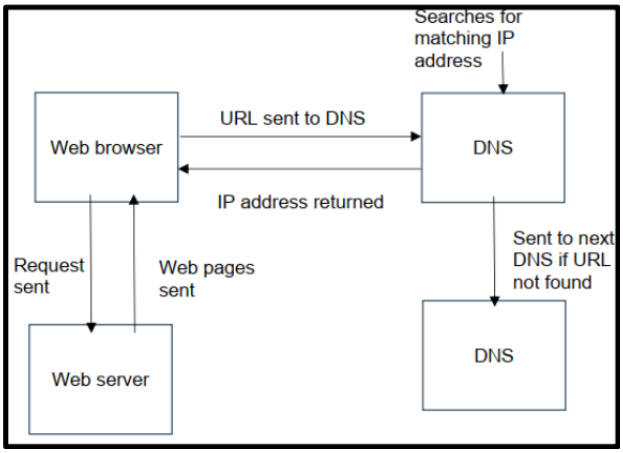
- Render **HTML** to display **web page**
- Stores **bookmarks** & **favourites**
- Stores user **history**
- Allows use of **multiple tabs**
- Stores **cookies**
- Provides **navigation tools**
- Providing an **address bar**

Web Pages

A web page **is a digital document on the internet that users can view using a** web browser**.**

How web pages are located, retrieved and displayed on a device

1. **Browser** sends **URL** to **DNS (domain name server)** using **HTTP/HTTPS**
2. **DNS** finds the matching **IP address** & returns it to the **browser**
3. **Browser** sends a **request** to the **web server**
4. **Web server** sends back **web pages** to **browser**
5. **Browser** interprets and renders **HTML** to display **web pages**



- **HTML (Hypertext Mark-up Language)** is used to create the website

Cookies

Cookies are small files that are stored on a user's device by a website

- **Session cookies**
  - Stored in RAM
  - Temporary – lost when a browser is closed / stored only during a user's browsing session
  - Used to maintain a user's activity during a session

- **Persistent cookies**
  - Stored in hard drive / secondary storage
  - Not lost when a browser is closed / stored on a user's device, until it is deleted by user
  - Used to remember user data e.g. preferences, browsing activity, purchases

Functions

- Saves personal details & login details
- Tracks user preferences for customised experience
- To hold items in an online shopping cart

5.2 Digital Currency

A **digital currency** is a currency that only exists electronically & is recorded on **blockchain**

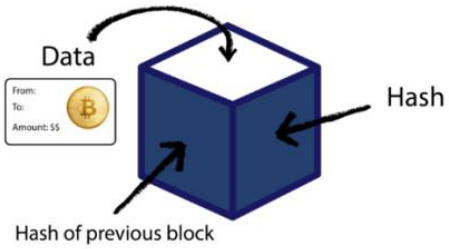
- Has no physical form like cash/coins
- Operates on a decentralised network (not controlled by a single entity e.g. central bank/government, recorded on blockchain)
- Used for transactions e.g. purchasing G&S, transferring money
- Can be highly volatile (value fluctuates rapidly over short periods of time)

Blockchain

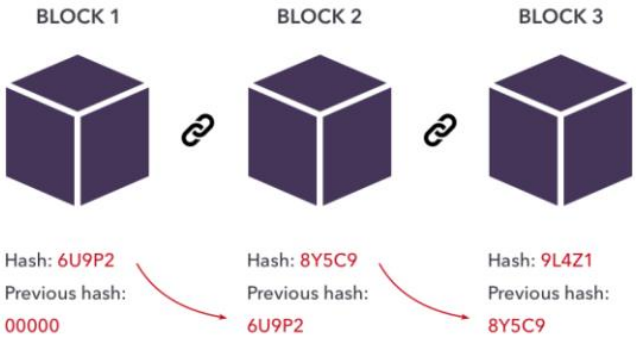
Blockchain is a digital ledger to track transactions that keeps a series of time-stamped series records that cannot be altered

- Blockchain is a decentralised database (not controlled by a single entity)
- Every participant in the network has a copy of the ledger and can verify the transactions independently
- The blockchain is made up of "blocks" of transactions that are linked together in a "chain" using cryptographic algorithms
  - If a hacker accessed a block and changed anything, the hash value of the block would change, meaning that all blocks beyond the hacked block would now be invalid because the chain would be broken.
- Each transaction in the blockchain must be verified by multiple participants in the network

Structure of a block



Structure of blockchain



5.3 Cyber Security

Cyber Security Threats

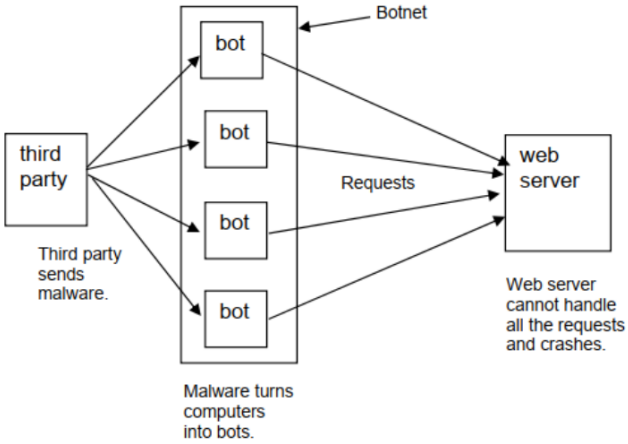
Cyber security threats are **potential dangers** that can harm computer systems, networks, or data. These threats come from hackers, malware, or system vulnerabilities and can lead to **data loss, financial damage, or identity theft**

DDoS Attack (Distributed Denial of Service)

1. Multiple computers floods a **server** with a large number of requests (traffic) all at the same time
2. The **server** is unable to respond to all requests & fails/crashes
3. This denies users access to a **website**

Method of prevention

- ♣ using an up-to-date malware checker
- ♣ setting up a firewall to restrict traffic to and from the web server or user's computer
- ♣ Applying email filters to filter out unwanted traffic (for example, spam)



Malware

- A malicious software designed to harm or gain unauthorised access to a system/network e.g. steal data, disrupt services
- Types of Malware
  - **Virus** - software that replicates when the user runs it → deletes/corrupts data

    Methods of prevention

    ♣ don't open emails from unknown sources,

    ♣ don't install non-original software

    ♣ always run an up-to-date anti-virus software

  - **Worm** - software that replicates on networks without user input → deletes/corrupts data, takes up bandwidth

    Methods of prevention

    ♣ Don't open emails from unknown sources,

    ♣ Always run an up-to-date anti-virus software

  - **Trojan horse** - software that is disguised as a legitimate software → installs the other malware it actually contains

    Methods of prevention

    ♣ Don't open emails from unknown sources,

    ♣ Avoid Downloading from Untrusted Sources

    ♣ Keep Your Operating System and Software Updated

  - **Spyware** - software that monitors user activity (key presses) and transmits these to a third party → steal personal data

    Methods of prevention

    ♣ Install and update **anti-spyware software**

    ♣ Avoid downloading software from **untrusted websites**

    ♣ Use a **firewall** to block unauthorized access

  - **Adware** - software that floods user with unwanted adverts → some may contain spyware, link to virus, fake websites

    Methods of prevention

    ♣ Install an **ad blocker**

    ♣ Do not click on suspicious ads or pop-ups

    ♣ Use antivirus software to detect adware

- **Ransomware** - software that stops a using accessing their data by encrypting it & a fee has to be paid to decrypt it

  Methods of prevention

  ♣ **Keep backups** of important files on external storage

  ♣ **Do not open** email attachments from unknown senders

  ♣ Use strong **antivirus and anti-ransomware software**

Hacking

- Gaining unauthorised access to a system/network to steal/manipulate data, disrupt services, or cause damage

  Methods of prevention

  ♣ Use firewall

  ♣ Use passwords

  ♣ Use biometrics security

Phishing

- The user is sent a legitimate-looking email where they are encouraged to click a link to a fake website designed to obtain user's personal information

  Methods of prevention

  ♣ Checking spelling/tone

  ♣ Not clicking on links in email unless your are 100% guarantee

  ♣ Use firewall

Pharming

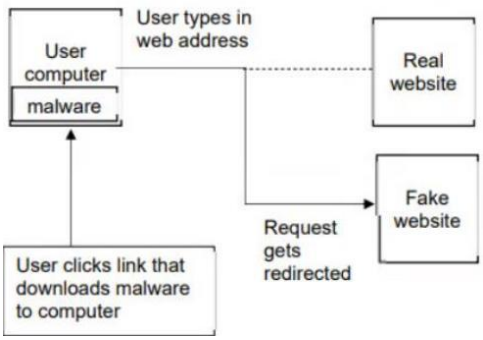
- **Malware** is downloaded without users' knowledge which redirects to a fake website designed to obtain personal information

  Methods of prevention

  ♣ Checking whether the URL is secure or not

  ♣ Checking the spelling of websites

  ♣ Use firewall



Brute-Force Attack

- A trial-and-error method to crack passwords by trying every possible combination to gain unauthorised access to a network

Methods of prevention

♣ Don't use the common passwords

♣ Use biometrics

♣ Use two factor authentications

Data Interception

- Eavesdropping on communication channels to steal sensitive information e.g. passwords, credit card numbers
- This is done by using devices such as a packet sniffer (A packet sniffer is a software or hardware tool used to capture, analyze, and monitor network traffic.)

Methods of prevention

♣ Use encryption

♣ Use passwords

Social Engineering

- Manipulating individuals to gain access to their personal information
- Methods of social engineering
  - Impersonation as someone else in emails/phone calls e.g. co-worker, IT support personnel, bank representative
  - Baiting – leaving a **malware**-infected memory stick which causes users to pick it up out of curiosity; installs malware when plugged into computer
  - Scareware - pop-up message claims that user's computer is infected with a virus, causing them to download a fake anti-virus out of fear
  - Instant messaging - links embedded to messages linking to fake websites

Methods of prevention

♣ Don't click on links or download attachments from unknown sources

♣ Use unique passwords for different accounts.

♣ Avoid entering passwords where others can see.

Keeping Data Safe

Anti-Malware e.g. anti-virus & anti-spyware (← Prevent from malware)

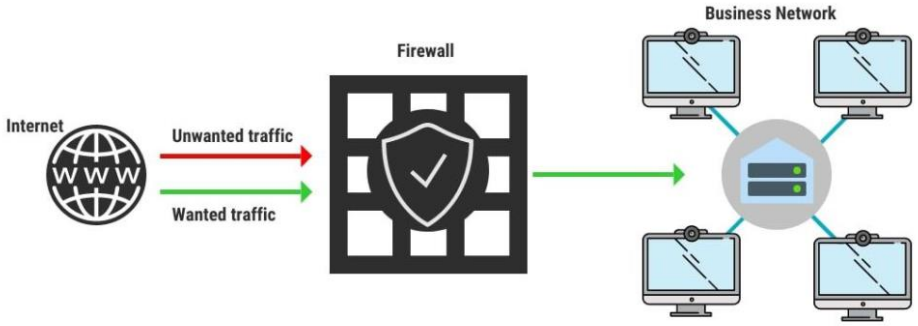
- Used to prevent and remove malware from a computer system
- Scans the computer system using a list of known malware → removes/quanrantines any malware found
- Checks data before download → stops download if malware found

Authentication (← Prevent from hacking, brute force attacks)

- Used to ensure that only authorised users can access data
- Methods of authentication
    - **Passwords**
        - Make it stronger/complex, change regularly, not reused for different accounts, lock out after # of attempts
    - **Biometrics** e.g. fingerprints, facial recognition, iris scans
        - Data entered is unique to individual & difficult to replicate, lock out after # of attempts
    - **Two-factor authentication (2FA)** e.g. password & verification code
        - Extra data has to be entered, difficult for hacker to obtain, cannot be attempted from a remote location

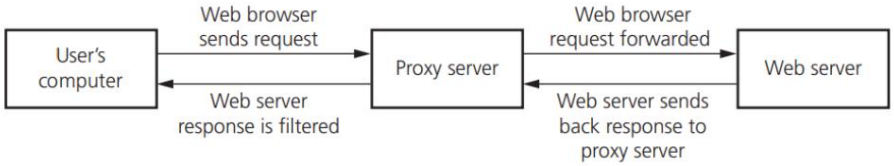
Firewalls (← Prevent from malware, hacking, DDoS, phishing, pharming)

- A firewall can be software or hardware
- Monitors & filters (accepts/rejects) **incoming and outgoing traffic** between the **computer** and the **network**
- Checks that traffic meets **criteria** set by user
- Blocks traffic that fails the criteria & adds to **blacklist**



Proxy Servers (← Prevent from DDoS)

- Acts as a **firewall** to filter incoming/outgoing traffic by set criteria
- Blocks traffic that fails the criteria & sends warning message to user
- Stop the website failing in a **DDoS attack** (DDoS attack hits the proxy server and not the web server)



Proxy Servers vs Firewall

- Proxy servers divert attack from server, firewalls stop unauthorised access
- Proxy servers can hide user's IP address, firewall does not hide the user's IP address

Secure Socket Layer (SSL) Security Protocol (← Prevent from data interception e.g. online transactions)

- **SSL** is a security protocol used to encrypt data transmitted over the internet
  1. **Browser** requests an **SSL digital certificate** from the **server**
  2. This is sent from the **web server** to the **browser**, containing a **public key** used for authentication
  3. Once the **certificate** is authenticated, the **transaction** will begin

Access Levels

- Different people have different levels of access
- Used to restrict access to sensitive information to prevent unauthorised access

Automating Software Updates

- Ensures that software is up-to-date with the latest security patches
- Scans the internet & installs **updates** to software

Checking the Spelling/Tone of Communications & The URL Attacked to a Link (← phishing)

- May contain misspelling of domain names, should usually be https and not http, large companies more commonly use .com

Privacy Settings

- Used to control the amount of personal information that is shared online
- Prevents identity theft & fraud