The Internet and its Uses

The internet and the world wide web, URLs and browsers, cookies, digital currency and blockchain, and the cyber security threats and the measures that stop them.

5.1 The internet and the world wide web

Internet and the World Wide Web

The **Internet** is a vast network of interconnected computers and servers around the world.

- It forms the infrastructure, which includes routers, switches, and data centres, that enables various types of digital communication.
- It uses standardized communication protocols like TCP/IP to transmit data.
- It provides the physical and logical connections needed for devices to communicate and enables the transfer of data across networks, including emails, file sharing, and streaming services.

> **NOTE**
>
> Think of the Internet as a global system of highways and roads that connect different cities (computers and servers).

The **World Wide Web** is a system of interlinked hypertext documents and multimedia content that can be accessed via the Internet using web browsers.

- It is the collection of web pages that contain text, images, videos, and other multimedia that software applications like Firefox allow people to access. The URLs (Uniform Resource Locators) specify the addresses of web pages.
- It uses hyperlinks to connect different web pages, allowing for easy navigation and discovery of related content.

> **NOTE**
>
> The World Wide Web is like a huge library of interconnected books and multimedia materials, where each book is a website, and hyperlinks are the references that guide you from one book to another.

Note Academy

Uniform Resource Locator (URL)

A **Uniform Resource Locator (URL)** is a text-based address that is used to access web pages and other resources on the Internet. It is a user-friendly version of the IP address.

Components of a URL

1. **Protocol:** It specifies the method used to access the resource. Some examples are http, https and ftp. It indicates the type of connection and the data transmission method.
2. **Domain name:** The readable address of the server hosting the resource. It identifies the location of the server on the Internet. It's mapped to an IP address via the Domain Name System (DNS).
3. **Path:** Specifies the exact location of the resource on the server. It directs the server to the specific file or page requested.

```
https://apple.com/iphone
^^^^^  ^^^^^^^^^ ^^^^^^^^
|     |       path
|     domain name
protocol
```

Hypertext Transfer Protocol (HTTP) is the foundation of data communication for the World Wide Web. It is a protocol/set of rules that are used when interacting on the World Wide Web.

Hypertext Transfer Protocol Secure (HTTPS) is the secure version of HTTP.

- It uses a TLS/SSL handshake. This process involves the exchange of cryptographic keys to establish a secure connection.
- It uses encryption to make the interaction secure.

Web Browsers

Browsers are one of the most used applications. Listed below are some of the **functions** that a browser can perform.

- Allows user to view web pages
- Renders HTML
- Allows user to bookmark/favourite web pages
- Provides navigation features
- Allows (multiple) tabs
- Stores cookies
- Records history of pages visited

Note Academy

- Has a homepage
- Runs active script

The primary function of a browser is to **render webpages**. This is how it does so:

- Sends the URL of the website to a Domain Name Server to find the IP address
- Connects to the webserver using the IP address using HTTP / HTTPS
- Renders the HTML
- Runs active scripts built into webpages
- Manages SSL/TLS certificate process
- Stores cookies

Cookies are text files with small pieces of data to enhance the experience of the user. It stores the user's preferences, account details, recent purchases, pages visited, shopping basket, etc.

Session cookies are temporary cookies that are deleted once you close your browser. They store information temporarily and are used for things like keeping you logged in as you navigate through different pages of a website during a single session, such as storing items in a shopping cart as you use other sites.

Persistent cookies are cookies that remain on your device for a set period of time or until you manually delete them. They store information for your future visits, making it easier and quicker for you to navigate the site. An example is saving login details so you don't have to enter your username and password every time you visit.

How cookies work

1. Webserver sends file to user's browser.
2. User's payment details stored in encrypted text file.
3. Cookie file is stored by browser.
4. When user revisits website, webserver can access the data stored in the cookie file to automatically enter details.

5.2 Digital currency

Digital Currency and Blockchain

Digital currencies, like Bitcoin and Ethereum, are growing in popularity and use every single day.

- Fundamentally, they only exist electronically.
- They use cryptography to track transactions.
- They are encrypted.

Note Academy

- They can be centralised, which means they are controlled by an authority, or decentralised.
- There are many uses of a digital currency, one of which is that it can be used to buy goods online.

Blockchain is a decentralized digital ledger that records transactions.

- Transactions cannot be altered once recorded.
- Each transaction is recorded with a time stamp.

This is what happens when a transaction takes place:

1. A user starts a transaction.
2. The transaction is broadcast to a network of nodes.
3. Nodes validate the transaction.
4. Each block contains a unique cryptographic hash, securing the data.
5. The validated transaction is added to a block.
6. The block, now containing the transaction and its hash, is added to the blockchain, making it immutable.
7. The ledger is updated across all nodes.

Proof-of-Work (PoW) is a consensus mechanism used in blockchain networks, where miners solve complex cryptographic puzzles to validate transactions and add new blocks, ensuring security and preventing tampering. This process is energy-intensive and time-consuming, but it provides a high level of security and decentralization.

5.3 Cyber security

Cyber Security Threats

Brute-force attack

Attackers use software to systematically try every possible combination of passwords until the correct one is found. This method is highly effective against weak passwords. Modern systems use rate-limiting and account lockouts to prevent this. Its **aim** is to gain unauthorized access to accounts by exploiting weak or simple passwords.

Data interception

Data is sent from one device to another over a network. During transmission, the data is examined using a packet sniffer. The intercepted data is reported to a third party and analyzed for useful information. The connection can be hacked to spoof the destination address, allowing attackers to redirect data to their own servers. Its **aim** is to capture sensitive information such as passwords, credit card numbers, and personal communications.

Distributed Denial of Service (DDoS) attack

Note Academy

Malware is downloaded to several computers turning them into a network of infected computers called a botnet. When the third party/hacker initiates the attack, the bots send requests to a web server at the same time. The web server fails due to the massive amount of requests. Legitimate requests cannot reach the web server. Its **aim** can be to test the resilience of a server, revenge, or to ruin a company's reputation.

Hacking

Attackers exploit vulnerabilities in software or hardware. They gain unauthorized access to systems, networks, or data. Hackers can install malware, steal data, or disrupt services. Its **aim** is to gain unauthorized access for various purposes, such as data theft, financial gain, or disruption of services.

Malware

Malware is malicious software designed to harm or exploit systems. Virus, worm, Trojan horse, spyware, adware and ransomware are all examples of malware.

Virus

A virus is a type of malicious software that attaches itself to a legitimate program or file. When the infected program or file is executed, the virus is activated and begins to replicate. It can spread to other programs, files, and systems. Its **aim** is to corrupt, delete, or steal data.

Worm

A worm is a standalone malware that replicates itself to spread to other computers. Unlike a virus, it does not need to attach itself to a program. Worms typically spread through networks by exploiting security vulnerabilities. Its **aim** is to consume bandwidth and system resources and to disrupt network operations.

Trojan horse

A Trojan horse appears to be a legitimate program but hides malicious code. Users unknowingly install the Trojan, thinking it is a useful or benign application. Once activated, it can execute its malicious payload. Its **aim** is to create backdoors for remote access and steal sensitive information.

Spyware

Spyware is a type of malware that secretly monitors and collects user information. It often tracks browsing habits, keystrokes, and personal information. Spyware can be installed through malicious downloads or as part of legitimate software. Its **aim** is to gather sensitive information such as passwords and credit card numbers.

Pharming

Attackers redirect traffic from legitimate websites to fake ones. Users are tricked into entering sensitive information on the fake site. The fake site collects this information for malicious use. Its **aim** is to steal sensitive information such as login credentials and financial details.

Phishing

Note Academy

Attackers send fraudulent emails or messages pretending to be from a trusted source. The messages contain links to fake websites or malicious attachments. Users are tricked into providing sensitive information or downloading malware. Its **aim** is to steal sensitive information such as usernames, passwords, and financial details.

Differences between phishing and pharming

- Phishing involves use of an email whereas pharming involves installing malicious code.
- Phishing involves clicking a link or an attachment whereas pharming creates a redirection.

Social engineering

Attackers manipulate individuals into divulging confidential information. Techniques include impersonation, pretexting, and baiting. The information is used to gain unauthorized access or perform malicious activities. Its **aim** is to exploit human psychology to gain access to systems or sensitive information.

Maintaining Cyber Security

Access levels

Access levels control who can view or use resources within a system. Different users are given different permissions based on their role. Helps in limiting access to sensitive information. It restricts access to critical data to only authorized personnel and prevents unauthorized changes or deletions of important files.

Anti-malware

Anti-virus software detects, prevents and removes viruses and other malware. Anti-spyware software is a specialized tool developed to detect, prevent, and remove spyware from your computer. It works similarly to antivirus software but is specifically focused on combating spyware threats.

Authentication

Username and password is a traditional and widely used method for authenticating users. When logging in, users enter their username and password. The system checks if the credentials match those stored in its database. If they match, access is granted.

Biometrics involves using physical or behavioural characteristics for authentication. Here are some common types:

- **Fingerprint scanning:** Uses unique fingerprint patterns.
- **Facial recognition:** Analyzes facial features.
- **Iris scanning:** Uses the unique patterns in the coloured part of the eye.

Note Academy

The system captures the biometric data during setup and stores it. During login, the user provides the same biometric data, which the system compares to the stored data for verification.

Two-step verification adds an extra layer of security beyond the username and password. After entering the username and password, the user must provide the second piece of information. This ensures that even if the password is compromised, the account remains secure.

- Provide a second piece of information, such as:
  - **SMS code:** A code sent to the user's mobile phone.
  - **Email code:** A code sent to the user's email.
  - **Authenticator app:** A time-based code generated by an app like Google Authenticator.

Automating software updates

Automating software updates ensures that all software is kept up-to-date with the latest security patches which prevents vulnerabilities from being exploited by attackers. It reduces the risk of security breaches by patching known vulnerabilities and ensures that the system has the latest features and improvements.

Checking the spelling and tone of communications

Phishing attacks often contain spelling errors or unusual tones. Being vigilant about the quality of communication can help identify and avoid phishing attempts.

Checking the URL attached to a link

Malicious links often lead to fake websites designed to steal information. Verifying the URL before clicking can prevent such attacks. This ensures that users are directed to legitimate websites and protects against phishing and malware distribution.

Firewalls

Firewalls examine the traffic between a user's computer and a public network.

- It checks whether incoming or outgoing data meets a given set of criteria.
- If the data fails the criteria, the firewall will block the 'traffic' and give the user (or network manager) a warning that there may be a security issue.
- The firewall can be used to log all incoming and outgoing 'traffic' to allow later interrogation by the user (or network manager).
- Criteria can be set so that the firewall prevents access to certain undesirable sites; the firewall can keep a list of all undesirable IP addresses.

Privacy settings

Privacy settings control what information is shared with others which can be configured on social media, browsers, and other online platforms. It protects personal information from being publicly accessible.

Note Academy

Proxy servers

Proxy servers act as intermediaries between a user's device and the internet. They can be used to anonymize web traffic and protect user privacy. They hide the user's IP address, making it harder for attackers to target them, and can be used to bypass geo-restrictions and access blocked content.

Difference between proxy servers and firewalls

- A proxy can hide the user's IP address whereas a firewall does not hide the user's IP address.
- A proxy's intention is to divert attack from the server, a firewall's is to stop unauthorized access.
- A proxy protects a server whereas a firewall protects an individual computer.
- A proxy examines requests for a website but a firewall does not.
- A proxy transmits website data to the user but a firewall does not.

Secure Socket Layer (SSL)

SSL is a standard security protocol for establishing encrypted links between a web server and a browser. It is used to protect sensitive information, such as credit card numbers and personal details, during online transactions. A locked padlock and https shows that SSL/TLS is being used.

The updated version of SSL is **TLS (Transport Layer Security)**.

Here is how SSL works:

1. Uses (digital) certificates requested from web server by client.
2. Server sends SSL/digital signature to client.
3. Client and server agree on encryption method to use that contains the server's public key.
4. Browser checks authenticity of certificate then session key is generated and sends signal to server to start transmission.

Note Academy