Name: Index: Reg. No.: Class: Date:

Chapter 5
The internet and its uses

The internet and the World Wide Web (WWW)

What is the internet?

- The Internet is the **infrastructure** that allows network & devices to connect to each other.

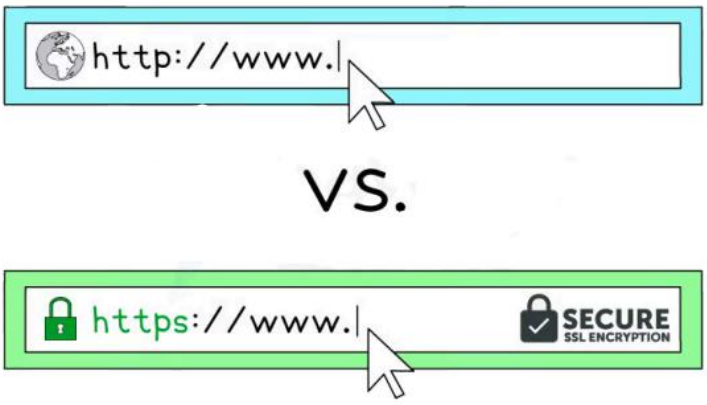
What is the World Wide Web?

- The world wide web, or **simply the web**, is a **collection of websites** and **web pages** that are **accessed using the internet**

Network Protocols

HTTP & HTTPS

- Hypertext Transfer Protocol (**HTTP**) allows communication between clients and servers for **website viewing**
- HTTP allows clients to **receive data** from the sever (fetching a webpage) and **send data** to the server (submitting a form, uploading a file)
- **HTTPS** works in the same way as HTTP but with an **added layer of security**
- All data sent and received using HTTPS is **encrypted**
- HTTPS is used to **protect sensitive information** such as passwords, financial information and personal data



Web Browser

What is a web browser?

- A web browser is a **piece of software** used to **access** and **display** information on the internet
- A web browser **displays web pages** by **rendering hypertext markup language (HTML)**
- Web browsers **interpret the code in HTML** documents and **translate** it into a visual display for the user

Functions of a web browser

Function	Description
Render/convert HTML	Display the web page
Provide navigation tools	E.g. back/forward buttons and home button, to help users move between pages
Storing bookmarks & favourites	Allow users to save links to frequently visited websites and access them easily
Storing cookies	A cookie is a tiny data file stored on a computer by browser software that holds information relating to your browsing activity
Record user history	Allow users to quickly revisit recently viewed web pages
Provide address bar	A place for user to type in the URL (link to URL page) of a web page to visit
Multiple tabs	Allow multiple web pages to be open at once so users can quickly switch between them

Web Pages

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

1. **Web Servers**
   - A web server is a **remote computer** that **stores the files needed to display a web page** on the Internet
   - Web servers are generally **available 24/7** and **security is managed** by the owner of the hardware
   - Web servers provide access to **multiple users at the same time**

2. Uniform Resource Locator (URL)

- A **Uniform Resource Locator** (URL) is a **unique identifier** for a web page, known as the **website address**
- It is **text based** to make it easier to remember
- A user **enters a URL** into a web browser to view a web page
- An example of a URL is:
  https://www.facebook.com/media/set/create
- A URL can typically be split into three parts:

Protocol	https	Communication method to transfer data between client and server
Domain name	www.facebook.com	Name of the server where the resource is located
Web page/file name	/media/set/create	Location of the file or resources on the server

3. Domain Name Server (DNS)

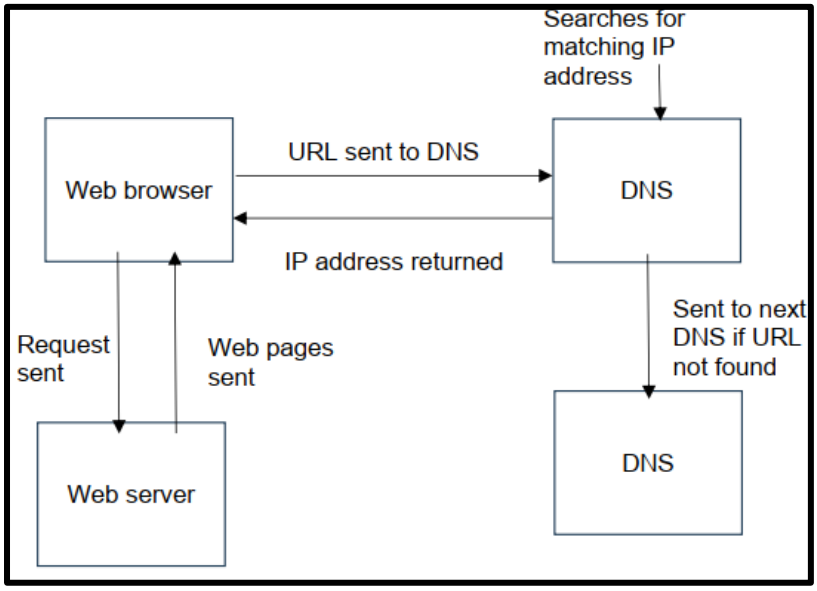
- The Domain Name Server (DNS) can be thought of as the Internet's equivalent to a **phone book**
- It is essentially a directory of domain names and is used to translate human-readable domain names to the numeric **IP addresses** that computers use
- When you type a URL into your browser, the **DNS translates the domain name into its associated IP address** so your computer can connect to the server hosting the website
- Without DNS, we would have to remember the IP address of every site we want to visit

4. HTML

- Hypertext Markup Language (**HTML**), is the foundational language **used to structure and present content on the web**
- Written in **plain text**
- HTML consists of a series of elements, often referred to as "**tags**"
- Used to tell the browser how to **display the page**

How web pages are located and retrieved?

- **URL** sent from **web browser** to the **DNS**
- DNS finding **matching IP address**
- If it cannot find the URL, it is sent to the next DNS (until found)
- **IP address** returned to **web browser**
- **Request** sent from **web browser** to **web server** (for web page)
- Web page/HTML files sent from **web server** to **web browser**
- Web browser **rendering HTML**



Cookies

- A cookie is a **tiny data file** stored on a computer by browser software that holds information relating to your **browsing activity**
- Typically a cookie will contain:
  - **Browsing history** - what websites you have visited
  - **Login information** - usernames & passwords
  - **Preferences** - language/font size/themes
- There are **two** types of cookie are:

1. Session Cookies

- These are stored in RAM only during a user's browsing session
- These are temporary means it lost when a browser is closed / stored only during a user's browsing session
- Used to maintain a user's activity during a session

2. Persistent Cookies

- Stored in hard drive / secondary storage of a device
- Not lost when a browser is closed and until it is deleted by user
- They are used to remember user preferences and settings, such as language preferences, login details, and shopping cart items

Functions of cookies

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

Digital Currency

What is digital currency?

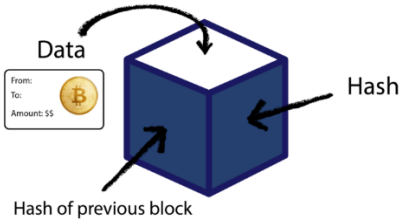
- Digital currency is one that **only exists in digital form**
- Currency is **stored in digital wallets** or accounts, there is **no physical bank notes** or **coins**
- Operates on a **decentralised network** (not controlled by a single entity e.g. central bank/government, recorded on blockchain)
- Used for **transactions** e.g. purchasing items, transferring money
- Can be **highly volatile** (value fluctuates rapidly over short periods of time)
- All transactions made using crypto currency are **publicly available** and tracked using **cryptography**
- Examples include:
  - Bitcoin
  - Ethereum

What is a blockchain?

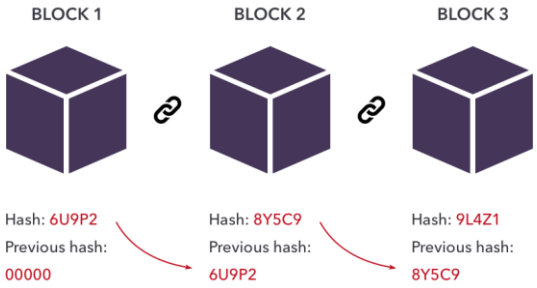
- A blockchain is a **digital ledger** that records every transaction made with a particular digital currency
- Transactions are **time-stamped** and added to the blockchain that cannot be **alterable**
- A blockchain is a **decentralised technology** (not controlled by a single entity or authority)
  - Instead, **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

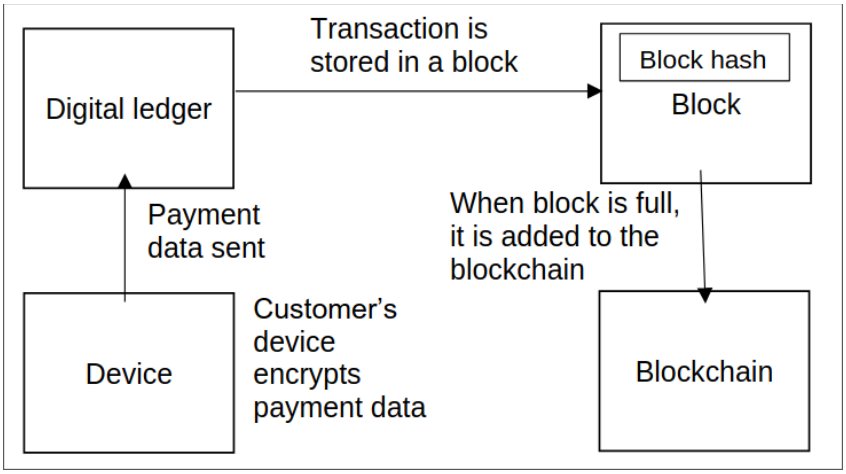


Structure of blockchain



Process of Blockchain

1. The customer makes a digital currency payment using their device.
2. The customer's device encrypts the payment data to keep it secure.
3. The payment data is sent to the digital ledger.
4. The transaction is stored inside a block in the digital ledger.
5. Each block contains:
    - Transaction data
    - A block hash
    - A link to the previous block
6. When the block becomes full, it is added to the blockchain.
7. The blockchain is updated across the network, creating a permanent and secure record of the transaction.

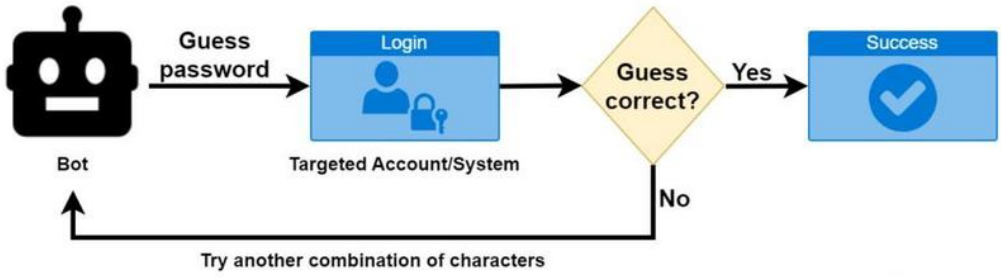


Cyber Security Threats

- **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**.
- The main threats posed are:
  - **Brute-force attacks**
  - **Data interception & theft**
  - **DDos attack**
  - **Hacking**
  - **Malware**
  - **Pharming**
  - **Phishing**
  - **Social engineering**

Brute Force Attack

- A brute force attack works by an attacker repeatedly trying **multiple combinations** of a user's password to **try and gain unauthorised access** to their accounts or devices
- The aim of this is to steal the your precious personal data or to use your account to buy products online.

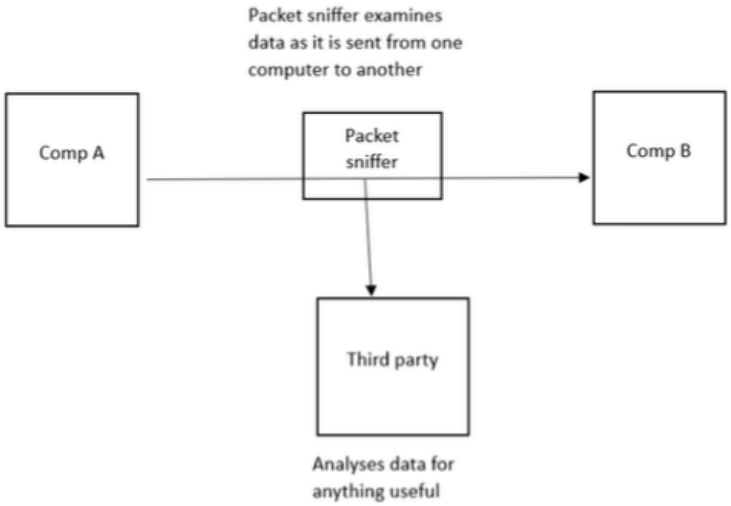


Method of prevention

- Use a strong password
- A biometric password and two-step verification
- Give a limited number of attempts

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**.)



Method of prevention

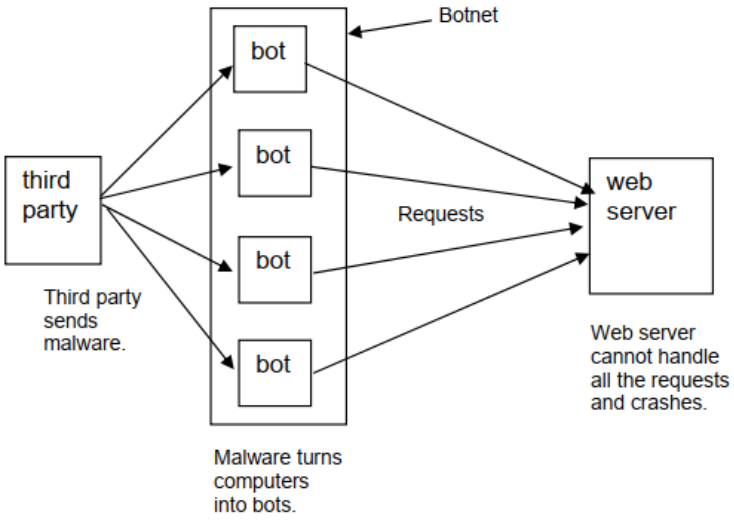
- Encrypt the data
- Check protocol to see if it uses HTTPS
- Use passwords in your data or account

DDoS Attack

- A **Distributed Denial of Service Attack** (DDoS attack) is a **large scale, coordinated** attack designed to **slow down a server** to the point of it becoming **unusable**
- Multiple computers floods a **server** with a **large number of requests** (traffic) all **at the same time**
- Obviously, the server can only handle a **finite number of requests**. So if it becomes **overloaded, it will crashes**
- The aim of this is to crash webserver. The perpetrator may be doing this to demand money for it to stop or as an act of revenge.

Method of prevention

- using an up-to-date malware checker
- setting up a proxy server to act as barrier that filters request to webserver.
- Applying email filters to filter out unwanted traffic (for example, spam).



Hacking

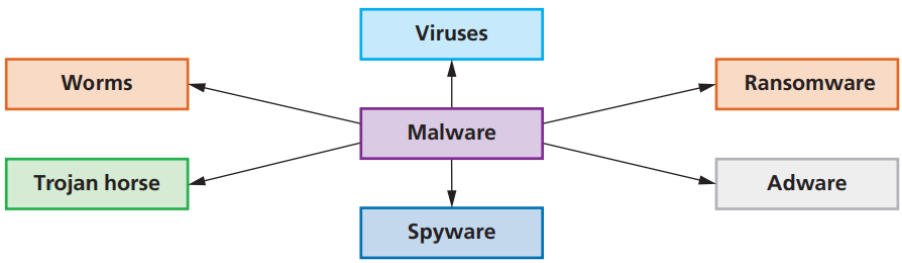
- Hacking is the process of **gaining unauthorised access** to a system or network by taking advantage of **security weaknesses** in the computer or network.
- It can lead to identity theft, gaining personal information or the loss/corruption of key data.

Method of prevention

- Use firewalls
- Use a strong password
- Use biometric systems

Malware

- Malware (**mal**icious soft**ware**) is the term used for any software that has been created with malicious intent to cause harm to a computer system
- Examples of issues caused by malware include
  - Files being **deleted, corrupted** or **encrypted**
  - Internet connection becoming **slow** or **unusable**
  - Computer **crashing** or **shutting down**
- There are various types of malware:



1. Viruses

- A virus is a program that is installed on a computer **without the user's knowledge** or **permission** with the purpose of doing harm.
- Viruses are often part of an **email attachment** and they require the user to take some action (for example, click on a link in the attachment) for the virus to **infect their computer**
- Examples of issues a user may experience are
  - **Corrupt files**
  - **Delete data**
  - **Prevent applications from running correctly**

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

2. Worms

- A worm is a type of **malware** that **copies itself** and spreads across a **network** without any **user action**.
- It can corrupt or delete data and uses up network bandwidth, slowing the network down.

Methods of prevention

- Use firewall
- Always run an up-to-date anti-virus software
- Avoid untrusted networks and downloads

3. Trojan Horse

- A software that is used to disguise other malware
- It is designed to looks like **legitimate software** to trick the user into installing it, but once installed it secretly carries out **harmful actions** or installs other **malware**.
- Examples of issues a user may experience are
  - **Steals personal data**
  - **Slows down your computer**
  - **Deletes or corrupts files**
  - **Uses your computer for illegal activities**

Methods of prevention

- Don't open emails from unknown sources,
- Avoid downloading from Untrusted Sources
- Keep Your Operating System and Software Updated
- Check Software Permissions

4. Spyware

- **Spyware** is a type of **malware** that **secretly monitors a user's activity** on a computer or device **without the user's knowledge or permission**.
- Embedded into other software such as games or programs that have been downloaded from **illegitimate sources**
- Can **record** your screen, log your **keystrokes** to gain access to **passwords** and more

Methods of prevention

- Install and update **anti-spyware software**
- Avoid downloading software from **untrusted websites**
- Use a **firewall** to block unauthorized access

5. Adware

- This is a software that is used to automatically created pop up and banner adverts when your online
- Can **redirect clicks** to unsafe sites that contain spyware

Methods of prevention

- Install an **ad blocker**
- Do not click on **suspicious ads or pop-ups**
- Use **antivirus software** to detect adware

6. Ransomware

- A software that encrypts a user's data and preventing access to it
- It is designed to **encrypts** your data and stops from gaining access to it
- A **demand is made for money** to receive the password that will allow the user to decrypt the files

Methods of prevention

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

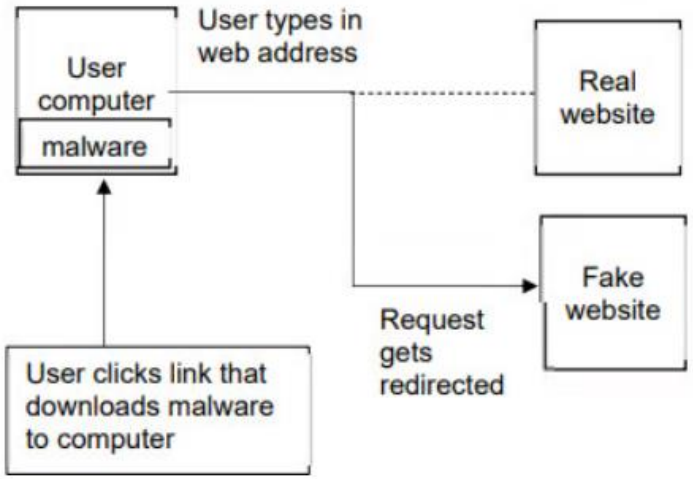
- **Do not open** email attachments from unknown senders
- Use strong **antivirus and anti-ransomware software**

Pharming

- Type of **malware** that is downloaded without the user's knowledge and **redirects them to a fake website** that is designed to **steal personal or confidential information**.
- The user **types in a web address** which is then **redirected** to the fake website

Methods of prevention

- Checking the **URL** is secure or not
- Checking the **spelling** of **websites**
- Use **secure DNS servers**
- Ensure browsers, antivirus, and firewalls are **regularly updated**

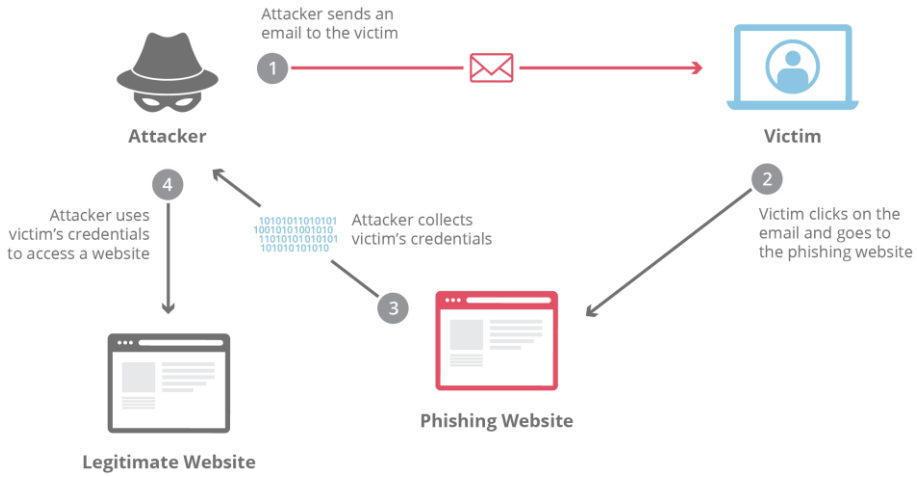


Phishing

- Phishing is the process of sending fraudulent emails/SMS to a large number of people, claiming to be from a **reputable company** or trusted source
- They require the user to take **some action** to initiate the phishing attack, for example, by clicking on the link in the email or attachment.
- Once a link is established, the user's browser is taken to a **fake website** where **personal information can be stolen**

Methods of prevention

- awareness training of users
- not clicking on links in emails unless you are 100% certain they are genuine
- running the anti-phishing tool in the browser
- using up-to-date browsers and run up-to-date firewalls



Social Engineering

- Social engineering is a type of cyber threat where attackers **trick people into giving away confidential information**, such as passwords, bank details, or personal data.
- Instead of **hacking** into a computer system, attackers **trick** or **persuade** people into **providing access**.
- There are **five types** of social engineering threats that commonly exist.

Instant messaging	Malicious links are embedded into instant messages, for example an important software upgrade (relies on user's curiosity).
Scareware (for example, fake antivirus that looks real)	This is often done using a pop-up message that claims that the user's computer is infected with a virus; the user is told they need to download the fake antivirus immediately (relies on user's fear).
Emails/phishing scams	The user is tricked by the apparent genuineness of an email and opens a link in the email; this redirects their browser to a fake website (relies on user's trust of well-known companies).
Baiting	The cybercriminal leaves a malware-infected memory stick somewhere where it can be found; the finder picks up the memory stick and plugs it into their computer (just to see who it belongs to) and unwittingly downloads malicious malware (relies on user curiosity).
Phone calls	For example, a so-called IT professional calls the user on their mobile claiming their device has been compromised in some way; the user is advised to download some special software that allows the cybercriminal to take over the user's device giving them access to personal information (relies on fear).

Methods of prevention

- Don't click on links or download attachments from unknown sources.
- Conduct awareness programs
- Never share passwords and use unique passwords for different accounts.

Keeping Data Safe

1. Access Levels

- Providing users with different permissions which limits their access to read and edit certain data.
- Users can have **designated roles** on a network
- Access levels can be set based on a user's **role, responsibility**, or **clearance level**
  - **Full access** - this allows the user to open, create, edit & delete files
  - **Read-only access** - this only allows the user to open files without editing or deleting
  - **No access** - this hides the file from the user

2. Anti-Malware

- Anti-malware software is a software used to prevent computers from being affected by **viruses** and other **malicious software**
- The different software anti-malware includes are
  - **Anti-virus**
  - **Anti-spam**
  - **Anti-spyware**

How does anti-malware work?

- Anti-malware **scans** through **email** attachments, **websites** and downloaded **files** to search for issues
- Anti-malware software has a **list of known malware**
- It **removes/quanrantines** any malware found

3. Authentication

- Authentication is the process of **ensuring** that only authorised users can access data
- Prevent from hacking, brute force attacks
- Authentication can be done in several ways, these include
  - **Usernames and passwords**
  - **Biometrics**
  - **Two-step verification**

➢ **Usernames and Passwords**

- Passwords are used to restrict access to data or systems. They should be hard to crack and changed regularly.

- It should not be easy to guess (for example, date of birth is a very weak password)
- Should not use same password for many devices
- Should be a strong password (at least eight characters including numbers, lower case letters, upper case letters and other keyboard symbols, for example, T7%%asR3£Sc is very strong but green is very weak).

➢ **Biometrics**

- Biometrics use **biological data** for authentication by identifying **unique physical characteristics** of a human such **as fingerprints, facial recognition, voice recognition** or **iris scans**
- Biometric authentication is **more secure** than using passwords as:
  - Data entered is unique to individual
  - It is very **difficult to fake** a biometric password
  - A biometric password **cannot be recorded** by spyware

➢ **Two-Step Verification**

- Two-step verification requires **two methods** of authentication to verify who a user is.
- For example:
  - a user logs onto a website using username and password and decides to use their credit card to buy something
  - as part of the security, an 8-digit PIN is sent back to the user either in an email or as a text message to a mobile phone number already registered on the website (this is known as a one-time pass code (OTP))
  - this 8-digit PIN is entered on the website proving the user's identity.

4. Automating Software Updates

- Automatic software updates mean **software** on computers and mobile phones/ tablets is **kept up-to- date**.
- It scans the internet & installs **updates** to software
- The updates will contain **patches** that could include updated virus checkers, software improvements and bug fixes

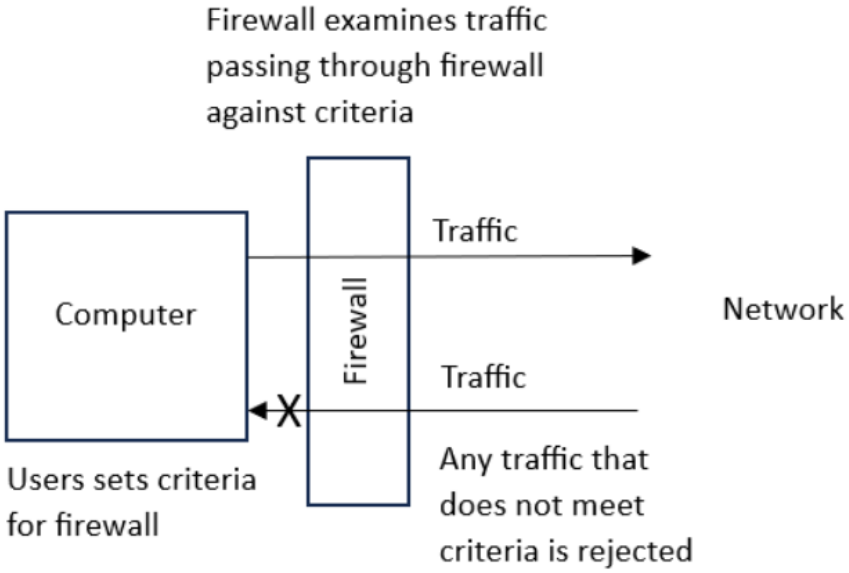
5. Check spelling and tone of communication and of URL links

- One way of protecting data is by **monitoring digital communication** to check for errors in the **spelling** and **grammar** or **tone** of the communication
- Phishing scams often involve communication with users

- Checking the URL attached to a link to confirm whether it uses https is another way to prevent phishing attacks
- If you are unsure, always check the website URL **before clicking any links** contained in an email

6. Firewalls

- A firewall **monitors incoming and outgoing network traffic** and uses a set of rules to determine which traffic to allow
- A firewall prevents **unwanted traffic** from entering a network. If the traffic fails the **criteria**, the firewall will **block** the 'traffic' and give the user a **warning** that there may be a **security issue.**
- Firewall **prevents** access to certain **undesirable sites**; the firewall can keep a list of all undesirable IP addresses
- It can **help prevent** viruses or hackers entering the user's computer.
- It can be both **hardware** and **software** and they are often used together to provide stronger security to a network

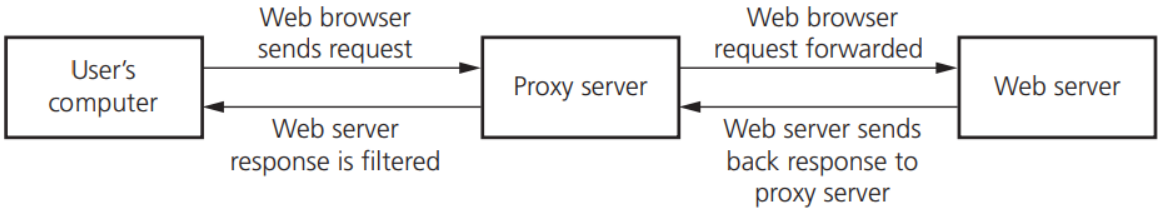


7. Privacy Settings

- Privacy settings are designed to **control who can access and see user's personal profile**
- They are an important measure to prevent identity theft and other forms of online fraud
- Users should **regularly review** their privacy settings and adjust them as needed
- Features of privacy settings include:
  - a '**do not track'** setting that stops websites collecting browsing data
  - Preventing apps sharing your location.

8. Proxy Servers

- **Proxy servers** are an intermediate device between a user and a web server

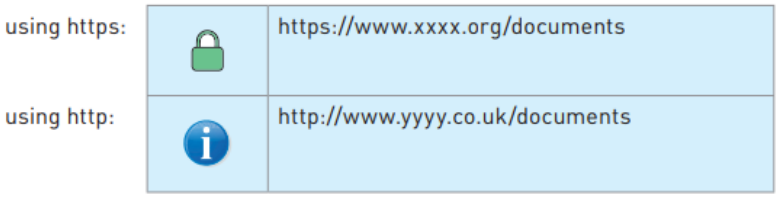


The main functions of proxy servers:

- It **hides a user's IP address** and **location**, making it more difficult for **hackers to track them**
- **It acts as a firewall by filter web traffic** by setting criteria for traffic
- It can **limit** the **number of requests** sent to the web server at a time
- Can **block** requests from certain **IP addresses.**
- Prevent direct access to a web server by sitting between user and server.
- The proxy server **stores a copy of the website's home page** in its cache.
- When the user visits the website again, the page is **loaded from the cache** instead to forwarding request to webserver

9. Secure Socket Layer (SSL)

- Secure Socket Layer (**SSL**) is a **security protocol** which is used to **encrypt data** transmitted **over the internet**
- The user knows if SSL has been applied when they see **https** and/or the green **padlock** on the browser **address bar**.



Process of SSL and how it provides a secure connection:

- SSL is a (security) **protocol**
- It **encrypts** any data that is sent
- It uses a **SSL digital certificate**
- **Browser** requests an **SSL digital certificate** from the **server**
- This is sent from the **web server** to the **browser**, containing a **public key** used for authentication
- Once the **certificate** is authenticated, the **transaction** will begin

Worked Example

(**i**) Identify a security solution that could be used to protect a computer from a computer virus, hacking and spyware.

Each security solution must be different

Threat	Security solution
Computer virus	
Hacking	
Spyware	

[3]

(**ii**) Describe how each security solution you identified in (**i**) will help protect the computer. **[6]**

Answers

(i)

Threat	Security solution
Computer virus	Anti-malware/virus (software) Firewall
Hacking	Firewall Passwords Biometrics Two-step verification
Spyware	Anti-malware/virus (software) Two-step verification Firewall

(ii) **Two** marks for each description

- **Anti-malware/virus (software)**
  - Scans the computer system (for viruses)
  - Has a record of known viruses
  - Removes/quarantines any viruses that are found
  - Checks data before it is downloaded
  - … and stops download if virus found/warns user may contain virus

- **Anti-malware/spyware (software)**
  - Scans the computer for spyware
  - Removes/quarantines any spyware that is found
  - Can prevent spyware being downloaded

- **Firewall**
  - Monitors traffic coming into and out of the computer system
  - Checks that the traffic meets any criteria/rules set
  - Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist

- **Passwords**
  - Making a password stronger // by example
  - Changing it regularly
  - Lock out after set number of attempts // stops brute force attacks // makes it more difficult to guess

- **Biometrics**
  - Data needed to enter is unique to individual
  - … therefore it is very difficult to replicate
  - Lock out after set number of attempts

- **Two-step verification**
  - Extra data is sent to device, pre-set by user
  - … making it more difficult for hacker to obtain it
  - Data has to be entered into the same system
  - … so if attempted from a remote location, it will not be accepted