5. THE INTERNET AND ITS USES

Internet	**World wide web**
The infrastructure	Collection of websites and web pages that are accessed using the internet.
Global network of computers and other electronic devices connected together through a system of routers & servers.	Consists of interconnected documents and multimedia files that are stored on web servers around the world.
Allows users to send and receive information, including email, instant messaging and file transfers. Provides access to other services: online gaming, video streaming, cloud computing.	Allows users to share and access information on a global scale.
Primarily hardware-based	More software-oriented
First version: ARPANET	First known as NSFNET
Uses IP address	Uses HTTP

Uniform Resource Locator

- Text-based address for a web page // user-friendly version of the IP address
- Identifies the location of a resource on the internet.

Components of a URL

1. Protocol
2. Domain name/ web server name
3. File name/ web page name

A URL looks like this: protocol://domain/path
E.g: https://www.example.com/index.html is a URL that consists of the HTTPS protocol, the domain name "www.example.com", and the file name is "/index.html".

- **Protocol:** communication protocol used to transfer data between client and server
- **Domain name:** name of the server where the resource is located.
- **File name:** location of the file or resource on the server.

Protocols

Used for transferring data between clients and servers on the internet.

Hypertext transfer protocol (HTTP)

- Main protocol that governs the transfer of data between client & server on the internet.
- Set of rules that need to be followed when transferring files across the internet.
- Stateless protocol: does not store information about previous responses & requests.
- Operates on port 80 by default .
- Doesn't encrypt data that is sent; data sent in plaintext format: vulnerable to interception
- When HTTP is used, padlock symbol in status bar is unlocked

Hypertext transfer protocol secure

- A secure protocol/ secure version of HTTP.
- Set of rules that need to be followed when transferring files across the internet.
- Operates on port 443 by default .
- Encrypts data that is sent: harder for unauthorised users to intercept/ manipulate data.
- It combines HTTP and SSL/TLS to transmit data.
- When HTTPS is used, padlock symbol in status bar is locked

Secure Sockets Layer (SSL)

- Security protocol to provide secure communication over the internet.
- Encrypts data that is sent using a combination of symmetric and asymmetric encryption.
- Operates at the transport layer: ensures that data is encrypted before it is sent over the network.

State how SSL protocol secures data for transmission

- It encrypts it
- Uses digital certificates

Transport Layer Security (TLS)

An updated version of the SSL protocol

<u>Layers of TLS</u>

1. **Handshake layer**
   - Carries out authentication of server & client // used to establish secure connection between server & client.
   - Handles encryption algorithms/ keys
2. **Record layer:** Responsible for securely transmitting data between the server and client

Protocols that can be used to transfer data securely

1. HTTPS
2. SSL
3. TLS

Ways that user can identify if website uses secure data transmission / HTTPS / SSL

- URL begins with HTTPS
- Padlock symbol is locked
- Check that the certificate is valid

How HTTPS protocol changes the data to transmit the data securely

- It encrypts it
- It applies encryption algorithm
- It applies an encryption key

How SSL protocol secures data for transmission

- It encrypts the data
- ... based on the authentication of an (SSL) certificate // and will only send it if the certificate is authentic

Benefit of using SSL connection

Data if intercepted cannot be understood // Data is encrypted // Data is scrambled // uses keys to encode/decode data

Process of SSL (or TLS) and how it provides a secure connection // How secure connection is created for website

- Uses a security protocol such as SSL/TLS
- Browser/client sends a request to the web server, to send/view the digital certificate
- Server sends SSL/digital certificate to browser/client
- Web browser checks that the certificate is valid/authentic
- If authentic, browser sends signal back to web server that the certificate is authentic
- If certificate is authentic, a secure connection/ session key is generated
- Client and server agree on encryption method to use
- ... that contains the server's public key
- Any data that is sent is encrypted
- Encryption may be asymmetric / symmetric / both
- It makes use of public and private keys.
- If connection is not secure, the browser will display an open padlock/warning message.

Applications of SSL & TLS

- Online banking
- Online shopping / Online payment / Online booking
- Cloud storage facilities
- Intranet/extranet
- VPN

- Email
- Voice over internet protocols (VoIP) / video conferencing
- Instant messaging (IM) / social networking / online gaming

Web browser

Software/ application that allows the user to view the contents of a web page.

Main purpose

- renders hypertext markup language (HTML)
- to display web pages.

Functions of web browser

a. Renders HTML: to display web page
b. Manages protocols: manage the HTTP and HTTPS protocols
c. Stores cookies: small text files containing user preferences & login details
d. Stores bookmarks/ favourites: users save frequently visited sites & easily access them
e. Records user history: users can quickly revisit recently viewed pages
f. Allows use of multiple tabs/ web pages to be open
g. Provides navigation tools: Allows movement between web pages
h. Provides an address bar: Allows users to enter URL/search to navigate to websites
i. Allows download of files from the internet
j. Runs active scripts (javascript): small programs embedded in web pages that allow interactive content such as animations, videos, and pop-up windows to be displayed

Web pages

How web pages are located, retrieved & displayed on a device when a user enters URL

- User enters URL into address bar
- Browser sends URL to DNS
- ... using HTTP/HTTPS
- DNS finds matching IP address for the URL
- DNS returns IP address to the browser
- Browser sends request to web server/IP address to obtain web pages
- Web server sends web pages back to browser
- Browser interprets/renders HTML (to display web pages)
- Security certificates exchanged
- HTTPS/SSL is used to secure data; encrypts any data that is sent.

How the URL is converted into IP address for website

- It is sent to a DNS ...
- which looks up the corresponding/matching IP address

Domain name server/DNS: The system that stores a database of uniform resource locators (URLs) and their corresponding IP addresses.

Hypertext mark-up language (HTML)

- A mark-up language used to create the structure & presentation of websites
- Written in plain text
- Used in the content layer
- It is made up of a set of mark-up codes
- It uses mark-up tags to define structure & presentation, eg. colour/size/font
- It is rendered by the web browser to display the contents of a web page.

Structure & Presentation

- Websites are separated into structure and presentation.
- Structure & presentation dictate the appearance of a website.
- They are defined using mark-up tags.
- On an HTML document, structure & presentation are kept separate from each other.
- Presentation is stored in a file called CSS.

HTML structure: Refers to the layout of the web page
Examples: position/placement of text/images/objects on the page // alignment, margins, line break, padding, borders (position/size), head, body, table, heading, subheading, paragraph

HTML presentation: Refers to the formatting of the web page
Examples: background colour, font colour, font size, font style, image size, border (style)

Why structure & presentation are kept separate

- Formatting of webpage can be changed, without altering structure
- ... This allows regular updates to be made to the design of websites
- The CSS file can be used to make a template for presentation/formatting
- ... This allows formatting to be easily applied as new content/web pages are added
- The CSS file can be reused again for several websites
- ... This allows the file to be created only once, but used several times
- ... This saves time during development of websites
- One person can develop the structure and one can develop the presentation
- ... This saves time when developing and updating a website

CSS

- A language used to create the presentation / formatting of the page
- Written in plain text
- Used in the presentation layer

- Used by websites to produce a consistent format between different web pages.

Cookies

- Small text files
- Stored by the web browser
- Contains data about a user's browsing habits/details/preferences
- Sent between a web browser and a web server when user visits the website

Functions of cookies

a. Saving personal details
    - to personalise user experience.
    - eg. name, email address, payment details

b. Storing login details
    - so user does not have to remember/enter them time they visit site
    - eg. usernames, passwords

c. Tracking user preferences
    - to tailor/ customise web page to user's presentation requirements
    - so user does not have to select preferences each time they visit the site
    - eg. language settings, font size, colour scheme

d. Holding items in an online/virtual shopping basket
    - so when user leaves the site items are still in their basket

e. Stores recent purchases
    - to allow the user to quickly reorder more items

f. Stores recently visited pages
    - to tailor adverts to a user / targeted advertising

How cookies can be used to store and automatically enter a user's payment details

- Web Server sends (cookie) file to user's browser
- User's payment details stored in encrypted text file // data is encrypted to be stored
- Cookie file is stored by browser/on user's HDD/SSD
- When user revisits website, webserver requests cookie file // webserver can access the data stored in the cookie file (to automatically enter details)
- ... and browser sends cookie file back to webserver (to automatically enter the details)

Why a user may be concerned about their personal data and online browsing habits being stored in cookies.

- User does not see what information is stored // might collect data that the user does not know about ...
- ... so, user may feel their privacy is affected
- A profile could be built about the user ...

- … that could expose a user's identity // lead to identity theft
- Sensitive information stored in cookies could be intercepted in transmission …
- Other websites could gain access to the cookies stored on a user's computer …
- Computer could be hacked to obtain data stored in cookies …
- … so, payment information could be stolen and used by a third party

Session cookie	**Persistent cookie**
Is lost when the browser is closed	It is not lost until it is deleted by the user/ until it expires
Is stored on the RAM	Is stored on the hard drive

Digital currency

- Currency that only exists in electronic form.
- Not backed by any physical commodity or government.
- Examples: Bitcoin, Litecoin, Ripple

Features of digital currency

a. <u>Only Exists Electronically</u>
    - do not exist in physical form like traditional currencies such as cash or coins.
    - are stored in digital wallets/ accounts.
    - can be transferred electronically between individuals or businesses.

b. <u>Decentralised</u>
    - not controlled by any central authority like a government/ financial institution.
    - transactions are verified and recorded on a public ledger called blockchain.

c. <u>Used for Transactions</u>
    - purchasing goods & services online
    - transferring money internationally
    - as investments // a store of value

d. <u>Volatile</u>
    - their value can fluctuate rapidly over short periods of time
    - so they are risky investments; difficult to use them as a stable store of value

Features

- Only exists electronically
- – Can be a decentralised system
- – Can be a centralised system
- – Usually encrypted

Blockchain

- It acts as a digital ledger
- … by tracking each transaction
- It consists of a time-stamped series of records
- … that cannot be altered
- Decentralised technology
- … not controlled by a single entity or authority
- … every participant in the network has a copy of the ledger and can verify the transactions independently

Process

- Made up of "blocks" of transactions linked together in a "chain" using cryptographic algorithms.
- This creates a secure, unalterable record of every transaction.
- Each transaction in blockchain must be verified by multiple participants in the network.
- Verification process ensures that transaction is legitimate & prevents fraudulent activity.

Cyber security threats

1. brute-force attack
2. data interception
3. distributed denial of service (DDoS) attack
4. hacking
5. malware (virus, worm, Trojan horse, spyware, adware, ransomware)
6. pharming
7. phishing
8. social engineering

Threat	Process	Aim	Prevention
<u>Brute-force attack</u>	- Trial-and-error method to guess passwords/ encryption keys - Combinations repeatedly tried/ entered - Until correct one found - Can be carried out manually/ automatically by software	- Install malware onto company network - Steal//access data - Delete data - Change data - Lock account// Encrypt data - Damage reputation of business	- Strong password - Biometrics - Two-step verification - Request partial entry of password - Set limit for login attempts - Drop-down box - Firewall // Proxy-server

Data interception	- eavesdropping on communication channels - to intercept/steal sensitive information (passwords/ credit card numbers/ personal data) - Data is being sent from one device to another - The data is being examined during transmission - Packet sniffer is used - Intercepted data is reported to a third-party during transmission ... - ... and analysed for anything useful - Connection hacked to spoof destination address	- to steal sensitive information for personal gain - to use it for further cyber attack	- Encryption: if data is intercepted it will be meaningless (because they don't have encryption key)
DDoS	- Attacker encourages people to download malware onto computer - Malware downloaded to several computers - Turns each computer into a bot - Creates a network of bots: botnet - Third party/hacker initiates attack - Bots flood web server with many requests sent at same time - The server cannot respond to all requests - Server crashes/times out - Legitimate requests cannot reach server - Users can no longer access websites	- Revenge - To affect company's reputation - Entertainment value - To demand ransom to stop it - To test system's resilience - Disrupt operation of server/ network - Deny users access to website	- Proxy server - Firewall - Scan computer w/ anti-malware
Hacking	- gaining unauthorised	- delete/steal/change/	- Firewall

	access to system/ network - Without user’s permission	manipulate data - disrupt services - personal gain - activism/ cyber espionage	- Passwords - Biometrics - Two-step verification - Encryption
Malware/ Malicious software	- replicates itself and fills the hard disk	- damage computer system/stored data - gain unauthorised access to system	
Phishing	- Legitimate looking email sent to user - Encourages user to click link/attachment that directs to fake website - User encouraged to enter personal details into a fake website	to obtain personal details from user - to steal sensitive information for personal gain - to use it for further cyber attack	- Check tone & spelling of email/website - Check URL attached to link - Don’t provide personal details online - Firewall
Pharming	- Malware downloaded without user knowledge - Redirects user to fake website - User encouraged to enter personal details into a fake website	to obtain personal details from user - to steal sensitive information for personal gain - to use it for further cyber attack	(phishing) + - Scan downloads w/ anti-malware - Only download software from trusted sources
Social engineering	- Manipulating/deceiving people - to obtain data // to force them to make an error	- to exploit human behaviour & vulnerability - gain unauthorised access to system	

Malware

How malware can be introduced to a company’s network

- A hacker could have hacked the network
- « and downloaded the malware onto the network
- Clicking a link/attachment/downloaded a file from an email/on a webpage
- « the malware could have been embedded into the link/attachment/file
- Opening an infected software package
- « this would trigger the malware to download onto the network
- Inserting an infected portable storage device
- « when the drive is accessed the malware is downloaded to the network

- Firewall has been turned off
- « so malware would not be detected/checked for when entering network
- Anti-malware has been turned off
- « so malware is not detected/checked for when files are downloaded

malware	description	prevention
Virus	- software/code that replicates itself - when the user runs it // with an active host - deletes/damages/corrupts data/files - takes up storage/memory space	- Anti-virus software - Do not download software or data from unknown sources - Firewall
Worm	- Software/code that replicates itself - without user input // without active host - Deletes/damages/corrupts data/files // takes up storage/memory space - Takes-up bandwidth - Opens back doors to computers over the network - Used to deposit other malware on networked computers	
Trojan horse	- Software/code that is hidden within other software // Software that is disguised as authentic software - when downloaded/installed the other malware it contains is installed	
Spyware	- Spyware installed/downloaded on user computer - Records key presses/ screen activity - And relays it to 3rd party	- Anti-spyware - Use data entry methods such as drop-down boxes to minimise risk
Adware	- Software/code that displays (unwanted) adverts on user's computer - Some may contain spyware/other malware - Some may link to viruses when clicked - Reduces device performance // reduces internet speed - Redirects internet searches/user to fake websites	
Ransom ware	- Software/code that stops a user accessing/using their computer/data - By encrypting the data/files/computer - A fee has to be paid to decrypt the data // A fee has to be paid to 'release' the	

	computer/device/data	

What could happen when a virus is downloaded

- It could cause the computer to crash / run slow / generate errors
- It could delete/ damage files
- It could fill up the storage space
- It could stop the hardware being able to communicate
- It could spread to other devices on the network

Prevention of viruses

- Anti-virus software // Anti-malware software
- Run an up-to-date virus scanner
- Use a firewall
- Use a proxy server
- Do not use / download software or files from unknown sources
- Do not open / attachments / links / emails from unknown sources
- Do not share external storage devices / USB pens
- Do not connect computer to network / use as stand-alone computer

How spyware can be used to find out someone's username and password

- Example of spyware e.g. Keylogger is used
- The user sent an email with an attachment/link containing spyware // user could clicks link on an untrusted website.
- Spyware is downloaded without knowledge
- Spyware records all key presses/screen clicks/screen activity
- Recorded data is sent back to the creator of the spyware/back to the third party
- Data is analysed
- Patterns in data reveal log-in details, so password or username can be identified.

Prevention of spyware

- Anti-spyware software / Anti-malware software
- Two-step verification / Two-factor authentication
- Use a biometric device: biological data (e.g. fingerprint) is also required
- Drop-down boxes / on screen / virtual keyboard:
    - Keylogger cannot collect data/ key presses cannot be recorded
    - and relayed to third party
- Only requires part of the password: Hacker doesn’t get the full password
- Firewall / proxy server

Phishing & Pharming

Similarities between phishing and pharming

- Purpose: designed to steal/obtain user's personal data/details
- They both pose as a real company/person
- Both use fake websites

Differences

phishing	pharming
involves use of email	involves installing malicious code on hard drive
involves clicking link/opening attachment	creates a redirection

Social engineering

- **Impersonation:** Posing as someone else (eg. IT technician/bank representative): to gain trust // access to sensitive information.
- **Baiting:** enticing victim with a desirable item to gain access to sensitive information. Attackers might leave USB drive with tempting labels like 'salary information' in a public place, and wait for someone to pick it up and plug into a computer.
- **Pretexting:** creating fake scenario to extract sensitive information

Accidental Damage

Example	Prevention
Power failure/ power surge	Use a UPS
Liquids being spilt	Don't have water near the device
Flooding	Keep device in a waterproof box when not in use
Fire	- Use electric items safely - keep device in a fireproof box when not in use.
Hardware failure	Correct care & maintenance of hardware
Software failure /crashing	Making sure software is always up to date
Human error - Accidentally deleting file/data	- Create backups: so data can be recovered - Add verification for data deletion: user can confirm they want to delete data - Set access levels: to limit who can delete data

- Shutting down computer before saving data	- Ensure that all data is saved before shutting down the computer.
- Incorrect use of storage device	- Making sure device is ejected before removing

Cyber security solutions

1. access levels
2. authentication (username & password, biometrics, two-step verification)
3. anti-malware (anti-virus and anti-spyware)
4. automating software updates
5. checking the spelling and tone of communications
6. checking the URL attached to a link
7. privacy settings
8. firewalls
9. proxy-servers
10. secure socket layer (SSL) security protocol

Access levels	- Providing users with different permissions for the data - Limiting access to reading/ viewing data - Limiting access to editing/changing/deleting data - Normally linked to a username
Authentication	User proves who they are - Passwords - Two-step verification - Biometrics
Anti-malware	to prevent and remove malware - If any malware is found, it is quarantined to prevent the spread - The malware is then deleted <u>Anti-virus</u> - Scans computer system // documents/files/incoming data from internet (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 - Constantly runs in the background - Can run a scheduled scan <u>Anti-spyware</u> - Scans the computer for spyware

	- Removes/quarantines any spyware that is found - Can prevent spyware being downloaded - Prevents data from being relayed to 3rd party (creator of spyware)
Automating software updates	- Ensures that software systems are up-to-date with latest security systems - Important for OS and software frequently targeted by hackers. - Scans internet for updates to software - If updates found, they can install automatically / notify user to install.
communication	checking spelling and tone of communications - phishing
URLs	- checking the URL attached to a link - phishing - hackers use fake URLs to trick users into visiting fake websites
Privacy settings	- Used to control amount of personal information shared online - Users should regularly review privacy settings - Prevents identity theft/online fraud
SSL	- Security protocol used to encrypt data transmitted over the internet - Helps to prevent eavesdropping / interception
	- Makes data meaningless, so not understood by hackers if stolen. - An encryption algorithm is used - « to scramble data - The original data is called the plain text - A key is used to encrypt the data - The key is applied to the plain text - Plain text is encrypted into ciphertext
Physical methods	Locked rooms, CCTV, bodyguards
Backups	- Making copy of files in case something happens to original - Multiple copies should be made - Should take regular backups - Should be stored in secure location
Firewalls & proxy servers	(see below)

Authentication

How to make a login system more secure, using passwords

- Make the password stronger
  - Make the password require more characters
  - Make the password require different types of characters

    - This makes the password harder to crack/guess
    - More possible combinations for the password
- Set number of password attempts (Lock out after set number of attempts)
- Ask for partial entry of password (Won't reveal entire password)
- Ask for password to be entered in random order (Won't reveal entire password)
- Drop-down boxes // on screen keyboard (prevents passwords obtained using keylogger)
- Change the password regularly

While entering a password, why does a system ask for 4 characters chosen at random?

- hacker never finds all characters on the first hack
- makes it more difficult for hackers to find the order of the characters
- hacker needs to hack the system several times to gain the whole password
- shoulder surfing will not give person full password

Why it's more secure to use drop-down boxes rather than entering characters using a keyboard

- to protect against keylogging software/spyware
- can stop key presses being recorded
- can stop key presses being relayed
- drop down boxes can be placed in different location on the screen each time (to overcome screen capture issues)

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

Biometric password

Uses biological data // characteristics/features that belong to a human

Examples:

- fingerprint scanner
- face recognition software
- retina scanner/iris scanner
- voice recognition software

<u>Advantages</u>

- Data needed to enter is unique to individual
- … therefore it is very difficult to replicate/ fake
- A biometric password cannot be guessed

- A biometric password cannot be recorded by a keylogger/spyware
- A perpetrator cannot shoulder surf to see a biometric password

Difference between text-based & biometric passwords

Text based password

- a minimum number of characters that can be typed on a keyboard
- can be changed by the user

Biometric password

- a stored physical measurement e.g. fingerprint
- that is compared to a previously scanned human measurement

Difference

- text based passwords are easier to hack than biometric passwords
- biometric passwords are unique to that person/cannot be shared

Firewalls & Proxy servers

Firewalls

- User sets criteria for the traffic (websites can be blacklisted/whitelisted)
- Examines outgoing traffic to check what is being requested.
- Examines incoming traffic to check the content of what is being received.
- Traffic is compared to set criteria/whitelist/blacklist
- If the traffic/data does/does not meet the criteria/rules/whitelist/blacklist it will be rejected/blocked…
- … and an alert can be sent to warn user
- Keeps a log of all attempts to access blocked websites
- Can prevent unauthorised access, hacking, malicious software

NOTE: Firewalls CANNOT automatically stop all malicious traffic // Firewalls CANNOT encrypt all data that is transmitted around a network // Firewalls CANNOT act as intermediary servers.

Proxy servers

a. Act as intermediary between browser & web server / prevents direct access to server
    - to monitors traffic to the server
    - to help stop malicious traffic to the web server

b. Helps to prevent DoS
    - monitors incoming traffic to server
    - limits number of requests // prevents web server being overloaded with requests
    - can block multiple requests from the same IP within a timeframe
    - Redirects attack away from server // if attack is launched it hits proxy server instead of web server

c. Acts as a firewall
   - Filters web traffic: Monitor/examines incoming and outgoing traffic
   - Rules/criteria for traffic can be set; blacklist/whitelist
   - Blocks any traffic that does not meet criteria ...
   - ... and can send a warning message to the user

d. To cache frequently viewed web pages
   - to allow faster response time for requests
   - to reduce the number of requests the server needs to process

Similarities between proxy servers & firewalls

- Check incoming and outgoing signals // filter traffic
- Store whitelist/blacklist
- Block incoming/outgoing signals
- Both block unauthorised access
- Keep a log of traffic
- Both can be hardware or software

Differences

Proxy server	**Firewall**
Aim is to divert attack from server	Aim is to stop unauthorised access
Protects server	Protects individual computer
Can hide user's IP address	Does not hide user's IP address
Allows faster access to web page using cache	Does not allow faster access// does not have a cache

Online security attacks that can be carried out using email

- Phishing
  - Email is sent to user to encourage them to click link
  - ... that takes user to fake website
- Pharming
  - Email is sent to user to encourage them to click link/download attachment
  - ... that triggers download of malicious code that will redirect user to fake website
- Virus/malware
  - Email is sent to user to encourage them to click link/download attachment
  - ... that triggers download of virus/malware
- Denial of service // DoS
  - A very large number of emails are sent to a server/network at the same time
  - ... crashing the server/network

Ways that stored data can be maliciously damaged

- Hacking
- Virus
- Malware

Identify and describe security measures that could be used to make sure that a file can be opened only after a specific time

- Password protection: Password is released on the release date
- Encryption: Encryption key is released on the release date

Methods to prevent loss of stored data

- <u>Backups</u>
    - Make a copy of the data
    - Copy stored away from main computer
    - If data is lost, it can be restored from backup
- <u>Install antivirus // Anti malware:</u> detects/deletes virus that could corrupt/delete data
- <u>Install firewall:</u> helps prevent hackers gaining access and deleting/corrupting data
- <u>Password / Biometrics</u>
- <u>Two factor authentication // two-step verification:</u> helps prevent unauthorised access and the deletion/corruption of data
- <u>Access rights:</u> helps prevent users accessing data they should not see and deleting it
- <u>Network/usage policy:</u> gives users guidance on data use // by example
- <u>Surge protection // Uninterrupted power supply (UPS):</u>
    - prevents loss of data that has not been saved
    - prevents damage to hardware (that stores data)
- <u>Physical method:</u>
    - Keep data in a fireproof / waterproof / protective case
    - Helps prevent unauthorised access and deletion/corruption of data
- <u>Use verification methods (for deleting files)</u>
- <u>Follow correct procedure</u> e.g. ejecting offline devices / regularly saving

Methods that could be used to steal bank details electronically

- Phishing
- Pharming
- Hacking
- Spyware

Internet service provider (ISP)

A company that provides a connection to access the Internet.

Role of ISP

- Provide access to the internet / dial up / broadband
- Determines maximum bandwidth available for users
- Monitors the volume of data downloaded by customers; monitors usage
- Provides IP address for the user
- Supports domain names
- Provide security services
- Provide web hosting facilities
- Provide access to Email / Mailbox
- Provides online data storage
- Usually charges a monthly fee