**Biometrics**

* The use of**unique physical** or **behavioural characteristics**of **individuals**, such as **fingerprints**, **facial recognition**, or**iris scans**, for authentication and access control
* Biometric data provides a**more secure method** of **identification**as it is **difficult to forge or replicate**

**Advantages and disadvantages of Biometrics**

|  |  |
| --- | --- |
| **ADVANTAGES** | **DISADVANTAGES** |
| * Harder to crack * Easier to use for individual * High accuracy | * Skin damage can stop identification * Facial features can change over time * Some biometrics are more expensive to set up than others * Voice recognition can be affected by illness |

**Digital certificate**

* An **electronic document** that **verifies**the **authenticity**and **integrity**of a **website**
* The purpose of a digital certificate is to **establish trust**between **parties**and **ensure secure communication**
* Contents of a digital certificate typically **include the entity's public key,** **identification information**, and the **digital signature of a trusted third party**

**Secure Socket Layer (SSL)**

* A **protocol**that establishes an **encrypted link**between a **server**and a **client computer**
* SSL ensures that**data transmitted**between the server and client **remain confidential** and **cannot be intercepted or adjusted**by unauthorised individuals
* Identified on a website by the **S** at the end of**HTTP**

**Encryption**

* The process of **converting data** into a **form that is unreadable** without a **decryption keys**
* Encryption is used to **protect data on hard disks,** **email communications, cloud storage**, and **secure websites** (HTTPS)
* It ensures that even **if data is accessed** by **unauthorised individuals**, it **cannot be understood** without a **decryption key**

**Firewall**

* A **network security device** that **monitors**and **controls incoming**and **outgoing network traffic**
* The purpose of a firewall is to **create a barrier between an internal network** and **external networks**, **filtering**traffic based on**predefined rules**
* It helps **prevent unauthorised access**, **malware**, and **other network threats**

**Advantages and disadvantages of Firewalls**

|  |  |
| --- | --- |
| **ADVANTAGES** | **DISADVANTAGES** |
| * Stops attacks from device * Stops fraudulent sites attacking the device | * Can affect the operation of the computer and some uploads * To upload some files, the firewall may need to be switched off, leaving the computer open to attacks * Can stop legitimate software from running |

**Two-factor authentication (2FA)**

* A security measure that **requires users to provide two separate forms** of **identification**to **verify their identity**
* The purpose of 2FA is to **add an extra layer** of security beyond just a username and password
* It usually involves a combination of something the**user knows (password),**something the**user has (smartphone or token)**, or something the **user is (biometric data)**

**User ID and password**

* A common method of authentication that involves a **unique identifier (user ID)** and a **secret code (password)**
* User ID and password are used to increase the security of data by allowing access only to **authorised individuals**
* **Strong passwords**and**regular password changes**are important to maintain security
* It is recommended to use a **combination of uppercase**and **lowercase letters**, **numbers**, and **special characters**in passwords

**Advantages and disadvantages of Passwords**

|  |  |
| --- | --- |
| **ADVANTAGES** | **DISADVANTAGES** |
| * Strong passwords are difficult to crack * Regularly changing passwords increases the security * Using a range of passwords over the system will stop or slow access to the full system | * Passwords too complex can be harder to remember * Too many passwords are hard to remember * Harder to choose unique passwords if regularly updating * Harder to remember if regularly updating * Hackers can break most passwords |