‘Your data is your digital footprint. Protect it as you would your own identity’

This section covers

- Hacking
- Phishing
- Smishing
- Vishing
- Pharming
- Spyware
- Viruses
- Spam
- Cookies

Let’s talk about Hacking!

HACKING

Description

This is the act of gaining unauthorized access to a computer system, network or data.

(white, black and gray-hat hacking)

Possible Effect

Can lead to identity theft or the misuse of personal information.

Data can be deleted, changed or corrupted on a user's computer

Methods to help

- Use Firewalls
- Enable 2Factor Authentication
- Update Software
- Secure your Wifi network
- Limit Personal Information Online

Let’s talk about Phishing!

PHISHING

Description

A cyber attack where scammers trick people into revealing sensitive information, like passwords or credit card details, by pretending to be a trustworthy entity. This is usually done through fake emails, messages, or websites.

Example of their trick

You receive an email that looks like it's from your bank, saying, "Your account has been compromised. Click the link below to verify your information." The link directs you to a fake website that looks identical to your bank's login page. If you enter your details, the hacker captures your username and password.

Methods to help

Use strong, unique passwords, enable multi-factor authentication, verify email sources, avoid clicking unknown links, and educate users on phishing risks.

SMISHING

Description

Short for SMS phishing that uses the SMS system of mobile phones to send out fake text messages.

Example of their trick

You receive a text message claiming to be from your bank: "Dear customer, your account has been locked due to suspicious activity. Click this link [fakebank-site.com] to verify your identity and restore access immediately."

Methods to help

Prevent smishing by not clicking unknown links, verifying message sources, using security software, and educating users about smishing risks.

VISHING

Description

it is a voicemail phishing, another variation of phishing. Use voicemail message to trick the user into calling the telephone number.

Example of their trick

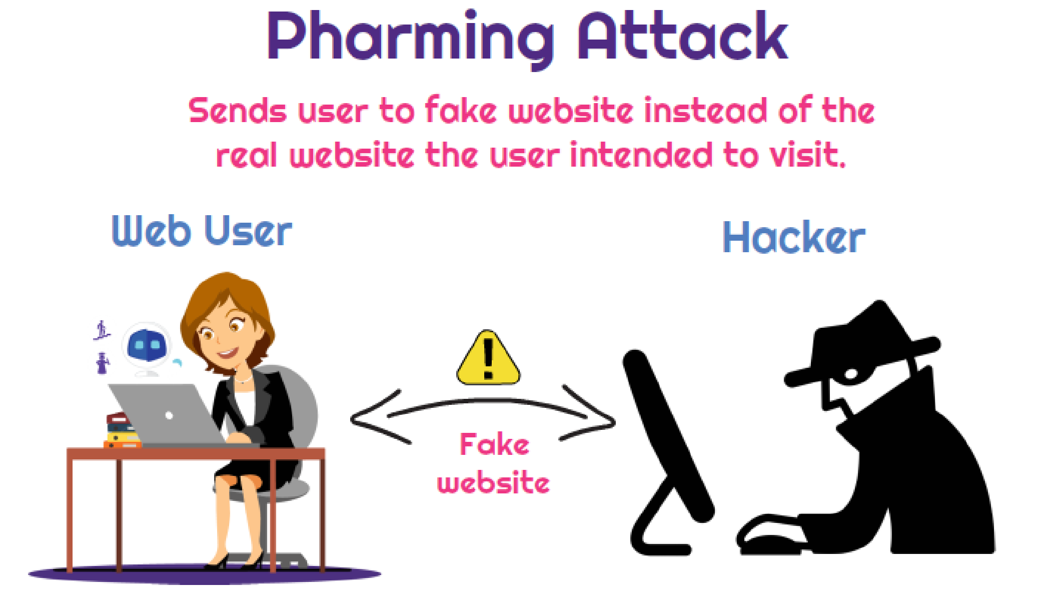
You receive a phone call from someone claiming to be from your bank's fraud department:

Caller: "Hello, this is John from World Bank. We detected unauthorized transactions on your account. To secure your funds, we need to verify your identity. Can you confirm your account number and PIN?"

Methods to help

Prevent vishing by not clicking unknown links, verifying message sources, using security software, and educating users about smishing risks.

Let's talk about Pharming!



Pharming Attack

Sends user to fake website instead of the real website the user intended to visit.

PHARMING

Description

is a cyber attack where hackers redirect users from legitimate websites to fake ones without their knowledge. This is done by altering DNS settings or infecting a user's device with malware. The goal is to steal sensitive information like login credentials or financial details.

Example of their trick

You type "www.yourbank.com" in your browser, expecting to visit your bank's official website. However, due to a hacker's attack, you are secretly redirected to a fake website that looks identical to the real one. If you enter your login details, the hacker captures them and gains access to your bank account.

Methods to help

secure DNS, keeping software updated, employing anti-malware tools, educating users, and monitoring network traffic.

Let’s talk about SPYWARE!

SPYWARE

Description

It is a type of malicious software that secretly installs on a device to monitor user activities, collect personal information, and send it to hackers without the user's knowledge. It can track keystrokes, steal passwords, and record browsing habits.

Example of their trick

You download a free game from an untrusted website. Without your knowledge, the game installs spyware on your device. The spyware tracks everything you type, including your email and banking passwords, and sends this information to hackers, who can then use it to steal your identity or money.

Methods to help

- use anti-spyware to reduce the risk
- the user should always be alert and check for clues that their keyboard activity is being monitored

Let’s talk about VIRUS!

VIRUS

Description

It is a type of malicious software that spreads by attaching itself to files or programs. When executed, it can replicate itself, damage files, slow down systems, or even crash a device.

Example of their trick

You receive an email with an attachment labeled "Invoice.pdf" from an unknown sender. When you open the file, a hidden virus installs itself on your computer. It starts corrupting your files and spreading to other documents, making your system slow and unresponsive.

Methods to help

- install anti-virus software and update it regularly
- don’t use software from unknown sources
- be careful when opening emails or attachments

Let’s talk about SPAM!

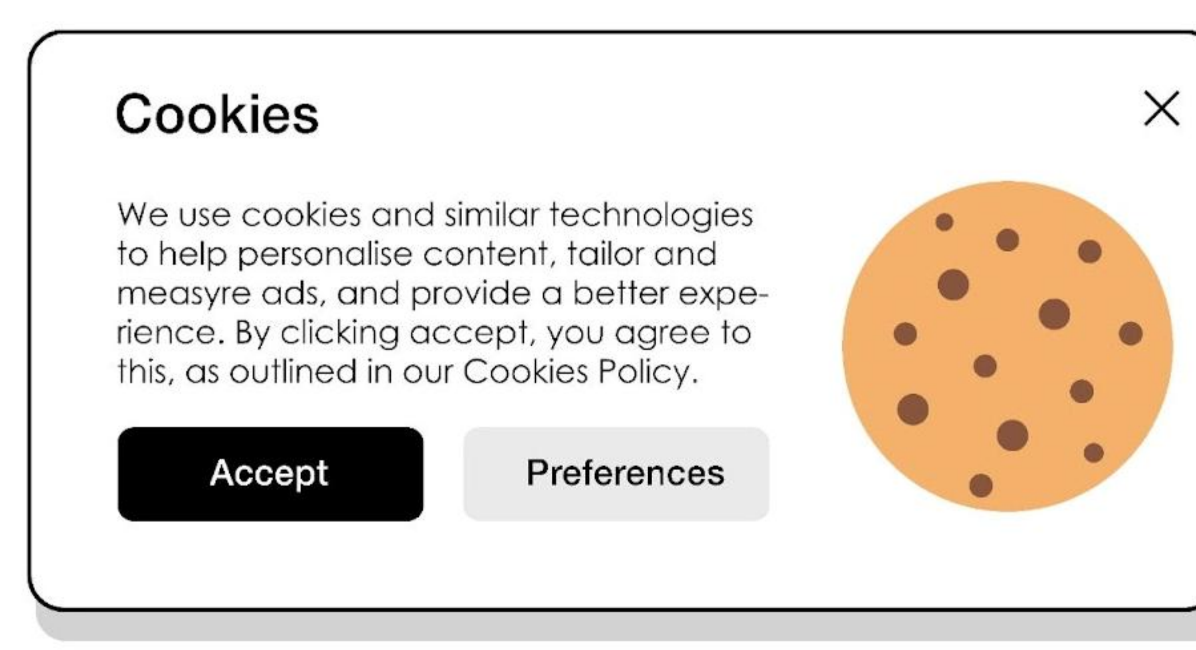
SPAM

Unwanted, irrelevant, or unsolicited emails sent in bulk, often for advertising, phishing, or spreading malware. These emails usually try to trick users into clicking harmful links or buying fake products.

You receive an email with the subject **"Congratulations! You won $1,000,000!"** from an unknown sender. The email asks you to click a link and provide your personal details to claim the prize. If you do, scammers might steal your information or install malware on your device.

COOKIES

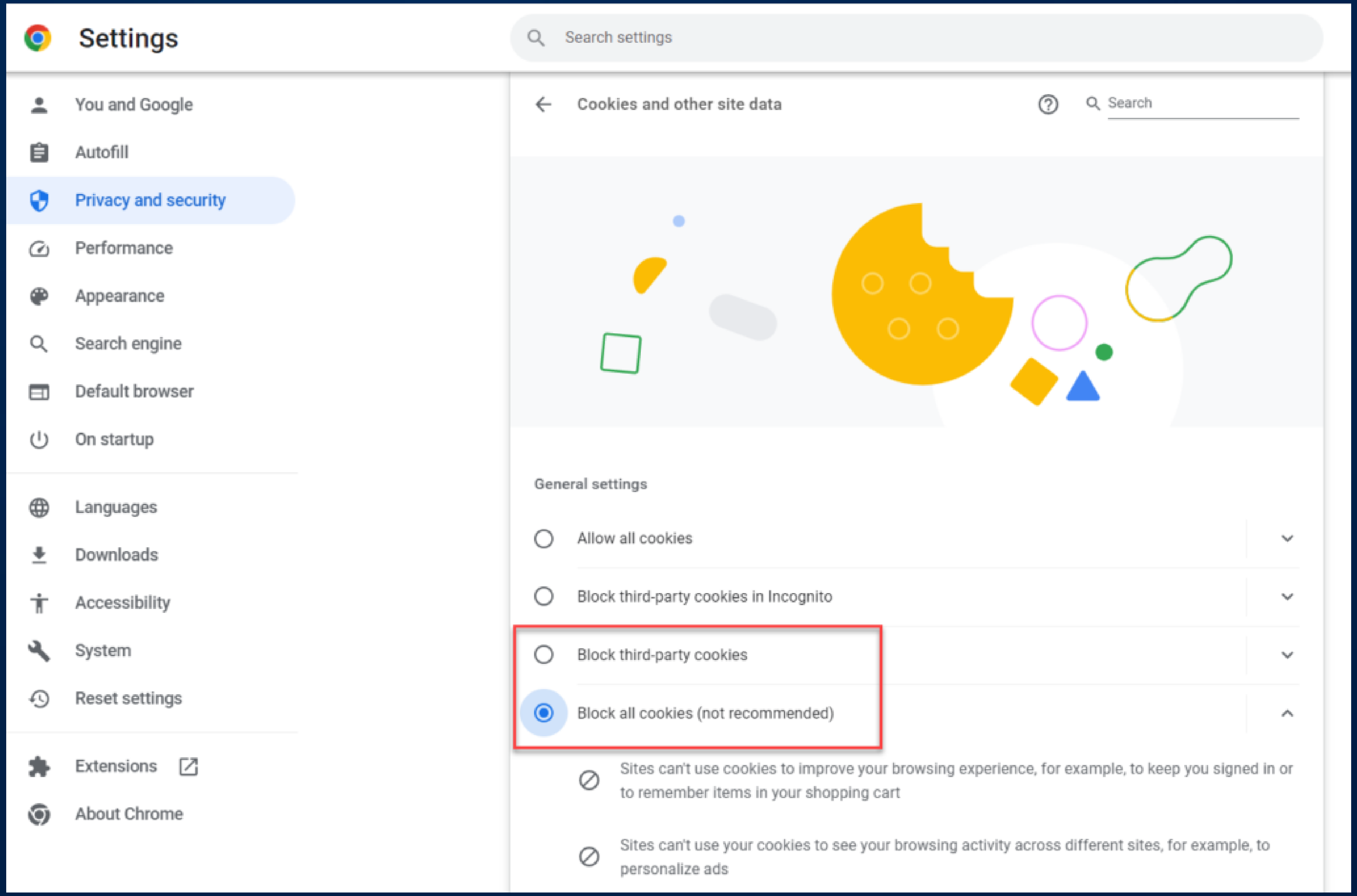
Are small **text files** stored on your device by websites you visit. They help websites remember your preferences, login details, and browsing activity to improve your online experience. However, some cookies can also track your behavior for targeted ads or marketing.



Cookies

We use cookies and similar technologies to help personalise content, tailor and measyre ads, and provide a better experience. By clicking accept, you agree to this, as outlined in our Cookies Policy.

Are cookies safe?



General settings

○ Allow all cookies

○ Block third-party cookies in Incognito

○ Block third-party cookies

● Block all cookies (not recommended)

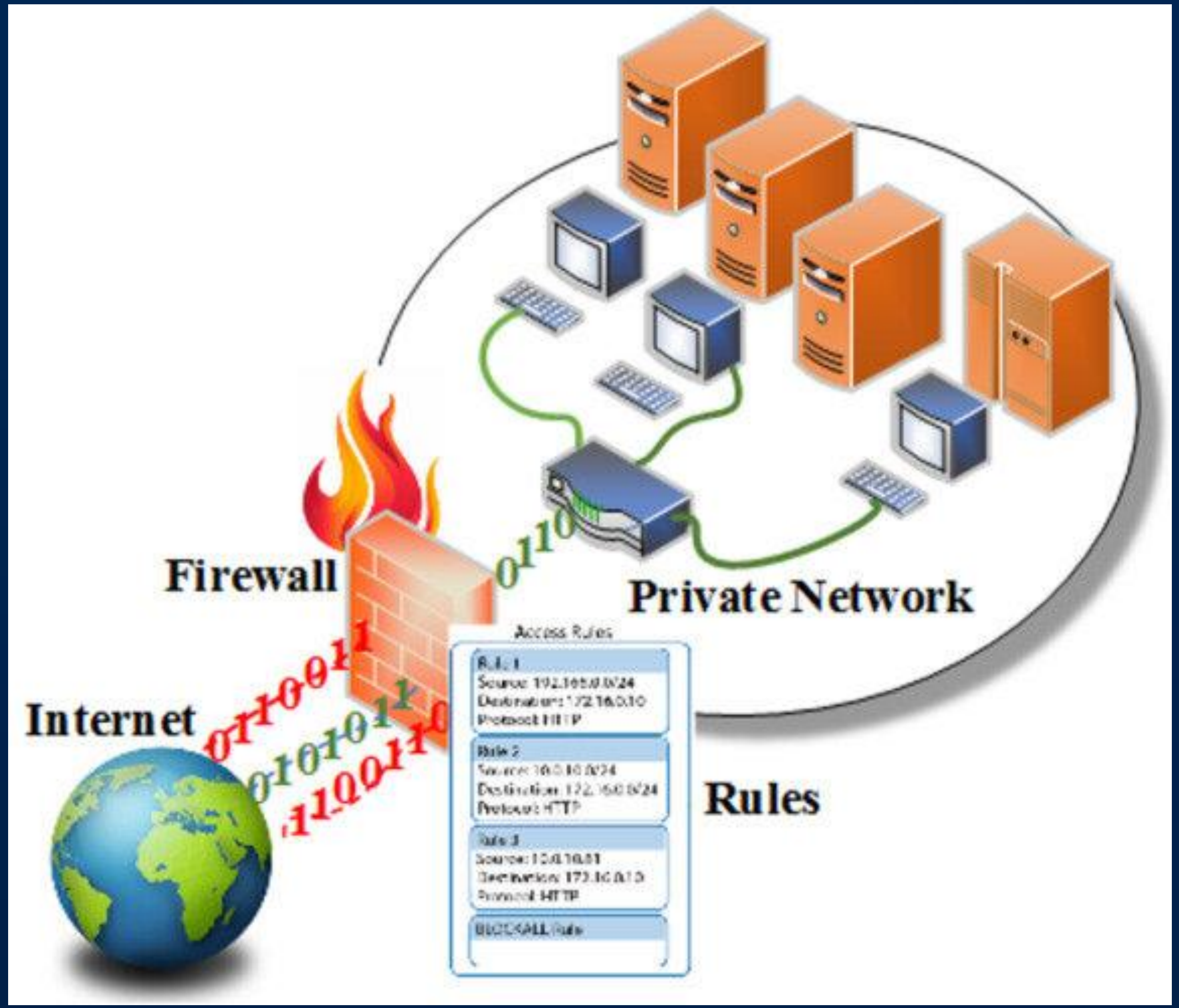
Sites can't use cookies to improve your browsing experience, for example, to keep you signed in or to remember items in your shopping cart

Sites can't use your cookies to see your browsing activity across different sites, for example, to personalize ads

Cookies are generally safe when used by legitimate websites for improving user experience, like remembering login details, language preferences, or items in a shopping cart. However, some cookies can track your browsing activity for advertising purposes, and third-party cookies can raise privacy concerns.

Additional security of data online

- Firewall
- Security Protocols
- Encryption
- Authentication



Firewall

It can either be a software or a hardware. It sits between the user's computer and an external network.

Security Protocol

It is a security protocol refers to a set of rules and procedures designed to ensure secure communication and data exchange over computer networks.

Two Forms of Security Protocols

SSL (Secure Socket Layer)

A type of protocol that allows data to be sent and received securely over the internet.

TLS (Transport Layer Security)

Similar to SSL but is more recent security system. Its more upgraded than SSL.

ENCRYPTION

Uses a secret key that has the capability of altering the characters in a message. If this key is applied to a message, its content is change, which then makes it unreadable unless the recipient also has the same secret key.

Examples

Encryption:

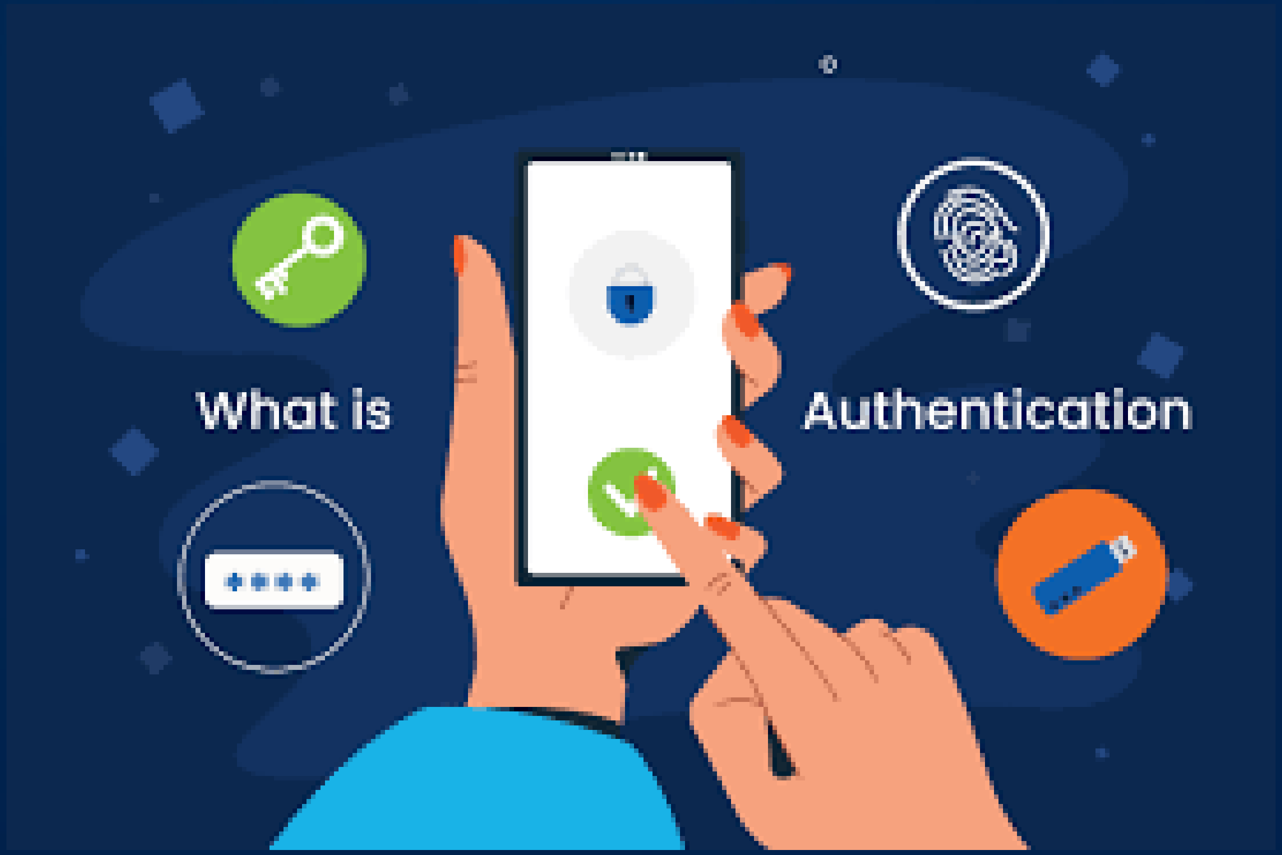
Similar to how the secret code determines how the message is scrambled, an encryption key defines the rules for encrypting and decrypting data.

Scrambling message:

Encryption transforms readable data into unreadable ciphertext, ensuring confidentiality and privacy.

Security:

Just as the secret code protects your message from being understood by unauthorized parties, encryption protects sensitive information from being accessed by unauthorized users.



Used to verify that the data comes from a secure and trusted source. It works with encryption to strengthen internet security.

AUTHENTICATION

Examples

Password Based Login:

When you access your email account, you enter username and password. The system verifies your credentials against stored data to grant or deny access.

Biometrics

Relies on certain unique characteristics of human beings.

Types of Biometrics

- Fingerprint scans
- Signature recognition
- Retina scan
- Iris recognition
- Face recognition
- Voice recognition

Advantages and Disadvantages of Biometric Techniques

Biometric Technique	Advantages	Disadvantages
Fingerprint scan	• Most developed biometric technique • Very high accuracy • Very easy to use • Relatively small storage requirements for the data created	• For some people it is very intrusive, since it is still related to criminal identification • It can make mistakes if the skin is damaged (eg., cuts)
Signature recognition	• Non intrusive • Requires very little time to verify (about 5 seconds) • Low cost technology	• If individual did not sign their names in a consistent manner, there may be problems with signature verification • High error rate
Retina scans	• Very high accuracy • There is no known way to replicate a person's retina	• It is very intrusive • It can be relatively slow to verify retina scan with stored scan • Very expensive to install and setup
Iris recognition	• Very high accuracy • Verification time is generally less than five seconds	• It is very intrusive • Uses a lot of memory for the data to stored • Very expensive to install and setup
Face recognition	• Non-intrusive method • Relatively inexpensive technology	• It affected by changes in lighting, the persons hair, their age, and the person if wearing glasses
Voice recognition	• Non-intrusive method • Verification takes less than five seconds • Relatively in expensive technology	• A person's voice can be recorded easily and used for unauthorized access • Low accuracy

Cloud Security

- it refers to a set of policies, technologies, controls, and practices designed to protect data, applications, and infrastructure associated with cloud computing services.

Examples

Building your own Library

- You set up and maintain your own servers, storage, and networking equipment.
- Full control over your infrastructure and data.
- High costs, requires significant management effort, and scalability is limited to your own resources.

Using the Public Library (Cloud Computing)

- You use computing resources provided by a cloud service provider (like Google Cloud). The provider maintains the hardware and infrastructure, and you access these resources over the internet.
- Cost-effective, scalable, and you only pay for what you use. The provider handles maintenance, upgrades, and ensures high availability.

Thank You