01 Zero & One

Unit 3: Information Security

Programming & AI, 1st secondary (Introduction to ICT)



Engineer Rahim

3-1 Threats and Countermeasures in Information Security [1]

- **What is information security?**
  - **Confidentiality:** only authorized people can reach the information.
  - **Integrity:** the information has not been destroyed, tampered with or erased.
  - **Availability:** the information is there and can be reached whenever it is needed.
- **Which element was hit?**
  - A website goes down because of a cyberattack → **availability** is lost.
  - Wrong data is typed in or data is changed → **integrity** is lost.
  - Personal data leaks or a stranger sees it → **confidentiality** is lost.
- **Unauthorized access and cracking**: **Unauthorized access:** someone without permission gets into a computer system.
- **Malware**
  - **Computer virus:** deliberately destroys data or programs.
  - **Trojan horse:** disguised as a normal program
  - **Worm:** copies itself and spreads across the Internet on its own, so the infection grows.
  - **Spyware:** collects your personal data without your knowledge and sends it to a third party
  - **Ransomware:** locks your data and demands money (a ransom) to give it back.
- **Cybercrime**
  - **Violating the Unauthorized Computer Access Law:** logging in to a computer with someone else's user ID and password
  - **Crimes involving computers or electronic records:** tampering with stored data or manipulating devices without permission.
  - **Network-based crimes:** fraud, defamation or copyright infringement committed through a network.
- **Denial-of-service attacks (DoS and DDoS)**: **Denial of Service (DoS):** the attacker floods a server with a huge number of requests from **one device**, so it slows down or crashes and cannot serve real users

Information security	Managing information properly and keeping it safe.
Confidentiality	Only authorized people can access the information.
Integrity	The information has not been destroyed, tampered with or erased.
Availability	The information can be accessed whenever it is needed.
Cracking	Illegally entering a system to tamper with, erase or steal data.
Malware	A general term for malicious programs made to harm computers.
Trojan horse	A program disguised as a legitimate one that quietly starts attacks.
Worm	A program that copies itself and spreads across the Internet.
Spyware	A program that collects personal data without the user's knowledge and sends it to others.
Ransomware	A program that makes data inaccessible and demands a ransom.

DoS attack	Denial of service: flooding a server with requests from one device so it cannot serve real users.
DDoS attack	Distributed denial of service: flooding a server with requests from many devices at the same time.

3-2 Threats and Countermeasures in Information Security [2]

- **Password**
  - Make it as **long** as you can.
  - **Mix:** uppercase and lowercase letters, numbers and symbols.
  - Do not use personal information (your birthday, email address, user ID).
  - Do not reuse the same password on several services, and change the default password you were first given.
- **Calculate it: how many combinations?**: With **n** allowed characters and a password length of **k**, the number of combinations = **n^k**
- **Authentication and its types**
  - **Knowledge-based authentication:** something only you know
  - **Biometric authentication (Biometrics):** a feature of your body or behaviour
  - **Possession-based authentication:** something you have
- **Two-factor or two-step?**
  - **Two-factor authentication:** two factors of **two different types** (e.g
  - **Two-step authentication:** two steps using two pieces of information of **the same type** (e.g
  - **One-time password:** changes at regular intervals and works only once, so a leaked normal password is not enough to log in.
- **Information security measures**
  - **Access control:** only specific users, verified by authentication, may use the system or data.
  - **Firewall:** at the network entrance
  - **Against viruses:** install **antivirus software** and keep its definitions updated, **update** the OS and applications to close **security holes**, and make **backups** regularly.
- **The least-privilege principle**: Part of **access control**: each user gets only the **minimum permissions** needed to do their job, and nothing more

Password	A string of characters that proves the user is the real account holder.
One-time password	A password that changes regularly and can be used only once.
Authentication	Verifying the identity of a user on a computer or network.
Biometric authentication	Authentication by physical or behavioural features such as fingerprint or iris.
Possession-based authentication	Authentication by something the user has, such as an IC card or SMS code.
Two-factor authentication	Authentication that combines two factors of different types.
Two-step authentication	Authentication in two steps using two factors of the same type.
Access control	Limiting a system or data to specific, verified users.
Firewall	A system at the network entrance that blocks outside unauthorized access and inside data leaks.
Security hole	A weakness in software, closed by updating it.

Least privilege	The rule that each user gets only the minimum access needed to do their job.

3-3 Threats and Countermeasures in Information Security [3]

- **Billing fraud**
  - **Fraudulent billing:** you are sent a bill for a fake service you never used, so they can take your money.
  - **One-click fraud:** you click a link on a website or email, a message says you have "signed a contract" for a service, and then a large payment is demanded.
- **Phishing**: A **fake** website disguised as a bank or an official body, usually reached through an email or message, that aims to steal your data such as your **PIN** or account details
- **Social engineering**
  - **Impersonation:** someone calls pretending to be another person (an employee, a manager) to get information.
  - **Shoulder surfing:** looking over your shoulder at the screen or keyboard while you type your password or PIN.
  - **Dumpster diving:** searching the trash for confidential papers that were thrown away.
- **Skimming**: Illegally copying the data of someone's **credit or debit card** and using it to make a **counterfeit card**.
- **Information Security Policy**
  - **Basic policy:** the organization's main principles and declaration about information security.
  - **Security standards:** the rules that put the basic policy into practice.
  - **Implementation procedures and operational rules:** clear steps based on the target audience and purpose.
- **Acceptable Use Policy**
  - Do not give your account or password to anyone, and do not log in with someone else's account.
  - Do not post offensive or harmful content, and respect copyright.
  - Use the devices and network for the purpose they were made for (for example, studying).
  - You are **responsible** for what is done with your account

Fraudulent billing	A scam that bills someone for a fake service they never used.
One-click fraud	A scam where one click on a link claims a contract was made and demands payment.
Phishing	A scam using a fake site disguised as a bank or official body to steal personal data.
Social engineering	Getting information by exploiting human psychology or carelessness.
Impersonation	Pretending to be someone else to obtain information.
Shoulder surfing	Peeking at someone's screen or keyboard to steal passwords or PINs.
Dumpster diving	Searching the trash for discarded confidential information.
Skimming	Illegally copying card data to make a counterfeit card.
Information security policy	An organization's basic rules and guidelines for protecting its information.
Acceptable use policy	Rules that state what users may and may not do with an organization's devices, network and accounts.

3-4 Information Technology for Safety [1]

- **Encryption terms**
  - **Encryption:** changing a message when it is sent so that nobody except the intended recipient can understand it if it is intercepted.
  - **Plaintext:** the original message before encryption, and **ciphertext:** the message after encryption.
  - **Decryption:** turning the ciphertext back into plaintext.
  - **Key:** the procedure or data used to encrypt and decrypt.
- **Symmetric key encryption**: **The same key:**
- **Public key encryption**: Two keys: the **public key**, open to anyone, and the **private key**, kept only by its owner
- **Comparison**
  - **Symmetric:** faster encryption and decryption
  - **Public key:** key management is easier because the public key can be shared freely
- **Session key method**: It combines the two: **public key encryption** to deliver the shared key safely, then **symmetric encryption** to encrypt the data itself quickly

Encryption	Changing data so that only the intended recipient can understand it.
Plaintext	The original message before encryption.
Ciphertext	The message after encryption.
Decryption	Turning ciphertext back into plaintext.
Key	The procedure or data used for encryption and decryption.
Symmetric key encryption	Encryption that uses the same shared key to encrypt and decrypt.
Shared key	The single key held by both sides in symmetric encryption.
Public key encryption	Encryption with the recipient's public key and decryption with their private key.
Private key	The secret key kept only by its owner and used to decrypt.
Session key method	A method combining symmetric key and public key encryption.

3-5 Information Technology for Safety [2]

- **Hash function**
  - Same data + same function → **always the same value**.
  - Change one character → a **completely different** value (not just one character).
  - It is **not possible** to get the original data back from the hash value.
- **Digital signature**: A technology that uses **public key encryption + hash values** to prove that the data **really came from the sender** and **was not tampered with**
- **The steps in order**
  - **Sender 1:** makes the hash value of the plaintext with the hash function.
  - **Sender 2:** encrypts the hash value with the **sender's private key** → this is the **digital signature**.
  - **Sender 3:** sends the plaintext + the digital signature.
  - **Recipient 4:** decrypts the signature with the **sender's public key** and gets the original hash value.
  - **Recipient 5:** makes a new hash value from the received text with the same function.
  - **Recipient 6:** compares the two values: **if they match** → the message is from the sender and was not changed.

- **Certification authority (CA)**: A signature alone does not stop **impersonation**: someone could claim that a certain public key is theirs
- **SSL/TLS and https**: **SSL/TLS:** encrypts the communication between the **web server** and the **web browser** using the **session key method**, and an encrypted page's URL starts with `https://`

Hash function	A function that calculates a unique value from input data.
Hash value	The output of a hash function; the original data cannot be restored from it.
Digital signature	Proof, using public key encryption and hash values, of the sender and that data was not altered.
Certification authority (CA)	A trusted third party that issues digital certificates.
Digital certificate	A certificate holding a public key and its owner's identity.
SSL/TLS	A technology that encrypts communication between a web server and a browser.
HTTPS	The start of the URL of a page encrypted with SSL/TLS.



Study the whole course free

Every lesson, questions with answers, a ministry-style bank and a timed mock exam

zerooneacademy.com

Engineer Rahim