UNITED ARAB EMIRATES
MINISTRY OF EDUCATION

Networks and The Internet

Cycle 3 – Grade 11

Section 2 : Security practices for software developers

Aim

In this section, you will explore how software developers engage with computer networks and their pivotal role in software development. Given the vulnerability of networks to cyberattacks, developers use various methods to safeguard devices and information within systems. You will also learn about the security practices used by software developers to protect software against potential attacks and safeguard devices and information.

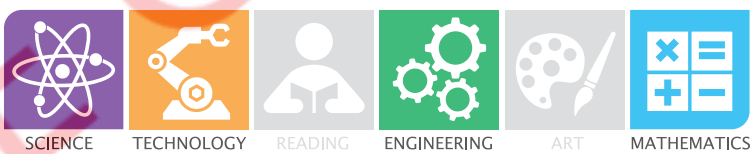
Learning outcomes

- Explain ways software developers protect devices and information from unauthorised access.

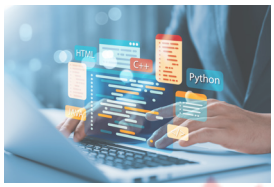
Prior knowledge

- Computer science terms
- Networking terminologies

My STREAM Focus

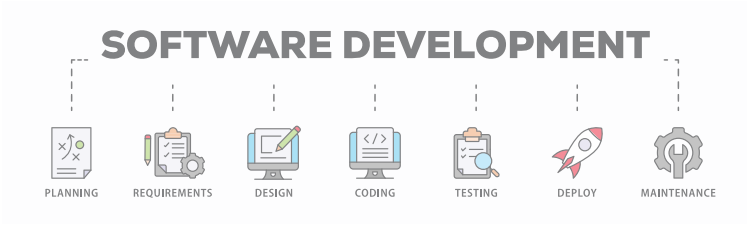


Key vocabulary

WORD	MEANING	PICTURE
software development	a process used by programmers to create and build computer programs	
software developers	people who use programming and design knowledge to design and create software that meets users' requirements	
software security	a practice followed by software developers to protect software applications, solutions and devices from attackers	

Software developers and computer networking

In a modern interconnected world, software developers play a vital role in creating applications that depend on network communication. To succeed in their field, software engineers must deeply understand computer networking, communication and network protocols.



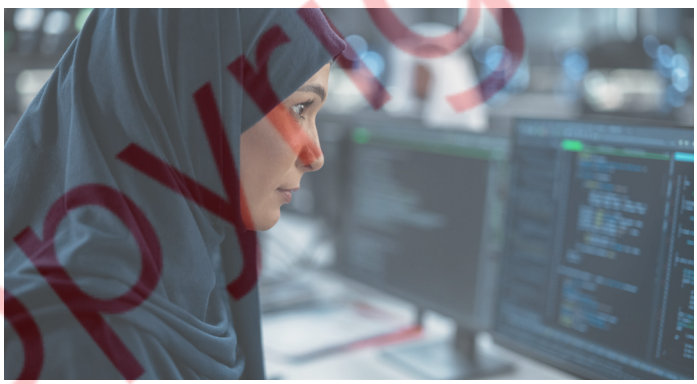


Figure 2.1.1: Software development

The role of a software developer is to build, create, or design software that meets users' needs. This involves completing various phases such as creating diagrams, prototyping and simulating models, writing code, and implementing computer programs and applications.

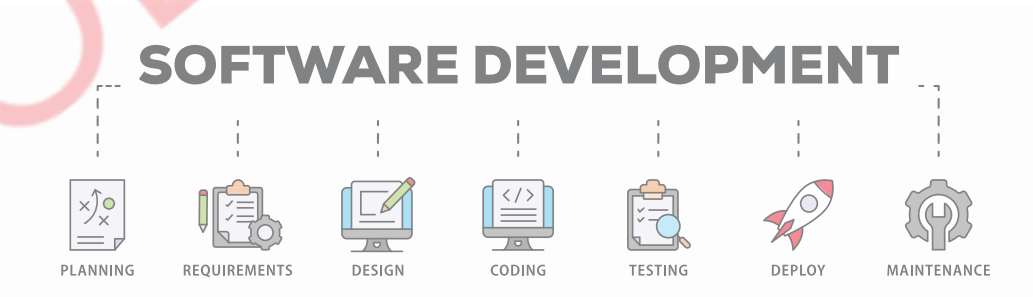


Figure 2.1.2: Software development stages

Two types of software developers are:
- application software developers who develop applications like web, desktop or mobile
- systems software developers who build enterprise solutions like banking or sales systems.

HB **Complete activity 2.2.1 in the workbook.**

Software Security

Today, most businesses depend on software programs to perform critical tasks. Software developers design various solutions to meet the needs of users and enterprise businesses. As digital solutions increase, software security threats are growing in strength and frequency. There has been an increase in cyberattacks involving viruses, malware, and other threats that can compromise sensitive data. Therefore, ensuring strong software security has become essential.

Figure 2.1.3: Software security

Every business must protect its digital solutions and business data from malicious attacks. To achieve this, software developers incorporate a set of practices during software development and testing that help safeguard software applications and digital solutions from cyberattacks. This is known as software security.

For example, a business can prevent attackers from stealing sensitive information such as passwords, credit card numbers, trade secrets, and customer information by implementing strong software security protocols in their digital solutions.

Do you know:

Figure 2.1.4: Software security Vs Cybersecurity

The terms "software security" and "cybersecurity" are two different concepts.

Software security protects software programs from malicious attacks, like viruses or malware.

Cybersecurity, or information security, protects networks, systems and programs from broader threats.

HB **Complete activity 2.2.2 in the workbook.**

Software security issues

In recent years, businesses have faced numerous security issues. Here are a few examples:

Distributed Denial of Service (DDoS) attacks	Software crashes when the cyber attackers overload the server, service or network with a DDoS malicious attack.
Third-party software attacks	Software code depends on third-party services like libraries. An attack happens when hackers exploit a third-party service to access business data or introduce vulnerabilities.
Phishing	Phishing occurs when an attacker acts as someone else and steals software credentials like logins or credit card details.
Injection attacks	Attackers can inject malicious code into users' applications to gain unauthorised access to the application software or backend database.
Weak authentication and authorisation mechanisms	Software designed/coded with weak authentication and authorisation mechanisms can allow attackers to bypass security controls and gain access to sensitive data.
Insufficient logging and monitoring	Without adequate logging and monitoring, it can be difficult to detect and respond to security incidents or identify the root cause of security issues.
Mobile application security	Attackers can exploit mobile applications through various attacks, targeting either the device itself or the application's backend servers.
Cloud service security	In cloud computing, the cloud infrastructure, cloud-based applications, and the data stored in the cloud can have vulnerabilities that hackers can exploit.

Figure 2.1.5: Security issues faced by businesses

Ensuring security in software development is a continuous process. When developing software, developers strive to provide robust security measures and create programs free of vulnerabilities by following the disciplines outlined below.

Figure 2.1.6: Practices for software security

HB **Complete activity 2.2.3 in the workbook.**

Software security – Practices used by software developers

Software developers follow best practices to ensure secure software development and protect against malicious users who target vulnerable areas to access, misuse, or destroy programs. To safeguard devices and information, developers implement security best practices from the beginning of the software development process. These practices are listed below.

Limited access control: Software developers implement the least privilege approach, granting the software only the minimum access necessary to perform its functions. This approach minimises the potential for a hacker to exploit the software, as it has fewer features, rights, and controls than what users typically have. This is also called the 'least privilege' approach.

Figure 2.1.7: Access control

Encrypt the software: Software developers encrypt the data stored in physical devices and the data when transmitting from source to destination. The encryption mechanism converts data from a readable format into an unreadable, protected format. Without the encryption key available, a hacker cannot access the information.

Figure 2.1.8: Software encryption

Automation of software security tasks: Software developers encrypt data stored on physical devices and during transmission from source to destination. Encryption converts data from a readable format into an unreadable, protected format. Without the encryption key, hackers cannot access the information.

Figure 2.1.9: Software automation

Two-Factor Authentication (2FA): Software developers protect the system and devices by implementing two-factor authentication, which prevents hackers from accessing the system with just one set of credentials. In this security protocol method, a user provides two pieces of information to log into their account. For example, after entering a password, the system sends a text message to the user's phone for further authentication. Additionally, software developers enforce strong password policies to improve application security.

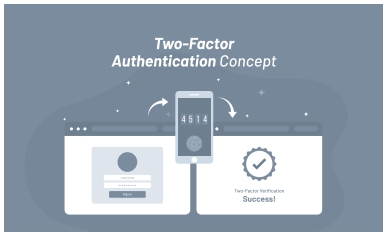


Figure 2.1.10: Software Two-Factor Authentication

Provide employee training: It is important to keep employees informed and updated about the latest technology, the importance of software security, malicious attacks, and prevention methods to protect sensitive data. Software security teams schedule regular training sessions to ensure employees stay up-to-date on system protection.

Figure 2.1.11: Employee training

Anti-malware protection: Malware is harmful software designed to attack a network or system without the user's permission. It includes Trojan horses, computer viruses, worms, and spyware. Malware can hide in emails, websites, file attachments, videos, or photos. It can give hackers unauthorised access to data, leading to security breaches and data theft. Anti-malware software is used to protect networks and essential data from these attacks.

Figure 2.1.12: Anti-malware

Zero trust approach: A stronger security control mechanism for preventing unauthorised data is whitelisting, also known as allowlisting. This cybersecurity strategy allows only approved applications, domain names, users, email addresses, and IP addresses to access a network or system. However, in a zero-trust security approach, software developers believe that even whitelisting is not entirely safe for protecting a network or system, as hackers may still find ways to attack. Therefore, in a zero-trust approach, every access request must be verified and authenticated, regardless of where the request comes from.

Figure 2.1.13: Zero trust approach

HB **Complete activities 2.2.4 and 2.2.5 in the workbook.**

Student reflection

List three things you have learned and two things you have enjoyed.

Three things I have learned:

1- .....

2- .....

3- .....

Two things I have enjoyed:

1- .....

2- .....

Learning outcome	Key skills (Please tick the box to show your understanding of the skills below).	I don't understand.	I understand.	I'm an expert.
Explain ways software developers protect devices and information from unauthorised access.	I can identify ways software developers protect devices and information from unauthorised access.			
	I can explain ways software developers protect devices and information from unauthorised access.			
Teacher's comment:				

MOEUAEofficial