

Network Security

1. Academic Perspective:

Information security is the discipline that explores the theories and strategies dedicated to protecting information from threats and from acts of violation.

2. Technical Perspective:

It refers to the tools, methods, and procedures that must be implemented to ensure protection of information against both internal and external risks.

3. Legal Perspective:

Information security is regarded as a subject of study concerned with the measures required to preserve the confidentiality, integrity, and availability of information. It also focuses on countering activities that compromise information or exploit information systems to commit crimes. Therefore, it constitutes the central objective of legislative frameworks designed to safeguard information and systems against unlawful and **illegal activities, commonly referred to as computer and internet crimes.**

What are the threats to computer network security?

External Threats

- **Malware** : Viruses, worms, Trojans, and ransomware that aim to steal or destroy data.
- **Eavesdropping / Sniffing** : Intercepting data while transmitted over the network to capture passwords or sensitive information.
- **Denial of Service (DoS / DDoS) Attacks (هجمات حجب الخدمة)**: Flooding servers or networks with fake requests to disrupt their availability.
- **Spoofing (انتحال الهوية)**: Pretending to be a trusted IP address or email source.

Protection:

- Use updated **antivirus software**.
 - Apply **encryption** to secure transmitted data.
 - Deploy **firewalls** and **IDS/IPS (Intrusion Detection/Prevention Systems)**.
 - Monitor network traffic to detect suspicious activity.
-

Internal Threats

- **Unauthorized Employees** : Misuse of privileges or intentional data leakage.
- **Human Errors** : Sharing passwords or clicking malicious links.
- **Weak Configurations** : Poorly secured systems or networks.

Protection:

- Implement precise **access control** based on the principle of least privilege.
- Conduct **security awareness training** for employees.
- Monitor **user activity** and enforce strict policies.
- Perform regular **audits** of system configurations.

3 Technical Threats

- **Software Vulnerabilities** : Bugs or flaws in software or operating systems exploited by attackers.
- **Weak Passwords** (كلمات مرور ضعيفة): Easily guessed or cracked through brute-force attacks.
- **Unpatched Systems** : Outdated systems with known vulnerabilities.

✓ Protection:

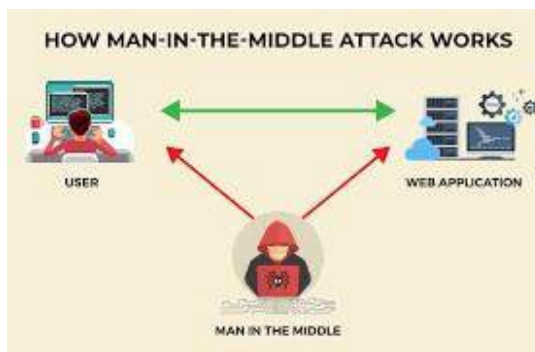
- Apply **regular updates and patches**.
- Use **strong passwords** and enable **multi-factor authentication (MFA)**.
- Conduct **penetration testing** to identify vulnerabilities.
- Perform regular **data backups**.

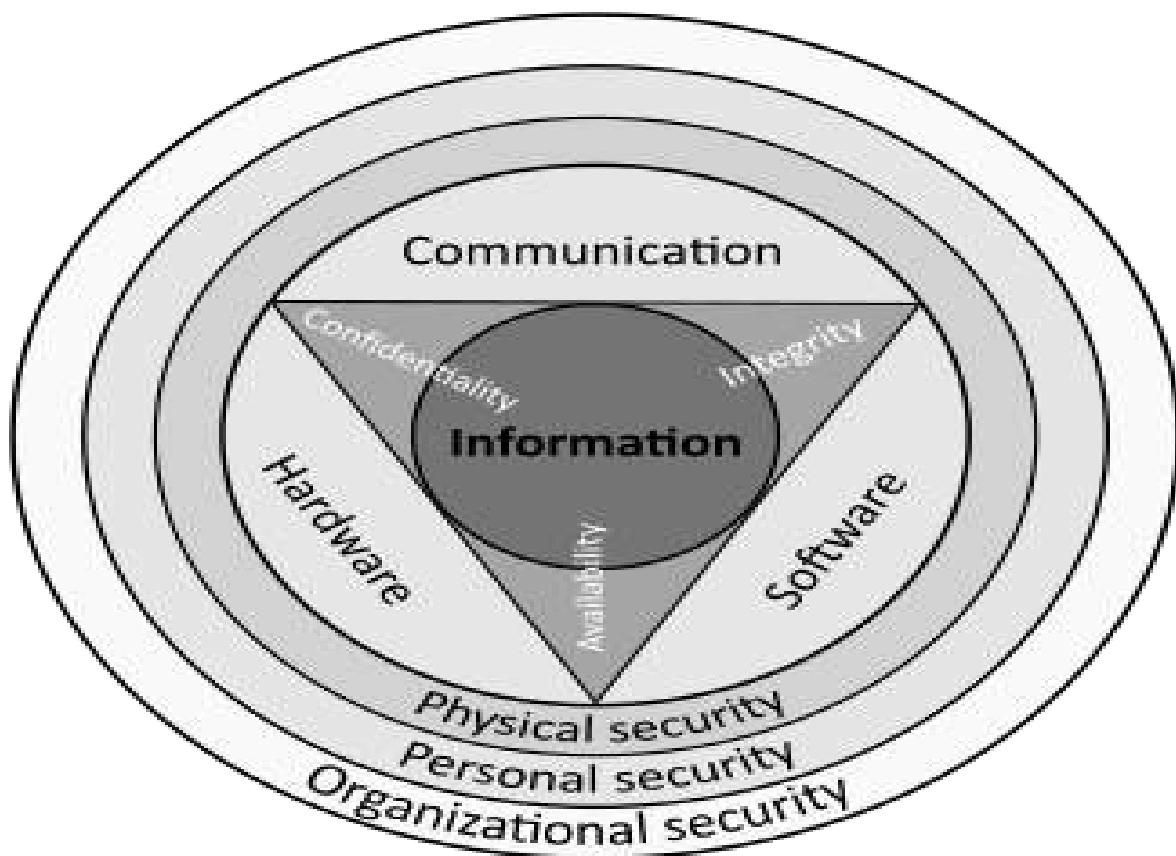
4 Social Threats

- **Phishing** : Fake emails or websites designed to trick users into revealing credentials.
- **Social Engineering** : Manipulating or deceiving people to gain unauthorized access or information.

✓ Protection:

- Provide **phishing awareness training** to employees.
- Educate staff about **social engineering tactics**.
- Use **email filtering systems** to detect malicious messages.
- Run **phishing simulation campaigns** to test employee readiness.





Chapter
Two
E-Commerce



First: What is E-Commerce?

E-commerce is the process of buying and selling goods or services over the Internet. It is considered one of the fastest-growing sectors worldwide, as it enables individuals and businesses to access global markets with ease and speed, without the necessity of physical presence. Moreover, it represents a modern economic model that fosters innovation and expands business opportunities.

Difference Between E-Commerce and Traditional Commerce

E-Commerce	Traditional Commerce
Conducted over the Internet without the need for physical presence	Requires a physical location to display and sell products
Provides easy and fast access to global markets	Limited access restricted to the geographical area of the store
Available 24/7 to customers	Restricted to official working hours
Lower operating costs (no need for large physical stores)	Higher operating costs due to rent and staff
Easy comparison of prices and products	Difficult to compare prices without visiting multiple stores
Relies on electronic payment systems	Relies on cash or card payments at the point of sale

The Importance of E-Commerce in the Modern Era

- 1. Saving Time and Effort:** Customers can shop conveniently from their homes..
- 2. Lower Operating Costs:** Compared to traditional retail stores.
- 3. Access to a Wider Audience:** Small and medium-sized businesses can sell their products globally.
- 4. Ease of Operations Management:** Through digital analytics and management tools

Examples of the Most Popular E-Commerce Platforms

- 1. Amazon:** The largest global online store offering a wide variety of products and advanced services.
- 2. AliExpress:** A Chinese platform that offers competitively priced products with international shipping options.
- 3. eBay:** An open marketplace that allows individuals and businesses to sell and purchase products.
- 4. Shopify:** A comprehensive platform for creating online stores easily without requiring advanced technical expertise.