Chapter 2

E Commerce Threats

Threat: A threat is an object, person , or other entity that represents a constant danger to an asset.

E-commerce threat is occurring by using the internet for unfair **means** with the intention of stealing, fraud and security breach. There are various types of E commerce Threats. Some are accidental, some are purposeful and some are due to human error.

1. Cyber security Attacks: E-commerce sites are susceptible to data breaches, hacking, and other cyber attacks that can compromise customer information, financial data, and business operations.

2. Fraudulent Activities: Online transactions are vulnerable to fraud, including credit card fraud, identity theft, and fraudulent chargebacks, which can lead to financial losses for both businesses and customers.

3. Phishing: Cybercriminals may attempt to deceive users by creating fake websites or emails that mimic legitimate e-commerce platforms, aiming to steal sensitive information like login credentials and financial details.

4. Data Privacy Concerns: With the increasing emphasis on data privacy, mishandling or improper use of customer data can lead to legal issues, loss of customer trust, and damage to the reputation of the e-commerce business.

5. Supply Chain Disruptions: E-commerce businesses relying on physical product delivery can face threats from disruptions in the supply chain, such as delays, inventory issues, or transportation challenges.

6. Website Downtime: Technical issues, server failures, or Distributed Denial of Service (DDoS) attacks can lead to website downtime, affecting the user experience and causing financial losses.

7. Regulatory Compliance: E-commerce businesses must adhere to various regulations and standards, and failure to comply can result in legal consequences and reputational damage.

8. Competition and Market Saturation: In a competitive e-commerce landscape, businesses face the threat of losing market share to competitors, especially when markets become saturated with similar products or services.

9. **Snoeshoe spam:-** Now spam is something which is very command . Almost each one of the us deals with spam mails in our mail box

10. Wi-Fi eaves dropping: It is also one of the easiest ways in e-commerce to steal personal data. It is like a virtual listening of information which is shares over a Wi-Fi network which is not encrypted . It can happen on public as well as on personal computers.

11. **Spamming:** Some bad players can send infected links via email, social media inboxes or messages.

12. Sniffing: type of eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network.

13. **Insider jobs:** a crime committed by or with the assistance of a person living or working on the premises where it occurred.

14. **Spoofing:** Misrepresenting oneself by using fake e- mail addresses or masquerading as someone else.

E Commerce Security: ECommerce security refers to the principles which guide safe electronic transactions, allowing the buying and selling of goods and services through the Internet, but with protocols in place to provide safety for those involved.

Types of E Commerce Security

1. Authentication and Authorization: Requires users to provide more than one form of identification (e.g., password and SMS code) to access their accounts.

2. Secure Payment Gateways: Using trusted and secure payment gateways that handle financial transactions securely, ensuring that sensitive payment information is protected.

4. Regular Security Audits: Conducting frequent audits to identify vulnerabilities and weaknesses in the system, and addressing them promptly.

5. Firewalls: Implementing firewalls to monitor and control incoming and outgoing network traffic, preventing unauthorized access and attacks.

6. Security Certifications: Obtaining and displaying relevant security certifications (e.g., PCI DSS for payment card industry compliance) to assure customers of adherence to industry security standards.

7. Secure Coding Practices: Employing secure coding practices to develop and maintain the e-commerce platform, reducing the risk of vulnerabilities.

8. Monitoring and Intrusion Detection: Implementing systems to monitor for suspicious activities and detect potential security breaches, allowing for timely responses.

9. Customer Education: Educating users about online security best practices, such as creating strong passwords and recognizing phishing attempts.

ENCRYPTION

What is encryption? The process of converting information or data into a code , especially to prevent unauthorized access.

In computing encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key.

Definition:- Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text.

Why use encryption?

- **Authentication:** Protects personal data such as passwords.
- **Privacy:** Provides for confidentiality of private information.
- **Integrity:** Ensures that a document or file has not been altered.
- **Accountability:** Prevents denial or plagiarism.

Types of Encryption

Symmetric Key Encryption A secret key, is applied to the text of a message to change the content in a particular way, uses the same keys for both encryption of plaintext and decryption of ciphertext.

Asymmetric Key Encryption Known as public-private key or public key encryption, Uses key pairs for encrypting or decrypting data. Public key is used to encrypt the data and private key is used to decrypt the data. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

Symmetric encryption (Secret key encryption)

- This is said to be the simplest and best-known encryption technique. As discussed already, it uses one key for both encryption and decryption.
- Because the algorithm behind symmetric encryption is less complex and executes faster, this is the preferred technique when transmitting data in bulk.
- The plaintext is encrypted using a key, and the same key is used at the receiving end to decrypt the received ciphertext. The host in the communication process would have received the key through external means.
- Widely used symmetric encryption algorithms include AES-128, AES-192, and AES-256.

Asymmetric encryption (Public key Encryption)

- This type of encryption is relatively new as compared to symmetric encryption, and is also referred to as public-key cryptography.
- Asymmetric encryption is considered to be more secure than symmetric encryption as it uses two keys for the process.
- The public key used for encryption is available to everyone but the private key is not disclosed.

Decryption: The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

Protecting Client Computer are protected using:

- Digital certificates
- Browser protection

- Antivirus software
- Computer forensics expert
- Privacy

Digital certificates:-

- "A digital certificate is an encrypted and password-protected file that contains sufficient information to authenticate and prove a person's or organization's identity."

Browser protection:-

- Netscape Navigator and Microsoft Internet Explorer browsers are equipped to allow the user to monitor active content before allowing it to download. In other words, when a user downloads web page and runs programs that are embedded in them, browsers give the user a chance to confirm that the programs are from a known and trusted source.

Antivirus software is a defense strategy. Application service providers (ASPs), such as Critical Path and Message Click supply e-mail services to companies to eliminate e-mail virus problems.

Computer forensic experts acquire and examine potential evidence during an investigation, including data that's been deleted, encrypted, or damaged.

Data privacy, also called information privacy, is an aspect of data protection that addresses the proper storage, access, retention, immutability and security of sensitive data.

Ecommerce Communication channels

1. Voice calls: is the ability to contact and converse with people in real-time with a telephone.

2. Vedio Calls: An act or instance of communicating with one or more people using a smartphone, mobile device, webcam, etc., to transmit and receive both audio and video.

3. Webchat: a type of service available on the internet that allows you to exchange written messages with someone else who is using the service at the same time, without the need to use special software.

4. Whatsapp and Telegram: WhatsApp and Telegram are called instant messaging platforms, designed to make communication quick and easy. Both apps are designed for a mobile and web version - that means the conversations can be managed on multiple devices, a feature that is valued highly by users.

5. Email: a system for sending messages to one or more recipients via telecommunications links between computers using dedicated software or a web-based service.

6. Short Message Service: SMS stands for Short Message Service and is commonly known as texting. It's a way to send text-only messages of up to 160 characters between phones.

7. Live chat: a discussion between two people that involves sending messages over the internet, especially to get or give information about a company's products.

8. Chatbot: A chatbot is a computer program that uses artificial intelligence (AI) and natural language processing (NLP) to understand customer questions and automate responses to them, simulating human conversation.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient.

Classical cryptography refers to the historical methods of encrypting and decrypting messages that were used before the advent of modern computer-based encryption techniques.

1. Substitution Ciphers: Each letter is replaced with another letter consistently throughout the message.

2. Transposition Ciphers: The plaintext is written diagonally and read off in rows.

3. Polyalphabetic Ciphers: Uses multiple Caesar ciphers based on a keyword. The key is repeated to encrypt the message.

4. One-Time Pad: message is used only once. Both the sender and receiver must have the same key.

5. Playfair Cipher: Uses a 5x5 matrix of letters to encrypt digraphs (pairs of two letters) from the plaintext.

Modern cryptography refers to the advanced techniques and algorithms used today to secure digital communication, protect data, and ensure the integrity of information.

1. Symmetric key cryptography: is a cryptographic approach where the same key is used for both the encryption of plaintext (original data) and the decryption of ciphertext (encrypted data). In this method, the communicating parties, or entities, must share the secret key securely to maintain the confidentiality and integrity of their communication.

2. Asymmetric key cryptography: also known as public-key cryptography, is a cryptographic method that involves the use of a pair of keys for secure communication: a public key and a private key.

3. Digital Signature: A digital signature is an electronic, encrypted, stamp of authentication on digital information such as email messages, macros, or electronic documents.

4. Public Key Infrastructure (PKI): A public key infrastructure is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

Why Do I Need SSL? (Secure Socket Layer)

SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser.

- **Encryption:** protect data transmissions (e.g. browser to server, server to server, application to server, etc.)
- **Authentication:** ensure the server you're connected to is actually the correct server.
- **Data integrity:** ensure that the data that is requested or submitted is what is actually delivered.

SSL can be used to secure:

- Online credit card transactions or other **online payments.**
- Intranet-based traffic, such as internal networks, **file sharing, extranets** and database connections.

- Webmail servers like **Outlook Web Access, Exchange** and Office Communications Server.
- The connection between an email client such as **Microsoft Outlook** and an email server such as Microsoft Exchange.
- The transfer of files over **HTTPS and FTP(s)** services, such as website owners updating new pages to their websites or transferring large files.
- System logins to **applications and control panels** like Parallels, cPanel and others.
- Workflow and virtualization applications like **Citrix Delivery Platforms or cloud-based computing platforms**.
- Hosting control panel logins and activity like **Parallels, cPanel and others**.

Important Definitions

Firewalls: A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

- **Types of Firewalls**
- **Packet filtering**
- A small amount of data is analyzed and distributed according to the filter's standards.
- **Proxy service**
- Network security system that protects while filtering messages at the application layer.
- **Dynamic packet filtering** that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall (NGFW)**
- Deep packet inspection Firewall with application-level inspection.

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

A network security policy delineates guidelines for computer network access, determines policy enforcement, and lays out the architecture of the organization's network security environment and defines how the security policies are implemented throughout the network architecture.

Access and Security: They determine whether something becomes part of the network and which resources the person or device has access to. Data access and security policies may be the most important types because the security of data and apps depends on them.

Application and QoS: These define the relative priority of different types of traffic and how they should be prioritized.

Traffic routing and service insertion: Traffic from specific user groups should be routed differently, such as through a firewall.

IP-based vs. group- or role-based: You can define policies at either an IP address level or by role. Dynamic role-based policies are easier to use than static ones, allow for greater flexibility, and provide a better user and device mobility support. IP-based policies don't scale well and are better suited for environments where things don't change too often.