Module No. 4: Security & Threats in E-Commerce:

Virus, Cyber Crime, Network Security: Encryption, Protecting Web server with a Firewall, Firewalland Security Policy, Network Fire walls and Application Firewalls, Proxy Server.

Virus:

Definition: A virus is a type of malicious software, or malware that spreads between computers and causes damage to data and software. Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage, it can perform various harmful activities, such as:

1. Replication: A virus can make copies of it and spread to other files or systems on the same network.

2. Damage or Alteration: Some viruses are programmed to delete or corrupt files, alter data, or modify system settings.

3. Network Exploitation: Viruses can exploit vulnerabilities in network protocols or operating systems to spread rapidly across interconnected systems.

4. Information Theft: Some viruses are designed to steal sensitive information like passwords, credit card numbers, or personal data.

To protect against viruses, users and organizations often use antivirus software, keep their operating systems and applications updated, avoid downloading files from unknown sources, and exercise caution when clicking on links or opening email attachments.

Types of Virus:

1. **WORM:** It is special type of computer program that acts as a carrier of virus and carries virus from one machine to another through Internet
2. **TROJAN HORSE:** A Program allows virus programs to enter into a computer system, steal password, email id from the hard disk, and send to another person. They are capable of sending bogus email.

Cyber Crime:

Cybercrime refers to criminal activities that are carried out using computers or the internet, often targeting individuals, businesses, or governments. It encompasses a wide range of illegal activities, including but not limited to:

1. Cyberfraud: This includes various scams such as phishing (attempting to obtain sensitive information like passwords or credit card details), identity theft, and online financial fraud.

2. Cyber stalking and Harassment: Using electronic communications to harass, threaten, or intimidate someone. This can include cyber bullying and online harassment.

3. Malware Attacks: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. This includes viruses, ransomware, and spyware.

4. Data Breaches: Unauthorized access to sensitive data such as personal information, financial records, or trade secrets, often resulting in theft or exposure of that data.

5. Online Child Exploitation: Involves the use of the internet to exploit children for sexual purposes, including grooming, trafficking, and distribution of child pornography.

6. Hacking: Unauthorized access to computer systems or networks, often for financial gain, espionage, or disruption of services.

7. Cyber Espionage: State sponsored or industrial espionage conducted through computer networks, targeting sensitive information or intellectual property.

8. Cyber Terrorism: The use of computer networks to conduct terrorist activities, such as spreading propaganda, inciting violence, or disrupting critical infrastructure.

Cybercrime presents significant challenges to law enforcement and cyber security professionals due to its borderless nature, anonymity of perpetrators, and rapidly evolving tactics. Preventing and combating cybercrime requires a combination of technical solutions, legal frameworks, international cooperation, and public awareness.

Network Security in ECommerce:

1. Encryption: Ensuring that data transmitted between the user and the ecommerce site is encrypted (e.g., using SSL/TLS) to prevent interception by unauthorized parties.

2. Payment Security: Protecting financial transactions using secure payment gateways that comply **with PCI DSS (Payment Card Industry Data Security Standard).**

3. Authentication: Implementing strong authentication mechanisms **(e.g., two factor authentication)** to verify the identity of users and prevent unauthorized access.

4. Data Privacy: Safeguarding personal information collected from customers, adhering to regulations like GDPR (General Data Protection Regulation) or CCPA (California Consumer Privacy Act).

5. Secure Software Development: Employing secure coding practices and regularly updating software to patch vulnerabilities and prevent exploitation.

6. Fraud Prevention: Using fraud detection systems to identify and mitigate fraudulent transactions and activities.

Threats in ECommerce:

1. Payment Fraud: Unauthorized use of credit card information or other payment methods for fraudulent transactions.

2. Phishing and Identity Theft: Fake websites, emails, or messages designed to trick users into providing sensitive information.

3. Data Breaches: Unauthorized access to customer data stored by the ecommerce site, leading to exposure of personal information.

4. DDoS Attacks: Distributed Denial of Service attacks aimed at disrupting the availability of the ecommerce website.

5. Account Takeovers: Unauthorized access to user accounts through credential theft or exploitation of vulnerabilities.

6. Malware and Ransomware: Malicious software designed to compromise systems or extorts money from ecommerce businesses.

Modes of Transmission:

1. Email Attachments: Viruses often spread through email attachments that contain infected files or links to malicious websites.

2. File Sharing: Infected files shared over peer to peer networks or removable storage devices (USB drives) can propagate viruses to other computers.

3. Network Vulnerabilities: Exploiting vulnerabilities in network protocols or software can enable viruses to spread across interconnected devices.

Effects of Computer Viruses:

1. Data Loss or Corruption: Viruses can delete, modify, or corrupt files and data stored on the infected system.

2. System Instability: Viruses may cause frequent crashes, freezes, or other malfunctions that disrupt normal system operations.

3. Security Breaches: Some viruses are designed to steal sensitive information (such as passwords or financial data) from infected computers.

Protection Against Computer Viruses:

1. Antivirus Software: Installing reputable antivirus software that can detect and remove viruses from your system.

2. Regular Updates: Keeping operating systems, software applications, and antivirus definitions up to date to patch vulnerabilities that viruses might exploit.

3. Safe Internet Practices: Avoiding clicking on suspicious links, downloading files from unknown sources, or opening attachments from unfamiliar senders.

4. Firewalls: Using firewalls to monitor and control incoming and outgoing network traffic to prevent unauthorized access and malware infections.

5. Backup and Recovery: Regularly backing up important data and having a recovery plan in place to restore systems in case of a virus infection.

Understanding the nature of computer viruses and implementing robust security practices can help individuals and organizations minimize the risk of infection and mitigate the potential damage caused by these malicious programs.

Network Fire walls and Application Firewalls:

Network firewalls and application firewalls are both essential components of cyber security that serve different purposes but work together to protect systems and networks. Here's an overview of each:

Network Firewalls:

Network firewalls operate at the network level, typically at the boundary between a private internal network and the public internet. Their primary function is to monitor and control incoming and outgoing network traffic based on predetermined security rules. Key points about network firewalls include:

1. Traffic Filtering: They inspect packets of data passing through them and decide whether to allow or block them based on predefined rules (like IP addresses, ports, protocols).

2. Security Zones: They establish security zones between internal networks, external networks (like the internet), and demilitarized zones (DMZs) where servers accessible from the internet reside.

3. Statefull Inspection: Modern network firewalls often use statefull inspection, which tracks the state of active connections and can make more informed decisions about allowing or denying traffic.

4. Protection against Network level Threats: They protect against threats like unauthorized access attempts (e.g., port scanning), denial of service (DoS) attacks, and other network based exploits.

Application Firewalls:

Application firewalls, on the other hand, operate at the application layer (Layer 7 of the OSI model). They provide a more granular level of security by monitoring and controlling the traffic based on specific applications or services rather than just IP addresses and ports. Key points about application firewalls include:

1. Deep Packet Inspection: They analyse the contents of packets beyond the header information, inspecting application layer data for signs of malicious activity or policy violations.

2. Protection against Application specific Threats: They protect against threats targeting specific applications or services, such as SQL injection attacks, cross site scripting (XSS), and application layer DoS attacks.

3. Context aware Filtering: They can make decisions based on the content of the application traffic, understanding the context of requests and responses to enforce security policies more effectively.

4. Enhanced Security for Web Applications: Application firewalls are particularly valuable for protecting web applications and APIs from common vulnerabilities and attacks.

Relationship and Integration:

While network firewalls primarily focus on controlling traffic flow between networks and enforcing basic security policies, application firewalls add an additional layer of security by inspecting and filtering traffic at the application level. Modern cyber security strategies often involve deploying both types of firewalls in a complementary manner:

Defence in Depth: Using multiple layers of security controls (including both network and application firewalls) to create a more robust defence against cyber threats.

Integrated Security: Many modern firewall solutions integrate both network and application firewall functionalities into a unified platform, providing centralized management and more comprehensive threat detection and prevention capabilities.

In conclusion, network firewalls and application firewalls are critical components of cyber security infrastructure, each serving distinct but complementary roles in protecting networks, applications, and data from various cyber threats.

Proxy Server:

A proxy server acts as an intermediary between clients (such as web browsers or other applications) and servers. It facilitates indirect network connections and can provide various functionalities and benefits depending on its configuration and purpose. Here are the key aspects and functions of a proxy server:

Functions of a Proxy Server:

1. Anonymity and Privacy:

Anonymous Proxy: Masks the IP address of the client, providing anonymity by hiding the original IP address from the server.

Transparent Proxy: Does not modify the client's IP address but intercepts and forwards traffic, often used for caching purposes.

2. Content Filtering and Access Control:

URL Filtering: Controls access to specific websites or categories of content based on predefined rules.

Content Inspection: Scans web traffic for malware, viruses, or prohibited content before it reaches the client.

3. Improved Performance:

Caching: Stores copies of frequently accessed resources locally, reducing bandwidth usage and speeding up access times for clients.

Load Balancing: Distributes incoming client requests across multiple servers, optimizing resource utilization and improving response times.

4. Access to Restricted Resources:

By passing Geolocation Restrictions: Allows access to websites or content restricted based on geographical location.

Firewall Bypassing: Enables access to resources blocked by local network firewalls or content filters.

5. Security and Monitoring:

Logging and Monitoring: Records detailed information about client server interactions for auditing, troubleshooting, or security analysis.

Types of Proxy Servers:

1. Forward Proxy: Acts on behalf of clients to access resources from servers. Clients configure their applications to use the proxy server for internet access, Provides benefits such as caching, filtering, and anonymity for clients.

2. Reverse Proxy: Acts on behalf of servers, receiving client requests and forwarding them to the appropriate backend servers. It enhances security by hiding server IP addresses and distributing client requests among multiple servers.

3. Open Proxy:

Accessible to any internet user and can be used for various purposes, including bypassing restrictions or anonymizing internet activities, often abused for malicious activities like spamming or launching distributed denial of service (DDoS) attacks.

Deployment Considerations:

Security: Proper configuration and monitoring are essential to prevent misuse (e.g., proxy abuse by attackers).

Performance: Caching and load balancing features can improve performance but require adequate resources and maintenance.

Policy Enforcement: Ensuring compliance with organizational policies regarding internet usage, content filtering, and data protection.

In summary, a proxy server plays a versatile role in networking and cyber security, offering functionalities ranging from enhancing privacy and security to optimizing network performance and facilitating access to restricted resources. Its deployment and configuration depend on specific organizational needs and security requirements.

Module5: Issues in Ecommerce

Understanding Ethical, Social and Political issues in ECommerce:

Understanding the ethical, social, and political issues in ecommerce is crucial as online transactions and digital interactions become increasingly integral to modern life. Here’s an overview of these issues:

Ethical Issues:

1. Privacy and Security: Privacy Concerns: Collection, storage, and use of personal data without consent.

Security: Vulnerabilities in transactions, data breaches, and cyber security threats.

2. Trust and Consumer Protection: Ensuring truthful representation of products and services, dealing with fraudulent activities like online scams and phishing.

3. Fairness: Addressing issues of price discrimination and unfair pricing practices, ensuring fair competition among businesses, especially small enterprises versus large corporations.

4. Intellectual Property: Protecting copyrights and trademarks in digital content and products, dealing with issues like digital piracy and unauthorized copying.

Social Issues:

1. Digital Divide: Disparities in access to technology and the internet among different socioeconomic groups, impact on opportunities for education, employment, and social inclusion.

2. Impact on Local Businesses: Effects of ecommerce giants on local economies and traditional brick and mortar businesses, challenges faced by small businesses to compete in the digital marketplace.

3. Consumer Behaviour: Shifts in purchasing habits and the rise of impulse buying, impact on sustainability due to increased packaging and shipping demands.

4. Workplace Issues: Job displacement due to automation and ecommerce platforms, effects on working conditions, especially in logistics and delivery sectors.

Political Issues:

1. Regulation and Governance:

Developing and enforcing laws related to ecommerce transactions, data protection, and consumer rights, balancing regulation to foster innovation while ensuring ethical business practices.

2. Taxation: Addressing challenges related to collecting taxes on digital transactions and cross border ecommerce, ensuring fair taxation practices for online businesses operating globally.

3. Jurisdiction and Global Trade: Resolving conflicts related to jurisdiction in cross border transactions, impact of international trade agreements on ecommerce policies and regulations.

4. Data Sovereignty: Concerns over where data is stored and who has access to it, navigating international data protection laws and regulations.

Information collected at ECommerce websites:

Information collected at ecommerce websites typically includes a wide range of data points that are crucial for various purposes such as personalization, marketing, transaction processing, and analytics. Here’s an overview of the types of information commonly collected:

1. Personal Information:

Identification: Name, gender, date of birth, social security number (depending on region).

Contact Details: Address, email, phone number.

Payment Information: Credit card details, billing address, payment history.

2. Transactional Data:

Order History: Details of past purchases, including products bought, dates, and amounts spent.

Shopping Preferences: Items viewed, wish lists, shopping cart contents.

Shipping Information: Shipping address, preferred delivery options.

3. Behavioural Data:

Website Interactions: Pages visited, time spent on each page, clicks, searches performed.

Device Information: Type of device used (desktop, mobile), operating system, browser type.

Referral Sources: How the user arrived at the website (search engine, direct visit, referral link).

4. User generated Content:

Reviews and Ratings: Customer feedback on products and services.

Comments and Messages: Communications with customer service or other users on the platform.

5. Cookies and Tracking Technologies:

Cookies: Small text files stored on the user's device to track preferences and activities, tracking Pixels and Beacons: Used for analytics, advertising, and tracking user behaviour across websites.

6. Location Data:

IP Address: General location based on IP address.

GPS and Geo-location: More precise location data if permission is granted by the user.

7. Preferences and Settings:

Account Settings: User preferences, notifications settings.

Marketing preferences: Opt-ins or opt-outs for marketing communications.

Purpose of Information Collection:

Personalization: Customizing the user experience based on past behavior and preferences.

Marketing and Advertising: Targeted ads and promotions based on user interests.

Transaction Processing: Facilitating payments and order fulfilment.

Analytics and Improvements: Understanding user behaviour to enhance website usability and performance.

Compliance and Security: Meeting legal and regulatory requirements, and ensuring data security.

Ethical and Privacy Considerations:

Consent: Ensuring users are informed and give consent for data collection and usage.

Security: Protecting collected data from unauthorized access, breaches, and misuse.

Transparency: Clearly communicating to users what data is collected and how it will be used.

Data Retention: Safely storing data and adhering to retention policies.

User Rights: Providing mechanisms for users to access, correct, or delete their personal data.

Legal protections Intellectual Property Rights:

Legal protections for intellectual property (IP) rights are crucial in ensuring creators and innovators have the necessary incentives and protections for their works and inventions. Here are the primary legal frameworks that protect **intellectual property rights:**

1. Copyright Law:

Purpose: Protects original works of authorship fixed in any tangible medium of expression (e.g., literary works, music, art, software).

Rights: Grants the creator exclusive rights to reproduce, distribute, perform, display, and create derivative works of their creation.

Duration: Generally lasts for the life of the author plus 70 years.

2. Patent Law:

Purpose: Protects inventions or discoveries that are novel, useful, and nonobvious.

Rights: Grants the inventor exclusive rights to prevent others from making, using, selling, or importing their invention for a limited period (usually 20 years).

Types: Utility patents (for processes, machines, articles of manufacture) and design patents (for ornamental designs of functional items).

3. Trademark Law:

Purpose: Protects words, phrases, symbols, or designs that distinguish goods or services in the marketplace.

Rights: Grants the owner exclusive rights to use the mark in commerce and to prevent others from using confusingly similar marks.

Duration: Can be renewed indefinitely as long as the mark is used and maintained properly.

4. Trade Secret Law:

Purpose: Protects confidential business information that provides a competitive advantage (e.g., formulas, processes, customer lists).

Rights: Protects against unauthorized use or disclosure as long as the information remains secret and efforts are made to keep it confidential.

Duration: Lasts indefinitely as long as the information remains secret.

International Treaties and Agreements:

WIPO (World Intellectual Property Organization): Administers international treaties such as the Berne Convention (copyright), the Paris Convention (industrial property), and the TRIPS Agreement (TradeRelated Aspects of Intellectual Property Rights).

TRIPS Agreement: Sets minimum standards for intellectual property regulation within member countries of the World Trade Organization (WTO).

Enforcement and Remedies:

Civil Remedies: Lawsuits for injunctions, damages, and account of profits.

Criminal Enforcement: Penalties for wilful infringement, counterfeiting, or piracy.

Customs Enforcement: Seizure and detention of infringing goods at borders.

Ethical and Policy Considerations:

Balancing Rights: Ensuring IP laws balance incentives for innovation with public access and competition.

Access to Knowledge: Promoting access to essential knowledge and cultural goods while respecting IP rights.

Global Challenges: Addressing international harmonization, enforcement challenges, and evolving technologies (e.g., digital piracy, AI-generated content).