**CHAPTER SEVEN**

**E-COMMERCE SECURITY**

**Learning Objectives**

By the end of this chapter the learner shall be able to;

i. Explain the challenges of stopping E-commerce crimes

ii. Explain the terms confidentiality, integrity and availability iii. Explain the security tools; both hardware and software

iv. Explain the different types of threats and Attacks; both Technical and Non-technical

v. Explain how E-commerce communications can be secured

**7.1 Why it’s Difficult to stop E-Commerce crimes**

It is quite difficult to stop E-crimes for the following reasons;

 Strong EC security makes online shopping inconvenient and demanding on customers. The EC industry does not want to enforce safeguards that would discourage online commerce.

 A second reason is the lack of cooperation from credit card issuers and foreign ISPs. There are insufficient incentives for credit card issuers to share leads on criminal activity with each other or law enforcement. It is much cheaper to block a stolen card and move on than to invest time and money in a prosecution with an uncertain outcome.

 The third reason pertains to customers. Online shoppers are to blame for not taking necessary precautions to avoid becoming a victim. Some shoppers rely too heavily on fraud protection provided by credit card issuers ignoring the bigger risk of identity theft. Phishing is rampant because some people respond to it making it profitable.

 A fourth reason arises from IS design and security architecture issues. It is well know that preventing vulnerability during the EC design and pre-implementation stage is far less expensive than mitigating problems later. The IS staff needs to plan security from the design stage because simple mistakes, such as not

insuring that all traffic into and out of network pass through a firewall, are often to blame for letting in hackers.

**7.2 Confidentiality, Integrity, and Availability**

The success and security of EC depends on the confidentiality integrity and availability of information and the business Web site.

1. Confidentiality is the assurance of data privacy the data or transmitted message is encrypted so that it is readable only by the person for whom it is intended. Depending on the strength of the encryption method, intruders or eavesdroppers might not be able to break the encryption to read the data or text. The confidentiality function prevents unauthorized disclosure of information.

2. Integrity is the assurance that data is accurate or that a message has not been

altered. It means that stored data has not been modified without authorization; a message that was sent is the same message that was received. The integrity function detects and prevents the unauthorized creation, modification, or deletion of data or messages.

3. Availability is the assurance that access to data, the Web site, or other EC data service is timely available, reliable, and restricted to authorized users.

Although the basic security concepts important to information on the Internet are confidentiality integrity and availability concepts relating to the people (users) are authentication, authorization, and nonrepudiation. Confidentiality, integrity availability authentication, authorization, and nonrepudiation are all assurance processes.

All the Confidentiality, integrity availability functions depend on Authentication, Authorization and Nonrepudiation;

**Authentication** is a process to verify (assure) the real identity of an entity which could be an individual, computer, computer program, or EC Web site. For transmissions, authentication verifies that the sender of the message is who the person or organization claims to be.

**Authorization** is the process of determining what the authenticated entity is allowed to access and what operations it is allowed to perform. Authorization of an entity occurs after authentication.

**Nonrepudiation** is Closely associated with authentication is, which is assurance that online customers or trading partners cannot falsely deny (repudiate) their purchase, transaction, and so on. For EC and other electronic transactions, including cash machines or ATMs, all parties in a transaction must be confident that the transaction is secure; the parties are who they say they are.

**7.3 Threats and Attacks**

Generally there are two typed of attacks nontechnical and technical although Most attacks involve a combination of the two types;

**Nontechnical attacks** are those in which a perpetrator uses some form of deception or persuasion to trick people into revealing information or performing actions that can compromise the security of a network.

**Technical attacks** are attacks perpetrated using software and systems knowledge or expertise. The time-to-exploitation of today’s most sophisticated spyware and worms has shrunk from months to days. Time-to-exploitation is the elapsed time between when a vulnerability is discovered and the time it is exploited.

There are several technical attacks that could be used as follows;

**Denial of service (DOS) attack**: Is an attack on a website in which an attacker uses specialized software to send a flood of data packets to the target computer with the aim of overloading its resources.

**Server and Web Page Hijacking:** Web servers and Web pages can be hijacked and configured to control or redirect unsuspecting users to scam or phishing sites. This technique uses 302 server redirects. This exploit allows any Web master (including criminals) to have his or her own ―virtual pages‖ rank for pages belonging to another Web master. When effectively employed, this technique will allow the offending Web

master (―the hijacker‖) to displace the pages of the ―target‖ or victim Web site in the search engine results pages (SERPS).This causes search engine traffic to the target Web site to vanish or redirects traffic to any other page of choice.

**Botnets:** This is a huge number of hijacked internet computers that have been setup to forward traffic, including spam and viruses, to other computers on the internet. **Malicious Code: Viruses, Worms, and Trojan Horses:** Sometimes referred to as malware (for malicious software), malicious code is classified by how it propagates (spreads). A virus is a piece of software code that inserts itself into a host, including the operating systems; running its host program activates the virus. A virus has two components. First, it has a propagation mechanism by which it spreads. Second, it has a payload that refers to what the virus does once it is executed. Sometimes a particular event triggers the virus’s execution.

**Phishing** is a way of attempting to acquire sensitive information such as usernames,

passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

**7.4 Securing E-Commerce Communications**

Most organizations rely on multiple technologies to secure their networks. These technologies can be divided into two major groups: those designed to secure communications across the network and those designed to protect the servers and clients on the network. Some technologies are considered below;

**Access Control**

Network security depends on access control. Access control determines who (person, program, or machine) can legitimately use a network resource and which resources he, she, or it can use. A resource can be anything—Web pages, text files, databases, applications, servers etc. Typically access control lists (ACI,s) define which users have access to which resources and what rights they have with

respect to those resources (ie., read, view, write, print, copy delete, execute, modify or move). Each resource needs to be considered separately and the rights of particular users or categories of users. Access control can also be implemented using biometric systems. Fingerprint scanners, iris scanners, facial recognition systems, and voice recognition all are examples of biometric systems that recognize a person by some biological characteristic or trait.

**Public Key Infrastructure**

The ―state of the art‖ in authentication rests on the public key infrastructure (PKI). In this case, the something a user has is not a token, but a certificate. PKI has become the cornerstone for secure e—payments. It refers to the technical components, infrastructure, and practices needed to enable the use of public key encryption, digital signatures, and digital certificates with a network application. PKI also is the foundation of a number of network applications, including SCM, VPNs, secure e-mail, and intranet applications. The are several techniques that could be applied in this;

**Private and Public Key Encryption:** PKI is based on encryption. Encryption is the

process of transforming or scrambling (encrypting) data in such a way that it is difficult, expensive, or time-consuming for an unauthorized person to unscramble (decrypt) it. The encryption algorithm is the set of procedures or mathematical functions to encrypt or decrypt a message.

**Symmetric key system:** is an encryption system that uses the same key to encrypt and decrypt the message.

**Public key encryption:** This sis a method of encryption that uses a pair of matched

keys-a public key to encrypt a message and a private key to decrypt it or vise versa. Digital signatures: this is the equivalent of a personal signature that cannot be forged. They are based on public keys for authenticating the identity of the sender of a message or document. They also ensure that the original content of an electronic message or document is unchanged.

Secure socket layer: This is a protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality.

**Securing E-Commerce networks**

Several technologies exist that ensure that an organization’s network boundaries are

secure from attacks such as;

**Firewalls:** they are barriers between a trusted network or PC and the untrustworthy internet. It’s a single point between two or more networks where all traffic must pass(choke point); the device authenticates, controls and logs all traffic.

**Virtual private network (VPN):** A network that uses the public Internet to carry

information but remains at private by using encryption to scramble the communications, authentication to ensure that information has not been tampered with, and access control to verify the identity of anyone using the network.

**intrusion detection systems (IDSs):** A special category of software that can

monitor activity across a network or on a host computer, watch for suspicious activity, and take automated action based on what it sees.

Honeypot: Production system (e.g., firewalls, routers, Web servers, database servers)

that looks like it does real work, but which acts as a decoy and is watched to study how network intrusions occur.