Security Threats and Countermeasures in E-commerce Environment

What is e-commerce security?

E-commerce security is protection the various e-commerce assets from unauthorized access, its use, or modification.

What is an e-commerce threat?

In simple words, you can say that using the internet for unfair means with an intention of stealing, fraud and security breach.

There are various types of e-commerce threats: Some are accidental, some are purposeful, and some of them are due to human error. The most common security threats are phishing attacks, money thefts, data misuse, hacking, credit card frauds, and unprotected services.

Inaccurate management: One of the main reasons for e-commerce threats is poor management. When security is not up to the mark, it poses a very dangerous threat to the networks and systems. Also, security threats occur when there are no proper budgets are allocated for the purchase of anti-virus software licenses.

Price Manipulation: Modern e-commerce systems often face price manipulation problems. These systems are fully automated; right from the first visit to the final payment getaway. Stealing is the most common intention of price manipulation. It allows an intruder to slide or install a lower price into the URL and get away with all the data.

Cyber Fraud and Solutions

For decades, computer security specialists have spent the lion’s share of their budgets hardening their organizations’ defenses against external fraud and cyber - crime threats. Most common Viruses, worms, Trojan horses, key loggers, and other common forms of malicious attack that resulted in either system damage, theft of confidential information, or diversion of the organization’s financial assets or those of its customers. Only in the past few years has it become abundantly clear that insiders are equally if not more serious fraud threats to their employers than outsiders.

Result

Today, any organization lacking a strict set of internal computer security policies, processes, and procedures to counter the numerous threats of insider fraud puts itself at serious risk of financial and reputational damage, as well as legal and regulatory consequence in the event of a successful insider attack.

Common Forms of Computer Fraud

They fall into three main categories:

1. Input transaction manipulation schemes: These include:

- **Extraneous transactions:** These are illegal transactions initiated by a trusted insider, such as unauthorized billing transactions that result in disbursement of company funds to the perpetrator or a shell company he or she controls. These frauds can also involve manipulating the organization's computer data pertaining to one or more customers, vendors, products, accounting entries, salespeople, and so on that the executor exploits at a later time.

- **Failure to enter transactions:** This is a common technique in many billing schemes.

  Examples: A purchasing associate who is perpetrating a billing scheme can intentionally prevent a bogus invoice from being entered into the payments system. Or a staffer responsible for accounts receivable can neglect to credit an account when payment is received (see also following discussion).

- **Transaction modification:** Also common in billing schemes or collusion, these involve fraudulently increasing or reducing amounts charged to a particular account.

- **Misuse of adjustment transactions:** Computer systems for legitimately correcting accounting errors or to record adjustments to inventory loss or spoilage can be abused by employees with access to such systems by falsifying entries to cover up outright theft or more elaborate billing schemes. Related schemes: Entering fraudulent error corrections or intentionally omitting such corrections to conceal fraud.

2. Unauthorized program modification schemes

This category of computer - generated insider schemes typically involves making unauthorized changes to automated payment or accounting software programs. A common form of this crime involves programming the system to execute high numbers of mini frauds such as rounding of numbers, fraudulently adding service charges, or diverting amounts of money so small as to fall below the radar of internal controls on accounts owned by the fraudster. Additional varieties:

- **Processing undocumented transaction codes:** By manipulating the payments sys-tem to accept undocumented, false transaction codes for small transactions in situations where controls are absent, the fraudster can program the sys-tem to process fraudulent transactions that are entered directly by the executor or by the computer via unauthorized programming changes.

- **Balance manipulation:** Here a dishonest internal computer programmer alters specific programs in a way that fraudulently forces account balances, in order to conceal misappropriation or other types of fraud that would otherwise be detectable by auditors.

- **Lapping schemes:** An insider with authorization to utilize the organization's automated accounting system can steal incoming payments and credit them to his or her own account and then manipulate the system to fraudulently credit the intended payee' s account with a payment subsequently received from another account. The process is repeated until, due to slipup in timing or sharp auditing, the scheme is detected.

- **Fraudulent file modifications:** These crimes involve secretly changing account status through basic computer programming. Examples: Opening a fraudulent new account to receive automatic payments from payroll, retirement, unemployment, or welfare systems, destroying records of a fraudulent account, or fraudulently increasing a credit limit on a revolving credit line.

3. File alteration and substitution schemes: Common examples:

- **Accessing a live master file:** The internal fraudster accesses the file and, using a specially written program or a general retrieval program, makes fraudulent adjustments to the file, such as a Vendor Master File, by modifying account balances, altering a payee, changing supplier addresses, adding bogus vendors, and so on.

- **Substitution of a dummy version of a real file:** The fraudster initiates the scheme by obtaining access to the master file and then uses a special computer program to run the legitimate master file in order to create a duplicate. However, the duplicate has a few modifications when it is substituted for the legitimate file, thereby enabling the fraudster to hide fraudulent transactions that would otherwise be detected.

Solutions/Preventions

- **Use a full-service internet security suite** to get real-time protection against existing and emerging malware including ransom ware and viruses, and protect your private and financial information when you go online.

- **Use strong passwords:** Don’t repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 10 letters, numbers, and symbols.

- **Keep your software updated:** This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you’ll become a cybercrime target.

- **Manage your social media settings:** Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better.

- **Strengthen your home network:** It’s a good idea to start with a strong encryption password as well as a virtual private network. A VPN will encrypt all traffic leaving your devices until it arrives at its destination. If cybercriminals do manage to hack your communication line, they won’t intercept anything but encrypted data. It’s a good idea to use a VPN whenever you a public Wi-Fi network, whether it’s in a library, café, hotel, or airport.

- **Keep up to date on major security breaches:** If you do business with a merchant or have an account on a website that’s been impacted by a security breach, find out what information the hackers accessed and change your password immediately.

- **Take measures to help protect you against identity theft:** Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. For example: You might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That’s why it’s important to guard your personal data. A VPN — short for virtual private network — can also help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

- **Know that identity theft can happen anywhere:** It’s smart to know how to protect your identity even when traveling. There are a lot of things you can do to help keep criminals from getting your private information on the road. These include keeping your travel plans off social media and being using a VPN when accessing the internet over your hotel’s Wi-Fi network.