**E-commerce security threats**

1. Financial Frauds

* Ever since the first online businesses entered the world of the internet, financial fraudsters have been giving businesses a headache.

1. Credit card fraud

* hackers target merchant servers use data to establish credit under false identity Spoofing
* sending spam and junk websites

1. Bots

* Some attackers develop special bots that can scrape your website to get information about inventory and prices. Such hackers, usually your competitors, can then use the data to lower or modify the prices in their websites in an attempt to lower your sales and revenue.

1. Malicious Code

* It includes virus, worms, backdoors, bots, threats at both client and server side
  + Phishing
    - E-mail scams
    - Social engineering
    - Identity theft
  + SQL Injection
  + Cross site scripting
  + Hacking

1. Distributed Denial of Service (DDoS) Attacks

* A DDoS attack involves your website’s servers being flooded with requests from potentially thousands of untraceable IP addresses. Often driven by the manipulation of IoT devices, today's more sophisticated attacks can cause your entire site to go offline, leaving it wide open to more vicious attacks, such as a malware infection.

1. Data breach

* Losing control over corporate information to outsiders.

1. Sniffing

* Eavesdropping program that monitors information traveling over a network.

**Tools for achieving security in e-commerce**

* E commerce security is the protection of e commerce asserts from unauthorized users

1. Encryption

* Transfer data in to cipher text readable only by sender and receiver
* Secure stored information and information transmission
* We need to consider the below for security services.
* Message integrity: information being displayed on website can’t be altered by any unauthorized party
* Non repudiation: The ability to ensure that e commerce participants not deny their online actions
* Authentication: Ability to identify the identity of a person
* Confidentiality: Ability to ensure that message or data available only to those who are authorized
* There are different types of encryption techniques:
  + Symmetric key encryption
  + Public key encryption
  + Digital signature (A digital signature is a type of electronic signature)

1. Firewalls

* A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.
* Accept: allow the traffic
* Reject: block the traffic but reply with an “unreachable error”
* Drop: block the traffic with no reply
* A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

1. Proxy servers

* Server that handles all communications originating from or being sent to internet

1. Virtual private network

* VPN stands for Virtual Private Network (VPN), that allows a user to connect to a private network over the Internet securely and privately.
* Allows users to securely access internal networks via internet
* It has OS security enhancements
  + Upgrades or patches

1. Transport Layer Security

* Write about CNS answer