1.1 INTRODUCTION

Commerce is basically an economic activity involving trading or the buying and selling of goods. The customer would physically visit to the shop, pick up the product he/she wants to purchase and make payment. As we enter the electronic age, all such activities are undertaken using internet, which is known as E-Commerce.

Changing lifestyle, online banking facilities, plastic money in the form of debit and credit cards, tech savvy generation, boom of IT companies and increase in disposable income are few of the reasons for e-

commerce boom in India. Apart from technical reasons one of the reasons for this change is the avoidance of all sorts of traffic and mental stress on the roads. To reach at the shopping place one has to travel through jam packed streets. With increase in the number of smartphones, mobile shopping becomes part of e-Commerce boom in India.

It was mid 1990s when the Internet companies started rising in India, but lack of awareness, low penetration of Internet and undeveloped payment system were the bottlenecks. Online classified, matrimonial and job portals were the main e-commerce portals at that time. The dot com started gaining recognition in 2000s which gave a push to the e-commerce industry in India. Along with the developments in dot com sector, India's retail sector started to excel. With time retail stores opened their virtual stores.

Recently, India's 14 billion e-commerce industry got a boost with the announcement of a proposal in the Union Budget 2014-15 which will allow foreign retailers to sell their products in the country via e-commerce platform. Brands like Nike, Puma, Marks & Spencer which were selling through licensing agents and franchisees will be benefited a lot with this announcement.

1.1.1 CONCEPT OF E-COMMERCE

E-commerce is a popular term for electronic commerce or even internet commerce. The name is self-explanatory; it is the meeting of buyers and sellers on the internet. This involves the transaction of goods and services, the transfer of funds and the exchange of data

So when a customer logs into his/her Amazon account and purchase a book, this is a classic example of an e-commerce transaction. Here customer interacts with the seller (Amazon), exchange data in form of pictures, text, address for delivery etc. and then he/she makes the payment.

In other words, E-Commerce refers to the buying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions. E-commerce is often used to refer to the sale of

physical products online, but it can also describe any kind of commercial transaction that is facilitated through the internet.

"E-Commerce describes the process of buying and selling or exchanging of products, services and information, via computer networks including the internet." **E. Turban**.

1.1.4 MAIN ACTIVITIES OF E-COMMERCE

1) **Registration:** In order to make a purchase, the user must register on the website by providing all necessary information for billing and shipping purposes. It also enables a firm to send updates and various offers to their customers. The information required for the registration process includes name, address, contact details, an alternative to the contact number, Email-ID and other relevant data of the customer. The system followed for the registration and shopping may vary from firm to firm. Further, all the data of customers is stored on a database of the e-commerce firm.

2) **Information Search:** After registration, users can surf for information about the product which they desire to purchase. They can compare different products before finalising what they wish to purchase. On some e-commerce websites, information search can be made first, and registration can be done at the time of purchasing a product.

3) **Electronic Data Interchange (EDI):** Electronic Data Interchange (EDI) is the computer-to-computer exchange of business documents in a standard electronic format between business partners. Many business documents can be exchanged using EDI, but the two most common are purchase orders and invoices.

4) **Negotiations:** E-Commerce facilitates negotiations between the buyer and the seller. A buyer can negotiate with two or more sellers through video-conferencing especially in case of B2B e-commerce. The buyer can negotiate for price, delivery schedule, quality, quantity and other terms and conditions.

5) **Placing order:** The buyer can place the order. On receipt of the order, the seller processes the order. The seller must undertake proper order management for timely delivery of product.

   In case of B2C e-commerce, the customer adds the product in shopping cart. Shopping cart is a tool which, like online basket, allows users to select products they want to purchase and then add them in their cart. After all the products are selected, the user can have a look at the number and types of products purchased by her/ him and also add or delete products as per their requirements.

6) **Payment:** After selecting products for purchase, the next step is to select payment options. The variety of payment options offered are cash on delivery, debit/credit card, net banking, payment by apps, etc. Customers can select any mode of payment as per their convenience and suitability.

7) **Logistics:** After the payment processing is done, logistics function comes into the picture for delivery of the product. This involves order processing, packaging, transportation, tracking of product, etc. It ensures timely delivery of product to the customer at his/her doorstep. E-commerce firms need to make proper arrangement of logistic activities so that the right product is sent to customers on time. Delay in delivery of products can result in customer dissatisfaction.

8) **After-sales Service:** After timely delivery of products to customers, the firm undertakes after-sales service wherein it takes customer feedback about delivery, quality, services, overall experience, etc. The firms also make service calls in case of durable products. They solve the queries of customers and provide information about latest offers and other products via e-mail, calls and SMS. This allows the e-

commerce firms to maintain long-term relationship with customers and increase customer loyalty

1.1.5 FUNCTIONS OF E-COMMERCE

1) **E-Marketing:** E-Marketing (Electronic Marketing) is also known as Internet Marketing, Web Marketing, Digital Marketing, or Online Marketing. E-marketing is the process of marketing a product or service using the Internet. E-marketing not only includes marketing on the Internet, but also includes marketing done via e-mail and wireless media. It uses a range of technologies to help connect businesses to their customers. Internet marketing is associated with several business models i.e., B2C, B2B, C2C. Internet marketing is inexpensive when examine the ratio of cost to the reach of the target.

2) **E-Advertising:** It is also known as online advertising it is a form of promotion that uses internet and World Wide Web to deliver marketing messages to attracts customers. Example: Banner ads, Social network advertising, online classified advertising etc. The growth of these particular media attracts the attention of advertisers as a more productive source to bring in consumers.

3) **E-Banking:** It refers to any user with a personal computer and browser can get connected to his bank website to perform any of the banking functions. In internet banking system the bank has a centralized data base i.e., web-enabled. Best example for E-Banking is ATM. An ATM enables handling cash deposits, transfer, Balance enquiries, cash withdrawals, and pay bills.

Services through E-Banking:

- Bill Payment Service
- Fund Transfer
- Investing through Internet Banking
- Shopping

4) **E-Learning:** E-Learning comprises all forms of electronically supported learning and teaching. E-Learning applications and processes include web-based learning, computer-based learning. Content is delivered via. The internet, intranet/extranet, audio, or video tape, satellite TV. E-Learning is naturally suited to distance and flexible learning, but can also be used conjunction with face-to-face teaching. E-Learning can also refer to the educational website such as those offering learning scenarios worst and interactive exercises for children. A learning management system (LMS) is software used for delivering, tracking, and managing training /education.

5) **Mobile Commerce:** Mobile Commerce also known as M-Commerce is the ability to conduct, commerce as a mobile device, such as mobile phone. Banks and other financial institutions use mobile commerce to allow their customers to access account information and make

transactions, such as purchasing, withdrawals etc., Using a mobile browser or apps customers can shop online without having to be at their personal computer.

6) **Online Shopping:** Online shopping is the activity or action of buying products or services over the Internet. It means going online, landing on a seller's website, selecting something, and arranging for its delivery. The buyer either pays for the good or service online with a credit or debit card or upon delivery.

7) **Entertainment:** The conventional media that have been used for entertainment are Books/magazines, Radio, Television/films, Video games etc.

   Online books /newspapers, online radio, online television, online films, and online games are common place in internet where we can entertain. Online social networking websites are one of the biggest sources of E-entertainment for today's tech-savvy generation.

1.1.6 SCOPE OF E-COMMERCE

E-Commerce is a general concept covering any form of business transaction or information exchange executed using information and communication technologies ((ICT's). It includes electronic trading of goods, services and electronic material.

It takes place between companies, between companies and their customers or between companies and public administrations

1) **Electronic Markets**: An electronic market is the use of ICT where seller offers a range of good and services so that the buyer can compare the prices of the goods and services and make a purchase decision. e.g. Airline Booking System

2) **Electronic Data Interchange**: Electronic Data Interchange (EDI) is the computer-to-computer exchange of business documents in a standard electronic format between business partners. Th
the documents that are typically exchanged between b
most common documents exchanged via EDI are pu
invoices, payment document and advance ship notices. There is no need for printed orders and invoices & delays & errors in paper handling. It is used by organizations that make a large number of regular transactions. Eg. The exchange of EDI documents is typically between two different companies, referred to as business partners or trading partners. For example, Company A may buy goods from Company B. Company A sends orders to Company B.

3) **Internet Commerce**: Internet Commerce is the use of the Internet for all phases of creating and completing business transaction. This application is both for Business to Business (B2B) & Business to Consumer (B2C) transactions.

1.2 BENEFITS AND CHALLENGES OF E-COMMERCE

A) Benefits to E-Commerce Firms

1. **Global Reach:** With e-commerce, a company can reach out to the customers worldwide. Unlike physical stores where only a limited number of customers can be served, e-commerce allows firms to deliver products online to customers in any corner of the world.

2. **Small Investment:** E-commerce firms do not have to make investment to purchase land or rent or lease space for physical stores. E-commerce is operated online through websites. There are many domains which allow firms to create websites, which is less costly and far more convenient. The marketer has to only create a website to target their customers. Logistic functions can be outsourced by them. It reduces the need to make heavy investments and also provides quick return on investment (ROI) to marketers.

3. **Less Operating Costs:** In e-commerce business, there is no need to hire a large number of employees unlike physical stores. It reduces training cost, salaries etc. that have to be paid to employees. Due to opening an online store there is no need of payment of rent, utility bills and other miscellaneous expenses which can be incurred in physical stores. This results into less operating cost of e-commerce firms.

4. **Higher profit margin:** E-commerce offers benefit of global reach, so the marketer can reach to customers located all over the world. There is also large demand for the products from all over the world. There are no intermediaries like agents, wholesaler or retailer. Mostly the transactions are done directly between trader and customers. So the commission of intermediaries is eliminated. So all this contributes to

1.4 CONCEPTS OF OTHER MODELS OF E-COMMERCE

1) **B2B (Business-to-Business):** When a business sells goods and services to another business online, it is called B2B transaction.

   In simple, one company will sell products or services to other companies. (i.e.,) wholesale distributors will sell products or services to retailers.

   Normally this field includes the selling of goods that are not used by customers. For instance, businesses that manufacture products sold in Walmart stores are operating under a business to business e-commerce model because they are a business selling products to another business.

2) **B2C (Business-to-Consumer):** When a business sells goods or services to an individual consumer online, it is called B2C transaction. Here, the consumer can view details of products online and make purchase decision as per her/ his requirements. E.g. individual buying clothes, shoes, kitchenware, etc. specifically from Amazon or Flipkart. These days, consumer awareness is increasing about B2C e-commerce, because of factors like rapid use of internet facility, computer literacy, revolution in technology, etc.

   Further, the Indian market for e-commerce has grown at a fast pace in the past few years due to absence of major entry barriers and presence of few e-retailers (electronic retailers). Omni-Channel retailers such as Shoppers Stop, Reliance, Croma, etc. have also entered the e-commerce field to increase digital footprints.

3) **C2C (Consumer-to-Consumer):** When consumers sell their own products or services to other consumer, it is called C2C transactions.

Individuals may have new or used products that they sell on eBay to another individual. eBay is a great example of C2C e-commerce because consumers are interested in buying a used product for a cheaper price.

These websites are usually free of cost as they promote products and charge only nominal fees for doing it. Customers can upload images of their old furniture, electronic goods or other things along with description of products and their price. Other customers interested in buying that product can communicate with the seller and place the order.

5) **C2B (Consumer-to-Business):** Consumer-to-Business (C2B) is a business model where an end user or consumer makes a product or service that an organization uses to complete a business process or gain competitive advantage. The C2B methodology completely transposes (alters) the traditional Business-to-Consumer (B2C) model, where a business produces services and products for consumer consumption.

   Example - To describe this business model we will use YouTube as an example. Popular YouTubers (vlogers) sell their ad spaces to advertisers (Businesses). The YouTuber (vloger) is also paid to review the product or service through vlog, posts and videos.

6) **B2G (Business-to-Government):** B2G e-commerce is one where a business sells its product or service to the Government. Here is a government website that opens bids for businesses with an online bidding system. If the business provides an exact product, within the delivery time frame, and under the previous price, then the website awards the contract automatically to the lowest bidder.

What is eCommerce or electronic commerce security?

eCommerce security is the guideline that ensures safe transactions through the internet. It consists of protocols that safeguard people who engage in online selling and buying goods and services. You need to gain your customers' trust by putting in place eCommerce security basics. Such basics include:

- Privacy
- Integrity
- Authentication
- Non-repudiation

1. Privacy

Privacy includes preventing any activity that will lead to the sharing of customers' data with unauthorized third parties. Apart from the online seller that a customer has chosen, no one else should access their personal information and account details.

A breach of confidentiality occurs when sellers let others have access to such information. An online business should put in place at least a necessary minimum of anti-virus, firewall, encryption, and other data protection. It will go a long way in protecting credit card and bank details of clients.

2. Integrity

Integrity is another crucial concept of eCommerce Security. It means ensuring that any information that customers have shared online remains unaltered. The principle states that the online business is utilizing the customers' information as given, without changing anything. Altering any part of the data causes the buyer to lose confidence in the security and integrity of the online enterprise.

3. Authentication

The principle of authentication in eCommerce security requires that both the seller and the buyer should be real. They should be who they say they are. The business should prove that it is real, deals with genuine items or services, and delivers what it promises. The clients should also give their proof of identity to make the seller feel secure about the online transactions. It is possible to ensure authentication and identification. If you are unable to do so, hiring an expert will help a lot. Among the standard solutions include client login information and credit card PINs.

***Also Read:** Security Audit Services: Importance, Types, Top 3 Companies*

4. Non-repudiation

Repudiation means denial. Therefore, non-repudiation is a legal principle that instructs players not to deny their actions in a transaction. The business and the buyer should follow through on the transaction part that they initiated. eCommerce can feel less safe since it occurs in cyberspace with no live video. Non-repudiation gives eCommerce security another layer. It confirms that the communication that occurred between the two players indeed reached the recipients. Therefore, a party in that particular transaction cannot deny a signature, email, or purchase.

Why you can't afford to overlook eCommerce security?

While growth in eCommerce has improved online transactions, it has attracted the attention of the bad players in equal measures. eCommerce cybercrime reports reveal that the industry is among the most vulnerable ones when it comes to cybercrimes.

The eCommerce world experiences about 32.4% of all attacks. 50% of small eCommerce store owners are lamenting that the attacks are becoming severe. Furthermore, the reports show that 29% of traffic accessing a website consists of malicious requests.

Such attacks have contributed to significant losses in financials, market shares, and reputation. Almost 60% of small eCommerce stores that experience cybercrimes don't survive more than six months.

Therefore, it is very crucial to put in place water-tight security measures and hire a robust team. It will ensure you run your business without worrying about closing down due to cybercriminals.

Common Ecommerce Security Issues

1. Lack of trust in the privacy and eCommerce security

Businesses that run eCommerce operations experience several security risks, such as:

- **Counterfeit sites**– hackers can easily create fake versions of legitimate websites without incurring any costs. Therefore, the affected company may suffer severe damage to its reputations and valuations.
- **Malicious alterations to websites**– some fraudsters change the content of a website. Their goal is usually to either divert traffic to a competing website or destroy the affected company's reputation.
- **Theft of clients' data**– The eCommerce industry is full of cases where criminals have stolen the information about inventory data, personal information of customers, such as addresses and credit card details.
- **Damages to networks of computers**– attackers may damage a company's online store using worm or viruses attacks.
- **Denial of service**– some hackers prevent legit users from using the online store, causing a reduction in its functioning.
- **Fraudulent access to sensitive data**– attackers can get intellectual property and steal, destroy, or change it to suit their malicious goals.

2. Malware, viruses, and online frauds

these issues cause losses in finances, market shares, and reputations. Additionally, the clients may open criminal charges against the company. Hackers can use worms, viruses, Trojan horses, and other malicious programs to infect computers and computers in many different ways. Worms and viruses invade the systems, multiply, and spread. Some hackers may hide Trojan horses in fake software, and start infections once the users download the software. These fraudulent programs may:

- hijack the systems of computers
- erase all data
- block data access
- forward malicious links to clients and other computers in the network.

3. Uncertainty and complexity in online transactions

Online buyers face uncertainty and complexity during critical transaction activities. Such activities include payment, dispute resolution, and delivery. During those points, they are likely to fall into the hands of fraudsters.

Businesses have improved their transparency levels, such as clearly stating the point of contact when a problem occurs. However, such measures often fail to disclose fully the collection and usage of personal data.

Also Read: ***SaaS Security Management- A Complete Guide To 6 Best Security Practices***

E-commerce website security measures to cover you 24/7

1. Use Multi-Layer Security

It is helpful to employ various security layers to fortify your security. A Content Delivery Network (CDN) that is widespread can block DDoS threats and infectious incoming traffic. They use machine learning to keep malicious traffic at bay.

Source: NIST

You can go ahead and squeeze in an extra security layer, such as Multi-Factor Authentication. A two-factor authentication is a good example. After the user enters the login information, they instantly receive an SMS or email for further actions. By implementing this step, it blocks fraudsters as they will require more than just usernames and passwords to access the legit users' accounts. However, hacking can still occur even if an MFA is in place.

> *Most companies that use MFA are still successfully hacked.*
>
> — Roger Grimes, 2018

2. Get Secure Server Layer (SSL) Certificates

One of the primary benefits of SSL Certificates is to encrypt sensitive data shared across the internet. It ensures that the information reaches only the intended person. It is a very crucial step because all data sent will pass through multiple computers before the destination server receives it.

Image Source: Comodo

If SSL certificate encryption is absent, any electronic device between the sender and the server can access sensitive details. Hackers can thus take advantage of your exposed passwords, usernames, credit card numbers, and other information. Therefore, the SSL certificate will come to your aid by making the data unreadable to unintended users.

2. Use solid-rock Firewalls

Use effective e-commerce software and plugins to bar untrusted networks and regulate the inflow and outflow of website traffic. They should provide selective permeability, only permitting trusted traffic to go through.

You can trust the Astra firewall to stop Spam, XSS, CSRF, malware, SQLi, and many other attacks on your website. It ensures that the only traffic that accesses your eCommerce store consists of the real users. Moreover, we have specialized WAF solutions for WordPress, Magento, Opencart, Prestashop, Drupal, Joomla, and custom made PHP sites.

In a nutshell, the Astra firewall protection from:

- OWASP top 10 threats
- Protection from bad bots.
- Spam protection.
- Protection against 100+ types of attacks.

How does the Astra Firewall work?

3. Anti-Malware Software

Your electronic devices, computer systems, and web system need a program or software that detects and block malicious software, otherwise known as malware. Such protective software is called Anti-malware software. An effective anti-malware should render all the hidden malware on your website.

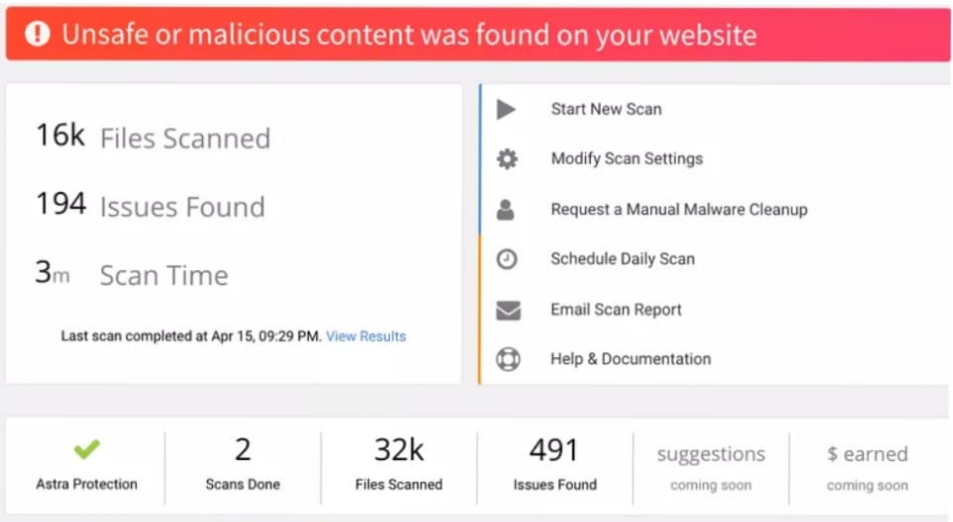
One such scanner is the Astra Malware Scanner. It scans your web system for all malicious software round the clock and is at your disposal It also lets you automate your scans with its "Schedule a Scan" feature. You can schedule the scans daily, weekly, monthly or fortnightly.

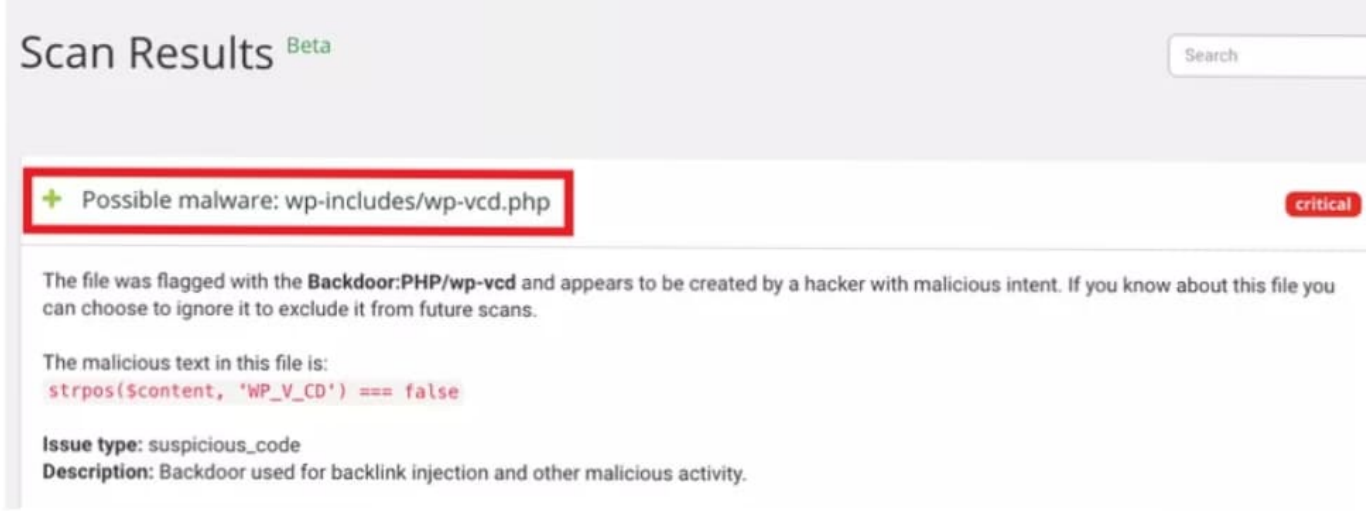
Related Blog – Astra's Sample Penetration Testing Report

With Astra Scanner, you can enjoy:

- unlimited scans
- Notifications in case of any changes in file
- scanning powered by machine learning.
- collective intelligence

It is capable of cleaning malware like credit card hack, Japanese spam, pub2srv, Pharma attacks, and malicious redirects.





WP-VCD malware flagged by Astra's Malware Scanner

4. Comply with PCI-DSS Requirements

Make it a routine to maintain the Payment Card Industry Data Security Standard (PCI-DSS) to protect all credit card data. All businesses that handle credit card transactions need to follow these requirements:

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI-DSS Requirements; Source: Medium

Conclusion

Businesses should employ several eCommerce security measures and protocols to keep security threats at bay all the time. Apart from the basic authentication systems like username and passwords, SSL, multi-factor authentication is essential.

Top 10 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. There are various kinds of financial frauds prevalent in the e-commerce industry, but we are going to discuss the two most common of them.

a. Credit Card Fraud

It happens when a cybercriminal uses stolen credit card data to buy products on your e-commerce store. Usually, in such cases, the shipping and billing addresses vary. You can detect and curb such activities on your store by installing an AVS – Address Verification System.

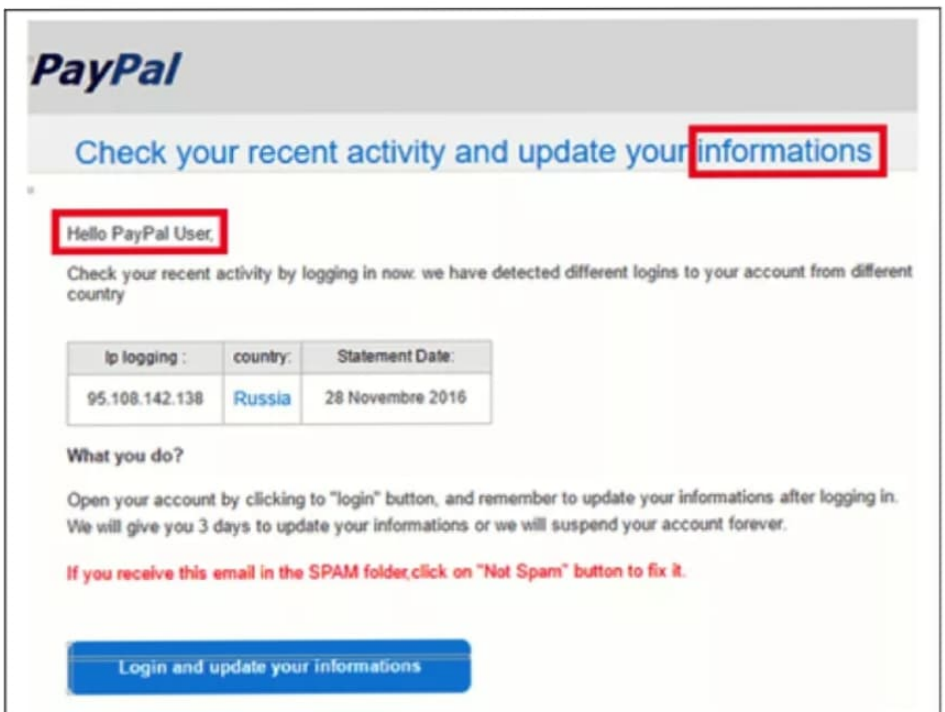
Another form of credit card fraud is when the fraudster steals your personal details and identity to enable them to get a new credit card.

b. Fake Return & Refund Fraud

The bad players perform unauthorized transactions and clear the trail, causing businesses great losses. Some hackers also engage in refund frauds, where they file fake requests for returns.

2. Phishing

Several e-commerce shops have received reports of their customers receiving messages or emails from hackers masquerading to be the legitimate store owners. Such fraudsters present fake copies of your website pages or another reputable website to trick the users into believing them. For example, see this image below. A seemingly harmless and authentic email from PayPal asking to provide details.



3. Spamming

Some bad players can send infected links via email or social media inboxes. They can also leave these links in their comments or messages on blog posts and contact forms. Once you click on such links, they will direct you to their spam websites, where you may end up being a victim.

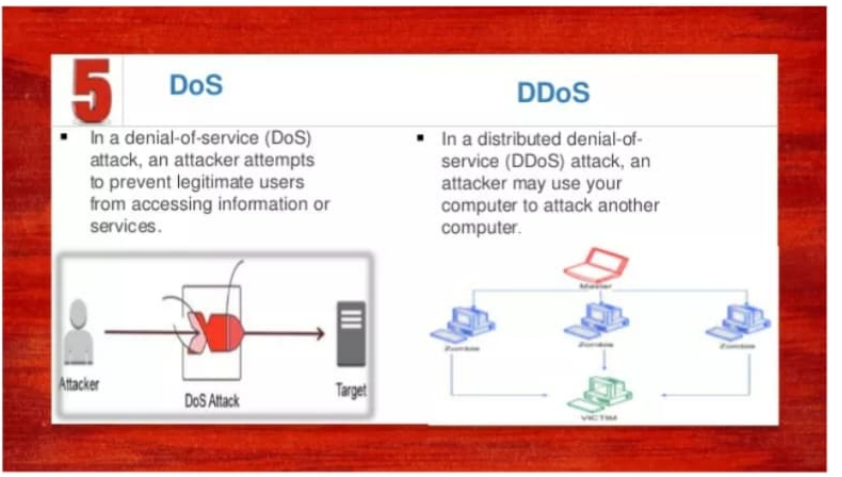
> Mass-mailed malware infection can quickly morph into a much more serious problem

says Brian Krebs, data security expert.

Apart from lowering your website security, spamming also reduces its speed and severely affects performance.

4. DoS & DDoS Attacks

Many e-commerce websites have incurred losses due to disruptions in their website and overall sales because of DDoS (Distributed Denial of Service) attacks. What happens is that your servers receive a deluge of requests from many untraceable IP addresses causing it to crash and making unavailable to your store visitors.



Source: Slideshare.net

5. Malware

Hackers may design a malicious software and install on your IT and computer systems without your knowledge. These malicious programs include spyware, viruses, trojan, and ransomware.

The systems of your customers, admins, and other users might have Trojan Horses downloaded on them. These programs can easily swipe any sensitive data that might be present on the infected systems and may also infect your website.

6. Exploitation of Known Vulnerabilities

Attackers are on the lookout for certain vulnerabilities that might be existing in your e-commerce store.
Often an e-commerce store is vulnerable to SQL injection (SQLi) and Cross-site Scripting (XSS).
Let's take a quick look at these vulnerabilities:

a. SQL Injection

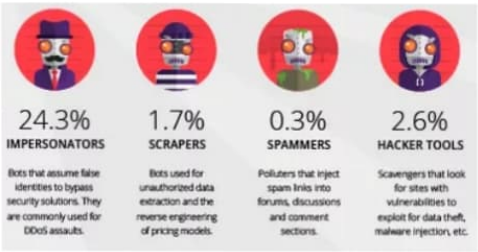
It is a malicious technique where a hacker attacks your query submission forms to be able to access your backend database. They corrupt your database with an infectious code, collect data, and later wipe out the trail.

b. Cross-Site Scripting (XSS)

The attackers can plant a malicious JavaScript snippet on your e-commerce store to target your online visitors and customers. Such codes can access your customers' cookies and compute. You can implement the Content Security Policy (CSP) to prevent such attacks.

7. 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.



Bad bots classification; Source: bizreport.com

8. Brute force

The online environment also has players who can use brute force to attack your admin panel and crack your password. These fraudulent programs connect to your website and try out thousands of combinations in an attempt to obtain you site's passwords. Always ensure to use strong, complex passwords that are hard to guess. Additionally, always change your passwords frequently.

9. Man in The Middle (MITM)

A hacker may listen in on the communication taking place between your e-commerce store and a user. Walgreens Pharmacy Store experienced such an incident. If the user is connected to a vulnerable Wi-Fi or network, such attackers can take advantage of that.

10. e-Skimming

E-skimming involves infecting a website's checkout pages with malicious software. The intention is to steal the clients' personal and payment details.

Are you an e-commerce business person? Don't downplay the seriousness of these e-commerce security threats.

E-commerce security solutions that can ease your life

1. HTTPS and SSL certificates

HTTPS protocols not only keep your users' sensitive data secure but also boost your website rankings on Google search page. They do so by securing data transfer between the servers and the users' devices. Therefore, they prevent any interception.

Do you know that some browsers will block visitors' access to your website if such protocols are not in place? You should also have an updated SSL certificate from your host.

2. Anti-malware and Anti-virus software

An Anti-Malware is a software program that detects, removes, and prevents infectious software (malware) from infecting the computer and IT systems. Since malware is the umbrella term for all kinds of infections including worms, viruses, Trojans, etc getting an efficient Anti-Malware would do the trick.

On the other hand, Anti-Virus is a software that was meant to keep viruses at bay. Although a lot of Anti-virus software evolved to prevent infection from other malware as well. Securing your PC and other complementary systems with an Anti-Virus keeps a check on these infections.

3. Securing the Admin Panel and Server

Always use complex passwords that are difficult to figure out, and make it a habit of changing them frequently. It is also good to restrict user access and define user roles. Every user should perform only up to their roles on the admin panel. Furthermore, make the panel to send you notifications whenever a foreign IP tries to access it.

4. Securing Payment Gateway

Avoid storing the credit card information of your clients on your database. Instead, let a third party such as PayPal and Stripe handle the payment transactions away from your website. This ensures better safety for your customers' personal and financial data. Did you know storing credit card data is also a requirement for getting PCI-DSS compliant?

5. Deploying Firewall

Effective firewalls keep away fishy networks, XSS, SQL injection, and other cyber-attacks that are continuing to hit headlines. They also help in regulating traffic to and from your online store, to ensure passage of only trusted traffic.

6. Educating Your Staff and Clients

Ensure your employees and customers get the latest knowledge concerning handling user data and how to engage with your website securely. Expunge former employees' details and revoke all their access to your systems.

7. Additional security implementations

- Always scan your websites and other online resources for malware
- Back up your data. Most e-commerce stores also use multi-layer security to boost their data protection.
- Update your systems frequently and employ effective e-commerce security plugins.
- Lastly, get a dedicated security platform that is secure from frequent cyber-attacks. You can read more about the security steps you need to take for your e-commerce store.

Astra Solutions to E-commerce Security Threats

Astra is among the leading providers of security solutions that enable e-commerce to enjoy uninterrupted business.

Our tested and proven web application firewall keeps away Bad Bots, Spam, SQL injections, XSS, and many other cyber threats. It works in real-time, ensuring your website is secure 24 hours per day, seven days every week. The firewall is intelligent enough to detect any unusual and malicious intent. It does so by monitoring the traffic patterns of everything that gets out and into your e-commerce store.

How does the Astra Firewall work?

We can also help you get rid of malware, malicious redirects, pharma attacks, and other similar threats with a record turnaround time. You can employ our intelligent malware scanner to detect any malware yourself and track changes in your files daily. We log any change in your codes for you to review and stay updated. Our machine learning intelligence powers all the scanning to ensure we don't miss anything.

NETWORK SECURITY

Network Security

- Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations.
- An effective network security strategy requires **identifying threats** and then **choosing the most effective set of tools to combat them.**

WHAT IS NETWORK SECURITY?

- Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

Network Security

- Today's system/network administration **should includes security** related activities such as patch management, OS, host and device hardening and network vulnerability assessment.
- System/Network Administrators **should be ready** to perform those related activities to protect and prevent from malicious hackers, external and internal attacks.
- Responsibilities of the System/Network Administrators **should not only limited** to managing and administering the existing system/network, security should be added since it's vital to protect the organization's assets (data, information and IP).

Threats to Network Security

- **Viruses**
  Computer programs written by devious programmers and designed to replicate themselves and infect computers when triggered by a specific event.
- **Trojan Horses Programs**
  Delivery vehicles for destructive code, which appear to be harmless or useful software programs such as games.
- **Vandals**
  Software applications or applets that cause destruction.

Threats to Network Security

- **Attacks**
  - **Reconnaissance attacks**
    Information-gathering activities to collect data that is later used to compromise networks.
  - **Access attacks**
    Exploit network vulnerabilities in order to gain entry to e-mail, databases, or the corporate network.
  - **Denial-of-service (DoS) attacks**
    Prevent access to part or all of a computer system.

Threats to Network Security

- **Data Interception**
  Involves eavesdropping on communications or altering data packets being transmitted.
- **Social Engineering**
  Obtaining confidential network security information through nontechnical means, such as posing as a technical support person and asking for people's passwords.

Virtual Private Networks (VPN)

- Virtual Private Networks (VPN) provide access control and data encryption between two different computers on a network.
- VPN allows remote workers to connect to the network without the risk of a hacker or thief intercepting data.

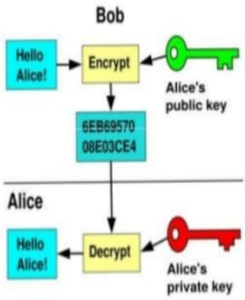
Firewalls

- Firewalls are access control devices for the network and can assist in protecting an organization's internal network from external attacks.
- By their nature, firewalls are border security products, meaning that they exist on the border between the internal network and the external network.
- Properly configured, firewalls have become a necessary security device.

Encryption

- Encryption is the primary mechanism for communications security. It will certainly protect information in transit.
- Encryption might even protect information that is in storage by encrypting files. However, legitimate users must have access to these files.
- The encryption system will not differentiate between legitimate and illegitimate users if both present the same keys to the encryption algorithm. Therefore, encryption by itself will not provide security.
- There must also be controls on the encryption keys and the system as a whole.

Encryption



Module 1 : Threats & Risk Management

Home

12.2 The Need for Security

- Data from Computer Security Institute and FBI indicate:
  - Cyber attacks are on the increase
  - Internet connections are increasingly a point of attack
- The variety of attacks is on the rise
- The reporting of serious crimes to law enforcement has declined

- According to the statistics reported to CERT/CC over the past year (CERT/CC 2002)
  - The number of cyber attacks skyrocketed from approximately 22,000 in 2000 to over 82,000 in 2002
  - First quarter of 2003 the number was already over 43,000

7

12.4 Basic Security Issues

Issues at a simple marketing site:

- **User's perspective**
  - Is Web server owned and operated by legitimate company?
  - Web page and form contain some malicious code content?
  - Will Web server distribute the user's information to another party?
- **Company's perspective**
  - Will the user attempt to break into the Web server or alter the site?
  - Will the user try to disrupt the server so it isn't available to others?
- **User and company perspective**
  - Is network connection free from eavesdropping?
  - Has information sent back and forth between server and browser been altered?

9

12.5 Type of Threats and Attacks *(Cont.)*

Technical attack:

An attack perpetrated using software and systems knowledge or expertise

The players
- Hackers
- Crackers
- Script kiddies

- Systems and software bugs and misconfigurations
- Distributed Denial-of-service (DDoS) attacks
- Malicious code
  - Viruses
  - Worms
  - Macro viruses and macro worms
  - Trojan horses

13

13.6 Security Risk Management

- Common mistakes in managing their security risks (McConnell 2002):
  - **Undervalued information**
  - **Narrowly defined security boundaries**
  - **Reactive security management**
  - **Dated security management processes**
  - **Lack of communication about security responsibilities**

- *Security risk management:*

  A systematic process for determining the likelihood of various security attacks and for identifying the actions needed to prevent or mitigate those attacks

- Required to determine security needs
  - **4 phases of risk management**
    - Assessment
    - Planning
    - Implementation
    - Monitoring

- Definitions involved in risk management
  - **Assets**—anything of value worth securing
  - **Threat**—eventuality representing danger to an asset
  - **Vulnerability**—weakness in a safeguard

13.6 Security Risk Management *(cont.)*

- *Assessment phase*

  evaluation of assets, threats, vulnerabilities
  - Determine organizational objectives
  - Inventory assets
  - Delineate threats
  - Identify vulnerabilities
  - Quantify the value of each risk

- *Planning phase of risk management*

  arrive at a set of security policies
  - Define specific policies
  - Establish processes for audit and review
  - Establish an incident response team and contingency plan

13.6 Security Risk Management *(cont.)*

- *Implementation phase of risk management*

  choose particular technologies to deal with high priority threats

- *Monitoring phase of risk management*

  ongoing processes used to determine which measures are successful, unsuccessful and need modification

Securing EC Communication

- *Authentication system:*
  System that identifies the legitimate parties to a transaction, determines the actions they are allowed to perform, and limits their actions to only those that are necessary to initiate and complete the transaction

Biometric systems:
Authentication systems that identify a person by measurement of a biological characteristic such as a fingerprint, iris (eye) pattern, facial features, or voice
  - Physiological biometric (fingerprint, iris, voice)
  - Behavioral biometric (keystroke monitoring)

Encryption:
The process of scrambling (encrypting) a message in such a way that it is difficult, expensive, or time-consuming for an unauthorized person to unscramble (decrypt) it

Security Protocol

- *Secure Socket Layer (SSL):*
  Protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality
- *Transport Layer Security (TLS):*
  As of 1996, another name for the SSL protocol
- *Secure Electronic Transaction (SET):*
  A protocol designed to provide secure online credit card transactions for both consumers and merchants; developed jointly by Netscape, Visa, MasterCard, and others

Securing EC Networks

- ***Firewall:*** A network node consisting of both hardware and software that isolates a private network from a public network
- ***Virtual private network (VPN):*** A network that uses the public Internet to carry information but remains 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

Types of E-commerce Contract

There are 4 types of E-commerce Contract

1. Electronic Contract
2. Shrink Wrap Contract
3. Click Wrap or Web Wrap Contract
4. Browse Wrap Contract

1st type : Electronic Contract

An e-contract is an agreement created and "signed" in electronic form—no paper is used.

An example is a contract that you write on your computer and email to a business associate and that the business associate emails back with an electronic signature indicating acceptance.

An e-signature is a digital file or symbol—such as a scanned pen-and-ink signature or a typed name—that someone attaches to or places on a contract or file to show that person's intent to sign the contract or file.

Definition

- **E- Contract**- a contract that is entered into in cyberspace and is evidenced only by electronic impulses (such as those that make up a computer's memory), rather than, for example, a typewritten form.
- Contract law forms the basis for most commercial activity and for business in general.
- E –commerce is a growing part of this commercial activity, with business –to- business (B2B) transactions estimated to soon exceed to a trillion dollars annually.

Meaning

E-contract is any kind of contract formed in the course of e-commerce by the interaction of **two or more individuals** using electronic means, such as e-mail, the interaction of an **individual with an electronic agent**, such as a computer program, or the interaction of at least **two electronic agents** that are programmed to recognize the existence of a contract.

E-contract is a contract modelled, specified, executed and deployed by a software system[4].

The 2 main parties to an e-contract are- The **Originator** and the **Addressee**.

- **Originator** according to the IT Act, 2008 is a person who sends, generates, stores or transmits any electronic message to be sent, generated, stored or transmitted to any other person and does not include an Intermediary.

An **Addressee** according to the IT Act, 2008 is a person who is intended by the originator to receive the electronic record but does not include any Intermediary.

2nd type : Shrink Wrap Contract

Meaning of Shrink Wrap Contract

A Shrink Wrap agreement can be defined as a legal agreement that is packaged within a product. In this type of agreement, products are sealed or enclosed in shrink wrap (plastic wrap) implying that the goods (and thus the legal document) can only be viewed by the customer who purchases it.

The Shrink wrap agreement generally includes specific terms and conditions of the product or purchase, such as price of products, warranties, right of use and guideline, limitations and licenses as the case may be.

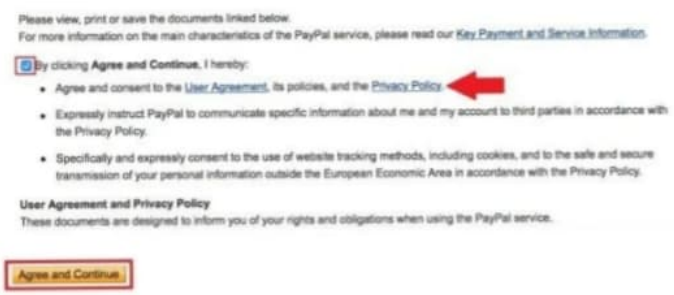
3rd type : Click wrap or Web wrap contract

Meaning

A clickwrap agreement is a type of contract that is widely used with software licenses and online transactions in which a user must agree to terms and conditions prior to using the product or service.

The format and content of clickwrap agreements vary by vendor. However, most of clickwrap agreements require the consent of end users by clicking an "OK," "I Accept" or "I Agree" button on a pop-up window or a dialog box. The user may reject the agreement by clicking the Cancel button or closing the window. Once rejected, the user us unable to use the service or product.

Examples of "Click to accept"



4th type : Browse wrap contract

Meaning

Browse-wrap agreements cover the access to or use of materials available on a website or downloadable product. Only if the person agrees to the terms and conditions on the web page, then he can access the contents of the web page.

In most cases, the website or the Browse-wrap includes a statement that the user's continued use of the website or the downloaded software manifests assents to those terms. Many times, the terms mentioned in the Browse-wrap are explicitly displayed on the website but the existence of such browse wrap is hidden or not seen on the page.