



JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

How does Cybersecurity affect in E-Commerce sites

Nair Remya Rajendran

Guide : Asst. Prof. Gauri Ansurkar

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India, First Semester, Department of Information Technology
University of Mumbai, Mumbai

remyanair.model@gmail.com

Abstract— E-commerce or Electronic commerce helps the enterprises in reducing prices, getting larger market and improving relationships between customers and vendors. Simultaneously, some new risks and threats have appeared, like as, mutual trust, protected innovation, intellectual property, network attacks and so on. E-commerce security is the process of web based business resources from illegal access, use, modification, or annihilation. E-Commerce offers the online trade gigantic number of opportunities, yet it makes an arrangement for a set of new risks and vulnerability such as security threats especially when e-commerce has flourished in this pandemic. The paper shows in time currently where we are and how digital wrongdoing has made its place with regards to the past and the Covid-19 pandemic. This paper also analyzes the classification of threats and preventive measures to help their security.

Keywords— E-commerce, Cybersecurity, Security mechanism, Security issues, Threats and Vulnerabilities.

I. INTRODUCTION



Fig 1. Cybersecurity in E-commerce

E-commerce is referred to as the offering and purchase of services over the Internet. One of the crucial success factors of web based business is its security. Without the assurance of security, e-commerce may not work usually. As we all know, the e-commerce industry of India has taken a boom

especially during this lockdown period, each lockdown faced a new change, so first of all we will discuss about e-commerce and then the changes occurred in the different phases so what is ecommerce in layman language.

II. WHY CYBERSECURITY IS SO IMPORTANT FOR ECOMMERCE?

Cyber security is vital in e-commerce as a result of cyberattacks will cause loss of revenue, knowledge and therefore the full practicality of companies. Cyber criminals use advanced techniques to steal information from businesses. With e-commerce, it is not simply your knowledge that you simply defend. It's your client knowledge that you simply have to remember of. Violations of your cyber security system may mean the loss of your client information which will ruin your business's trust and name.

III. SECURITY ISSUES

E-commerce business security is the fortification of e-commerce business resources from illegal access, utilization, alteration, or annihilation. Although security features do not assure a protected framework, they are essential to put up a secure system. Security features like Authentication, Authorization, Encryption, Auditing, Non repudiation, Availability, Integrity and so forth are a must for a system to work correctly. Three types of security threats exists they are

1. Denial of service (DOS)
2. Unauthorized access
3. Fraud and theft
4. Digital Signature

1. Denial of Service (DOS) :

Two major types of DOS attacks: spamming and viruses. Spamming is sending spontaneous business messages to people, E-mail bombing caused by a hacker targeting

one computer or network, and sending a huge number of email messages to it. Surfing includes programmers, hackers placing software agents onto an outsider framework and setting it off to send requests to an expected target.

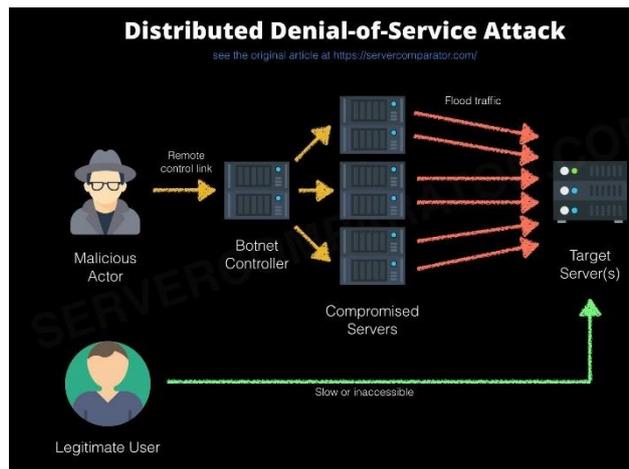


Fig 2. DOS and DDOS Attack

2. Unauthorized access

The Illegal access to frameworks, systems, applications, information or data, Passive unauthorized access – listening to communications channel for discovering privileged insights. It might utilize content for destructive purposes, Changes intent of messages, e.g., to prematurely end or postpone a negotiation on a transaction. Masquerading or spoofing – sending a message that appears to be from someone else.

3. **Theft or Fraud** occurs when the stolen information is utilized or adjusted. Theft of software through illegal replicating from organization's servers. Robbery of equipment, specifically laptops or workstations is also among the major security threat.

4. A **digital signature** means giving a unique identify to your message. Actually, it is a process of encrypting the message with the private specifically used for verification purpose. The linkage between data and the signature doesn't allow any alteration and if anyhow data is altered signature is automatically invalidated. Thus digital signature helps in maintaining the confidentiality of the data.



Fig 3. Digital Signature

To analyse the significance of E-commerce security.

- ♣ To analyse and examine the purpose of Security in E-commerce.

- ♣ To identify the involvement of outsider hazard in Online Shopping.

IV. SECURE ONLINE SHOPPING GUIDELINES

1. Shop at Secure Web Sites :

How can we check whether a Web site is secure or not? Secure websites utilize encryption techniques to exchange data or information from your computer to the online trader's website. Here's the manner by which you can tell when you are working with a secure website:

- If you look at the address bar of your browser where the Web site address is shown, you are supposed to see https://. The "s" that is shown after "http" demonstrates that the Website is secure. Normally, you don't see the "s" until the point that you really move to the order page of the Website.
- Another approach to find out whether a Web site is secure is to search for a shut lock displayed on the address bar of the website. If that lock is modifiable, you should presume it is not a safe website.

2. Research the Web Site before :

You Order Work with organizations you already know. In the event that the organization is new, do your homework before purchasing their items. If you decide to buy something from an obscure organization, start with a low-priced order to learn if the organization is reliable. Dependable organizations ought to advertise their physical business address and at least one telephone number, either customer service or a helpline.

3. Read the Web Site's Privacy and Security Policies :

Every trustworthy online Website provides data about the manner it processes your request. It is typically recorded in the area entitled —Privacy Policy. You can check out whether the vendor expects to share your data with a third party or associate organizations. Do they ensure these organizations to abstain from marketing to their customers? If not, you can anticipate to get spammed and even post or telephone requests from these organizations.

4. Know about Cookies and Behavioral Marketing :

Online vendors as well as other websites try to keep a watch on our shopping and surfing behavior by using "cookies," an online tracking system that appends bits of code to our web browsers to follow and track which websites we look through the internet. "Persistent" cookies stay put on your PC while "session" cookies do expire when you close the web browser. Online vendors utilize cookies to remember you and accelerate the shopping process whenever you visit the next time.

5. Address and Card Verification System:

Research Objectives :

An Address or a Card Verification Value is a great way to weed out the possibilities of fraudulent charges. It is a win-win situation for you as well as your customers. The CVV is the three or four digit number that is imprinted on the back of user's credit or debit card. The user and none else has access to it. Combined with One Time Password, it is a formidable security measure that can prevent online credit card information leaks. Asking for direct input of CVV on checkout has become a default process for most online stores. It ensures that only those payments which the customer sanctioning is getting through.

6. Training and Awareness for Employees:

When it comes to organizational information security, employees seem to be careless in practicing password hygiene and safety. We all have that colleague in our office, who keeps the username and password in broad daylight to be seen by all. Nothing could be more dangerous than this. This login credentials in wrong hands can spell doom to the entire organization. It is never too late to make your employees aware of the pitfalls in sharing passwords, login credentials, use of USB devices, unsecured networks, etc. Even if they are shared, they must be immediately replaced with a new password to sustain security.

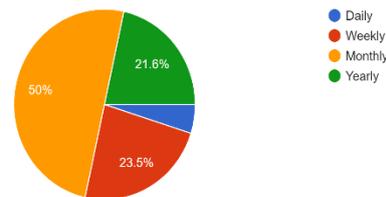
V. COVID-19 HAS CHANGED ONLINE SHOPPING FOREVER

The pandemic has quickened the move towards a more computerized world and set off changes in web-based shopping practices that are probably going to have enduring impacts. The COVID-19 pandemic has perpetually changed internet shopping practices, as indicated by a study of around 3,700 buyers in nine arising and created economies. The review, named "Coronavirus and E-business", analyzed how the pandemic has changed the manner in which shoppers use web based business and advanced arrangements. Following the pandemic, the greater part of the study's respondents currently shop online all the more often and depend on the web more for news, wellbeing related data and computerized amusement. Purchasers in arising economies have made the best move to web based shopping, the overview shows. "The COVID-19 pandemic has quickened the move towards a more computerized world. The progressions we make presently will have enduring impacts as the world economy recuperates," said UNCTAD Secretary General Mukhisa Kituyi. He said the quickening of internet shopping universally underscores the desperation of guaranteeing everything nations can take advantage of the lucky breaks offered by digitalization as the world moves from pandemic reaction to recuperation.

Public Survey

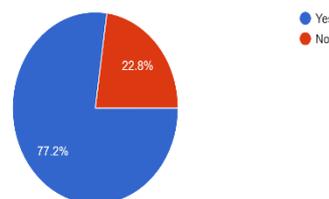
How often do you make an online shopping?

How often do you make an online shopping?
102 responses



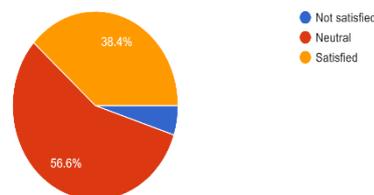
Has there been any increase in your online shopping during the lockdown period?

Has there been any increase in your online shopping during the lockdown period?
101 responses



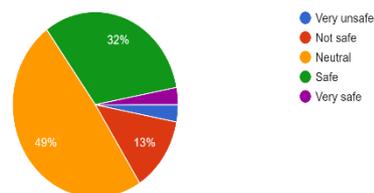
How satisfied are you with the quality and availability of the products?

How satisfied are you with the quality and availability of the products?
99 responses



How safe do you feel while sharing your credit card details?

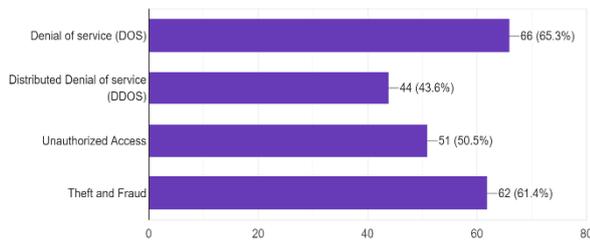
How safe do you feel while sharing your credit card details?
100 responses



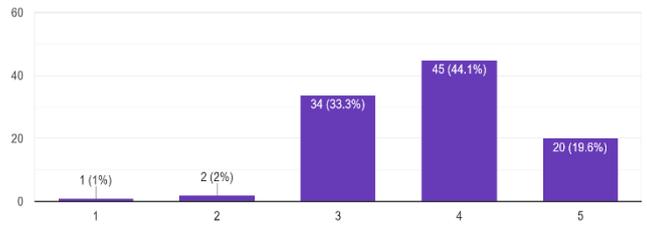
From the below mentioned day-to-day attacks, select the ones which you are aware of.

VI. FIGURES AND RESULTS

From the below mentioned day-to-day attacks, select the ones which you are aware of.
101 responses

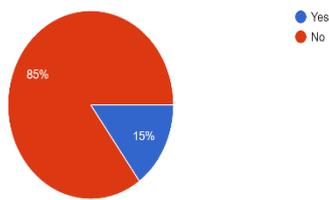


On a scale of 1-5, kindly rate your opinion regarding ecommerce sites.
102 responses



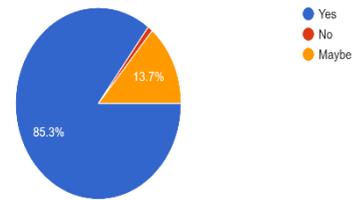
Have you ever experienced any sort of cyber security attack till date when made an online purchase?

Have you ever experienced any sort of cyber security attack till date when made an online purchase?
100 responses



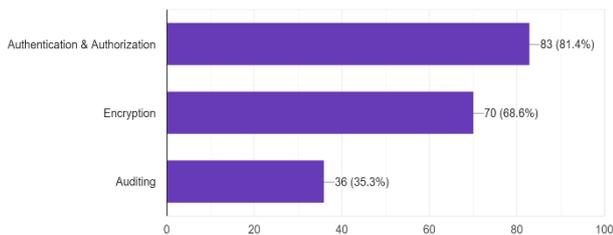
So, do you think that creating an awareness about the cybersecurity issues over E-commerce websites is both mandatory and helpful?

So, do you think that creating an awareness about the cybersecurity issues over E-commerce websites is both mandatory and helpful?
102 responses



From the below mentioned security features, select the ones which you are aware of.

From the below mentioned security features, select the ones which you are aware of.
102 responses

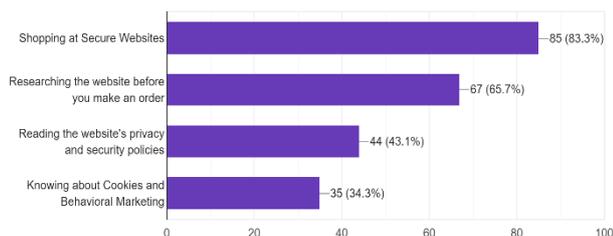


VII. HYPOTHESIS TESTING

Hypothesis testing is a sort of statistical reasoning that includes analysing data from a sample to derive inferences about a population parameter or probability distribution. First, a hypothesis is created regarding the parameter or distribution. This is known as the null hypothesis, abbreviated as H_0 . After that, an alternative hypothesis (denoted H_a) is defined which is the polar opposite of the null hypothesis. Using sample data it determines whether H_0 is accepted or rejected. The conclusion states that the alternative hypothesis H_a goes true if H_0 is rejected.

Amongst all the below steps, which of the following ones you perform before making an online purchase?

Amongst all the below steps, which of the following ones you perform before making an online purchase?
102 responses



So, in this paper,
Null Hypothesis (H_0) : No awareness and use of ecommerce sites.

Alternative Hypothesis (H_1) : Make awareness and use of ecommerce sites.

There are 3 tests based on which we can determine that our hypothesis is true or not :

1. Chi – squared test
2. T – test
3. Fisher’s Z test

In this paper, we will be using a 2 tailed T-test.

A T-test is an inferential statistic that determines if there is a significant difference in the means of two groups that are related in some manner.

On a scale of 1-5, kindly rate your opinion regarding ecommerce sites.

- **Level of Significance**

The chance of rejecting the null hypothesis when its true is the significance level i.e. A significance level of 0.05 means that there’s a 5% probability of discovering

a difference. Lower significance levels indicates that more evidences will be required to reject the hypothesis.

- **Level of Confidence**

The confidence level indicates that the probability of a statistical parameter measured in a sample survey is also true for the entire crowd.

Sr. No.	Data
1	50
2	77.2
3	56.6
4	49
5	66
6	85
7	83
8	85
9	45
10	85.3
Mean (x)	68.21
Standard Deviation (s)	16.781104

Level of Significance = 0.05 i.e. 5%

Level of Confidence = 95%

The formula to find t-score is:

$$t = (x - \mu) / (s / \sqrt{n})$$

where x is the sample mean,

μ is the hypothesized mean,

s is the sample standard deviation, and n is the sample size.

The p-value, also known as the probability value, indicates how probable your data is to have happened under the null hypothesis. Once we know the value of t, we can find the corresponding p-value. If the p-value is less than some alpha level (common choices are .01, .05, and .10) then we can reject the null hypothesis and conclude that 5G is a Boon..

Calculation of t-value:

Step 1: Determine what the null and alternative hypotheses are.

Null hypothesis (H₀): No awareness and use of ecommerce sites.

Alternative hypothesis (H_a): Make awareness and use of ecommerce sites.

Step 2: Find the test statistic.

In this case, the hypothesized mean value is considered 0.

$$t = (x - \mu) / (s / \sqrt{n}) = (68.21 - 0) / (16.781104 / \sqrt{10}) = 12.853$$

$$t\text{-value} = 12.853$$

Calculation of p-value:

Step 3: Calculate the test statistic's p-value.

The t-Distribution table with n-1 degrees of freedom is used to calculate the p-value. In this paper, the sample size is n = 10, so n-1 = 9.

By plugging the observed value in the calculator, it returns a p-value. In this case, the p-value returned is less than 0.00001.

Since this p-value is less than our chosen alpha level of 0.05, we can reject the null hypothesis. Thus, we have sufficient evidence to say that we need to make awareness and use of ecommerce sites.

VIII. CONCLUSION

So, as per the public survey and all the testings we, hereby conclude that ecommerce is good to a great extent but just we need to be more concerned about the threats and vulnerabilities. It is a shocking truth that the society will take a long time to recover from the COVID-19 pandemic. Coronavirus has carried alongside it huge episodes of confusion and madness. These things massively affected the psychological condition of people and the Cybersecurity scene changed enormously, practically overnight.

IX. FUTURE SCOPE

As we all know that a coin has got its both sides and all the things in our lives has got its own pros and cons. Similarly, the ecommerce sites has got a lot of good points because it has made our shopping more comfortable, just with one click our order and payment is made simultaneously. However, it also has got some drawbacks and that is the cybersecurity issues. And because nowadays, especially the online purchase has increased, so the thefts and frauds. But we can overcome all this if done wisely. For that, we must first be aware of the thefts that's been happening in our society and educate ourselves about this.

X. ACKNOWLEDGEMENT

It gives me immense pleasure to present my Research paper on "Correspondence Study". I would like to convey my sincere thanks to all the teachers who helped us throughout. I would like to acknowledge the help and guidance provided by our professors in all place during the presentation of this research paper. We are also grateful to, Head of Department. This acknowledgement will remain incomplete if we do not mention sense of gratitude towards our esteemed Principal who provided us with the necessary guidance, encouragement and all the facility available to work on this project.

XI. REFERENCES

- [1] Ranie B. Canlas, MSCpE Graduate School and College of Computing Studies, Don Honorio Ventura State University, Philippines - CAPTURING SECURITY MECHANISMS APPLIED TO ECOMMERCE: AN ANALYSIS OF TRANSACTION SECURITY, pp.1-10, ISSN: 2207-9629, Vol. 15, International Journal of Security and Its Applications.
- [2] Mr.Amit N. Chaudhari, Prof. Priya V. Shirbhate – “The study of E-Commerce Security Issues and Solutions”. pp. 022-28, ISBN 2394-8299 Vol.1, Spl. Issue-1, International Journal of Research In Science & Engineering.
- [3] CH. Sireesha, V.Sowjanya, Dr K.Venkataramana - Cyber security in E-commerce, ISSN 2229-5518, Volume. 8, International Journal of Scientific & Engineering Research.
- [4] Dr. Rajesh Kumar Mahajan Principal, D.A.V. College, Abohar - Security Issues and Guidelines for a Successful E-Commerce System, ISSN 2348 -1269, Print ISSN 2349-5138, Volume. 5, International Journal of Research and Analytical Reviews.
- [5] 1Student, Faculty of Computer Application, Bachelor of Computer Application, Manavrachna international Institute of Research and Studs, Faridabad, India 2Student, Faculty of Computer Application, Bachelor of Computer Application, Manavrachna international Institute of Research and Studs, Faridabad, India 3Student, Faculty of Computer Application, Bachelor of Computer Application, Manavrachna international Institute of Research and Studs, Faridabad, India, e-ISSN: 2395-0056, p-ISSN: 2395-0072, Volume. 7, International Research Journal of Engineering and Technolog.

