

A STUDY ON E-COMMERCE SECURITY ISSUES AND THEIR SOLUTIONS

Submitted in partial fulfilment of the requirements for the award of

MASTER OF BUSINESS ADMINISTRATION

By

KISHEN G

REGISTER NO:42410236



**DEPARTMENT OF BUSINESS
ADMINISTRATIONSCHOOL OF MANAGEMENT
STUDIES**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade “A++” by NAAC I 12B Status by UGC I
CATEGORY - 1 UNIVERSITY BY UGC I Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI- 600119**

December 2023



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
CATEGORY - 1 UNIVERSITY BY UGC**

SCHOOL OF MANAGEMENT STUDIES

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the Bonafide work of **KISHEN G 42410236** who carried out the Project Training “**A STUDY ON E-COMMERCE SECURITY ISSUES AND THEIR SOLUTIONS**” under my supervision from October 2023 to December 2023.

Internal guide

External Guide

**Dr. BHUVANESWARI. G, MBA., Ph.D.
Dean – School of Management Studies**

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I KISHEN G (42410236) Hereby declare that the Project Report entitled "**A STUDY ON E-COMMERCE SECURITY ISSUES AND THEIR SOLUTIONS**" done by me under the guidance of **Ms. SHAHINA BEGUM** Assistant Professor, School of Business Administration is submitted in partial fulfilment of the requirements for the award of Master of Business Administration degree.

DATE:

PLACE: CHENNAI

KISHEN G

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to Board of Management of SATHYABAMA for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my sincere thanks to Dr. BHUVANESWARI G., Dean, School of Business Administration and Dr. PALANI A., Head, School of Business Administration for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide Ms. SHAHINA BEGUM, Assistant Professor of the Department, School of Management for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the School of Business Administration who were helpful in many ways for the completion of the project.

KISHEN G

ABSTRACT

The study on E-commerce security issues and their solutions delves into the world of online shopping from the perspective of e-commerce platform users. Through a comprehensive analysis of user demographics and behaviours, this research provides crucial insights into the state of online shopping security. The study's findings reveal a balanced gender distribution among respondents, with an active participation of users across various age groups, especially those under 25 years old. Notably, while a majority of users express a feeling of security when making online payments, a substantial number have discontinued using e-commerce platforms due to security concerns. This underscores the significance of transparency in security practices and user trust.

Security challenges such as phishing attempts and payment fraud are prevalent, requiring focused attention from e-commerce platforms. Additionally, the study highlights the need for personalized, mode-specific security recommendations and educational resources. In conclusion, this research underscores the imperative for e-commerce platforms to adapt their security practices, engage users effectively, and fortify the online shopping experience to address the ever-evolving landscape of security concerns in e-commerce.

LIST OF CONTENTS

S. No	Content Details	Page No
	CHAPTER I	
1	INTRODUCTION	
1.1	Introduction of the Study	1
1.2	Objective of the study	3
	CHAPTER II	
2	LITREATURE REVIEW	4
	CHAPTER III	
3	RESEARCH METHODOLOGY	
3.1	Research methodology	13
3.2	Research design	13
3.3	Target population	13
3.4	Sources of data	14
3.5	Sampling technique	14
3.6	Statistical tools	15
3.7	Hypothesis	15
	CHAPTER IV	
4	DATA ANALYSIS AND INTERPRETATION	
4.1	Gender	16
4.2	Age group	17
4.3	Number of times they use online platforms for shopping in a month	19
4.4	Which product do you purchase more often online?	21
4.5	Do they feel safe while making online payment	23

4.6	Do they find e-commerce websites easy to navigate?	24
4.7	Have they ever stopped using an e-commerce platform due to security concerns?	25
4.8	In your opinion, how transparent are e-commerce platforms about their security practices?	26
4.9	How concerned are they about the security of their personal and financial information when making online purchases?	28
4.10	Have they ever experienced a security breach or unauthorized access to their account on e-commerce platforms?	30
4.11	When using an e-commerce platform, what is their primary concern regarding security?	32
4.12	Are they aware of the potential security risks associated with online shopping, such as data breaches or phishing attacks?	34
4.13	Do they believe that e-commerce platforms take adequate measures to protect their personal and financial information?	36
4.14	Have they ever experienced unauthorized access to their online shopping?	38
4.15	Which of the following security challenges have they encountered while shopping online?	39
4.16	How often do they encounter captcha or security checks during online shopping to verify that they are not a bot?	41
4.17	Do they regularly update their passwords for their e-commerce accounts?	43
4.18	How do they typically respond to security warnings or alerts from their web browser when visiting e-commerce websites?	45
4.19	Have they enabled multi-factor authentication (mfa) for their e-commerce accounts when available?	47
4.20	Do they use antivirus or anti-malware software on their devices for added security while shopping online?	49
4.21	Which of the following secure payment methods do they prefer when shopping online?	51

4.22	How would they prefer to receive security tips and recommendations for safer online shopping?	53
4.23	Are they interested in educational resources or tutorials that teach them how to recognize and avoid online security threats?	55
4.24	Relationship between the age of the respondents and security awareness among the users of the e-commerce platform	57
	CHAPTER V	
5	SUMMARY OF FINDINGS, SUGGESTIONS, AND CONCLUSION	
5.1	Findings of the study	60
5.2	Suggestions	64
5.3	Conclusion	65
	References	66
	Annexure	70

LIST OF TABLES

TABLE. NO	TITLE	PAGE. NO
1	Gender	16
2	Age group	17
3	Number of times they use online platforms for shopping in a month	19
4	Highest purchased product	21
5	Confidentiality while making online payment.	23
6	E-Commerce websites are easy to navigate or not.	24
7	Stopped using an e-commerce platform due to security concern.	25
8	How transparent are e-commerce platform about their security practices.	26
9	How concerned are they about the security of their personal and financial information when making online purchases.	28
10	Experience on a security breach or unauthorised access to their account on e-commerce platforms	30
11	Primary concern regarding security while using an e-commerce platform.	32
12	Awareness of the potential security risks associated with online shopping, such as Data breaches or Phishing attacks.	34
13	E-commerce platforms take adequate measures to protect their personal and financial information.	36
14	Ever experienced an unauthorized access to their online shopping.	38
15	Security challenges have they encountered while shopping online	39
16	Number of times they encounter captcha or security checks during online shopping to verify that they are not a Bot.	41
17	Regularly update their passwords for their e-commerce accounts	43

18	Responses to security warnings or alerts from their web browser when visiting e-commerce websites	45
19	Enabled multi factor authentication for their e-commerce accounts when available	47
20	Usage of antivirus or anti-malware software on their devices for added security while shopping online.	49
21	Payment methods preferred when shopping online	51
22	Preferable way to receive security tips and recommendations for safer online shopping.	53
23	Interest in educational resources or tutorials that teach them how to recognize and avoid online security threats	55
24	Relationship between the age of the respondents and security awareness among the users of the e-commerce platform	58

LIST OF CHARTS

TABLE. NO	TITLE	PAGE. NO
1	Gender	16
2	Age group	17
3	Number of times they use online platforms for shopping in a month	19
4	Highest purchased product	21
5	Confidentiality while making online payment.	23
6	E-Commerce websites are easy to navigate or not.	24
7	Stopped using an e-commerce platform due to security concern.	25
8	How transparent are e-commerce platform about their security practices.	26
9	How concerned are they about the security of their personal and financial information when making online purchases.	28
10	Experience on a security breach or unauthorised access to their account on e-commerce platforms	30
11	Primary concern regarding security while using an e-commerce platform.	32
12	Awareness of the potential security risks associated with online shopping, such as Data breaches or Phishing attacks.	34
13	E-commerce platforms take adequate measures to protect their personal and financial information.	36
14	Ever experienced an unauthorized access to their online shopping.	38
15	Security challenges have they encountered while shopping online	39
16	Number of times they encounter captcha or security checks during online shopping to verify that they are not a Bot.	41
17	Regularly update their passwords for their e-commerce accounts	43

18	Responses to security warnings or alerts from their web browser when visiting e-commerce websites	45
19	Enabled multi factor authentication for their e-commerce accounts when available	47
20	Usage of antivirus or anti-malware software on their devices for added security while shopping online.	49
21	Payment methods preferred when shopping online	51
22	Preferable way to receive security tips and recommendations for safer online shopping.	53
23	Interest in educational resources or tutorials that teach them how to recognize and avoid online security threats	55

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. Today, privacy and security are a major concern for electronic technologies. M-commerce shares security concerns with other technologies in the field. Privacy concerns have been found, revealing a lack of trust in a variety of contexts, including commerce, electronic health records, e-recruitment technology and social networking, and this has directly influenced users.

Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce. Web e-commerce applications that handle payments (online banking, electronic transactions or using debit cards, credit cards, PayPal or other tokens) have more compliance issues, are at increased risk from being targeted than other websites and there are greater consequences if there is data loss or alteration. Online shopping through shopping websites having certain steps to buy a product with safe and secure.

The e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the ecommerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture. Trojan horse programs launched against client systems pose the greatest threat to e-commerce because they can bypass or subvert most of the authentication and authorization mechanisms used in an ecommerce transaction. These programs can be installed on a remote computer by the simplest of means: email attachments.

Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for e-

Commerce providers. eCommerce security refers to protecting a business website and all online transactions that happen on it from unauthorized access. Thus, you need a solid security foundation to become a secure and reliable online store so that you can make money online without any issues. Whether you're building a site on an eCommerce platform or a CMS, there is no one-size-fits-all approach when it comes to protecting your site from possible security issues. There are numerous industry regulations, standards, and solutions you can follow to minimize security risks. The following are the six factors of eCommerce security that must be considered:

- Integrity – ensure that no unauthorized entity has altered any information. It is all about providing consistent, accurate, and reliable information.
- Non-repudiation – confirms that both buyers and sellers received the information sent from each other. In other words, buyers can't deny the legitimacy of a recorded transaction.
- Authenticity – both sellers and buyers must present their identity verification to ensure the safety of the transaction.
- Confidentiality – when it comes to sensitive data, only those with proper authorization can access, change, or use it.
- Privacy – refers to protecting customer data from unauthorized parties.
- Availability – an eCommerce site must be accessible 24/7 for customers.

Since cybercriminals are becoming more inventive these days, eCommerce websites are vulnerable to various approaches, such as malware injection, spam emails, social engineering attacks, and many more. Implementing proactive solutions against cyberattacks is essential to protect your customers and business. Here are 11 measures to keep eCommerce security threats under control:

1. Implement password best practices
2. Opt for a secure hosting
3. Get an SSL certificate
4. Install security plugins and anti-virus software

5. Schedule regular site updates
6. Perform timely backups
7. Add multi-factor authentication
8. Use a CDN
9. Regulate user roles and permissions
10. Use a secure payment gateway
11. Avoid storing confidential data

1.2 OBJECTIVES OF THE STUDY

- To study about the e-commerce security issues and its solution
- To identify the most prevalent e-commerce security challenges faced by online users, such as data breaches, phishing attempts, or payment fraud.
- To assess online users' security practices and behaviours, including their password management, use of multi-factor authentication, and response to security warnings.
- To explore the awareness and adoption of security solutions among online users, such as antivirus software, secure payment methods, and secure browsing practices.
- To formulate user-centric security recommendations and best practices to empower online users to protect themselves while engaging in e-commerce activities.

CHAPTER 2

REVIEW OF LITERATURE

VARIOUS REVIEWS

Mohanad Halaweh & Christine Fidler (2018) stated that, Security is one of the crucial part restrict customers and organizations engaging with e- ecommerce. The aim of this paper is to explore the perception of security in e-commerce basically on business to customer B2C and customer to customer C2C websites from both customer and organizational perspectives.

Walch (2015) stated that Globalization as well as information technology (IT) change the method of the business doing by the organizations. In almost all companies that have invested largely in the IT infrastructure for the ultimate growth of their company, the IT system is implemented and integrated. The utilization of e-commerce (EC) as a way to execute transactions related to business is increasing concern. It has been a priority for many companies.

Turban et al Eds. (2017) - With EC, businesses will link "Just in Time production" and "Just in Time" to their trading partners, who boost their strategic abilities worldwide. EC's description is not widely agreed upon. From the communications point of view, EC may represent information, services as well products or online payments through telephone lines, computer networking, or other means from a communication point of view. EC implements technology for automating corporate transactions and workflows from a business process perspective. From a service viewpoint, EC is a way of lowering services costs while enhancing product efficiency and speeding up the delivery of services, which addresses industry, customers and management's desire.

Grandon & Pearson (2016) - EC offers online shopping and distributing goods and information for the Internet and other online resources from an online point of view. Because of Internet and network technology's popularity and accelerated expansion, the electronic industry has become a significant field for contemporary enterprises. Large company operations are being carried out online today. People sell and purchase products and services online, and without internet infrastructure, certain purchases cannot be done

Gefen (2019) - E-commerce is referred to as electronic commerce. It means the electronic media and the internet for dealing with goods and services. E-Commerce entails a company accessing the internet as well as IT, such as the electronic data interchange (EDI). E-

commerce concerns an internet vendor's website, trading goods or services to the user directly from the platform. The gateway uses a wireless purchase cart or a purchase basket to pay by credit card, debit card or Electronic fund transfer (EFT). A further description is as follows: Electronic communications and digital information processes in business transactions are used to create, modify and redefine value generation relations between, and between, organizations and individuals.

Peterson (2015) - With the increasing spread of ICTs, specifically the Internet, the global corporate world pushes rapidly into e-commerce (Business-to-Business). As the Internet enables consumers to enter the global economy, they can compare prices across areas, find out how they vary by request, and become aware of substitution. The buyers obtain a distinct advantage. Thanks to market openness, consumers can conveniently compare e-commerce ings from different websites. The rivals would immediately be one click away from the customer if the company is electronic. If consumers aren't comfortable with certain e-goods, content's pricing or services, they can adjust even more quickly than in traditional terms. They don't need a physical store from the point of view of the vendors.

Yuanqiao Wen & Chunhui Zhou (2017) stated that with the rapid growth of global market in E-commerce, security issues are arising from people's attention. The security for the online transaction is the core and key issues of the development of E-commerce. This paper about the security issues of Ecommerce activities put forward solution strategy from two aspects that are I. technology and system, so as to improve the environment for the development of E-commerce and ii. Promote the further development of E-commerce.

Biswajit Tripathy & Jibitesh Mishra (2019) pointed out that Web applications increasingly integrate third-party services. The integration introduces new security challenges due to the complexity for a web application to coordinate its internal states with those of the component services and the web client across the Internet.

Shazia Yasin, Khalid Haseeb (2017) stated that, Now a days the owners of Ecommerce web site are thinking of how to attract more customers and how to make the visitors feel secured when purchasing goods on the site, on the other side how the end users should rate an ecommerce website and what they should do to protect themselves as one among the online community. The main objective of writing this research analysis journal is to make the readers to get clarity of thoughts on the web technology which will help all the online customers to do secure transactions along with safety tips and tricks. There for the online ecommerce site owners, have to make their online visitors to be of much comfort or Trust an ecommerce site via Trust marks, and by their security strategies.

Abdulghader.A.Ahmed.Moftah (2020) reviewed that the traditional authentication mechanism is based on identity to provide security or access control methods. To avoid this kind of problem some traditional encryption and authentication algorithm require for high computing power of computer equipment. How to improve the authentication mechanism and optimize the traditional encryption and authentication algorithm may be the focus of peer to peer (P2P) e-commerce.

Sengupta & Mazumdar (2021) - All the E-Commerce transactions offer the banking industry with a great opportunity, but at the same time it creates a set of new risks and problems such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. As the money transactions are very important factor for e-commerce they require a coordinated match of algorithm and technical solutions.

Randy C. Marchany, Joseph G. Tront (2014) - Viruses are a nuisance threat in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool. The Trojan horse remote control programs and their commercial equivalents are the most serious threat to e-commerce. Trojan horse programs allow data integrity and fraud attacks to originate from a seemingly valid client system and can be extremely difficult to resolve. A hacker could initiate fraudulent orders from a victim system and the ecommerce server wouldn't know the order was fake or real. Password protection, encrypted client-server communication, publicprivate key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all clear-text before it gets encrypted.

Rashad Yazdanifard, Noor Al-Huda Edres (2019) - Due to the increase in warnings by the media from security and privacy breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information.

Seyyed Mohammad Reza Farshchi (2015) - The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of

Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to consumer e-commerce destinations.

Dr. Nada M. A. Al-Slamy (2017) - The analysis of G2C based online payment systems triggered conclusions which led to emphasize research on the security aspect on online payment systems. It was found that the credit card-based payment systems were the most widely used means of conducting online payments. It was also extracted from the study that users want more simplified, convenient and secure online payment systems.

Jeberson & Gurmit Singh (2013) The effect of security, protection and trust towards consumers as well as attitudes plays a key role in ecommerce implementation however, if well implemented, instantaneous flow of goods and services internally and externally. Besides, vital information could also be simultaneously processed to matched with data flowing from external ecommerce transactions which could allow for efficient and effective integration into organizational processes.

Biswajit Tripathy & Jibitesh Mishra (2013) stated clearly, the online transaction requires consumers to disclose a large amount of sensitive personal information to the vendor, placing themselves at significant risk. Understanding (indeed, even precisely defining) consumer trust is essential for the continuing development of e-commerce.

Pradnya, Rane & Meshram (2015) - In online shopping online electronic payment function is the key issue to ensure the consumers are fast and convenient, we have to ensure the safety and secrecy of the parties to a transaction, which requires a complete electronic trading system.

Niranjanamurthy & Kavyashree (2018) - Most of the e-commerce Transactions occur between buyers and sellers. This kind of transactions in e-commerce includes requests for quotation of prices, information, payment, delivery of orders, and finally services after receiving of the product to customer. The high degree of confidence needed in the authenticity, confidentiality, and timely delivery of such transactions can be difficult to maintain where they are exchanged over the Internet.

Yang Jing (2009) stated that on e-commerce the Privacy and security can be viewed as ethical questions. At the same time the privacy and security area attracts a large amount of attention from the commercial sector because it has the potential to determine the success or failure of many business ventures, most obviously commerce activities.

Thomas (2018) - In online shopping of e-commerce the payment function is the key issue to ensure that, the consumers or buyers are fast and convenient, there the safety and secrecy of the parties to a transaction, which requires a complete electronic trading systems.

Kolesar and Galbraith (2019) - Trust is something that greatly affects where and how people buy their goods. In general trust can be hard to gain on the internet because there is a lack of assurance

Ltifi and Gharbi (2021) - E-commerce risk is a part of a broader idea of consumer trust. E-commerce consumers' e-satisfaction is influenced by risk and emotional states, which then in turn creates loyalty to a specific website

Dowling and Staelin (2022) - Risk has two different levels that work together. One aspect of risk is the size of the problem that could be created and then how likely is it that this problem will actually happen. These two different dimensions work together to create either a high or low level of perceived risk. It is important to realize that risk is not one dimensional and is assessed differently by people. People will assign different magnitudes to each level risk and different probabilities of these risks.

Kim and Benbasat (2015) - Research has been done about a few types of risk that consumers face while engaging in online shopping. One risk that has been found to be very important is the risk of the loss of time. People do not want to waste their time on looking for something on a website. The point of shopping online is to find something quickly and easily. Additionally, it was found that in regards to e-satisfaction, financial risk was not a concern.

Michalowska, Kotylak & Danielak (2018) - People generally feel confident in the integrity of the company to deliver the product the way that they say they will, especially when the price is higher signifying quality. But financial risk does vary based on the consumer's wealth level. If the consumer does not value a minor monetary loss then financial risk will not be calculated into their overall risk level.

Sinha and Singh (2016) - Risk is also influenced by ratings about the website. Consumers will do their research to look at average rating scores when evaluating the riskiness of a website. Further, in terms of the item being purchased, more risk is associated with sensory items.

Joonkyum and Bumsoo (2016) - In an e-commerce environment, there are many avenues for consumers to experience risk. One area of risk that is a cause of great concern is security risk. Security risk refers to the threat of a security breach of personal information that people submit online. Uncertainty is a major concern for shoppers and has an impact on the amount of potential profit for an online retailer.

Miyazaki and Fernandez (2012) - It has been shown that security issues regarding both personal and financial information are one of the top concerns of internet users. This

concern is highest when a country's population has just begun to have the opportunity of e-commerce.

Turban (2018) - There are different perceptions of aspects of security based on the individual's usage of the internet. A light user is someone who uses the internet no more than 15 hours per week while a heavy user is anyone who uses the internet more than 15 hours per week. Light users are better with password practices, perhaps because they are in general more cautious because they do not have as much awareness. Heavy users in turn are more informed about risk awareness and phishing awareness and are better about updating antivirus software.

Pavlou (2017) stated that increase of usage of internet does not decrease overall perceptions of security risk. In order for people to complete a purchase online, they need to feel secure and feel that the risk is relatively low. There are regulations applied by governing bodies about online security, and specifically the security of information people provide in regards to e-commerce. Many people are not satisfied with these laws and think that they are not strict enough to fully protect their confidential information.

Bente et al., (2014) - Companies utilizing e-commerce need to have alternatives to increase the consumers' trust and satisfaction compare to the traditional physical stores, because there are no face-to-face interactions. Online websites do not allow for a customer to have an interaction with a real customer service representative. However, there are certain ways for companies to recreate this physical interaction. One of these alternatives is social presence.

Moon et al (2014) stated that when a company uses real-time audio or audio-visual channels for communication, interpersonal trust will increase. This would be something like providing an avatar or having a live online chat with a customer service representative. When a company specifically uses an avatar, a user will feel that there is a greater sense of social presence and purchase intention.

Zhang et al., (2015) - Social presence can especially play an important role when examining consumer mood. Social presence can increase the mood of the customer which will then increase their intention to purchase. Social presence has been proven to greatly enhance the online shopping experience.

Dash and Saji (2017) - In terms of shopping, intention to purchase is very important. Companies exist because of people actually purchasing goods from that company. Intention to purchase can be influenced by a variety of things including trust, usefulness, satisfaction, and risk. Overall satisfaction and attitude are something that influence intention to

purchase. When a consumer has a positive experience with the online website and is satisfied, they are more likely to make a purchase and then to make a repeat purchase as well.

Ltifi and Gharbi (2016) stated that, Not only is satisfaction important during the purchase, it is also important for the post-purchase phase for repeat purchase intention. Risk is something else that negatively affects intention to purchase.

Muhannad & Ahmed (2018) stated that when a consumer is a heavy online shopper, risk will not influence intention to purchase as heavily as when a consumer is a light online shopper. Trust has been found to be a mitigating relationship for purchase intention. When a consumer feels like they can trust the website, maybe due to good visual design or a highly informative website, they are more likely to make a purchase.

Shin and Shin (2020) - The safety of services provided via Internet, especially services within e-commerce, and its perception by customers can be affected by various types of problems to which the customer may be exposed. Therefore, if customer faces many problems during online shopping, he does not feel safe for example about delivery, payment, personal data.

Gupta and Dubey (2016) stated that the internet is also full of opinions and information about products or services. It is a huge resource of knowledge about shops, service providers and enterprises. Due to this fact, the customer can get a lot of additional information, which he/she would not have obtained from the enterprises and shops, and which can greatly influence the decision to make a purchase.

Israel (2015) - Functional risk can be defined as the perception that a product or service may not perform as needed or expected and suffering from the loss of the desired benefits. The loss incurred when a brand or product does not perform as expected, is largely due to the shoppers inability to accurately evaluate the quality of the product online.

Heng (2022) stated that Consumers are worried that the Internet still has very little security with respect to using their credit cards and disclosing personal information. The potential net loss of money, and includes consumers sense of insecurity regarding online credit card usage, which has been evidenced as a major obstacle to online purchases.

Muijs (2021) stated that the possibility of being embarrassed, disappointed, or suffering from status loss from family or friends by making a poor choice describes social risk. The potential loss of status in consumes social group due to either the inappropriateness of the product or disapproval of using internet as a shopping channel.

According to **Sekaran (2016)** said that e-commerce or online shopping dates for over 40 years, and it is constantly growing with new innovations and technologies, and many businesses are entering to online markets. Online shopping can be determined as activity that deals with selling of goods and services through internet and for businesses is important to be aware of how consumers perceive online purchases. Now many people are predicting that soon the period of e-commerce could easily be replacing the traditional business of brick and mortar.

Tang et al (2017) state that there are lots of people online around the world, and each of them represent possible customer of stores which offer online sale. While there are a lot of them, it is essential to know what they really need and want from the product. The primary step is classifying and examining some influencing factors for online purchases, so examining those factors that influence consumers behaviour via the internet is vital.

Barry Silverstein (2016) stated that people are doing business online and trade has become more easy and fast due to internet that provides new ways to promote business. Website has become the essence tool of online business as to show their services and products. Internet gathers all competitors and consumers in one place. It brings new lane to promote and advertise products and services in market.

According to **Chu and Yuan (2016)** E-trust is most imperative for e-commerce. It plays a significant role in generating satisfaction and gains expected consequences in online transactions.

Kimery & McCord (2020) stated that Trust is an individual expectation; behaviour inside the society where they live and they are ruled, trust can be granted upon an individual, an organization, an institution (the government), an object (product) or a role (Barber, 1983). Furthermore, trust is customer expectations to admit weakness in online shopping that is based on optimistic expectations about future online shopping behaviour.

According to **Ali (2019)** product risk is on second highest risk or second level in fear following financial risk. Product risk actually is a threat in consumer mind about a product that might be a product not meet expectations and fail to perform an original function.

Tanadi, Samadi & Gharleghi (2021) - Product risk and privacy risk are the main risks associated with online shopping behaviour trust in companies necessary to increase sales and positive image in the consumer mind. Moderator use to strength the relationship so in this study we use a moderator to strengthen relationship by minimizing risks and increase online shopping behaviour with trust building.

Srikanth (2022) stated that the growth and trust upon E-Commerce business totally depend on the security and privacy policy of the site and for the development of E-commerce business most important factor is to build trust among users. To maintain privacy in the E-commerce business, a complete and secure system is required. Users feel hesitation in E-Commerce although online payment system is more secured and convenient.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 RESEARCH METHODOLOGY

Research Methodology is a systematic way of solving the problem. It includes the overall research design, the sampling procedures, data collection method and analysis procedure methodology shall be considered as the methods used in this study in selecting samples, sample size, data collection and various tools for data analysis and interpretation. The present study is an empirical and analytical investigation, including a field survey. The data collected has been analysed and tabulated in suitable forms, keeping in view the objectives of the study.

3.2 RESEARCH DESIGN:

Research design is the framework of research methods and techniques chosen by a researcher to conduct a study. The design allows researchers to sharpen the research methods suitable for the subject matter and set up their studies for success. In this survey Descriptive Research Design is used. It includes surveys and fact-finding inquiries of different kinds. The major purpose of descriptive research is description of state of affairs, as it exists at present. The survey used members of the population as the main source of data which it used in determining the effect of the variables on the population. The descriptive survey is designed to obtain precise information concerning the status of phenomenon.

3.3 TARGET POPULATION

The target population is the group of individuals that the intervention intends to conduct research in and draw conclusions from. In cost-effectiveness analysis, characteristics of the target population and any subgroups should be described clearly. The target population in this study are the e-commerce platform users.

Data Collection

A comprehensive questionnaire was prepared to meet out the needs of the objective. Questionnaires for respondents were self-administered which was, therefore, dropped and later picked.

3.4 SOURCES OF DATA

Data collection method is the backbone of the research design. The source of data utilized for analysis and report preparation is both primary and secondary.

Primary data

Primary data was collected through the interview and getting the questionnaires filled. The questionnaire was given only to the users of e-commerce platform who were willing to share their views.

Secondary data: The main source of secondary data was internet.

3.5 SAMPLING TECHNIQUE:

The Convenience Sampling Method is used for the survey. Convenience or opportunistic sampling is the crudest type of non-random sampling. Convenience sampling involves using respondents who are “convenient” to the researcher. There is no pattern whatsoever in acquiring these respondents—they may be recruited merely asking people who are present in the street, in a public building, or in a workplace, for example.

Sampling Unit:

The users of e-commerce platform were met and the survey was made based on their response.

Sampling Area:

The sampling area considered for the current research is users of e-commerce platform residing in Chennai.

Sample Size:

60 e-commerce platform users were surveyed during the study period.

Questionnaire Design

Questionnaires were used as the main instruments of data collection in the study. The questionnaire was close-ended. As multi- option is given to the e-commerce platform users for their convenience. 5-point rating scale is used in the study. The use of the close ended question was aimed at controlling responses that gave rise for quantitative analysis. There were two main sections of questions; General information and e-commerce security information.

3.6 STATISTICAL TOOLS:

Simple percentage analysis and tabulation is used to analysis the data. Pie chart and bar diagram is used to give pictorial representation to the analysis.

PERCENTAGE ANALYSIS:

Simple percentage analysis refers to a special kind of ratio in making comparison between two or more data and to describe relations between the data. Percentage can also be used to compare the relative terms, the distribution of two or more series of data.

$$\text{Simple percentage} = \frac{\text{No. Of respondents} \times 100}{\text{Total no. of respondent}}$$

CHI-SQUARE TEST

Pearson's chi-squared test is used to determine whether there is a statistically significant difference between the expected frequencies and the observed frequencies in one or more categories of a contingency table. The basic idea behind the test is to compare the observed values in your data to the expected values that you would see if the null hypothesis is true.

3.7 HYPOTHESIS

Hypothesis 1

H0: There is no relationship between age of the respondents and security awareness among the users of e-commerce platform

H1: There is relationship between age of the respondents and security awareness among the users of e-commerce platform

Hypothesis 2

H0: There is no relationship between security issues and secured online shopping experience among its users

H1: There is relationship between security issues and secured online shopping experience among its users

CHAPTER 4

DATA ANALYSIS AND INTERPRETATION

4.1 GENDER

The following table shows the gender of the respondents.

Table 1: Gender

S. No.	Gender	No. of Respondents	% Of Respondents
1	Male	31	51
2	Female	29	49
	Total	60	100

The following chart shows the data that has been obtained from the respondents in the pictorial format.

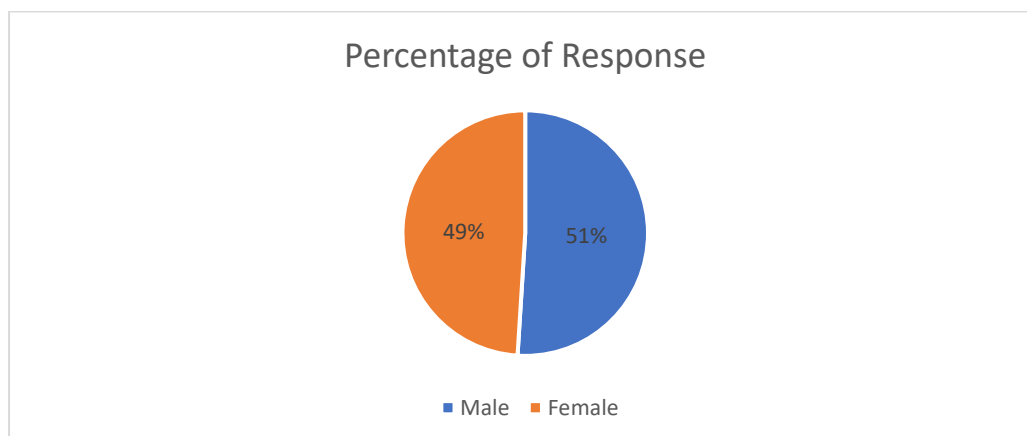


Chart 1: Gender

Interpretation

The above table shows the gender of the respondents. About 51% of the respondents are male and about 49% of the respondents are female.

4.2 AGE GROUP

The following table shows the age group of the respondents.

Table 2: Age group

S. No.	Age Group	No. of Respondents	% Of Respondents
1	Below 25 years	20	33
2	25 – 30	15	25
3	31 – 35	4	6
4	36 – 40	3	5
5	41 – 45	12	21
6	45 and above	6	10
	Total	60	100

The following chart shows the data that has been obtained from the respondents in the pictorial format.

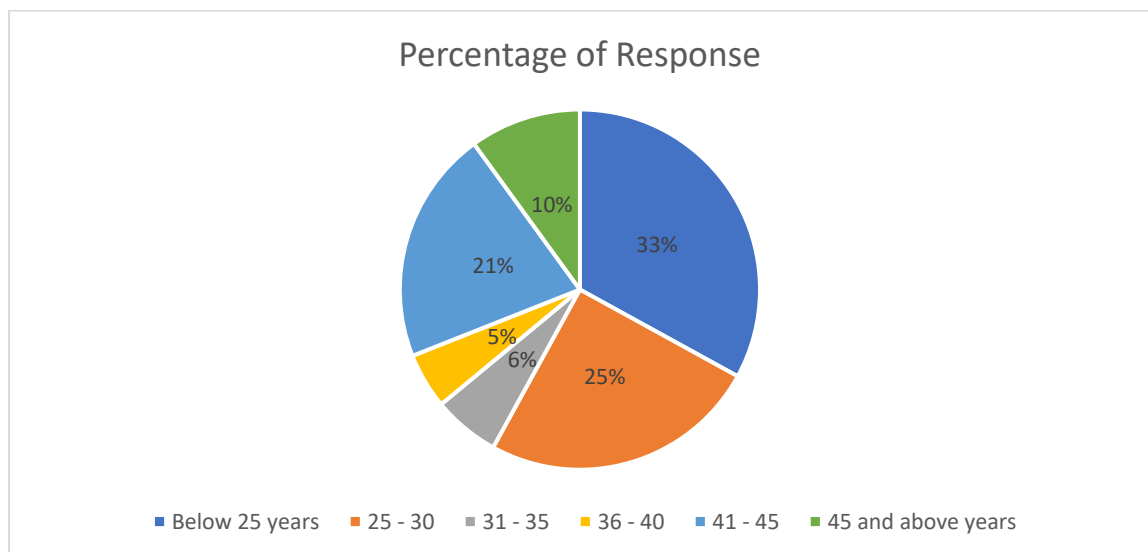


Chart 2: Age group

Interpretation

The above table shows the age group of the respondents. About 33% of the respondents are below the age of 25 years of age, about 25% of the respondents are between the age of 25 to 30 years of age, about 6% of the respondents are between the age of 31 to 35 years of age, about 5% of the respondents are between the age of 36 to 40 years of age, about 21% of the respondents are between the age of 41 to 45 years of age, and about 10% of the respondents are above 45 years of age.

4.3NUMBER OF TIMES THEY USE ONLINE PLATFORMS FOR SHOPPING IN A MONTH

The following table shows the respondent's view on how often they use online platforms for shopping in a month.

Table 3: Number of times they use online platforms for shopping in a month

S. No.	Number of times they use online platforms for shopping in a month	No. of Respondents	% Of Respondents
1	More than once	26	44
2	1 – 4	17	28
3	4 – 8	13	21
4	8 – 12	2	4
5	More than 12	2	3
	Total	60	100

Here the respondents were asked how often do they use online platforms for shopping in a month. The following chart shows the data what has been obtained from the respondents in the pictorial format.

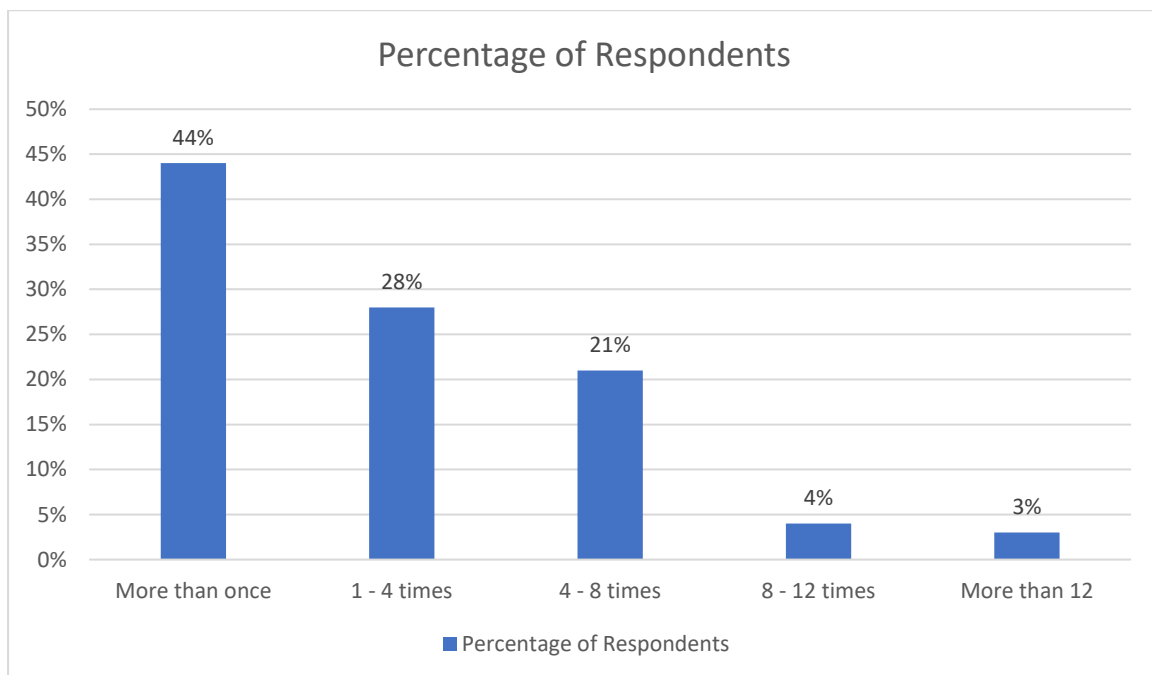


Chart 3: Number of times they use online platforms for shopping in a month

Interpretation

The above table shows how often do they use online platforms for shopping in a month. About 44% of the respondents do online shopping more than once, about 28% of the respondents shop around 1 to 4 times, about 21% shop for 4 to 8 times and 4% of the respondents shop from 8 to 12 times. However, 3% of the respondents shop more than 12 times in online platforms.

4.4 WHICH PRODUCT DO YOU PURCHASE MORE OFTEN ONLINE?

The following table shows the respondent's view on the highest purchased product.

Table 4: Highest purchased product

S. No.	Highest purchased product	No. of Respondents	% Of Respondents
1	Grocery	9	15
2	Electronics	11	19
3	Textile	16	27
4	Beauty Products	6	10
5	Furniture	1	2
6	Pharmacy	11	18
7	Books	3	5
8	Toys	1	1
9	Others	2	3
	Total	60	100

Here the respondents were asked whether the respondent's view on the highest purchased product.

The following chart shows the data what has been obtained from the respondents in the pictorial format.

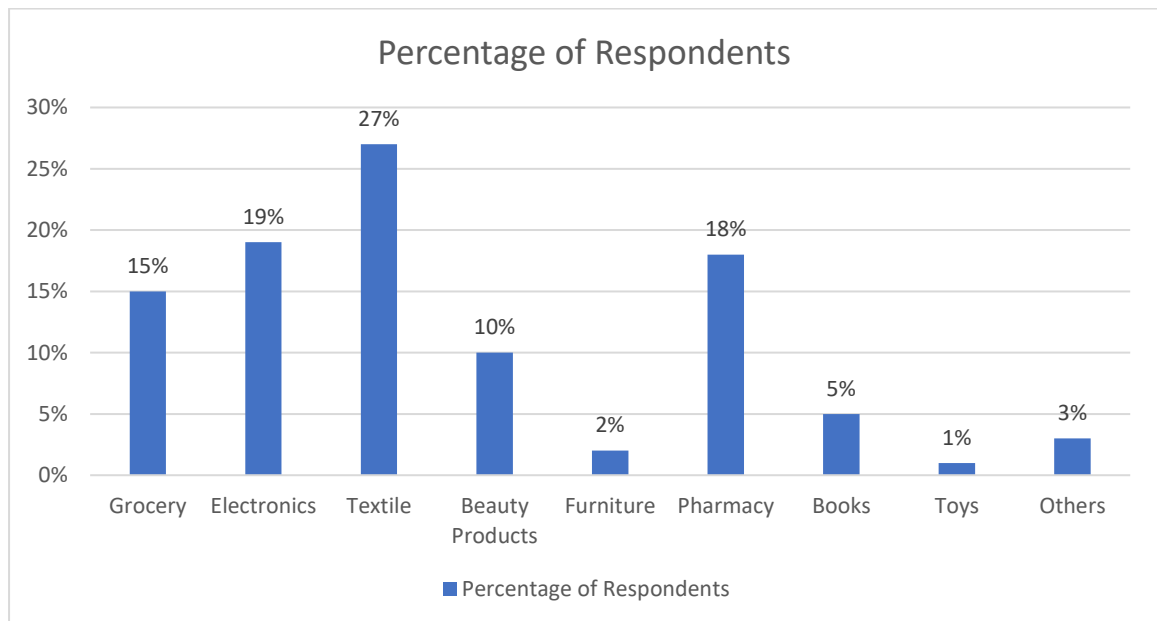


Chart 4: Highest purchased product

Interpretation

The above table shows the highest purchased product in online. About 15% of respondents purchased Grocery through online, 19% of respondents preferred to buy electronics, 27% of respondents buy textile products, 10% of respondents bought beauty products, 2% of respondents bought furniture, 18% of respondents used online platform to buy pharmacy items, 5% of respondents used to purchase books, 1% of respondents bought toys and 3% of respondents preferred to buy products other than items specified.

4.5 DO THEY FEEL SAFE WHILE MAKING ONLINE PAYMENT

The following table shows the respondents view about whether they feel safe while making online payment.

Table 5: Confidentiality while making online payment.

S. No.	Confidentiality while making online payment	No. of Respondents	% Of Respondents
1	Yes	40	67
2	No	20	33
	Total	60	100

Here the respondents were asked whether they feel safe while making online payment. The following chart shows the data what has been obtained from the respondents in the pictorial format.

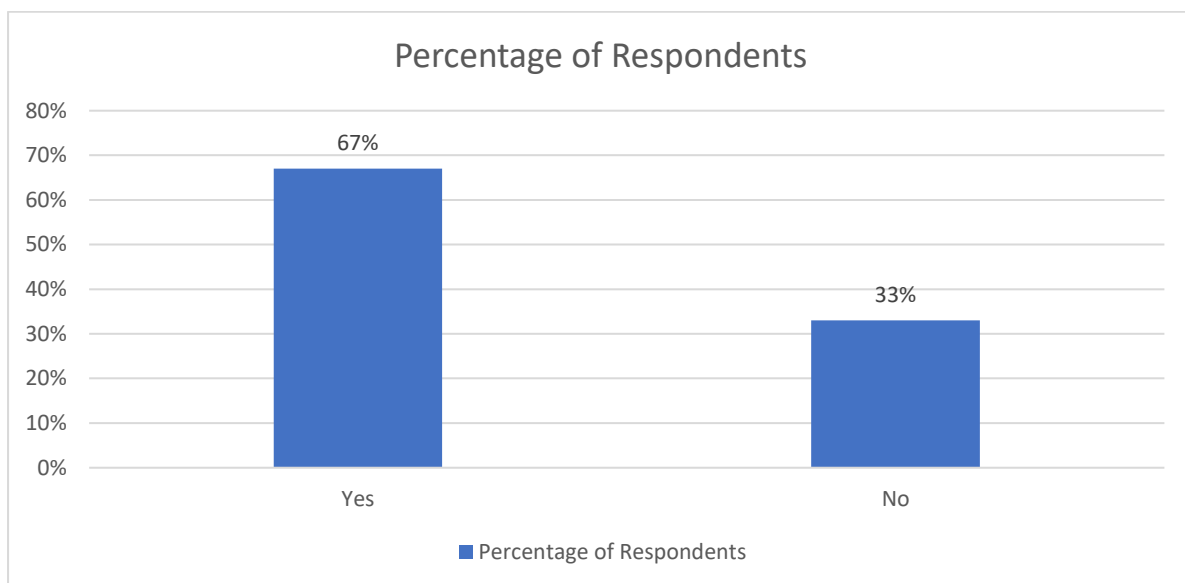


Chart 5: Confidentiality while making online payment

Interpretation

The above table shows whether the respondents feel safe while making online payment. About 67% of respondents feel safe while making online payment, 33% of respondents doesn't feel safe while making online payment.

4.6 DO THEY FIND E-COMMERCE WEBSITES EASY TO NAVIGATE?

The following table shows the respondent's view on e-commerce websites whether they are easy to navigate or not.

Table 6: E-Commerce websites are easy to navigate or not.

S. No.	E-Commerce websites are easy to navigate or not	No. of Respondents	% Of Respondents
1	Yes	34	56
2	No	26	44
	Total	60	100

Here the respondents were asked whether E-commerce websites are easy to navigate. The following chart shows the data what has been obtained from the respondents in the pictorial format.

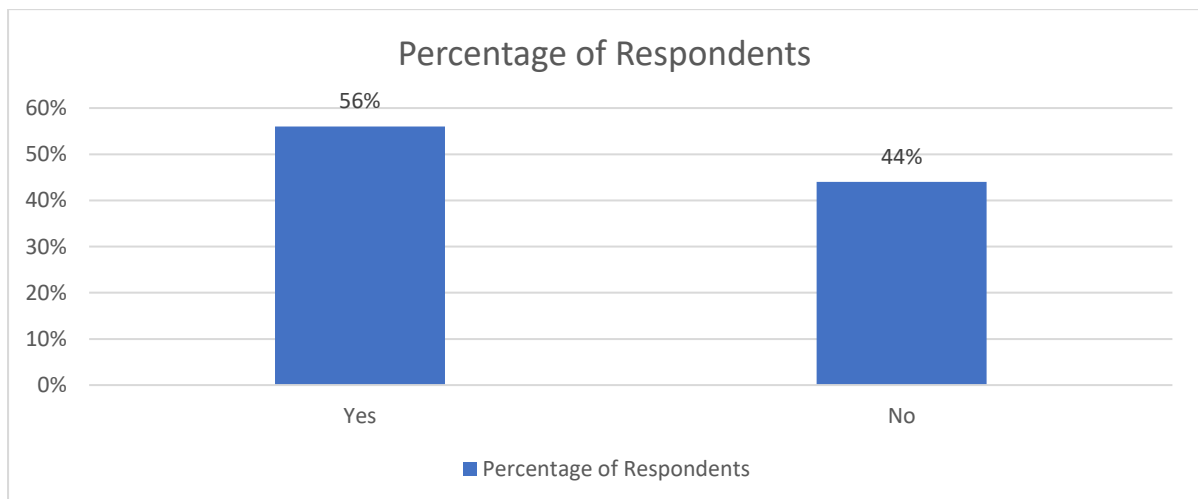


Chart 6: E-Commerce websites are easy to navigate or not.

Interpretation

The above table shows whether e-commerce websites are easy to navigate or not. About 56% of respondents felt easy to navigate e-commerce websites, 44% of respondents doesn't feel that e-commerce websites are easy to navigate.

4.7 HAVE THEY EVER STOPPED USING AN E-COMMERCE PLATFORM DUE TO SECURITY CONCERNS?

The following table shows the respondent's view about whether they stopped using an e-commerce platform due to security concerns.

Table 7: Stopped using an e-commerce platform due to security concern.

S. No.	Stopped using an e-commerce platform due to security concern	No. of Respondents	% Of Respondents
1	Yes	55	92
2	No	5	8
	Total	60	100

Here the respondents were asked whether they stopped using e-commerce platform due to security concern. The following chart shows the data what has been obtained from the respondents in the pictorial format.

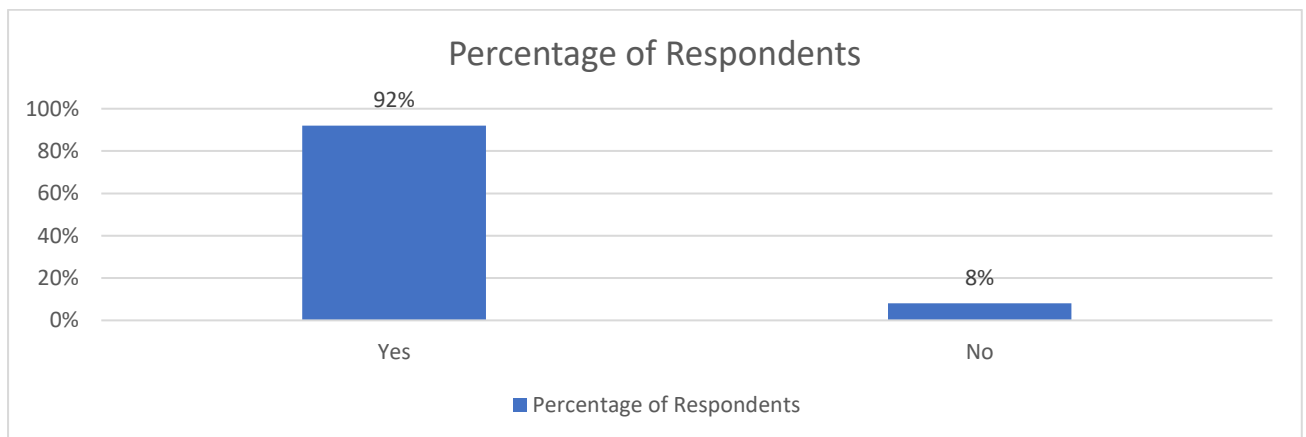


Chart 7: Stopped using an e-commerce platform due to security concern.

Interpretation

The above table shows the respondents view about have they ever stopped using an e-commerce platform due to security concern. About 92% of respondents have stopped using e-commerce platform due to security concern, 8% of respondents doesn't stopped using an e-commerce platform due to security concern.

4.8 IN YOUR OPINION, HOW TRANSPARENT ARE E-COMMERCE PLATFORMS ABOUT THEIR SECURITY PRACTICES?

The following table shows the respondent's views on how transparent are e-commerce platforms about their security practices.

Table 8: How transparent are e-commerce platform about their security practices.

S. No.	How transparent are e-commerce platform about their security practices.	No. of Respondents	% Of Respondents
1	Very transparent	21	35
2	Somewhat transparent	29	49
3	Not very transparent	4	7
4	Not at all transparent	6	9
	Total	60	100

Here the respondents were asked how transparent are e-commerce platform about their security practices. The following chart shows the data what has been obtained from the respondents in the pictorial format.

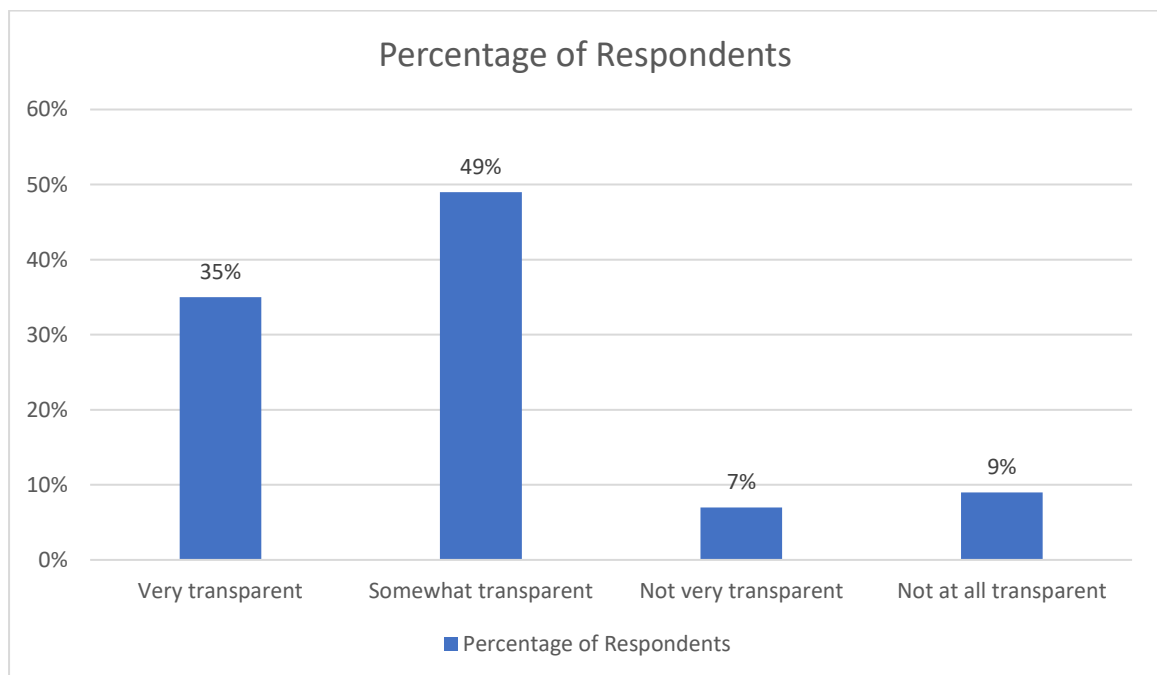


Chart 8: How transparent are e-commerce platform about their security practices.

Interpretation

The above table shows how transparent are e-commerce platform about their security practices. About 35% of respondents say that e-commerce websites are very transparent about their security practices, 49% of respondents says e-commerce websites are somewhat transparent about their security practices, 7% of respondents says e-commerce websites are not very transparent about their security practices and 9% of respondents says e-commerce websites are not at all transparent when it comes to security practices.

4.9 HOW CONCERNED ARE THEY ABOUT THE SECURITY OF THEIR PERSONAL AND FINANCIAL INFORMATION WHEN MAKING ONLINE PURCHASES?

The following table shows the respondent's views about how concerned are they about the security of their personal and financial information when making online purchases.

Table 9: How concerned are they about the security of their personal and financial information when making online purchases.

S. No.	How concerned are they about the security of their personal and financial information when making online purchases	No. of Respondents	% Of Respondents
1	Very concerned	15	26
2	Somewhat concerned	26	43
3	Not very concerned	10	16
4	Not concerned at all	9	15
	Total	60	100

Here the respondents were asked how concerned they are about the security of their personal and financial information when making online purchases. The following chart shows the data what has been obtained from the respondents in the pictorial format.

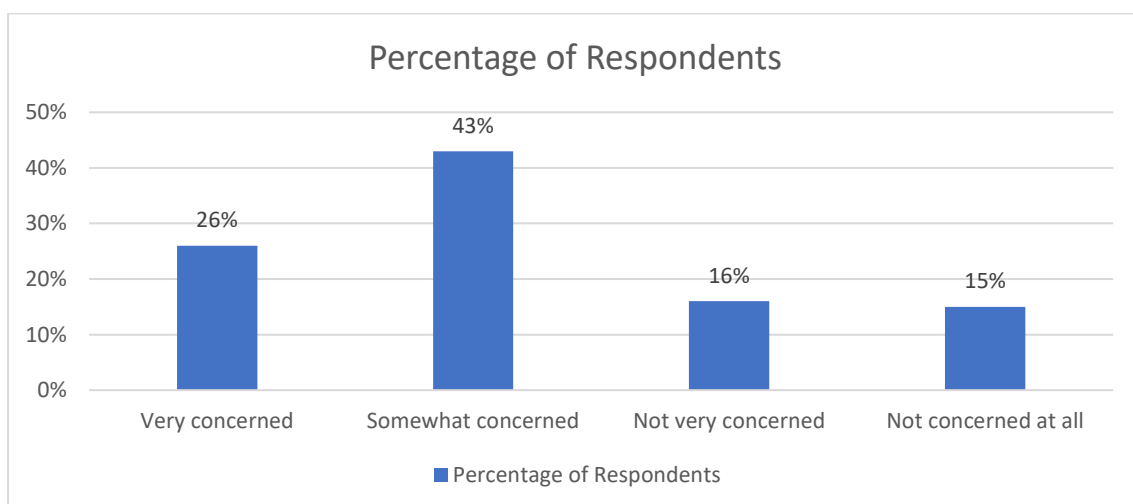


Chart 9: How concerned are they about the security of their personal and financial information when making online purchases.

Interpretation

The above table shows how concerned are the respondents about the security of their personal and financial information when making online purchases. About 26% of respondents are very concerned about the security of their personal and financial information when making online purchases, 43% of respondents are somewhat concerned about the security of their personal and financial information when making online purchases, 16% of respondents are not very concerned about the security of their personal and financial information when making online purchases and 15% of respondents are not concerned at all about the security of their personal and financial information when making online purchases.

4.10 HAVE THEY EVER EXPERIENCED A SECURITY BREACH OR UNAUTHORISED ACCESS TO THEIR ACCOUNT ON E-COMMERCE PLATFORMS?

The following table shows the respondent's view on whether they experienced a security breach or unauthorised access to their account on e-commerce platforms.

Table 10: Experience on a security breach or unauthorised access to their account on e-commerce platforms

S. No.	Experience on a security breach or unauthorised access to their account on e-commerce platforms	No. of Respondents	% Of Respondents
1	Yes	4	6
2	No	45	76
3	Not sure	11	18
	Total	60	100

Here the respondents were asked whether they experienced on a security breach or unauthorised access to their account on e-commerce platforms. The following chart shows the data what has been obtained from the respondents in the pictorial format.

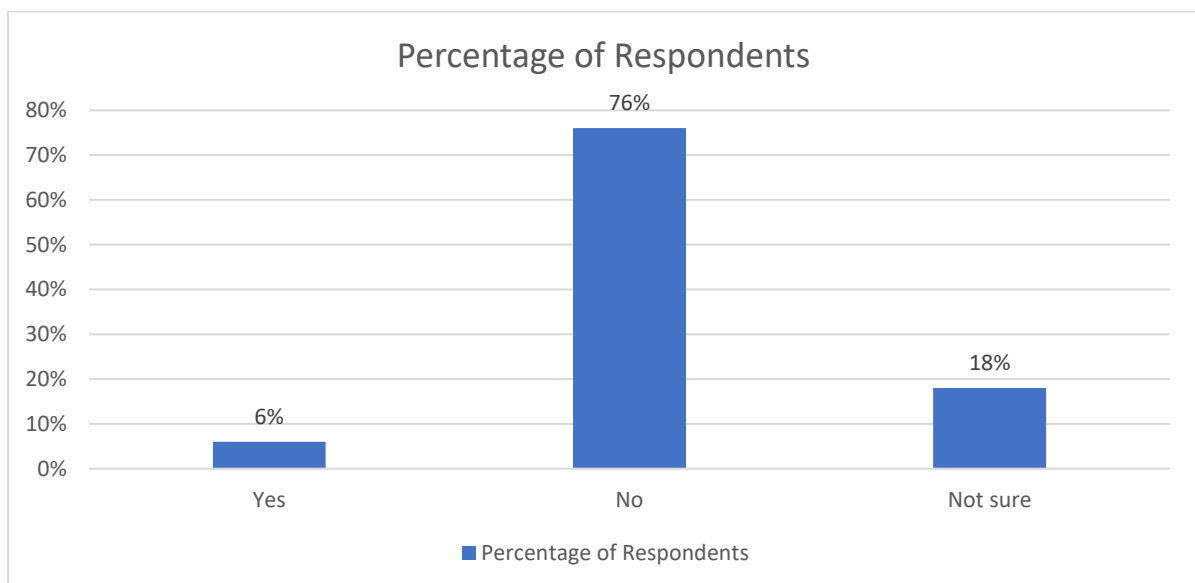


Chart 10: Experience on a security breach or unauthorised access to their account on e-commerce platforms.

Interpretation

The above table shows whether they experienced on a security breach or unauthorised access to their account on e-commerce platforms. About 6% of the respondents has experienced on a security breach or unauthorised access to their account on e-commerce platforms, 76% of the respondents doesn't experience on a security breach or unauthorised access to their account on e-commerce platforms and 18% of the respondents are not sure about whether they faced such kind of situation.

4.11 WHEN USING AN E-COMMERCE PLATFORM, WHAT IS THEIR PRIMARY CONCERN REGARDING SECURITY?

The following table shows the respondent's view on what is their primary concern regarding security while using an e-commerce platform.

Table 11: Primary concern regarding security while using an e-commerce platform.

S. No.	Primary concern regarding security while using an e-commerce platform.	No. of Respondents	% Of Respondents
1	Speed of delivery	19	31
2	Protection of personal and financial information	8	14
3	Variety of product choices	23	39
4	Availability of customer reviews	10	16
	Total	60	100

Here the respondents were asked what is their primary concern regarding security while using an e-commerce platform. The following chart shows the data what has been obtained from the respondents in the pictorial format.

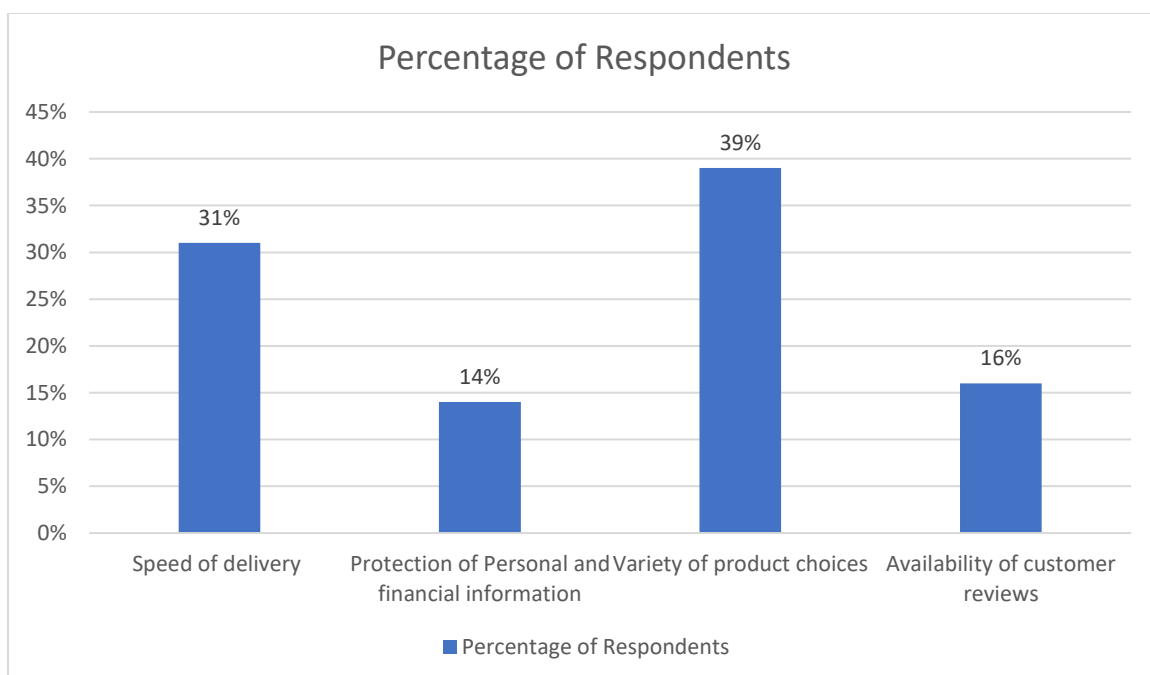


Chart 11: Primary concern regarding security while using an e-commerce platform.

Interpretation

The above table shows what is their primary concern regarding security while using an e-commerce platform. About 14% of the respondents strongly agree and about 22% of the respondents agree to a greater extent on this context. But 40% of the respondents remain neutral on the objective and process of performance appraisal were described clearly. About 14% of the respondents disagree and about 10% of the respondents strongly disagree.

4.12 ARE THEY AWARE OF THE POTENTIAL SECURITY RISKS ASSOCIATED WITH ONLINE SHOPPING, SUCH AS DATA BREACHES OR PHISHING ATTACKS?

The following table shows the respondent's view about whether they are aware of the potential security risks associated with online shopping, such as data breaches or phishing attacks.

Table 12: Awareness of the potential security risks associated with online shopping, such as Data breaches or Phishing attacks.

S. No.	Awareness of the potential security risks associated with online shopping, such as Data breaches or Phishing attacks.	No. of Respondents	% Of Respondents
1	Yes, very aware	6	11
2	Yes, somewhat aware	16	26
3	No, not very aware	21	35
4	No, not aware at all	17	28
	Total	60	100

Here the respondents were asked whether they are aware of the potential security risks associated with online shopping, such as data breaches or phishing attacks. The following chart shows the data that has been obtained from the respondents in the pictorial format.

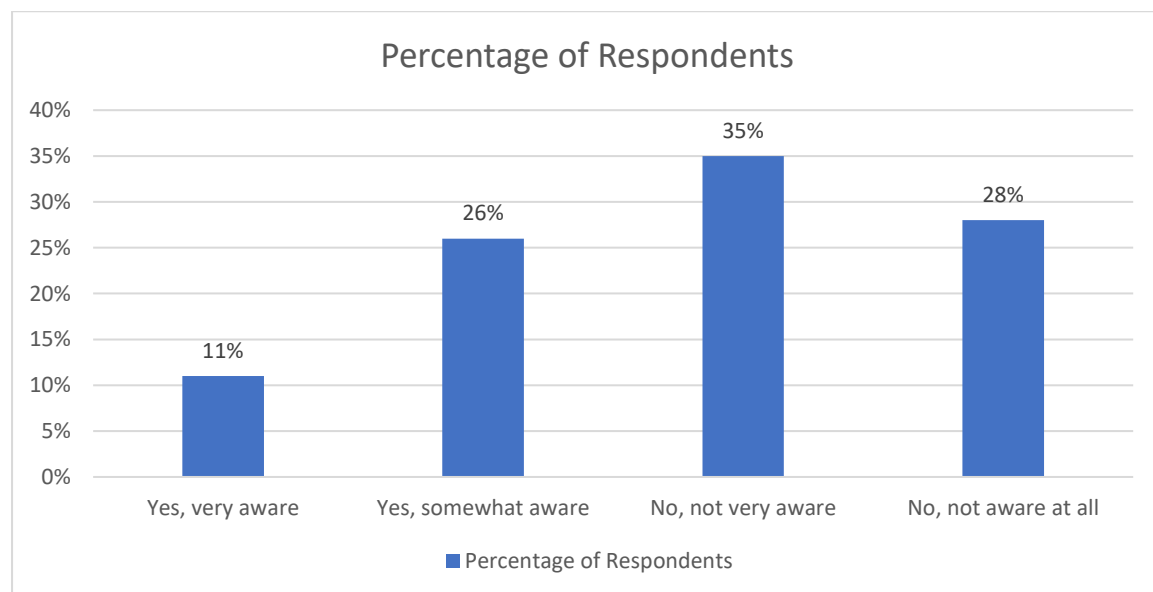


Chart 12: Awareness of the potential security risks associated with online shopping, such as Data breaches or Phishing attacks.

Interpretation

The above table shows whether they are aware of the potential security risks associated with online shopping, such as data breaches or phishing attacks. About 11% of the respondents are very aware about the potential security risks associated with online shopping, such as data breaches or phishing attacks, 26% of respondents are somewhat aware about the risks associated with online shopping, such as data breaches or phishing attacks, 35% of the respondents are not very aware about the potential security risks with online shopping, such as data breaches or phishing attacks and 28% of respondents are not at all aware about the risks associated with online shopping, such as data breaches or phishing attacks.

4.13 DO THEY BELIEVE THAT E-COMMERCE PLATFORMS TAKE ADEQUATE MEASURES TO PROTECT THEIR PERSONAL AND FINANCIAL INFORMATION?

The following table shows the respondent's view on e-commerce platforms whether they take adequate measures to protect their personal and financial information.

Table 13: E-commerce platforms take adequate measures to protect their personal and financial information.

S. No.	E-commerce platforms take adequate measures to protect their personal and financial information.	No. of Respondents	% Of Respondents
1	Strongly Agree	8	14
2	Agree	14	22
3	Neutral	24	40
4	Disagree	8	14
5	Strongly Disagree	6	10
	Total	60	100

Here the respondents were asked whether e-commerce platforms take adequate measures to protect their personal and financial information. The following chart shows the data what has been obtained from the respondents in the pictorial format.

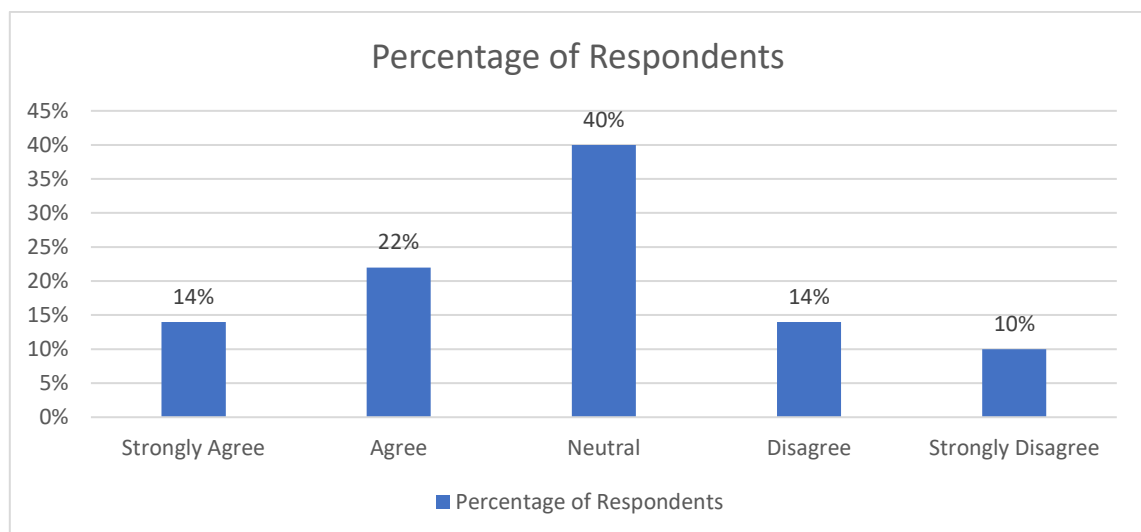


Chart 13: E-commerce platforms take adequate measures to protect their personal and financial information.

Interpretation

The above table shows whether e-commerce platforms take adequate measures to protect their personal and financial information. About 14% of the respondents strongly agree and about 22% of the respondents agree to a greater extent. But 40% of the respondents remain neutral. About 14% of the respondents disagree and about 10% of the respondents strongly disagree on e-commerce platforms take adequate measures to protect their personal and financial information.

4.14 HAVE THEY EVER EXPERIENCED UNAUTHORIZED ACCESS TO THEIR ONLINE SHOPPING?

The following table shows the respondent's view on whether they experienced unauthorised access to their online shopping.

Table 14: Ever experienced an unauthorized access to their online shopping.

S. No.	Ever experienced an unauthorized access to their online shopping	No. of Respondents	% Of Respondents
1	Strongly Agree	59	98
2	Agree	1	2
	Total	60	100

Here the respondents were asked whether they experienced an unauthorized access to their online shopping. The following chart shows the data what has been obtained from the respondents in the pictorial format.

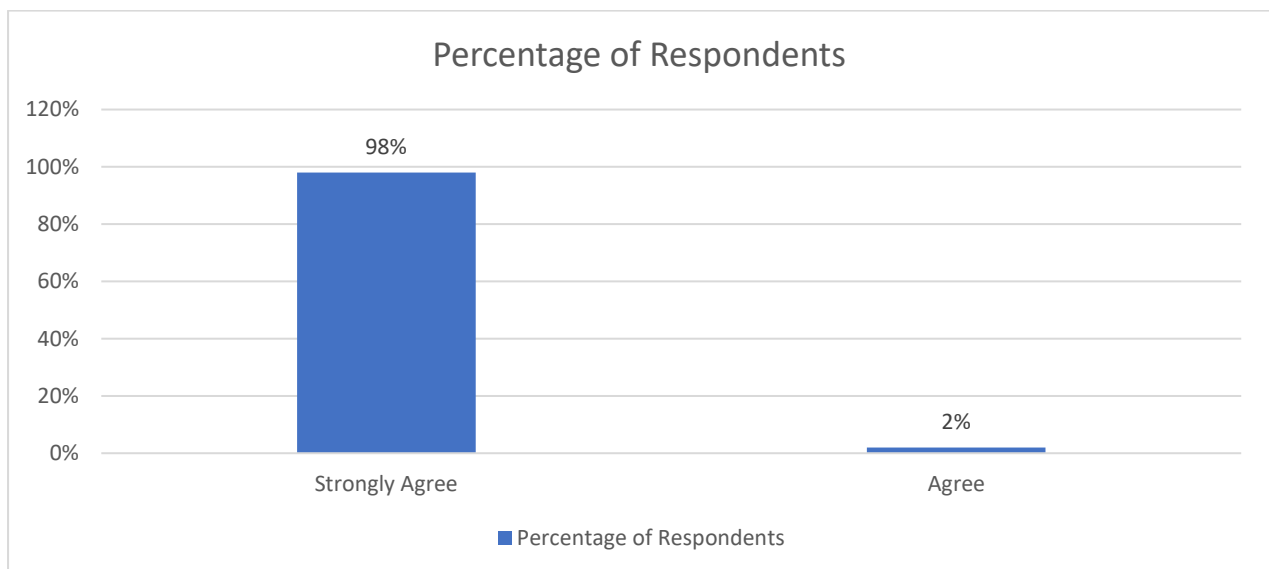


Chart 14: Ever experienced an unauthorized access to their online shopping.

Interpretation

The above table shows whether they experienced an unauthorized access to their online shopping. About 98% of the respondents strongly agree that they experienced an unauthorised access to their online shopping and 2% of respondents agreed to it.

4.15 WHICH OF THE FOLLOWING SECURITY CHALLENGES HAVE THEY ENCOUNTERED WHILE SHOPPING ONLINE?

The following table shows the respondent's view on security challenges have they encountered while shopping online.

Table 15: Security challenges have they encountered while shopping online

S. No.	Security challenges have you encountered while shopping online	No. of Respondents	% Of Respondents
1	Phishing attempts	12	21
2	Payment fraud	21	35
3	Data breaches or information leaks	16	26
4	Unauthorized access to your account	4	6
5	None of the above	7	12
	Total	60	100

Here the respondents were asked on security challenges have they encountered while shopping online. The following chart shows the data what has been obtained from the respondents in the pictorial format.

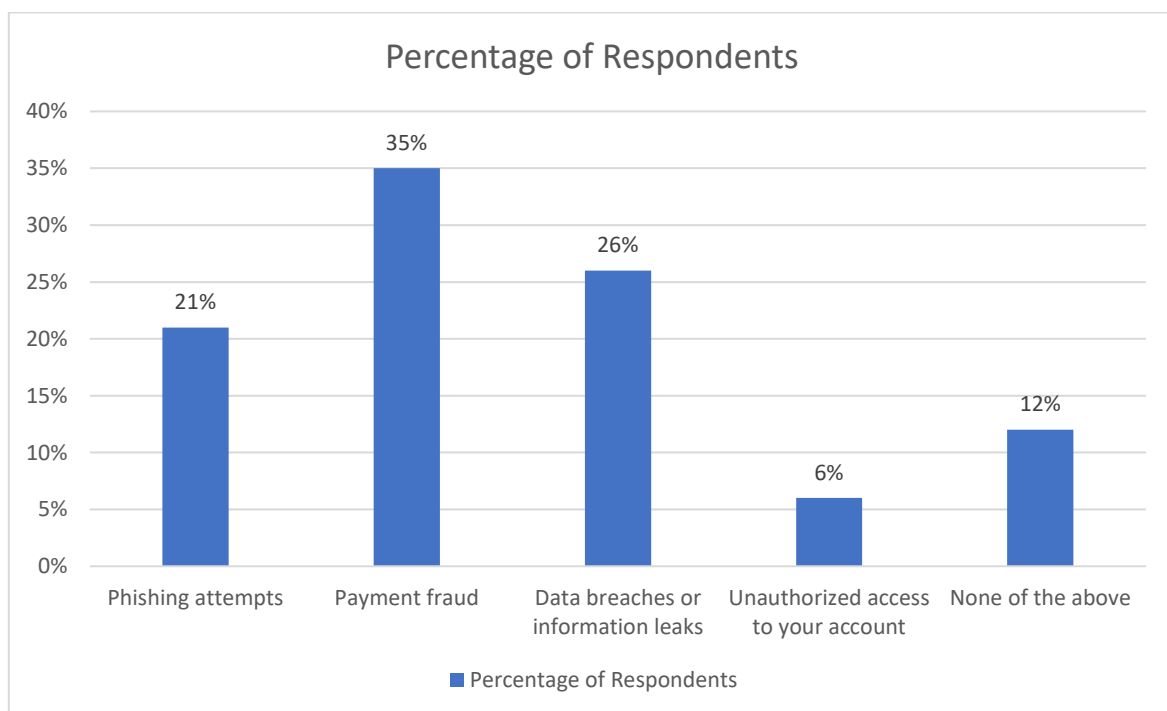


Chart 15: Security challenges have they encountered while shopping online.

Interpretation

The above table shows on security challenges have they encountered while shopping online. About 21% of the respondents have encountered phishing attempts while shopping online, 35% of the respondents have encountered payment fraud while shopping online, 26% of the respondents have data breaches or information leaks while shopping online, 6% of the respondents have encountered unauthorised access to your account while shopping online and 12% of the respondents have encountered none of the above while shopping online.

4.16 HOW OFTEN DO THEY ENCOUNTER CAPTCHA OR SECURITY CHECKS DURING ONLINE SHOPPING TO VERIFY THAT THEY ARE NOT A BOT?

The following table shows the respondent's view about whether they encounter captcha or security checks during online shopping to verify that they are not a bot.

Table 16: Number of times they encounter captcha or security checks during online shopping to verify that they are not a Bot.

S. No.	Number of times they encounter captcha or security checks during online shopping to verify that they are not a Bot	No. of Respondents	% Of Respondents
1	Very often	24	40
2	Often	13	22
3	Occasionally	9	14
4	Rarely	10	17
5	Never	4	7
	Total	60	100

Here the respondents were asked whether they encounter captcha or security checks during online shopping to verify that they are not a bot. The following chart shows the data what has been obtained from the respondents in the pictorial format.

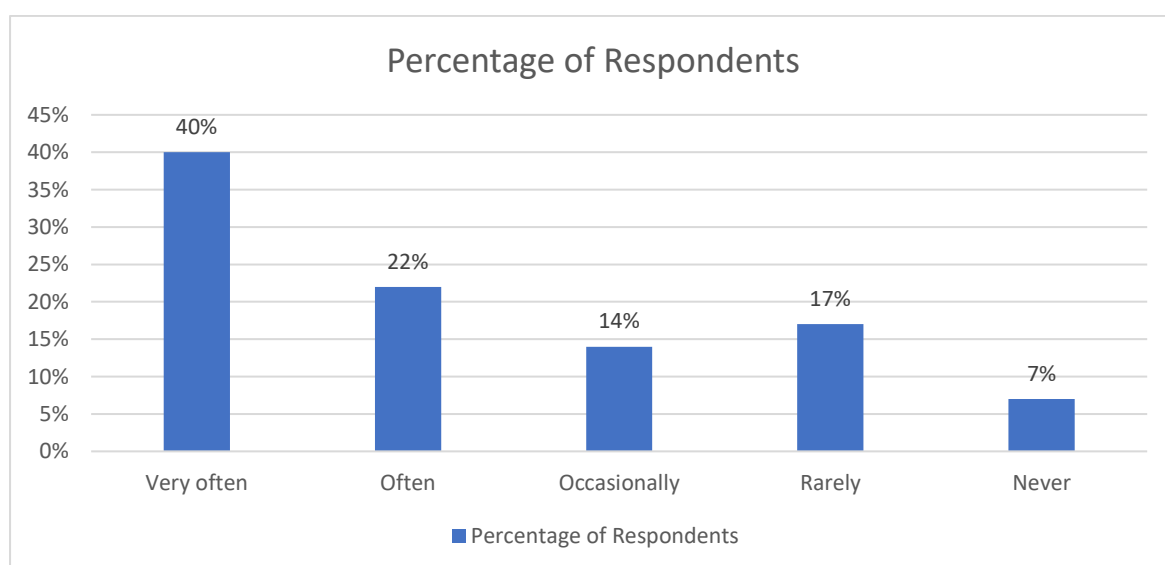


Chart 16: Number of times they encounter captcha or security checks during online shopping to verify that they are not a Bot.

Interpretation

The above table shows number of times they encounter captcha or security checks during online shopping to verify that they are not a Bot. About 40% of the respondents very often encountered captcha or security checks during online shopping and about 22% of the respondents often encountered to a greater extent on this context. But 14% of the respondents occasionally encountered the same. About 17% of the respondents rarely and about 10% of the respondents never encountered captcha or security checks during online shopping to verify that they are not a bot.

4.17 DO THEY REGULARLY UPDATE THEIR PASSWORDS FOR THEIR E-COMMERCE ACCOUNTS?

The following table shows the respondent's view whether they regularly update their passwords for their e-commerce accounts.

Table 17: Regularly update their passwords for their e-commerce accounts

S. No.	Regularly update their passwords for their e-commerce accounts	No. of Respondents	% Of Respondents
1	Yes, every few months	2	4
2	Yes, once a year	8	13
3	No, rarely	23	38
4	No, never	27	45
	Total	60	100

Here the respondents were asked whether they regularly update their passwords for their e-commerce accounts. The following chart shows the data what has been obtained from the respondents in the pictorial format.

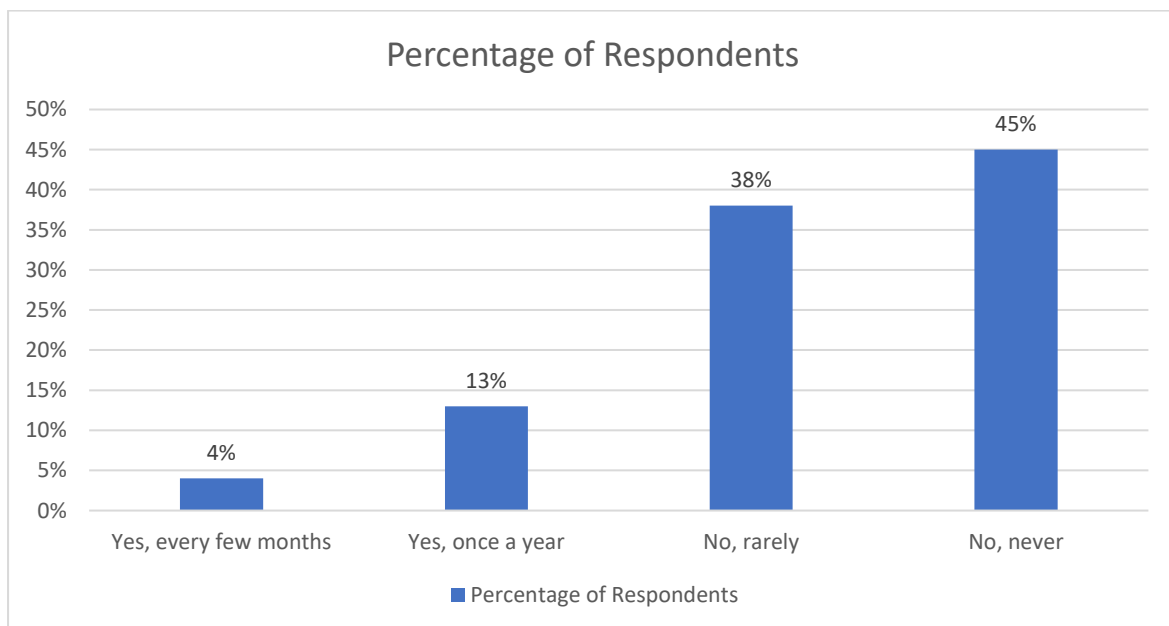


Chart 17: Regularly update their passwords for their e-commerce accounts

Interpretation

The above table shows whether they regularly update their passwords for their e-commerce accounts. About 4% of the respondents updating their passwords for every few months and about 13% of the respondents updating their passwords for at least once in a year. But 38% of the respondents will update their passwords rarely. About 45% of the respondents never update their passwords for their e-commerce accounts.

4.18 HOW DO THEY TYPICALLY RESPOND TO SECURITY WARNINGS OR ALERTS FROM THEIR WEB BROWSER WHEN VISITING E-COMMERCE WEBSITES?

The following table shows the respondent's view about how they respond to security warnings or alerts from their web browser when visiting e-commerce websites.

Table 18: Responses to security warnings or alerts from their web browser when visiting e-commerce websites

S. No.	Responses to security warnings or alerts from their web browser when visiting e-commerce websites	No. of Respondents	% Of Respondents
1	Always take them seriously and exit the site	9	15
2	Sometimes take them seriously, depending on the message	9	15
3	Ignore them and continue browsing	37	62
4	Not sure	5	8
	Total	60	100

Here the respondents were asked how they respond to security warnings or alerts from their web browser when visiting e-commerce websites. The following chart shows the data what has been obtained from the respondents in the pictorial format.

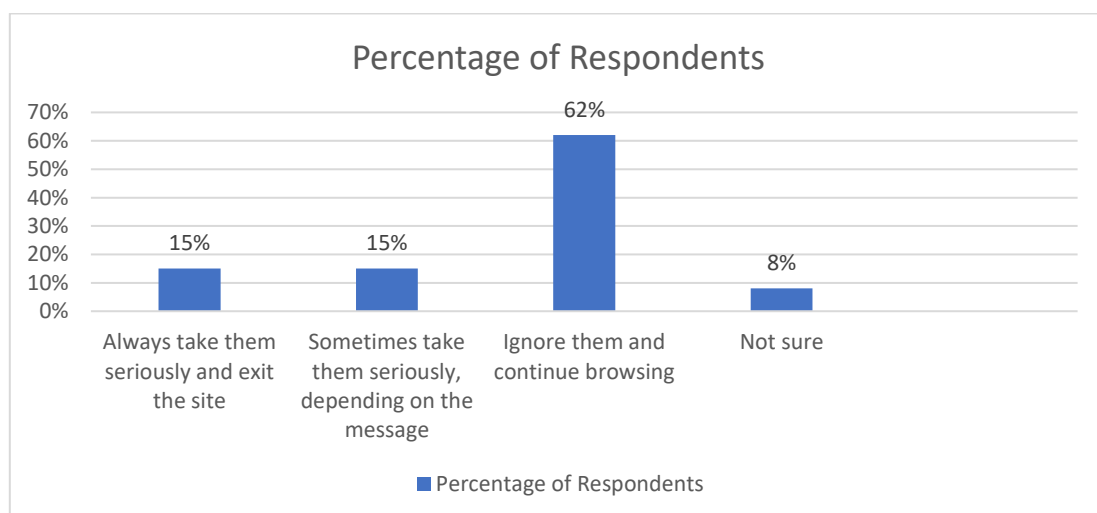


Chart 18: Responses to security warnings or alerts from their web browser when visiting e-commerce websites.

Interpretation

The above table shows how they respond to security warnings or alerts from their web browser when visiting e-commerce websites. About 15% of the respondents always take them seriously and exit the site and about 15% of the respondents take them seriously, depending on the message. But 62% of the respondents ignore them and continue browsing and 10% of the respondents are not sure about what they do when it comes to security warnings or alerts arises from their web browser while visiting e-commerce websites.

4.19 HAVE THEY ENABLED MULTI-FACTOR AUTHENTICATION (MFA) FOR THEIR E-COMMERCE ACCOUNTS WHEN AVAILABLE?

The following table shows the respondent's view on whether they enabled multi factor authentication for their e-commerce accounts when available.

Table 19: Enabled multi factor authentication for their e-commerce accounts when available

S. No.	Enabled multi factor authentication for their e-commerce accounts when available	No. of Respondents	% Of Respondents
1	Yes, for all accounts	24	40
2	Yes, for some accounts	16	27
3	No, for any accounts	13	22
4	Not sure what multi-factor authentication is	7	11
	Total	60	100

Here the respondents were asked whether they enabled multi factor authentication for their e-commerce accounts when available. The following chart shows the data what has been obtained from the respondents in the pictorial format.

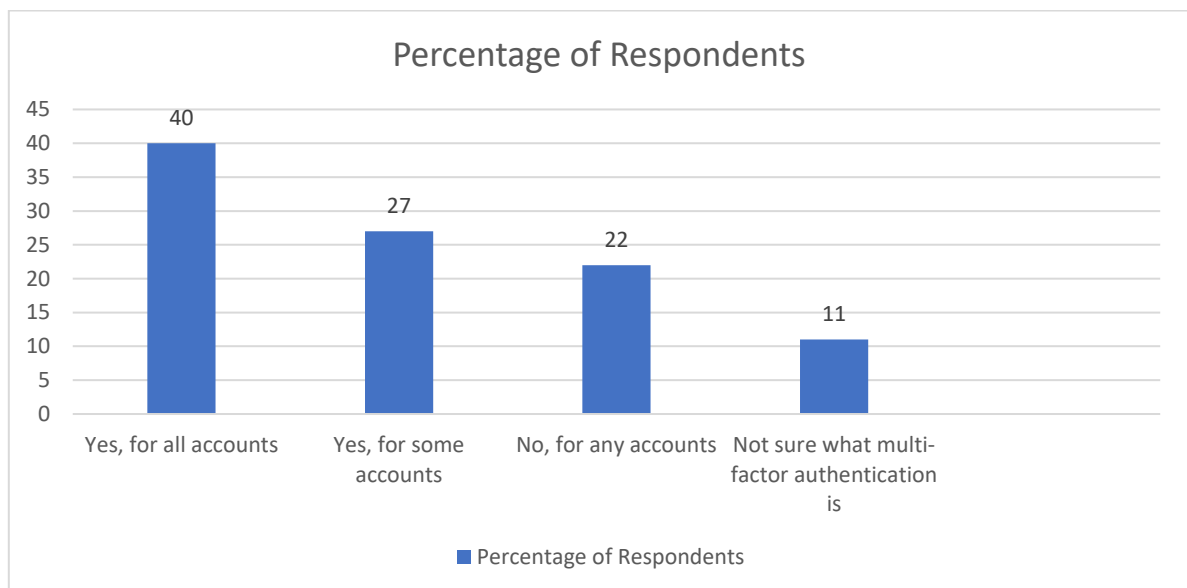


Chart 19: Enabled multi factor authentication for their e-commerce accounts when available.

Interpretation

The above table shows whether they enabled multi factor authentication for their e-commerce accounts when available. About 40% of the respondents enabled multi factor authentication for their e-commerce accounts and about 27% of the respondents enabled their authentication factor to some accounts. But 22% of the respondents didn't enable multifactor authentication to any of the accounts and 11% of the respondents was not sure about multifactor authentication.

4.20 DO THEY USE ANTIVIRUS OR ANTI-MALWARE SOFTWARE ON THEIR DEVICES FOR ADDED SECURITY WHILE SHOPPING ONLINE?

The following table shows the respondent's view on their usage of antivirus or anti-malware software on their devices for added security while shopping online.

Table 20: Usage of antivirus or anti-malware software on their devices for added security while shopping online.

S. No.	Usage of antivirus or anti-malware software on their devices for added security while shopping online	No. of Respondents	% Of Respondents
1	Yes, on all devices	51	85
2	Yes, on some devices	7	13
3	No, on any device	2	2
4	Not sure	1	1
	Total	60	100

Here the respondents were asked whether they use antivirus or anti-malware software on their devices for added security while shopping online. The following chart shows the data what has been obtained from the respondents in the pictorial format.

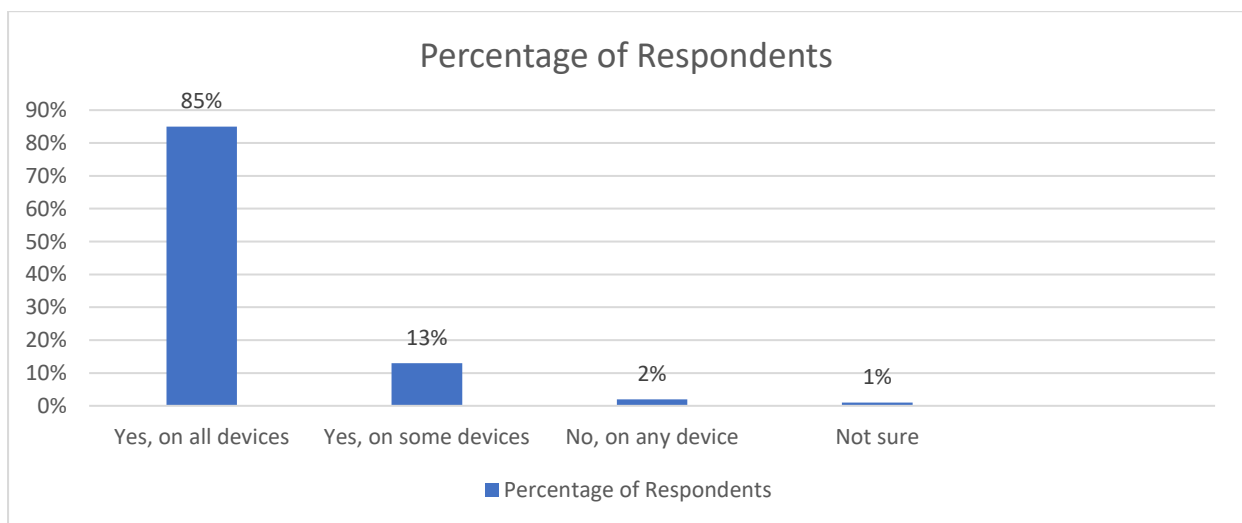


Chart 20: Usage of antivirus or anti-malware software on their devices for added security while shopping online.

Interpretation

The above table shows the Usage of antivirus or anti-malware software on their devices for added security while shopping online. About 85% of the respondents uses antivirus or anti-malware software on all of their devices, 13% of the respondents uses antivirus software only on some devices. But 2% of respondents doesn't use antivirus or anti-malware software on their devices for added security while shopping online and 1% of respondents didn't sure about using antivirus or anti-malware software.

4.21 WHICH OF THE FOLLOWING SECURE PAYMENT METHODS DO THEY PREFER WHEN SHOPPING ONLINE?

The following table shows the respondent's view about their secure payment methods they prefer when shopping online.

Table 21: Payment methods preferred when shopping online

S. No.	Payment methods preferred when shopping online	No. of Respondents	% Of Respondents
1	Credit card with fraud protection	12	20
2	PayPal	22	36
3	Digital wallets	18	30
4	Cryptocurrency	3	5
5	Bank transfer	4	7
6	Other	1	2
	Total	60	100

Here the respondents were asked about the secure payment methods they prefer when shopping online. The following chart shows the data what has been obtained from the respondents in the pictorial format.

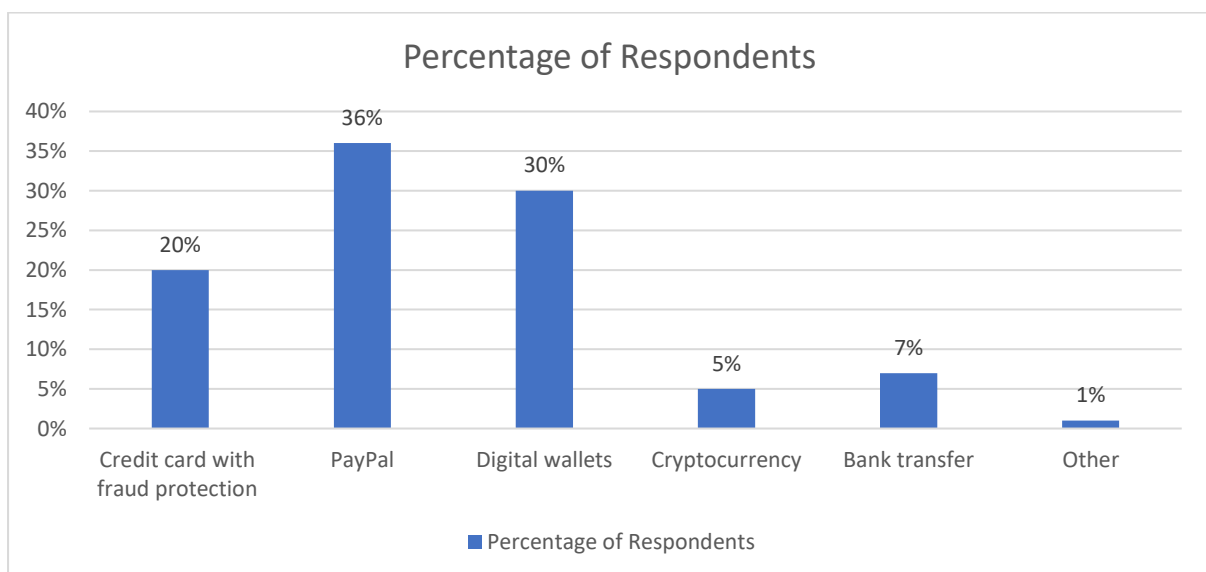


Chart 21: Payment methods preferred when shopping online.

Interpretation

The above table shows the secure payment methods they prefer when shopping online. About 20% of the respondents uses credit card with fraud protection for payment, 36% of the respondents uses PayPal to make payment while shopping online. But 30% of respondents use digital wallets as their payment methods preferred when shopping online. About 5% of respondents use cryptocurrency and 1% of respondents use other methods to make payment when they shop in online.

4.22 HOW WOULD THEY PREFER TO RECEIVE SECURITY TIPS AND RECOMMENDATIONS FOR SAFER ONLINE SHOPPING?

The following table shows the respondent's view about their preference to receive security tips and recommendations for safer online shopping.

Table 22: Preferable way to receive security tips and recommendations for safer online shopping.

S. No.	Preferable way to receive security tips and recommendations for safer online shopping	No. of Respondents	% Of Respondents
1	Email newsletters	11	19
2	In-app notifications from e-commerce platforms	20	34
3	Social media posts	18	30
4	Dedicated security app	10	15
5	Other	1	2
	Total	60	100

Here the respondents were asked about their preference to receive security tips and recommendations for safer online shopping. The following chart shows the data what has been obtained from the respondents in the pictorial format.

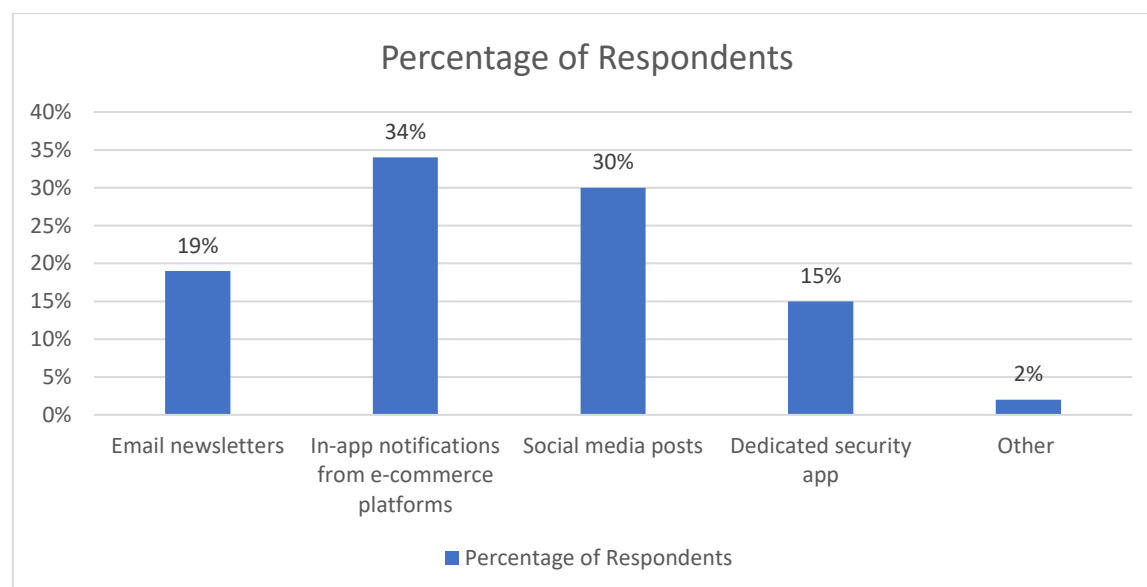


Chart 22: Preferable way to receive security tips and recommendations for safer online shopping

Interpretation

The above table shows about their preference to receive security tips and recommendations for safer online shopping. About 19% of the respondents prefer email newsletters to receive security tips, 34% of respondents prefer In-app notifications from e-commerce platforms to receive tips and recommendation for safer shopping. But 30% of respondents prefer social media posts to get their tips and recommendations for safer online shopping. About 15% of respondents prefer dedicated security app and 2% of respondents prefer other mode to receive security tips and recommendations for safer online shopping.

4.23 ARE THEY INTERESTED IN EDUCATIONAL RESOURCES OR TUTORIALS THAT TEACH THEM HOW TO RECOGNIZE AND AVOID ONLINE SECURITY THREATS?

The following table shows the respondent's view about their interest in educational resources or tutorials that teach them how to recognize and avoid online security threats.

Table 23: Interest in educational resources or tutorials that teach them how to recognize and avoid online security threats

S. No.	Interest in educational resources or tutorials that teach them how to recognize and avoid online security threats	No. of Respondents	% Of Respondents
1	Very interested	23	38
2	Somewhat interested	15	25
3	Not very interested	18	30
4	Not interested at all	4	7
	Total	60	100

Here the respondents were asked about their interest in educational resources or tutorials that teach them how to recognize and avoid online security threats. The following chart shows the data what has been obtained from the respondents in the pictorial format.

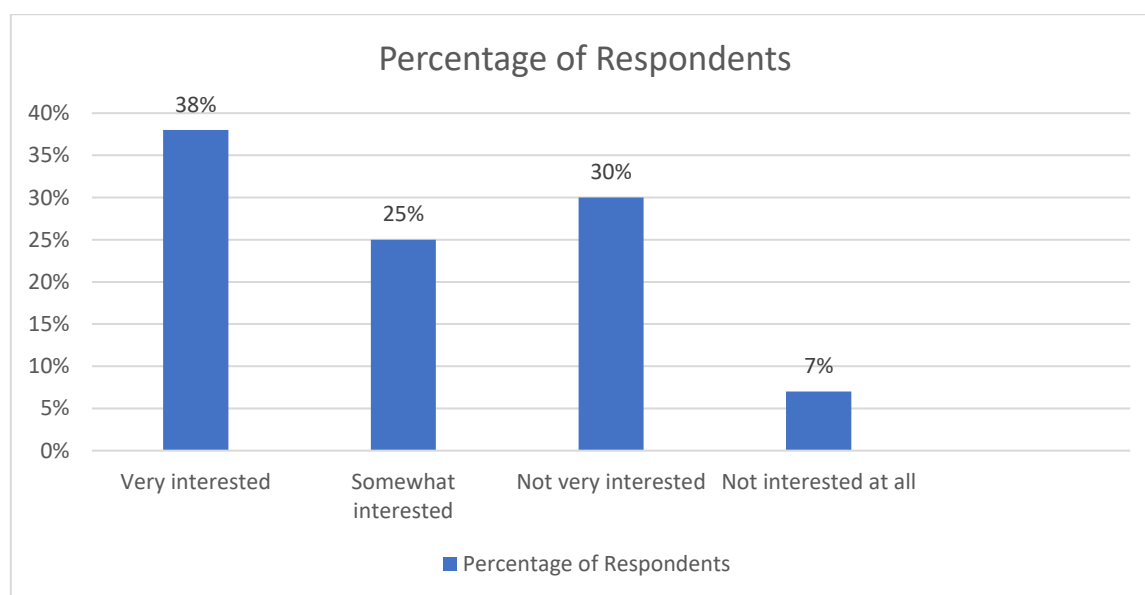


Chart 23: Interest in educational resources or tutorials that teach them how to recognize and avoid online security threats.

Interpretation

The above table shows about respondents' interest in educational resources or tutorials that teach them how to recognize and avoid online security threats. About 38% of the respondents very interested in get guidance using educational resources or tutorials that teach them how to recognize and avoid online security threats, 25% of the respondents were somewhat interested in getting awareness through tutorials. But 30% of the respondents were not very interested in educational resources or tutorials to recognise and avoid online security threats. About 7% of the respondents not at all interested in any of the resources that teach them to avoid security threats.

CHI SQUARE ANALYSIS

4.24 RELATIONSHIP BETWEEN THE AGE OF RESPONDENTS AND SECURITY AWARENESS AMONG THE USERS OF THE E-COMMERCE PLATFORM

The relationship between the age of the respondents and security awareness among the users of the e-commerce platform has been analysed using the chi-square test.

Age group

S. No.	Age Group	No. of Respondents	% Of Respondents
1	Below 25 years	20	33
2	25 – 30	15	25
3	31 – 35	4	6
4	36 – 40	3	5
5	41 – 45	12	21
6	45 and above	6	10
	Total	60	100

Awareness of the potential security risks associated with online shopping, such as Data breaches or Phishing attacks.

S. No.	Awareness of the potential security risks associated with online shopping, such as Data breaches or Phishing attacks.	No. of Respondents	% Of Respondents
1	Yes, very aware	6	11
2	Yes, somewhat aware	16	26
3	No, not very aware	21	35
4	No, not aware at all	17	28
	Total	60	100

H0: There is no significant relationship between age of the respondents and security awareness among the users of e-commerce platform

H1: There is a significant relationship between age of the respondents and security awareness among the users of e-commerce platform

O – Observed Frequency

E – Expected Frequency

Expected frequency of any cell = $(\text{Row total of any cell}) * (\text{Column total of any cell})$

Overall Total

Table No: 24 Relationship between the age of the respondents and security awareness among the users of the e-commerce platform

Age \ Security awareness among the users of e-commerce platform	Yes, very aware	Yes, somewhat aware A	No, not very aware	No, not aware at all	Row Total
Below 25 years	1	4	5	10	20
25 – 30	2	5	5	3	15
31 – 35	0	2	1	1	4
36 – 40	1	0	1	1	3
41 – 45	1	4	5	2	12
45 and above	1	1	4	0	6
Column Total	6	16	21	17	60

O	E	O-E	(O-E) ²	(O-E) ² / E
1	2	-1	1	0.5
4	5.33	-1.33	1.7	0.33
5	7	-2	4	0.57
10	5.67	4.33	18.7	3.3
2	1.5	0.5	0.25	0.16
5	4	1	1	0.25
5	5.25	-0.25	0.06	0.01
3	4.25	-1.25	1.56	0.3
0	0.4	-0.4	0.16	0.4

2	1.06	0.94	0.88	0.8
1	1.4	-0.4	0.16	0.11
1	1.13	-0.13	0.01	0.01
1	0.3	0.7	0.49	1.6
0	0.8	-0.8	0.64	0.8
1	1.05	-0.05	0.0025	0.002
1	0.85	0.15	0.0225	0.02
1	1.2	-0.2	0.04	0.03
4	3.2	0.8	0.64	0.2
5	4.2	0.8	0.64	0.15
2	3.4	-1.4	1.96	0.57
1	0.6	0.4	0.16	0.26
1	1.6	-0.6	0.36	0.22
4	2.1	1.9	3.61	1.71
0	1.7	-1.7	2.89	1.7
			Calculated Value	14.20

Calculated Value = 14.20

Degrees of Freedom = $(r-1) * (c-1) = (6 - 1) * (4 - 1)$

= 15

Level of Significance = 5%

Table value 25.00

Here the calculated value is lesser than the table value ($CV < TV$ i.e. $14.20 < 25.00$). So, accept H_0 , hence there is no significant relationship between the age of the respondents and security awareness among the users of the e-commerce platform.

CHAPTER 5

FINDINGS, SUGGESTION AND CONCLUSION

5.1 FINDINGS OF THE STUDY

- About 51% of the respondents are male and about 49% of the respondents are female.
- About 33% of the respondents are below the age of 25 years of age, about 25% of the respondents are between the age of 25 to 30 years of age, about 6% of the respondents are between the age of 31 to 35 years of age, about 5% of the respondents are between the age of 36 to 40 years of age, about 21% of the respondents are between the age of 41 to 45 years of age, and about 10% of the respondents are above 45 years of age.
- How often do they use online platforms for shopping in a month. About 44% of the respondents do online shopping more than once, about 28% of the respondents shop around 1 to 4 times, about 21% shop for 4 to 8 times and 4% of the respondents shop from 8 to 12 times. However, 3% of the respondents shop more than 12 times in online platforms.
- The highest purchased product in online. About 15% of respondents purchased Grocery through online, 19% of respondents preferred to buy electronics, 27% of respondents buy textile products, 10% of respondents bought beauty products, 2% of respondents bought furniture, 18% of respondents used online platform to buy pharmacy items, 5% of respondents used to purchase books, 1% of respondents bought toys and 3% of respondents preferred to buy products other than items specified.
- The respondents feel safe while making online payment. About 67% of respondents feel safe while making online payment, 33% of respondents doesn't feel safe while making online payment.
- E-commerce websites are easy to navigate or not. About 56% of respondents felt easy to navigate e-commerce websites, 44% of respondents doesn't feel that e-commerce websites are easy to navigate.
- The respondents view about have they ever stopped using an e-commerce platform due to security concern. About 92% of respondents have stopped using e-commerce platform due to security concern, 8% of respondents doesn't stop using an e-commerce platform due to security concern.

- How transparent are e-commerce platform about their security practices. About 35% of respondents say that e-commerce websites are very transparent about their security practices, 49% of respondents says e-commerce websites are somewhat transparent about their security practices, 7% of respondents says e-commerce websites are not very transparent about their security practices and 9% of respondents says e-commerce websites are not at all transparent when it comes to security practices.
- How concerned are the respondents about the security of their personal and financial information when making online purchases. About 26% of respondents are very concerned about the security of their personal and financial information when making online purchases, 43% of respondents are somewhat concerned about the security of their personal and financial information when making online purchases, 16% of respondents are not very concerned about the security of their personal and financial information when making online purchases and 15% of respondents are not concerned at all about the security of their personal and financial information when making online purchases.
- They experienced on a security breach or unauthorised access to their account on e-commerce platforms. About 6% of the respondents has experienced on a security breach or unauthorised access to their account on e-commerce platforms, 76% of the respondents doesn't experience on a security breach or unauthorised access to their account on e-commerce platforms and 18% of the respondents are not sure about whether they faced such kind of situation.
- What is their primary concern regarding security while using an e-commerce platform. About 14% of the respondents strongly agree and about 22% of the respondents agree to a greater extent on this context. But 40% of the respondents remain neutral on the objective and process of performance appraisal were described clearly. About 14% of the respondents disagree and about 10% of the respondents strongly disagree.
- They aware of the potential security risks associated with online shopping, such as data breaches or phishing attacks. About 11% of the respondents are very aware about the potential security risks associated with online shopping, such as data breaches or phishing attacks, 26% of respondents are somewhat aware about the risks associated with online shopping, such as data breaches or phishing attacks, 35% of the respondents are not very aware about the potential security risks with online shopping, such as data

breaches or phishing attacks and 28% of respondents are not at all aware about the risks associated with online shopping, such as data breaches or phishing attacks.

- E-commerce platforms take adequate measures to protect their personal and financial information. About 14% of the respondents strongly agree and about 22% of the respondents agree to a greater extent. But 40% of the respondents remain neutral. About 14% of the respondents disagree and about 10% of the respondents strongly disagree on e-commerce platforms take adequate measures to protect their personal and financial information.
- They experienced an unauthorized access to their online shopping. About 98% of the respondents strongly agree that they experienced an unauthorised access to their online shopping and 2% of respondents agreed to it.
- Security challenges have they encountered while shopping online. About 21% of the respondents have encountered phishing attempts while shopping online, 35% of the respondents have encountered payment fraud while shopping online, 26% of the respondents have data breaches or information leaks while shopping online, 6% of the respondents have encountered unauthorised access to your account while shopping online and 12% of the respondents have encountered none of the above while shopping online.
- Number of times they encounter captcha or security checks during online shopping to verify that they are not a Bot. About 40% of the respondents very often encountered captcha or security checks during online shopping and about 22% of the respondents often encountered to a greater extent on this context. But 14% of the respondents occasionally encountered the same. About 17% of the respondents rarely and about 10% of the respondents never encountered captcha or security checks during online shopping to verify that they are not a bot.
- They regularly update their passwords for their e-commerce accounts. About 4% of the respondents updating their passwords for every few months and about 13% of the respondents updating their passwords for at least once in a year. But 38% of the respondents will update their passwords rarely. About 45% of the respondents never update their passwords for their e-commerce accounts.
- They respond to security warnings or alerts from their web browser when visiting e-commerce websites. About 15% of the respondents always take them seriously and exit the site and about 15% of the respondents take them seriously, depending on the

message. But 62% of the respondents ignore them and continue browsing and 10% of the respondents are not sure about what they do when it comes to security warnings or alerts arises from their web browser while visiting e-commerce websites.

- They enabled multi factor authentication for their e-commerce accounts when available. About 40% of the respondents enabled multi factor authentication for their e-commerce accounts and about 27% of the respondents enabled their authentication factor to some accounts. But 22% of the respondents didn't enable multifactor authentication to any of the accounts and 11% of the respondents was not sure about multifactor authentication.
- The Usage of antivirus or anti-malware software on their devices for added security while shopping online. About 85% of the respondents uses antivirus or anti-malware software on all of their devices, 13% of the respondents uses antivirus software only on some devices. But 2% of respondents doesn't use antivirus or anti-malware software on their devices for added security while shopping online and 1% of respondents didn't sure about using antivirus or anti-malware software.
- The secure payment methods they prefer when shopping online. About 20% of the respondents uses credit card with fraud protection for payment, 36% of the respondents uses PayPal to make payment while shopping online. But 30% of respondents use digital wallets as their payment methods preferred when shopping online. About 5% of respondents use cryptocurrency and 1% of respondents use other methods to make payment when they shop in online.
- About 19% of the respondents prefer email newsletters to receive security tips, 34% of respondents prefer In-app notifications from e-commerce platforms to receive tips and recommendation for safer shopping. But 30% of respondents prefer social media posts to get their tips and recommendations for safer online shopping. About 15% of respondents prefer dedicated security app and 2% of respondents prefer other mode to receive security tips and recommendations for safer online shopping.
- About 38% of the respondents very interested in get guidance using educational resources or tutorials that teach them how to recognize and avoid online security threats, 25% of the respondents were somewhat interested in getting awareness through tutorials. But 30% of the respondents were not very interested in educational resources or tutorials to recognise and avoid online security threats. About 7% of the respondents not at all interested in any of the resources that teach them to avoid security threats.

- There is no significant relationship between the age of the respondents and security awareness among the users of the e-commerce platform

5.2 SUGGESTION

- Since 30% of respondents prefer social media for security tips, e-commerce platforms should leverage these channels to share regular updates and recommendations on safer online shopping.
- Given that 67% of respondents feel safe making online payments, e-commerce platforms should maintain and communicate their strong security practices to bolster users' trust.
- Encourage more users to enable multi-factor authentication, as 22% didn't enable it and 11% were unsure. E-commerce platforms can emphasize the importance of this security feature.
- Promote password updates as 45% of respondents never update their passwords. Encourage users to update their passwords regularly to enhance security.
- Raise awareness about the significance of responding to security warnings in web browsers, as 62% of respondents tend to ignore them. Users should be educated on the potential risks.
- E-commerce platforms should implement strong measures to protect users from phishing attempts and payment fraud, as these were significant challenges for 21% and 35% of respondents, respectively.
- Explore ways to reduce the frequency of captcha checks during online shopping for the 40% of users who very often encounter them, as this can improve the user experience.
- Address the security concerns of the 44% of respondents who don't feel that e-commerce websites are easy to navigate. Improving website usability can enhance the overall security experience.

5.3 CONCLUSION

The study on E-commerce security issues and their solutions provides valuable insights into the perceptions, behaviours, and concerns of e-commerce platform users. The findings shed light on several key aspects of online shopping security: Firstly, it is evident that the gender distribution among respondents is almost balanced, with a slightly higher representation of males (51%) compared to females (49%). This highlights the need for gender-inclusive security measures and educational resources. Secondly, the age distribution reveals that a significant portion of users (33%) falls below the age of 25, indicating that younger generations are actively engaging in online shopping. Tailoring security practices to this demographic is essential.

The study underscores the importance of user experiences and preferences. While a considerable portion of users feels safe making online payments (67%), a significant number (92%) have stopped using e-commerce platforms due to security concerns. This highlights the paramount importance of transparent security practices and the need to address user concerns to retain and expand the e-commerce user base. Furthermore, the study shows that security challenges like phishing attempts and payment fraud are prevalent concerns among users. Addressing these specific issues and providing guidance through educational resources and tutorials is crucial.

In summary, the study emphasizes the necessity for e-commerce platforms to enhance transparency, security education, and user engagement. By understanding the diverse needs and concerns of their user base, e-commerce platforms can fortify their security measures, build trust, and foster a safer and more enjoyable online shopping environment.

REFERENCES

1. Mohanad Halaweh, Christine Fidler (2008) - " Security Perception in Ecommerce: Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008-IEEE
2. Yuanqiao Wen, Chunhui Zhou (2008) "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management.
3. Biswajit Tripathy, Jibitesh Mishra (2013). "Protective measures in ecommerce to deal with security threats arising out of social issues a framework" iaeme-issn 0976 – 6375(online) volume 4, issue 1, January- February (2013),
4. Shazia Yasin, Khalid Haseeb (2012). "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012
5. Abdulghader.A.Ahmed.Moftah (2012)."Challenges of security, protection and trust on e- commerce: a case of online Purchasing in Libya". Issn: 2278-1021-ijarcce vol. 1, issue 3, May 2012.
6. A Sengupta, C Mazumdar (2005) "e-commerce security – a life cycle approach" sadhana vol. 30, parts 2 & 3, April/June 2005
7. Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues “Proceedings of the 35th Hawaii International Conference on System Sciences - 2002
8. Rashad Yazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development “International Conference on Information Communication and Management - IPCSIT vol.16 (2011)
9. Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSIT vol.9 (2011)
10. Dr. Nada M. A. Al-Slamy, "E-Commerce security" IJCSNS - VOL.8 No.5, May 2008
11. W. Jeberson, Prof. (Col.). Gurmit Singh. "Analysis of Security Measures Implemented on G2C Online Payment Systems in India" MIT International Journal of Computer Science & Information Technology Vol. 1 No. 1 Jan. 2011
12. Biswajit Tripathy, Jibitesh Mishra. "PROTECTIVE MEASURES IN ECOMMERCE TO DEAL WITH SECURITY THREATS ARISING OUT OF SOCIAL ISSUES – A FRAMEWORK" IAEME -ISSN 0976 – 6375(Online) Volume 4, Issue 1, January-February (2013)

13. Pradnya B. Rane, Dr.B.B.Meshram. "Transaction Security for Ecommerce Application"
IJECS -ISSN- 2277-1956. 2012
14. Yang Jing "On-line Payment and Security of E-commerce". ISBN 978- 952-5726-00-8
, 2009 International Symposium on Web Information Systems and Applications
(WISA'09)
15. Niranjana Murthy M, Kavyashree N, Mr S.Jagannath —MCOMMERCE: SECURITY
CHALLENGES ISSUES AND RECOMMENDED SECURE PAYMENT METHOD||
- IJMIE Volume 2, Issue 8 ISSN: 2249-0558 -2012
16. Thomas L. Mesenbourg, An Introduction to E-commerce, Philippines: DAI-AGILE,
(2000)
17. R. E. Walch, "Electronic commerce," in Key Aspects of German Business Law (Fourth
Edition): A Practical Manual, 2009.
18. E. Turban, J. Whiteside, D. King, and J. Outland, Introduction to Electronic Commerce
and Social Commerce. 2017.
19. E. E. Grandon and J. M. Pearson, "Electronic commerce adoption: An empirical study
of small and medium US businesses," Inf. Manag., 2004, doi:
10.1016/j.im.2003.12.010
20. D. Gefen, "E-commerce: The role of familiarity and trust," Omega, 2000, doi:
10.1016/S0305-0483(00)00021-9
21. D. Peterson, "Introduction to E-commerce," in Financial Services Information Systems,
2000.
22. Kolesar, M.B., & Galbraith, R. W. (2000). A services-marketing perspective on e-
retailing: Implications for e-retailers and directions for further research. Internet
Research, 10(5), 424-38. [Http://dx.doi.org/ 10.1108/10662240010349444](http://dx.doi.org/10.1108/10662240010349444)
23. Ltifi, M., & Gharbi, J. (2012). E-satisfaction and e-loyalty of consumers shopping
online. Journal of Internet Banking and Commerce, 17(1).
24. Dowling, G.R., & Staelin, R. (1994). A model of perceived risk and intended risk
handling activity. Journal of Consumer Research, 21(1), 119-34. [Http://
dx.doi.org/10.1086/209386](http://dx.doi.org/10.1086/209386)
25. Kim, D., & Benbasat, I. (2009). Trust-assuring arguments in B2C ecommerce: Impact
of content, source, and price on trust. Journal of Management Information Systems,
26(3), 175-206. [Http://dx.doi.org/10.2753/ mis0742-1222260306](http://dx.doi.org/10.2753/mis0742-1222260306)

26. Sinha, P., & Singh, S. (2014). Product characteristics vis-à-vis consumers' risk perception: A conceptual study of online shopping. *IUP Journal Of Marketing Management*, 13(2), 40-57.
27. Joonkyum, L., & Bumsoo, K. (2014). Assortment optimization under consumer choice behavior in online retailing. *Management Science & Financial Engineering*, 20(2), 27-31. [Http://dx.doi.org/10.7737/msfe.2014.20.2.027](http://dx.doi.org/10.7737/msfe.2014.20.2.027)
28. Miyazaki, A., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *J Consum Aff*, 35(1), 27-44. [Http://dx.doi.org/10.1111/j.1745-6606.2001.tb00101.x](http://dx.doi.org/10.1111/j.1745-6606.2001.tb00101.x)
29. Turban, E. (2012). *Electronic commerce*. Upper Saddle River, NJ: Prentice Hall.
30. Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, 31(1), 105-36. [Http://www.jstor.org/stable/25148783](http://www.jstor.org/stable/25148783)
31. Bente, G., Ruggenberg, S., Kramer, N.C., & Eschenburg, F. (2008). Avatar-mediated networking: Increasing social presence and interpersonal trust in net-based collaborations. *Hum Commun Res*, 34(2), 287-318. [Http://dx.doi.org/10.1111/j.1468-2958.2008.00322.x](http://dx.doi.org/10.1111/j.1468-2958.2008.00322.x)
32. Moon, J. H., Kim, E., Choi, S. M., & Sung, Y. (2013). Keep the social in social media: The role of social interaction in avatar-based virtual shopping. *Journal of Interactive Advertising*, 13(1), 14-26. [Http://dx.doi.org/10.1080/15252019.2013.768051](http://dx.doi.org/10.1080/15252019.2013.768051)
33. Zhang, H., Lu, Y., Shi, X., Tang, Z., & Zhao, Z. (2012). Mood and social presence on consumer purchase behaviour in C2C E-commerce in Chinese culture. *Electronic Markets*, 22(3), 143-54. [Http://dx.doi.org/10.1007/s12525-012-0097-z](http://dx.doi.org/10.1007/s12525-012-0097-z)
34. Dash, S., & Saji, K.B. (2007). The role of consumer self-efficacy and website social presence in customers' adoption of b2c online shopping: An empirical study in the Indian context. *Journal of International Consumer Marketing*, 20(2), 33-48. [Http://dx.doi.org/10.1300/j046v20n02_04](http://dx.doi.org/10.1300/j046v20n02_04)
35. Ltifi, M., & Gharbi, J. (2012). E-satisfaction and e-loyalty of consumers shopping online. *Journal of Internet Banking and Commerce*, 17(1).
36. Muhannad, K., & Ahmed, G. (2014). Customer perceptions of e-commerce in the United Arab Emirate. *International Journal of Global Business*, 7(1), 95-109.
37. Shin, D., & Shin, Y. (2011). Consumers' trust in virtual mall shopping: the role of social presence and security. *Int J Hum Comput Interact*, 27(5), 450-75. [Http://dx.doi.org/10.1080/10447318.2011.552060](http://dx.doi.org/10.1080/10447318.2011.552060)

38. Gupta, P., Dubey, A., (2016). E-Commerce-Study of Privacy, Trust and Security from Consumer's Perspective, *International Journal of Computer Science and Mobile Computing* 5, 6, 224–232.
39. Michałowska, M., Kotylak, S., Danielak, W., 2015. Forming relationships on the e-commerce market as a basis to build loyalty and create value for the customer, Empirical findings. *Management* 19, 1, 57-72, 10.1515/manment-2015-0005.
40. Barry, S. (2002). *Business to Business internet marketing*. Canada: Jim Hoskins.
41. Tang, T.L.P., Luna Arocas, R & Sutarso, T. (2005). From income to pay satisfaction: The love of money and pay equity comparison as mediators and culture (The US and Spain) and gender as moderators, *management research, The journal of the Iberoamerican academy of management* 3 (1), pp 7-26.
42. Heng, M. (2003). Understanding electronic commerce from a historical perspective. *Communication of the association for information systems*.
43. Sekaran, U. (2000). *Research methods for business: A skill business approach*. John Wiley & Sons, New York.
44. Muijs, D. (2004). *Doing quantitative research in education with SPSS*, 2nd edition.
45. Israel D. Fianyi (Nov, 2015) "Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics" *International Journal of Computer Science*, Volume 12, Issue 6
46. Chu, K.-M., & Yuan, J. (2013). The effects of perceive interactivity on e-trust and e-consumer behaviors: the application of fuzzy linguistic scale. *Journal of Electronic Commerce Research*, 14(1), 124
47. Kimery, K. M., & mccord, M. (2002). Third party assurances: mapping the road to trust in etailing. *Journal of Information Technology Theory and Application (JITTA)*, 4(2), 7.
48. Ali, K. M. (2014). Consumer Perceived Risk, Attitude and Online Shopping Behaviour; Empirical Evidence from Malaysia. Paper presented at the IOP Conference Series: Materials Science and Engineering.
49. Tanadi, T., Samadi, B., & Gharleghi, B. (2015). The impact of perceived risks and perceived benefits to improve an online intention among generation-Y in Malaysia. *Asian Social Science*, 11(26), 226.
50. V.Srikanth "Ecommerce online security and trust marks". *IJCET* ISSN 0976 – 6375, Volume 3, Issue 2, julyseptember (2012).

ANNEXURE

QUESTIONNAIRE

1. Gender

- ☐ Male
- ☐ Female

2. Age Group

- ☐ Below 25 years
- ☐ 25-30
- ☐ 31-35
- ☐ 36-40
- ☐ 41-45
- ☐ 45 and above

3. How often do you use online platform for shopping in a month?

- ☐ More than once
- ☐ 1 – 4
- ☐ 4 – 8
- ☐ 8 – 12
- ☐ More than 12

4. Which product do you purchase more often in online?

- ☐ Grocery
- ☐ Electronics
- ☐ Textile
- ☐ Beauty product
- ☐ Furniture
- ☐ Pharmacy
- ☐ Books
- ☐ Toys
- ☐ Others

5. Do you feel safe while making online payment

- ☐ Yes
- ☐ No

6. Do you find e-commerce websites easy to navigate?
- ☐ Yes
 - ☐ No
7. Have you ever stopped using an e-commerce platform due to security concerns?
- ☐ Yes
 - ☐ No
8. In your opinion, how transparent are e-commerce platform about their security practices?
- ☐ Very transparent
 - ☐ Somewhat transparent
 - ☐ Not very transparent
 - ☐ Not at all transparent
9. How concerned are you about the security of your personal and financial information when making online purchases?
- ☐ Very concerned
 - ☐ Somewhat concerned
 - ☐ Not very concerned
 - ☐ Not concerned at all
10. Have you ever experienced a security breach or unauthorised access to your account on an e-commerce platform?
- ☐ Yes
 - ☐ No
 - ☐ Not sure
11. When using an e-commerce platform, what is your primary concern regarding security?
- ☐ Speed of delivery
 - ☐ Protection of personal and financial information
 - ☐ Variety of product choices
 - ☐ Availability of customer reviews
12. Are you aware of the potential security risks associated with online shopping, such as data breaches or phishing attacks?
- ☐ Yes, very aware

- ☐ Yes, somewhat aware
 - ☐ No, not very aware
 - ☐ No, not aware at all
13. Do you believe that e-commerce platforms take adequate measures to protect your personal and financial information?
- ☐ Strongly agree
 - ☐ Agree
 - ☐ Neutral
 - ☐ Disagree
 - ☐ Strongly disagree
14. Have you ever experienced unauthorized access to your e-commerce account or any suspicious activities related to your online shopping?
- ☐ Yes
 - ☐ No
15. Which of the following security challenges have you encountered while shopping online? (Select all that apply)
- ☐ Phishing attempts (fraudulent emails or messages)
 - ☐ Payment fraud
 - ☐ Data breaches or information leaks
 - ☐ Unauthorized access to your account
 - ☐ None of the above
16. How often do you encounter captcha or security checks during online shopping to verify that you are not a bot?
- ☐ Very often
 - ☐ Often
 - ☐ Occasionally
 - ☐ Rarely
 - ☐ Never
17. Do you regularly update your passwords for your e-commerce accounts?
- ☐ Yes, every few months
 - ☐ Yes, once a year
 - ☐ No, rarely
 - ☐ No, never

18. How do you typically respond to security warnings or alerts from your web browser when visiting e-commerce websites?
- ☐ Always take them seriously and exit the site
 - ☐ Sometimes take them seriously, depending on the message
 - ☐ Ignore them and continue browsing
 - ☐ Not sure
19. Have you enabled multi-factor authentication (MFA) for your e-commerce accounts when available?
- ☐ Yes, for all accounts
 - ☐ Yes, for some accounts
 - ☐ No, for any accounts
 - ☐ Not sure what multi-factor authentication is
20. Do you use antivirus or anti-malware software on your devices for added security while shopping online?
- ☐ Yes, on all devices
 - ☐ Yes, on some devices
 - ☐ No, on any devices
 - ☐ Not sure
21. Which of the following secure payment methods do you prefer when shopping online?
(Select all that apply)
- ☐ Credit card with fraud protection
 - ☐ PayPal
 - ☐ Digital wallets (e.g., Apple Pay, Google Pay)
 - ☐ Cryptocurrency
 - ☐ Bank transfers
 - ☐ Other (please specify)
22. How would you prefer to receive security tips and recommendations for safer online shopping?
- ☐ Email newsletters
 - ☐ In-app notifications from e-commerce platforms
 - ☐ Social media posts
 - ☐ Dedicated security app
 - ☐ Other (please specify)

23. Are you interested in educational resources or tutorials that teach you how to recognize and avoid online security threats?

- ☐ Very interested
- ☐ Somewhat interested
- ☐ Not very interested
- ☐ Not interested at all