e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

IMPROVE THE SECURITY IN MONEY TRANSACTIONS

Iyer Anish Subramanian*1, Asst. Prof. Gauri Ansurkar*2

*1Student, Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra, India.

*2Guide, Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra, India.

ABSTRACT

The rapid growth of the Internet in recent years has increased the use of electronic commerce (e-business). Electronic business is conducted online without face-to-face interaction. Various electronic payment systems (electronic payments) have been developed and are increasingly used in electronic commerce. Electronic fraud (fraud) has become a major problem in the electronic payment system. As the Internet expands business opportunities, fraudsters are developing new and sophisticated fraudulent techniques. Like other electronic systems, electronic payment platforms are vulnerable to hacking. Fraud management is a significant and growing cost for merchants. This research provides an overview of electronic payment security threats and concerns and as well as the plan to protect the data from fraud and hackers.

Keywords: Online Payment Issues, Online Fraud, Payment Gateway Security, Online Security, Online Authentication.

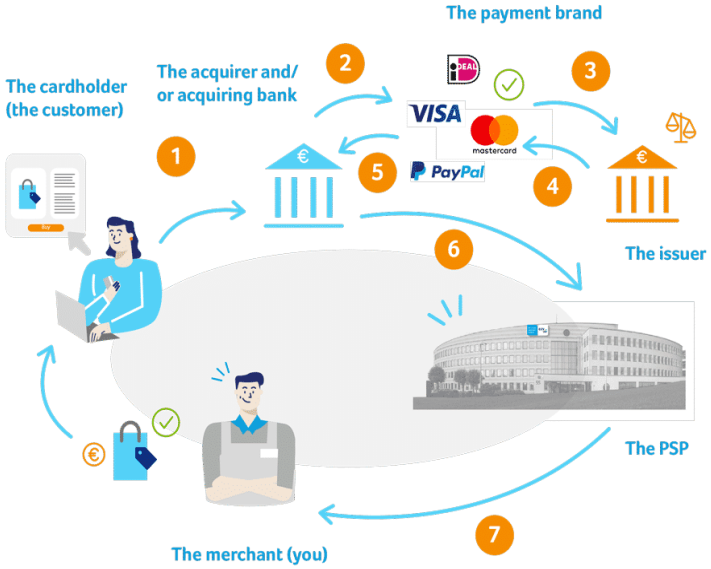
I. INTRODUCTION

E-commerce is growing rapidly and offers companies the opportunity to increase their sales over the Internet. Today, any person or business familiar with e-commerce can sell and buy products and services. The advent of electronic commerce has created new financial needs that are not effective in many cases and coincide with traditional payment systems. An electronic payment system is coming to, replace cash payment system. The sale of goods and services increased significantly with the introduction of electronic payment systems, making electronic payments an increasingly important part of payment. system.

Online Payment is a system that supply tools for paying for services or merchandise carried over the Internet. The electronic payment system provides the ease of processing e-commerce transactions between consumers and sellers. Using the electronic payment system has many benefits for payers, payees, e-commerce, banks, companies, and governments. These benefits can lead to widespread electronic payment systems around the world. A well organized and reliable electronic payment system enables faster payments, better tracking, transparent transactions, reduced time spent, cost savings and more trust between sellers and buyers.

The development and introduction of technology in the electronic payment system involves financial transactions, assimilated users and high-quality electronic payment technology tend to form their own perceptions and expectations. Electronic payment systems are widely used today, such as transactions through ATMs, using credit or debit cards, through online banking and mobile banking. Electronic payment offers significant cost savings over paper payments The online payment system has many financial risks that can arise during the transaction process. Negative effects from online payments can occur for many reasons. Due to the nature of the Internet, the authenticity and security of payments cannot be guaranteed by technologies not designed for electronic commerce. We need an electronic payment system (electronic payment) that not only offers a secure payment system, but also features such as online customer and seller authentication, Proof of customer-authorized transactions for both sellers and banks, customer privacy and transaction data security In some cases, it creates a sense of insecurity and takes risks when shopping online. More than years were many e-commerce technologies that have been developed.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com



Online Payment Model

Online Payment flow

There are four key players involved in every online transaction:

- Cardholder: – the person who owns a credit card
- Merchant: – the owner of the business
- Acquirer: – a bank that processes and routes credit card payments on the merchant's behalf across the card networks (like Visa, Mastercard, Discover or American Express) to the issuing bank. Sometimes acquirers can also work with a third party to help process payments.
- Issuing Bank: - The bank that issues credit cards and cards to consumers on behalf of the card networks.

II. SECURITY THREAT TO ONLINE PAYMENT

An electronic payment system carries a high risk of fraud. Computing devices use a person's identity to authorize a payment, example- Identification lock and safety questions. These authentications are not a complete test to determine an individual's identity. If the password and the answers to the security questions match, the system doesn't care who is on the other side. If someone has access to our password or the answers to our security question, they can access our money and steal it from us.

Electronic commerce refers to purchase and selling things over the internet. It simply refers to business transactions that take place online. Electronic commerce can be based on many technologies such as mobile commerce, internet marketing, online transaction processing, supply chain management, electronic data interchange (EDI), inventory management systems and automated systems, data collection.

The e-commerce threat comes from the unfair use of the Internet with intent to steal, commit fraud and breach security. There are different types of e-commerce threats. Some are accidental, some are intentional, and some are due to human error. The most common security threats are an electronic payment system, cash, data breaches, credit/debit card fraud, etc.

1. Scam

Users have PINs or passwords to facilitate an online transaction. But payment authorization, based only on passwords and security questions, does not guarantee an individual's identity. This can lead to a fraud case if someone else obtains our passwords. In this way, the third person can easily steal money.

2. Tax evasion

Companies provide paper invoice to verify tax collection. But in an online environment, things get fuzzy and the Internal Revenue Service rises to the challenge. They find it difficult to process tax collection and verify whether the organization is ethical or not.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

3. Payment Disputes

These transactions take place between automated electronic systems and users. Because it is ultimately a machine, errors in payment processing are possible. These failures and anomalies lead to payment disputes and users end up losing their funds.

4. E-cash

Paperless cash structure uses online wallets such as PayPal, Google Pay, Paytm, etc. Since all financial information resides in this app, a single security breach can result in private information disclosure and financial loss.

It consists of four components: issuers, customers, intermediaries and regulators. The issuers are the financial institutions, the customers are the ones who use that money, the intermediaries are the ones who earn it, and the regulators are there to monitor their movements. Some of the threats that e-commerce websites face when using electronic money are:

- **Direct Access Attacks**

Hackers gain direct access to the device and install programs on it without permission. This software contains worms that automatically save device information without getting caught. This can root server paralysis and eventually take you offline. It can also slow things down and result in consumers returning with a negative experience. To solve this particular problem always use a web application firewall or in worst case change the IP of the server.

- **Denial of Service Attack and Distributed Denial of Service Attacks (DDOS)**

The hacker breaks into the system and removes all user access. It bans users from all functions and resources and crashes the system temporarily. This mostly happens over an internet network and hackers can demand ransoms/ favours to reactivate the device. In the case of DDoS, hackers use your computer to sabotage the security of another computer.

HOW TO PREVENT FROM SECURITY ATTACKS

1. HTTPS and SSL Certificates SSL

Certificate is one of the ways to protect user's personal information on the Internet. You may have seen that there are two types of browser addresses: HTTP and HTTPS. Both abbreviations stand for communication protocol. The protocol is a set of rules that define the exchange of data between browser and server, what kind of information should be there and what should be done with that data.

HTTPS is a protected version of HTTP. It is an SSL protocol that is activated after setting up the SSL certificate and encrypts personal data before the information is transmitted to the e-commerce website or application owner. Thus, SSL Certificate helps to make your payment secure on website.

2. Use Payment Tokenization.

Credit card tokenization de-identifies sensitive payment information by converting it into a string of randomly generated numbers called a "token." As a token, the information can be sent over the internet or payment networks to complete the payment without exposing yourself.

3. Match IP and billing address information

Verifying the details provided during the transaction can help **identify** a potentially fraudulent transaction and protect the business before fraud **occurs. The Address** Verification Service (AVS) compares the **shopper's** IP address to the billing address **on** the credit card to **ensure** the customer is the cardholder.

4. Continuous Fraud Monitoring

Merchants need a payment gateway that observe and manages fraud. The integrated fraud monitoring identifies where there is a real risk of a fraudulent purchase. Businesses can set rules based on their situation and risk tolerance that limit or reject transactions that are deemed too risky or that require manual approval before a transaction is completed.

5. Managing PCI Compliance

Merchants that process, store or transmit credit card data must be PCI compliant. The consequences of a data breach for a company that fails to comply are notable and can include costly fines and penalties in addition to

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

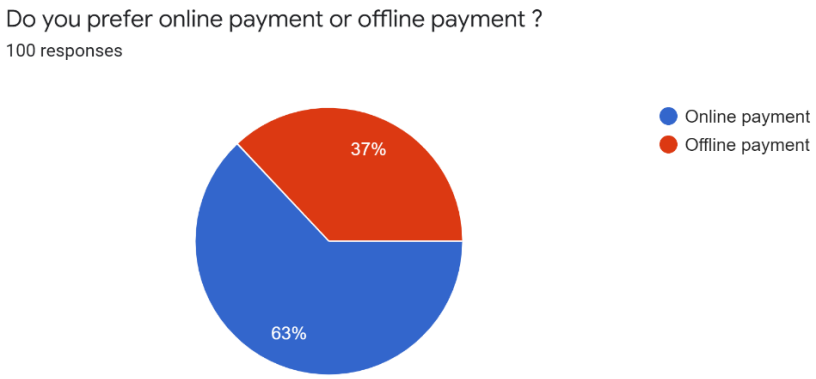
significant reputational damage. Payment processors play an important role in helping merchant manage and maintain compliance, but businesses must take a proactive role in understanding their compliance obligations and requirements.

6. PUBLIC SURVEY

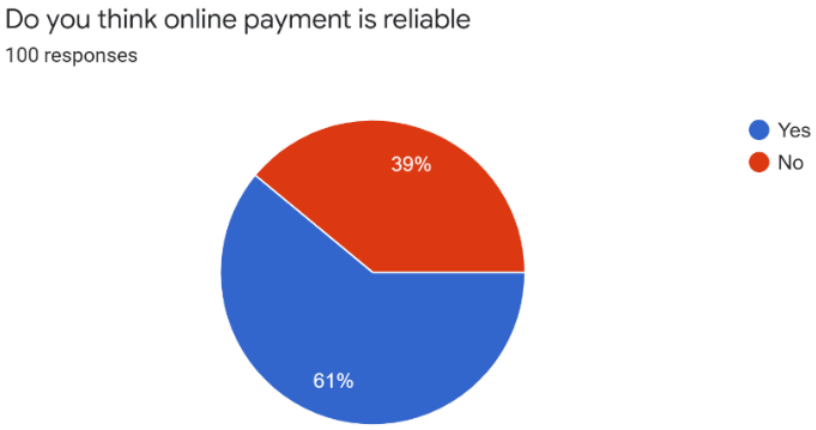
We are Trying to gather data by taking survey from public regarding which payment method do they prefer offline or online and how concerned are they with attacks occurring while using online payment system and how to solve those security concerns

7. QUESTIONNARE

- Do you prefer online payment or offline payment?
- Do you think online payment is reliable?
- In general, how concerned are you about security on the Internet?
- If you have never used internet banking, what are the main reasons? (Check all that apply)
- Are you willing to use your credit card on the web?
- Would security features be a factor at all in your choosing whether or not to do business with an Internet-based company?
- What are the security measures that could secure you against various kinds of online banking attacks?
- e-Payment systems save you time and money?
- e-Payment systems are better than cash?
- A digital customer has to be alert to security issues when using e-Payment systems?
- e-Payment systems can be easily understood and readily adopted?
- Which following payment methods do you use?
- Which of these security threats have you been a victim of? (i.e. you have lost money or could have done) - Tick all that apply

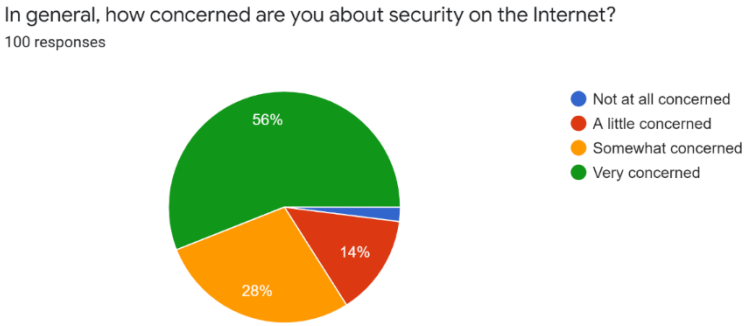


When we asked people about which payment mode they prefer offline or online 63% people said online and 37% people said offline

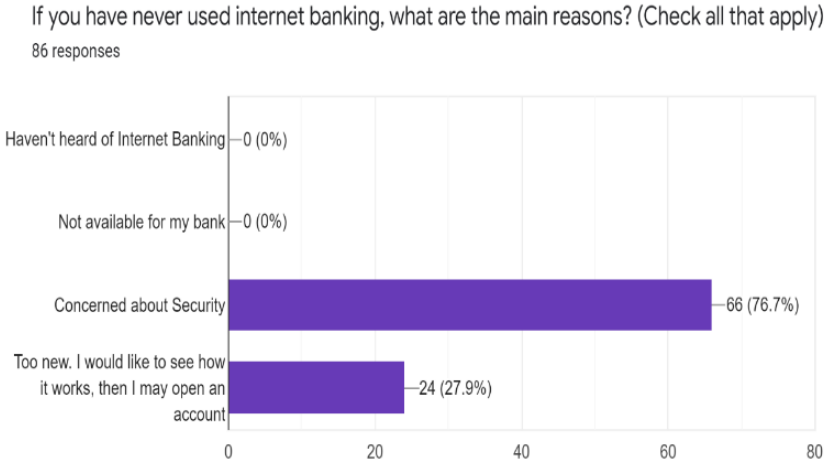


When we asked people about is online payment reliable 61% people prefer reliable 39% people not Prefer it is reliable

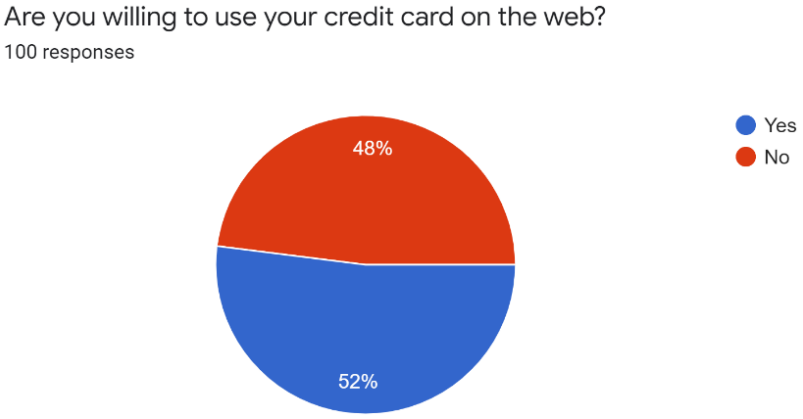
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com



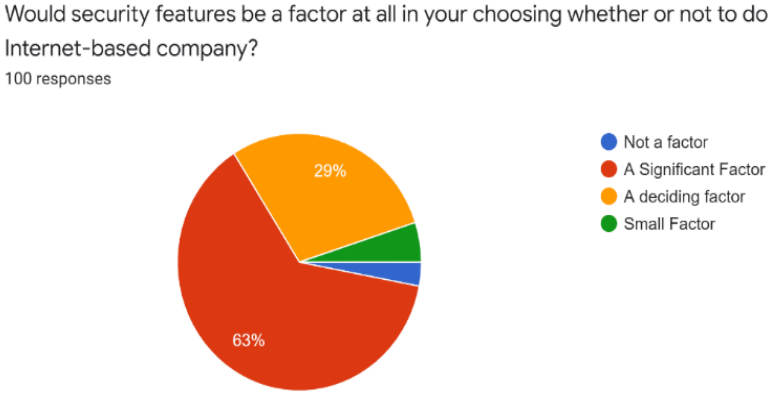
When asked how concerned are you about security on the Internet 56% people said very concerned ,28% Somewhat Concerned, 14% A little concerned and 2% people Not at all concerned



When we asked If you have never used internet banking, what are the main reasons, 76.7% people concerned about security 27.9% people said too new to use but they are interested in using this online service

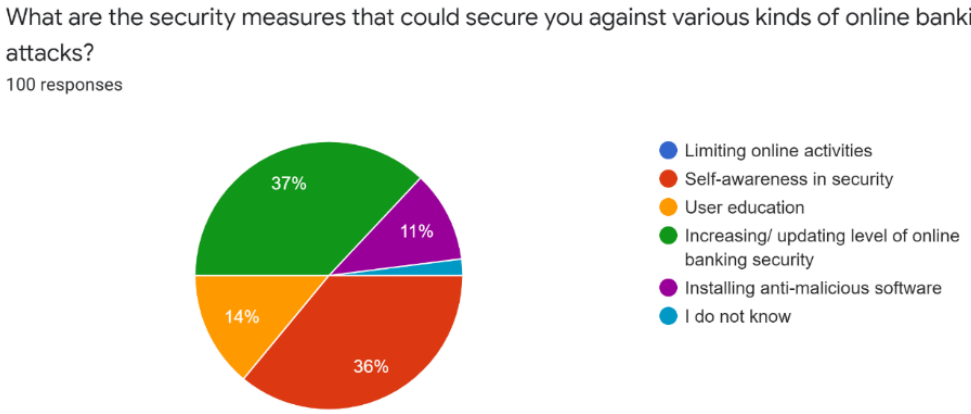


When we asked people about are they willing to use credit card on web 52% said yes and 48% said no

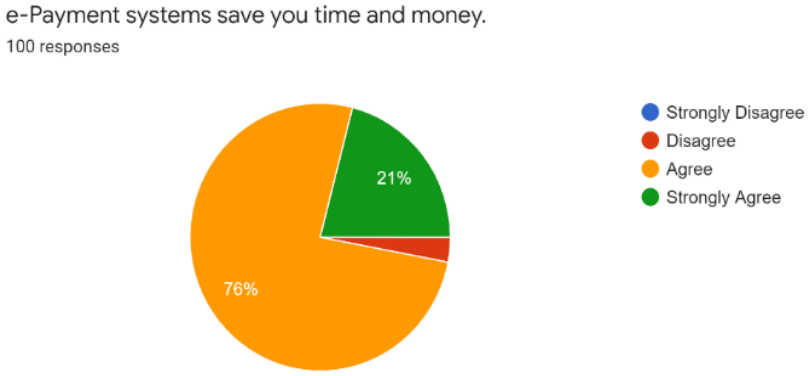


e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

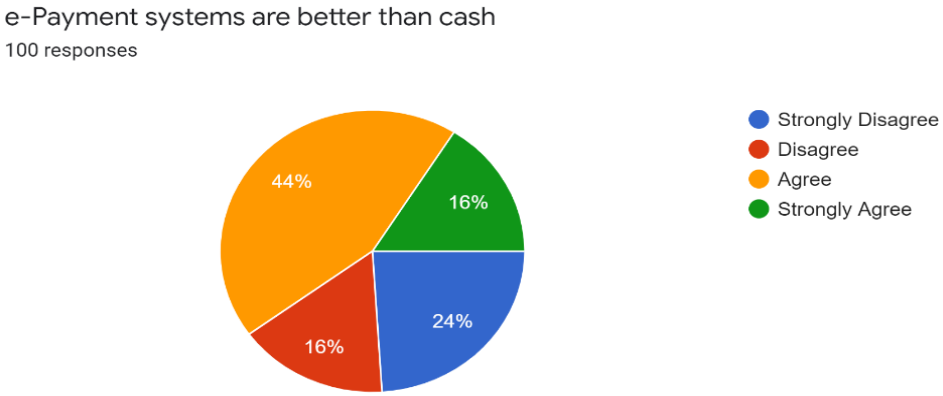
When we asked people about are security features will be a factor while choosing to do business with the internet-based company 63% people said A Significant factor, 29% people said A deciding factor 5 % said small factor and 3% people said Not a factor.



When we asked people about What are the security measures that could secure you against various kinds of online banking attacks 37% people said Increasing / Updating level of online banking security, 36% people said Self-awareness in security, 14% people said User education and 11% people said Installing anti-malicious software and 2% they don't know

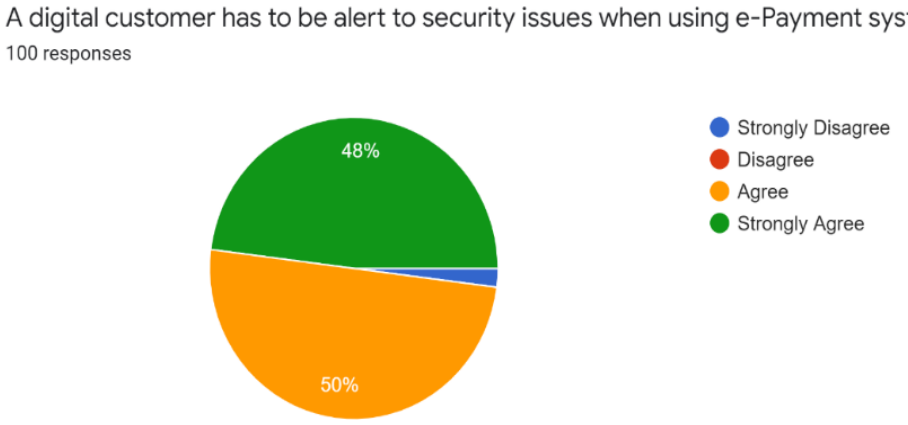


When we asked people about does e-payment system save time and money 76% people agree and 21% people strongly agree 3% people disagree

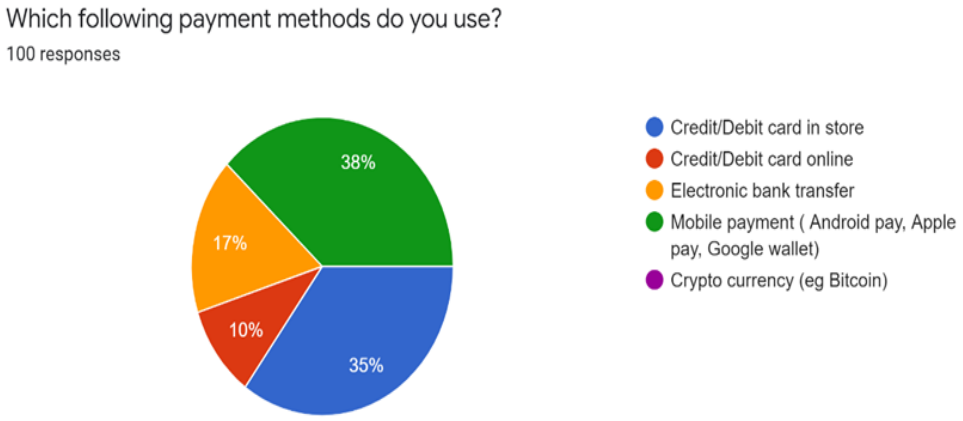


When we asked people about e-payment system are better than cash 44% people agree, 16% people disagree 24% people Strongly disagree, 16 % people strongly agree

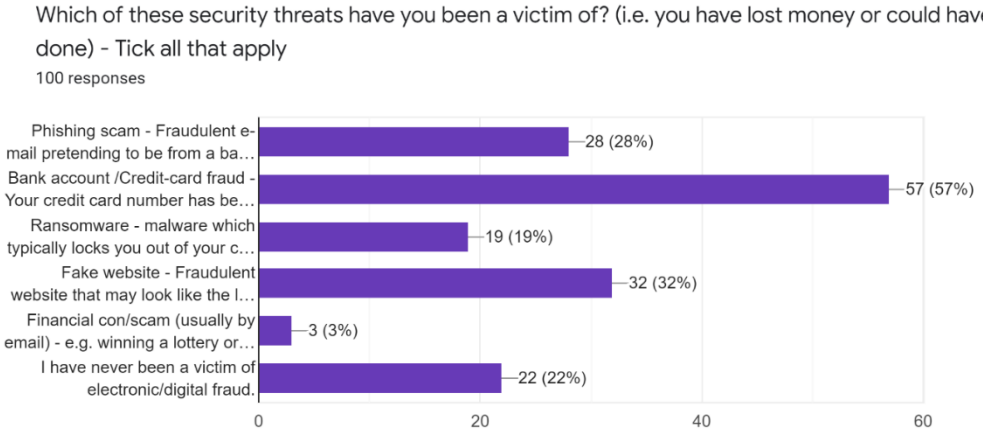
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com



When we asked people about should customer be alerted to security issue when using e-payment system 48% people Strongly agree, 50% people agree, 2% people Strongly Disagree.



When we asked people about which payment method do they use 38% people use Mobile payment and 35% people said Credit/Debit card in store, 17% people said Electronic bank Transfer and 10% people said Credit/Debit card online.



When we asked people about which of this security threat they have been victim of, 58% people said Bank account/Credit card fraud, 32% people said fake Website, 3% people Financial scam by email, 19% people said Ransomware, 32% people said by fake website, and 28% people said by phishing scam

8. HYPOTHESIS TESTING

Hypothesis testing is a type of statistical reasoning that analyse sample data to derive inferences about a population parameter or probability distribution. First, a hypothesis is made about the parameter or distribution. This is known as the null hypothesis, abbreviated as H0. An alternative hypothesis (indicated as Ha) is then defined, which is the exact opposite of the null hypothesis. Using sample data, the hypothesis

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

testing technique determines whether or not H0 can be rejected. The statistical conclusion is that the alternative hypothesis Ha is true when H0 is rejected.

Null hypothesis (H0): Is online payment Secure and Trustworthy

Alternative hypothesis (Ha): Is online payment not Secure and not Trustworthy

We will check by using T-test whether to reject null Hypothesis or not

T-test

A t-test is an inferential statistic that determines whether there is a significant difference between the means of two groups that are related in some way.

Level Of Significance

The chance of rejecting the null hypothesis when true is the significance level (also known as alpha or α). For example, a significance level of 0.05 means that there is a 5% chance of detecting a difference when there is none. Lower significance levels of indicate that more evidence is needed to reject the null hypothesis.

Level of Confidence

The confidence level indicates the probability that the position of a statistical parameter (e.g. the arithmetic mean) measured in a sample survey also applies to the entire population.

Sr no.	Data
1	63.4
2	61.4
3	16
4	28
5	53
6	8
7	98.1
8	97
9	60.4
10	98
11	93
12	22.8
Mean(x)	58.25
Standard Deviation(s)	33.6122

Level of significance = 0.05 i.e.5%

Level of Confidence = 95%

The formula to find t-score is:

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

where x is the sample mean,

μ is the hypothesized mean,

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

The p-value, also known as the probability value, indicates how likely it is that your data occurred under the null hypothesis. Once we know the value of t, we can find the corresponding p-value. If the p-value is less than an alpha level (common choices are 0.01, 0.05, and 0.10), we can reject the null hypothesis and conclude that smart devices are not secure and our privacy is not trusted can.

Procedure 1-

Find out what null and alternative hypothesis are

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

- Null hypothesis (H0): Is online payment Secure and Trustworthy
- Alternative hypothesis (Ha): Is online payment not Secure and not Trustworthy

Procedure 2 –

Find out test statistic

In this case Hypothesized mean value is considered 0.

$t = (x-\mu) / (s/\sqrt{n}) = (58.25-0) / (33.6122/\sqrt{12}) = 6.00329$

Procedure 3 –

Calculate the test statistic p – value

The t-distribution table with Degree of Freedom n-1 to calculate p-value is n=12,

n-1 = 11

On checking the p-value in t-distribution table the value got is less than 0.00001

Since the p-value is less than alpha value which is 0.05 we can reject the null hypothesis and can say that Online payment is not Secure and Trustworthy.

III. OBSERVATION

1. People must check whether the website is genuine while using online method for payment they must go through the website whether they are providing security measures
2. People must update the apps while using those apps for online payment like bank apps, google-pay, pay-tm, phone-pe etc. They must try to update those apps while using for payment.
3. People must try to remove the credit/Debit card details and all information regarding card in any app while using that app for Online Shopping, because this apps can also track your data and can break the loophole and can gather your valuable information
4. There must be a Continuous Fraud Monitoring System on Online gateway so whenever transaction occurs between merchant and customer and if any Man in the Middle try to gain the access of customers card information the payment must be immediately blocked and the data of customer must be secured or must get converted in cipher language so that Hacker in the middle will not able to get access through customers data.
5. Try to add and update E-commerce Security plugins so whenever you try to visit e-commerce webapp they will provide you security from bad-bots, SQLi, XSS. and several other attacks.
6. People must try to update themselves by understanding the Security issues or challenges they face when they try to use online system over offline system, they must update their Security patches in mobile, they must know what threats are going while using online payment, they must never share or store bank information in any website.
7. If anyone's credit card or mobile is stolen the card bank must immediately get the data of that particular customer and their card must get blocked immediately so that the customer must consider that he/she is safe.

IV. CONCLUSION

It's a wise approach to be aware of the threats that exist in your immediate online environment. People should also know how to protect themselves from such e-commerce threats. The top e-commerce security threats we've examined are potentially devastating not just for retailers, but for customers as well. Therefore, appropriate measures should be taken and strategies developed to address them. take it easy when it comes to protecting websites or customer data. The aim should be to offer consumers a safe place on the Internet. Aside from the ecommerce security threats and solutions we have outlined here, conduct regular website security checks to stay ahead of the curve. Dangers Make a habit of giving people sensible safety measure. Invest in PCI DSS compliance to protect transactions. Set up high-quality active site protection to prevent DDoS campaigns. Finally, make it a habit to use high-quality passwords and set up multi-factor authentication to prevent entire site from being compromised. As a newly developed, convenient, fast and real-time capable method, online payment plays an increasingly irreplaceable role in e-commerce. More attention should be paid to security issues As Visa said, the security of the entire online payment industry is not measured by the security measures

taken; however, it depends on the weakest link. In other words, improving the risk resistance capacity in each weak link is the best way to effectively ensure the security of the entire payment industry.

V. REFERENCES

[1] "A Review of E-Payment System in E-Commerce"
[2] https://data-flair.training/blogs/threats-to-e-commerce-security
[3] https://phoenixnap.com/blog/ecommerce-
[4] https://star-knowledge.com/blog/ecommerce-security-threats-issues-solutions
[5] https://upc.ua/en/3d-secure-issuing-access-control/
[6] https://www.getastra.com/blog/knowledge-base/ecommerce-security-threats