IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A STUDY ON EFFECTS OF ONLINE TRANSACTION

Mrs K. Prasanthi, Assistant Professor, Department of MBA,

Sridevi women's engineering college, Vattinagulapally

VADLA PAVANI, MBA 2nd year,

Sridevi women's engineering college, Vattinagulapally

Abstract

Online transaction, which are essential to modern commerce, present a complex web of risks that require close scrutiny. In the financial word, the threat of fraud is ever – present, including fraudulent transactions and increasingly sophisticated phishing attacks that exploit vulnerabilities in payment systems. Privacy risks increase as platforms accumulate vast amounts of user data, putting individuals at risk of identity theft and unfair profiling. Vulnerabilities such as malware and data breaches pose a threat to the confidentiality and integrity of transactional data, and despite advances in encryption and authentication, cyber threat dynamics require continued adaptation. Users play a critical role in this ecosystem and are encouraged to strengthen their defines through strong passwords, regular software updates, and increased awareness of website legitimacy. The complex intertwining of financial, privacy, and security risks highlights the need for a holistic approach that includes personal, corporate, and cybersecurity frameworks. Addressing these challenges requires continued collaboration to strengthen the digital infrastructure that supports online transactions and protects the trust that underlies e-commerce.

Key words: Fraud, Identity Theft, Phishing, Scams, Unauthorized.

Introduction

Online trading has become an integral part of modern commerce, offering convenience and efficiency. However, this convenience comes with risks that users must consider. A significant risk is that cybercriminals may compromise sensitive information such as credit card details. When transactions occur over the internet, malicious attackers may attempt to intercept and exploit this information, resulting in financial loss or identity theft. Additionally, the prevalence of phishing attacks poses a significant threat to online transactions. Cybercriminals often use deceptive techniques such as fraudulent emails and fake websites to trick users into revealing their login credentials and personal information. careless people can unknowingly fall victim to

these schemes and jeopardize the security of their online transactions. Another significant risk is the vulnerability of online platforms to data breaches. Even reputable companies can experience security vulnerabilities that can expose user data to unauthorized access. This not only puts personal privacy at risk, but also raises concerns about the integrity of financial transactions conducted on these platforms. The evolving cyber threat landscape further complicates the risks associated with online transactions. As hackers develop more sophisticated techniques, the potential for new and unexpected vulnerabilities in online security systems increases.

This dynamic environment requires continuous efforts by both users and service providers to stay ahead of new threats and effectively protect online transactions. Despite advances in security protocols, the human factor continues to contribute significantly to the risks of online transactions. Users often ignore basic security practices such as:B. You are using weak passwords or not updating your software regularly. These failures can create opportunities for cybercriminals to exploit vulnerabilities and compromise the security of online transactions. In summary, while online trading offers unparalleled convenience, users must be aware of the risks associated with the digital world. From the potential for sensitive information to be compromised to the ever -present threat of phishing attacks and data breaches, understanding and mitigating these risks is critical to ensuring the security and integrity of your online transactions. Online trading has become an integral part of modern commerce, providing convenience and efficiency for both consumers and businesses. However, this convenience comes with risks arising from the digital nature of these transactions. The main concern is the possibility of data breaches and cyberattacks. As sensitive financial information travels over the internet, it is vulnerable to interception by malicious attackers seeking to exploit vulnerabilities in security systems. Another significant risk associated with online transactions is the prevalence of fraud. As cybercrime becomes more sophisticated, techniques such as phishing, identity theft, and credit card fraud are becoming more common. Consumers may unknowingly share their personal information with malicious companies, potentially leading to fraudulent transactions and financial losses. Despite advances in security measures, the dynamics of cyber threats require continuous adaptation and vigilance to stay ahead of potential risks. Additionally, online transactions lack personal interaction. Trust is a key element in traditional commerce, where people can physically verify the legitimacy of businesses and individuals in the online space, building trust relies heavily on digital credentials, reviews, and secure platforms. However, even with these mechanisms in place, the risk of falling victim to fraud and fraudulent schemes still exists and requires strong cybersecurity measures and consumer education to effectively.

Review of literature

Joseph A. Ojeniyi is a lecturer in the Department of Cyber Security Sciences, Faculty of Information and Communication Technology, Federal University of Technology (FUT), Minna, Nigeria. He received his Ph.D. He received a master's degree in cybersecurity science from the same university. He holds a PhD in Computer Science and a Bachelor of Engineering degree from the University of Ibadan, Nigeria. He holds a PhD in Mathematics/Computer Science from FUT Minna, Nigeria. He has been appointed as a reviewer for several indexed journals. Currently serves as the chairperson of the Faculty Association Organizing Committee"

ICTA 2018." His areas of interest include cybersecurity, digital forensics, deep learning, artificial intelligence in information assurance/security, and cyber-physical systems. Shafi Muhammad Abdulhamid received his Ph.D. He holds a PhD in Computer Science from Universiti Teknologi Malaysia (UTM), a Masters in Computer Science from Bayero University Kano (BUK), Nigeria, and a Mathematics/Computer Science degree from the Federal University of Technology, Minna, Nigeria. holds a Bachelor of Technology degree in Science.His current research interests include cybersecurity, cloud he computing, soft he computing, Internet of Things security, malware detection, and big he data. He has published many scientific papers in reputed international journals, conference proceedings and book chapters. He was appointed to the editorial board **of** the Journal of Computer Science and Information Technology (JCS). He is also a member of ISI and Scopus indexed international journals such as Journal of Network and Computer Applications (JNCA) Elsevier, Applied Soft Computing (ASOC) Elsevier, Journal of King Saud University Computer and Information Sciences (JKSU-CIS), etc. Elsevier, Neural Computing and Applications (NCAA) Springer, Cluster Computing Springer, Egyptian Informatics Journal (EIJ) Elsevier, IEEE Access Journal (USA), Wireless Networks Springer, Plos One Journal, International Journal Engineering Science and Technology (JESTHC) Elsevier, To name a few: Brazilian Journal of Science and Technology (BJST) Springer; He has also served on the program committees (PCs) of numerous national and international conferences. He is a member of the IEEE Computer Society, International Association of Computer Science and Information Technology (IACSIT), Computer Professionals Registration Council of Nigeria (CPN), International Association of Engineers (IAENG), Internet Society (ISOC), and Cyber.

Objectives

- Understand the inherent risks associated with online transactions.
- Identify the most common types of fraud or security breaches in online transactions.
- Analysis the impact of these risks on businesses and consumers.
- Evaluate the effectiveness of current security measures to mitigate these risks.
- Suggest improvements or new ways to improve the security of online transactions.

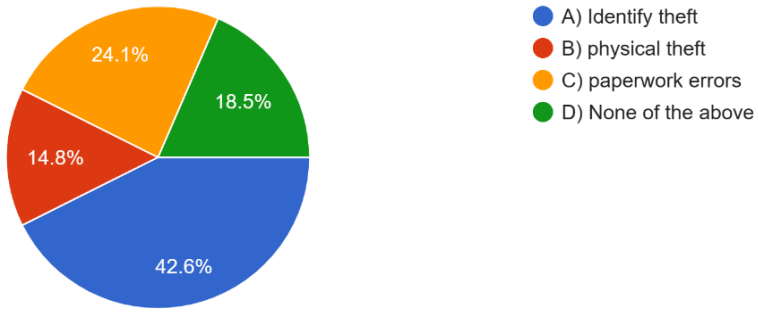
Research Methodology

The article is used descriptive research quantitative approach and the sampling technique is purposive sampling and the sampling size is 54. The data source is collected primary and through a google form to elicit the views of the respondents and the secondary data is collected from articles and journals.

Data Analysis

Table 1 : which of the following is a common risk associated with online transactions.

Particulars	No of Respondents	Percentage %
Identify theft	23	42.6%
Physical theft	8	14.8%
Paperwork errors	13	24.1%
None of the above	10	18.5%
Total	54	100%

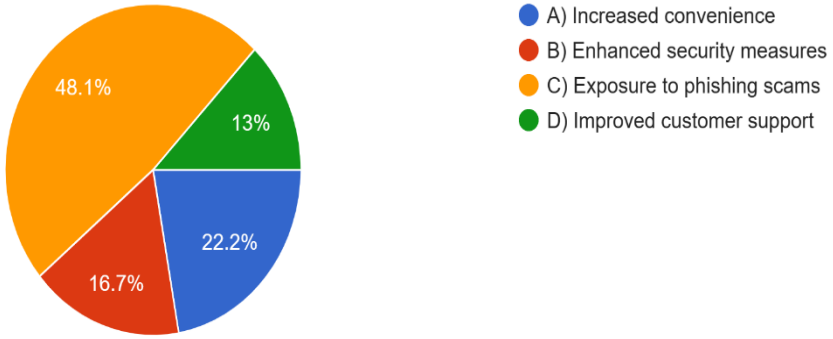


Interpretation

From the above image of the survey conducted, the responses i.e ; 42.6% agreed that the most common risk in online transactions is the identification of theft. The lowest percentage, 14.8%, agreed that physical theft is the most common risk for online transactions.

Table 2: A potential risk of online transactions.

Particulars	No. of respondents	Percentage %
Increased convenience	12	22.2%
Enhanced security Measures	9	16.7%
Exposure to phishing scams	26	48.1%
Improved customer support	7	13%
Total	54	100%

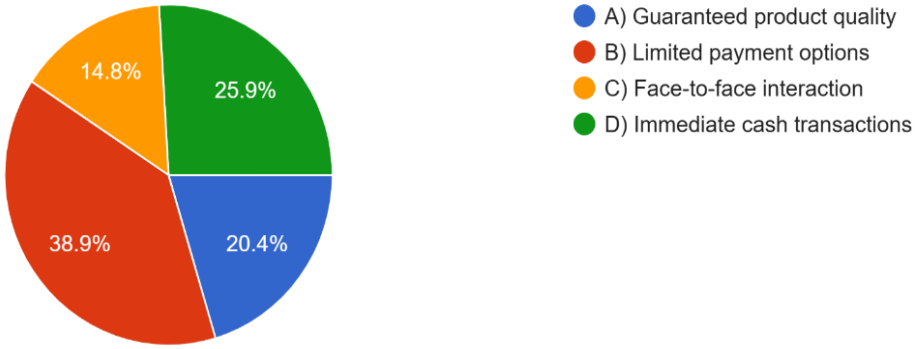


Interpretation

From the above figure of the survey conducted, it is seen that Exposure to phishing scams is the most potential risk of online transaction with 48.1% and there is a less risk in improved customer support with 13%.

Table 3: A risk related to online transactions.

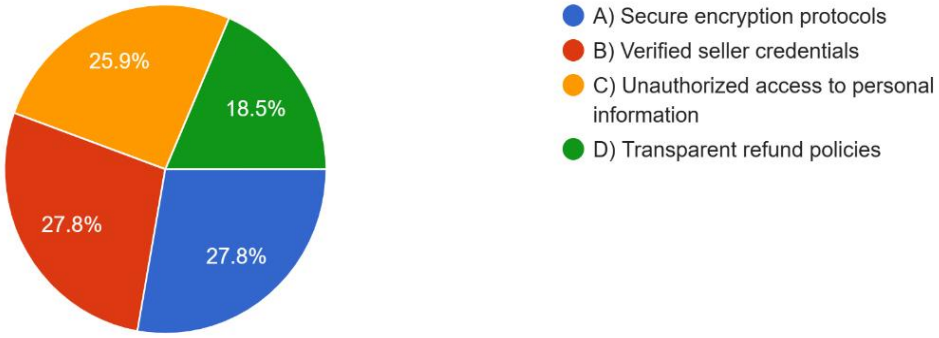
Particulars	No of respondents	Percentages %
Guaranteed product quality	11	20.4%
Limited payment options	21	38.9%
Face-to-face interaction	8	14.8%
Immediate cash transactions	14	25.9%
Total	54	100%



Interpretation

Table 4: A common concern when making online payment.

Particulars	No of respondents	Percentages %
Secure encryption protocols	15	27.8%
Verified seller credentials	15	27.8%
Unauthorized access to personal information	14	25.9%
Transparent refund policies	10	18.5%
total	54	100%

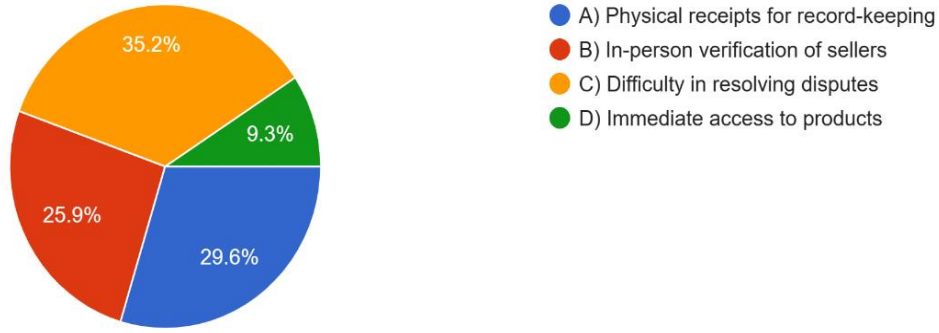


Interpretation

From the above chart of the conducted research, the ratio of secure encryption protocols and verified merchant credentials is the same at 27.8%, while transparent refund policy is lower at 18.5%.

Table 5: A risk associated with online transactions.

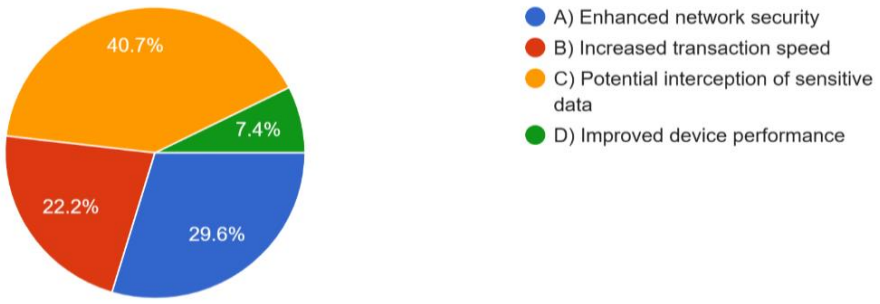
Particulars	No of respondents	Percentages %
Physical receipts for record-keeping	16	29.6%
In-person verification of sellers	14	9.3%
Difficulty in resolving disputes	19	35.2%
Immediate access to products	5	25.9%
Total	54	100%



From the above chart of the research conducted, it can be seen that the risks associated with online transactions are the highest with physical receipt for record keeping at 29.6% and the lowest with immediate access to goods at 9.3%.

Table 6: Common risk of using public Wi-Fi for online transactions.

Particulars	No of respondents	Percentages %
Enhanced network security	16	29.6%
Increased transaction speed	12	22.2%
Potential interception of sensitive data	22	40.7%
Improved device performance	4	7.4%
Total	54	100%

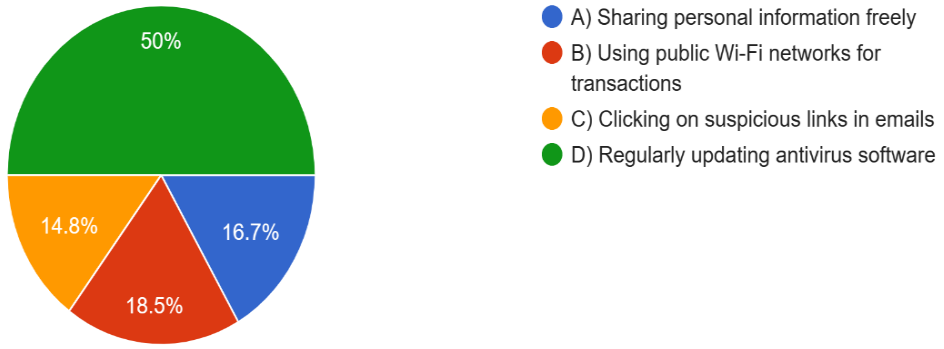


Interpretation

From the above chart of the research conducted, the most common risk when using public Wi-Fi for online transactions is the possibility of interception of sensitive data at 40.7%, and with the increase in device performance General risk is the lowest at 7.4%.

Table 7 : A recommended way to protect yourself from online transaction risks.

Particulars	No of respondents	Percentages %
Sharing personal information freely	9	16.7%
Using public Wi-fi networks for transactions	10	18.5%
Clicking on suspicious links in emails	27	14.8%
Regularly updating antivirus software	9	50%
Total	54	100%

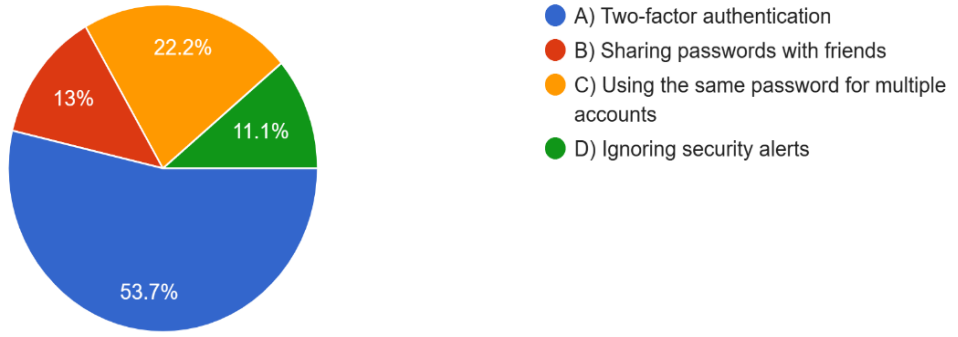


Interpretation

From the above table of conducted research, the most recommended ways to protect yourself from the risks of online transactions are to regularly update 50% of your antivirus software and you can see that it has decreased by 14.8%.

Table 8 : A common security measure used in online transactions.

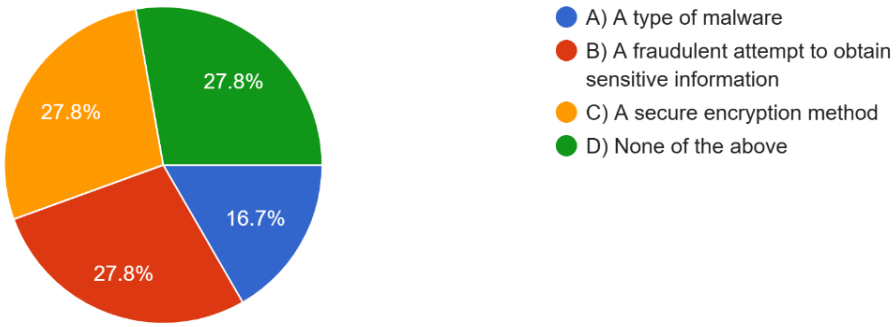
Particulars	No of respondents	Percentages %
Two-factor authentication	29	53.7%
Sharing passwords with friends	7	13%
Using the same password for multiple accounts	12	22.2%
Ignoring security alerts	6	11.1%
Total	54	100%



From the above chart of the conducted research, the most used security measure for online transactions is two-factor authentication at 53.7%, while ignoring warnings is less secure at 11.1%.

Table 9: Phishing

Particulars	No of respondents	Percentages %
A type of malware	9	16.7%
A fraudulent attempt to obtain sensitive information	15	27.8%
A secure encryption method	15	27.8%
None of the above	15	16.7%
Total	54	

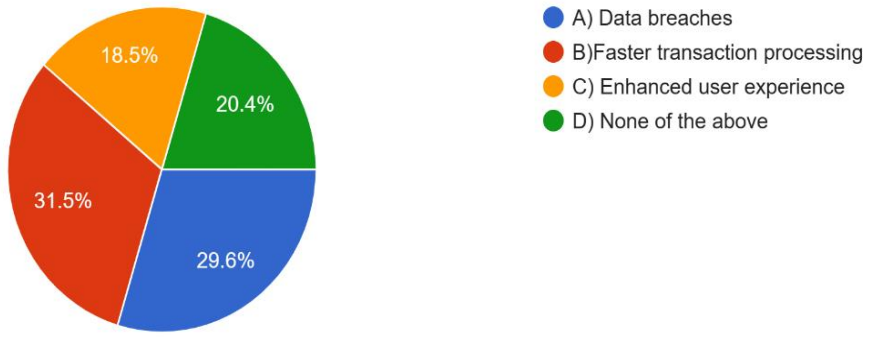


Interpretation

From the above figure of the survey conducted, phishing is a type of malware, and 27.8% of the respondents answered that phishing is a type of malware with fast transaction. processing and secure encryption method, and 16.7% of the respondents answered that it is a type of malware.

Table 10 : A potential risk of using unsecured websites for online transactions.

Particulars	No of respondents	Percentages %
Data breaches	16	29.65
Faster transaction processing	17	31.5%
Enhanced user experience	10	18.5%
None of the above	11	20.4%
Total	54	100%



Interpretation

From the above figure of the research conducted, the biggest potential risk when using insecure websites for online transactions is faster transaction processing at 31.5% and improved user experience at 18.5%.You can see that it is the lowest.

Findings

1. 42.6% of respondents agreed that identity theft occurs more easily compared to paper errors (24.1%) and physical theft (14.8%).
2. We found that the biggest potential risk in online transactions is the threat of phishing at 48.1%.
3. For online transactions, restricted payment options were found to pose the highest risk at 38.9%.
4. The ratio of secure encryption protocols and verified merchant credentials is equal at 27.8%.
5. Risks associated with online transactions were found to be highest with physical receipts for record keeping at 29.6%.
6. We found that the most common risk when using public Wi-Fi for online transactions is the possibility of interception of sensitive data, at 40.7%.
7. 50% found regularly updated antivirus software to be the most recommended way to protect themselves from the risks of online transactions.
8. Two-factor authentication was found to be the most commonly used security measure for online transactions at 53.7%.

9. We found that 27.8% of respondents equally agreed that phishing is a type of malware that represents faster transaction processing and secure encryption methods.

10. He found at 31.5% that the biggest potential risk when using insecure websites for online transactions is faster transaction processing.

Conclusion

Online trading has become an essential part of our daily lives, offering convenience and efficiency. However, there are also inherent risks that individuals and businesses must consider. One of the main concerns is the risk of cyber attacks and data breaches. Because transactions occur over the Internet, sensitive information such as credit card details and personal information is vulnerable to hacker attacks. Cybercriminals use a variety of techniques, including phishing, malware, and ransomware, to exploit vulnerabilities in online transactions. Gaining unauthorized access can compromise your financial accounts and steal valuable information. This poses a serious threat not only to individuals, but also to businesses that store large amounts of customer data. The consequences of such violations range from financial loss to reputational damage.

Additionally, online transactions are vulnerable to identity theft. Personal information is easily available online, allowing fraudsters to impersonate you and cause fraudulent transactions and financial loss. Although digital platforms aim for seamless transactions, technical issues can occur that lead to failed payments or fraudulent transactions. These errors can lead to user dissatisfaction and financial consequences.

In summary, while online trading offers unparalleled convenience, it also comes with risks that you need to be proactive about. Cybersecurity awareness combined with technological advances in secure transaction protocols is paramount to building a more secure digital financial ecosystem. As society continues to embrace digital transactions, managing these risks becomes a collective responsibility to ensure the integrity and safety of online financial activities.

Reference

1. K. Chitra and B. Subashini, "Data Mining Techniques and its Applications in Banking Sector", Volume 3, Issue 8, August 2013.

2. Abhijit A. Sawant and P. M. Chavan, "Study of Data Mining Techniques used for Financial Data Analysis", Volume 2, Issue 3, May 2013.

3. Dinesh J. Prajapati, Jagruti H. Prajapati, "Handling Missing Values: Application to University Data Set", Issue 1, Vol.1, August-2011, ISSN 2249--6149.

4. Sandeep Karamongikar, P. Radha Krishna, Satyabrata Pradhan and Siva Viswanathan, "Risk Analysis of Loan Portfolio Using Social Data", 2014.

5. A. J. Feelders, A. J. F. le Loux, and J. W. van'tZand, "Data Mining for loan evaluation at ABN AMRO: a case study", Proceedings KDD-95 USA, 1995