JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBERSECURITY THREATS IN E-COMMERCE PLATFORMS AND PROTECTIVE MEASURES

Shreya Sunil Londhe [1], Himanshu Nilesh Patil[2],

Dr. Shivajirao Bachchav Patil, [3] Prof. Priyanka Kajale[4]

1, 2 Students ,Department of Master of Computer Applications, Dr. D. Y. Patil Centre for Management & Research, Chikhali, Pune, India 3 Associate Professor , Department of Master of Computer Applications, Dr. D. Y. Patil Centre for Management & Research, Chikhali, Pune, India

4 Assistant Professor , Department of Master of Computer Applications, Dr. D. Y. Patil Centre for Management & Research, Chikhali, Pune, India

z Abstract :

This research investigates the growing cybersecurity threats affecting e-commerce platforms and evaluates protective measures that can safeguard consumers and businesses. With the increasing dependence on digital transactions and online shopping, cybersecurity challenges such as phishing attacks, identity theft, payment fraud, and data breaches are becoming more prevalent. Data from a survey of 21 respondents indicates that phishing attacks are perceived as the most common threat (47.62%), while the majority of users prefer UPI/mobile wallet transactions (52.38%). Furthermore, 47.62% of participants reported receiving suspicious e-commerce messages occasionally, revealing a concerning cybersecurity exposure. The study highlights the significance of strong encryption, consumer awareness, and regular security audits in enhancing e-commerce trust and security. The findings contribute to understanding how users perceive cybersecurity risks and provide strategic recommendations for strengthening protection mechanisms.

Keywords:Cybersecurity, E-commerce, Phishing, Data Breach, Online Fraud, Digital Payments, Encryption

I. INTRODUCTION

E-commerce has changed the shopping experience for people by offering easy access to products and services. As more customers use online platforms, the need for secure transactions becomes very important. Cybersecurity plays a major role in protecting users from online fraud and data theft. E-commerce platforms often face threats such as phishing, identity theft, payment fraud, and fake websites. If these threats are not managed properly, they can cause financial loss and reduce customer trust.

This study focuses on understanding the cybersecurity issues faced by online shoppers and the protective measures that can help create a safe online environment.

II. REVIEW OF THE LITERATURE

Several studies have explained the growing concern regarding cybersecurity in online shopping. Researchers highlight that as e-commerce grows, cyber threats also increase. Phishing and payment fraud are frequently reported in many countries. According to previous research,

one of the major reasons for cyberattacks is the lack of awareness among users. Studies also show that people sometimes share personal information without verifying the website's security.

Literature also discusses the importance of strong encryption, multi-factor authentication, and regular system updates. Researchers recommend that e-commerce platforms should educate users about online safety and adopt advanced security

tools. Overall, earlier studies suggest that cybersecurity is important for protecting customers and maintaining trust.

III. OBJECTIVES OF THE STUDY

1. To identify the common cybersecurity threats experienced by online shoppers.
2. To understand users' awareness and behavior related to online safety.
3. To analyze how users respond to suspicious online activities.
4. To find out which security measures users prefer.
5. To provide suggestions for improving cybersecurity in e-commerce platforms.

IV. RESEARCH METHODOLOGY

This study uses a quantitative survey-based approach to identify cybersecurity threats in e-commerce platforms and to provide suggestions for improving security. A total of 21 respondents aged 18–35, who actively use e-commerce platforms, participated in the research. The survey focused on usage behavior, awareness of cyber threats, payment safety, and trust in platform security.

1.1. Data Collection and Preprocessing

Data was collected through a structured **online questionnaire** consisting of close-ended questions. Processing steps:

- **Validation:** Incomplete and duplicate responses removed
- **Encoding:** Options converted into numeric labels for analysis
- **Normalization:** Values converted into percentage distribution
- **Visualization Prep:** Data formatted for charts (pie and bar graphs)

1.2. Workflow of System

Data Collection → Cleaning & Encoding → Percentage Analysis → Chart Visualization → Interpretation of Cybersecurity Concerns → Suggestions for Improvement

1.3. Evaluation Metrics

$$PR=(RF/N)\times 100$$

Where:

PR = Percentage Rate

RF = Response Frequency

N = Total Respondents (21)

These metrics help identify dominant threats, security awareness levels, and preferred safety measures.

1.4 Model Design

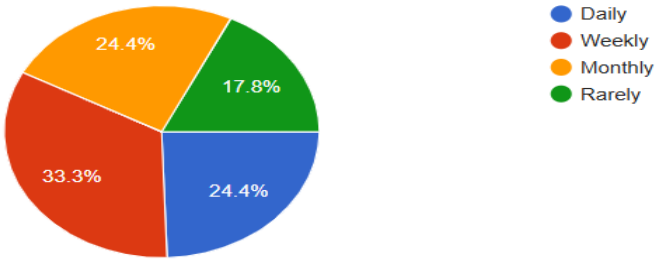
The study evaluates cybersecurity across five key areas:

1. **Data Security** (Encryption, secure servers)
2. **Access Control** (Strong passwords, MFA)
3. **Payment Security** (UPI, secure gateways)
4. **User Awareness** (Phishing and fraud recognition)
5. **Platform Transparency** (Breach reporting, trust policy

DATA ANALYSIS AND INTERPRETATION

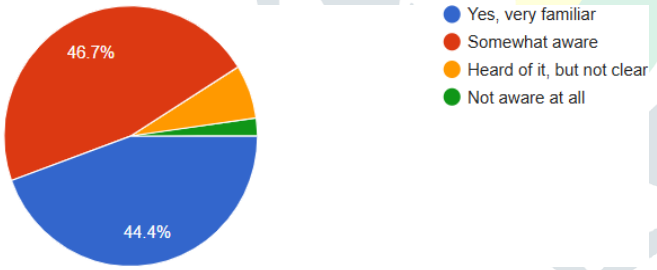
1. How often do you use e-commerce platforms (e.g., Amazon, Flipkart, Myntra, etc.)?

Options	Respondents	Percentage
Daily	11	24.4
Weekly	15	33.3
Monthly	11	24.4
Rarely	8	17.8
Total	**45**	**100%**



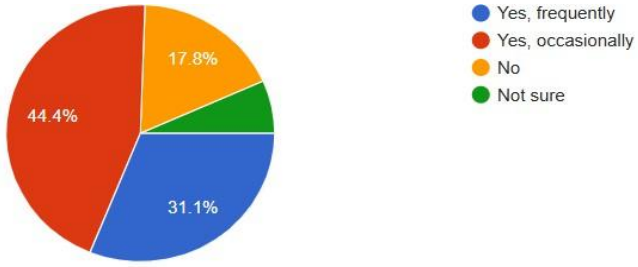
2. Are you aware of the term "cybersecurity"?

Options	Respondents	Percentage
Yes very familiar	20	44.4
Somewhat aware	21	46%
Heard of it but not clear	3	6.7%
Not aware at all	1	2.1%
Total	45	**100%**



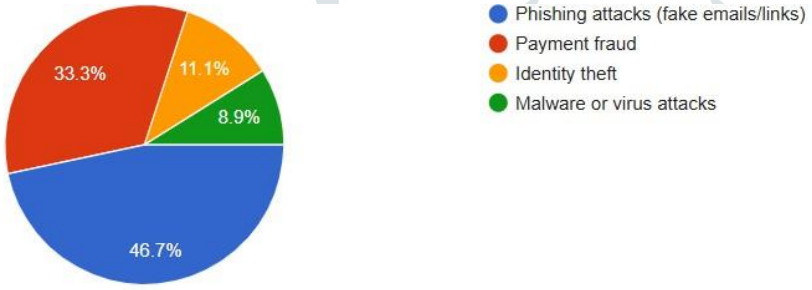
3. Have you ever received suspicious emails/messages claiming to be from e-commerce platforms?

Options	Respondents	Percentage
Yes, frequently	14	31.1%
Yes, occasionally	20	44.4%
No	8	17.8%
Not sure	3	1%
Total	45	**100%**



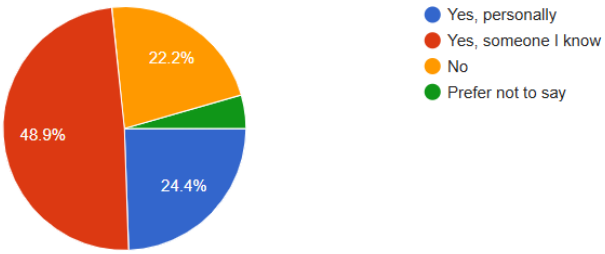
4. Which of the following threats do you consider most common in e-commerce?

Options	Respondents	Percentage
Phishing attacks	21	46.7%
Payment fraud	15	33.3%
Identity theft	5	11.1%
Malware or virus attacks	4	8.9%
Total	45	**100%**



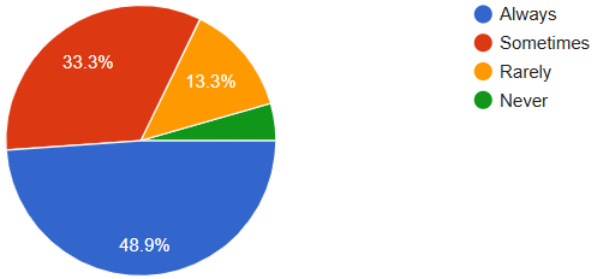
5. Have you or someone you know faced financial loss due to online shopping fraud?

Options	Respondents	Percentage
Yes,personally	11	24.4%
Yes,someone I Know	22	48.9%
No	10	22.2%
Prefer not to say	2	4.4%
Total	45	**100%**



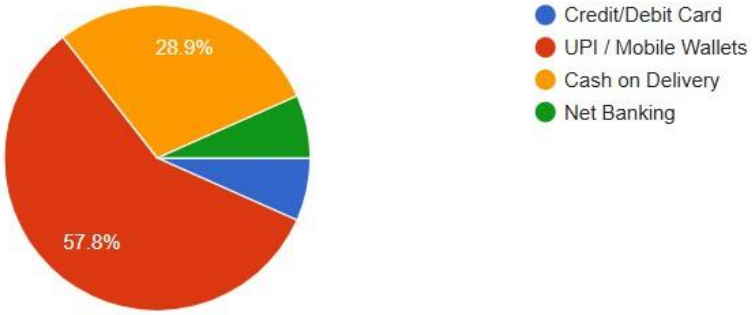
6. Do you use strong and unique passwords for e-commerce accounts?

Options	Respondents	Percentage
Always	22	48.9%
Sometimes	15	33.3%
Rarely	6	13.3%
Never	2	4.4%
Total	45	**100%**



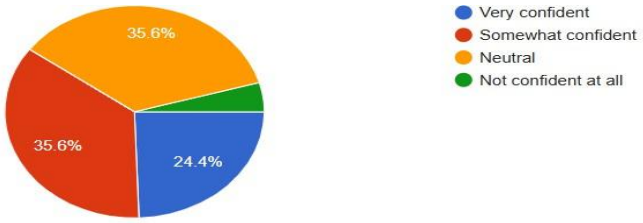
7. When shopping online, which payment method do you prefer?

Options	Respondents	Percentage
Credit/Debit Card	3	6.7%
UPI	26	57.8%
Cash on Delivery	13	28.9%
Net Banking	3	6.7%
Total	45	**100%**



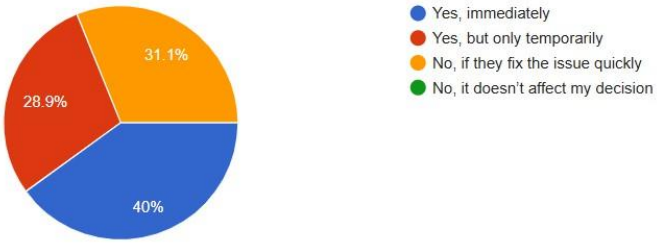
8. How confident are you in the security measures of the e-commerce platforms you use?

Options	Respondents	Percentage
Very confident	11	24.4%
Somewhat confident	16	35.6%
Neutral	16	35.6%
Not confident at all	2	4.4%
Total	45	**100%**



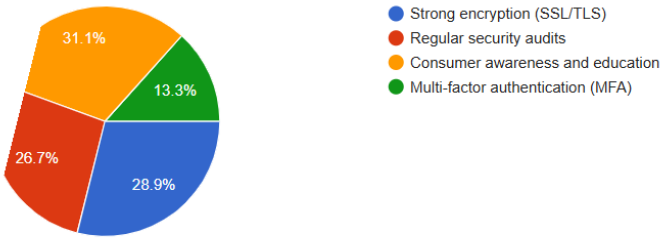
9. Would a major data breach (leak of customer details) make you stop using an e-commerce platform?

Options	Respondents	Percentage
Yee, immediately	18	40%
Yes, but only temporarly	13	28.9%
No,if they fix the issue quickly	14	31.1%
No,itvdoesn't affect my decisions	0	0%
Total	**63**	**100%**



10. In your opinion, what is the most important protective measure for e-commerce platforms?

Options	Respondents	Percentage
Strong encryption	13	28.9%
Regular security audits	12	26.7%
Consumer awarness and education	14	31.1%
Multi-factor authentication	6	13.3%
Total	**45**	**100%**



V. FINDINGS OF THE STUDY

1. The majority of respondents (33.33%) use e-commerce platforms weekly, indicating frequent engagement with online shopping activities. Very few reported rare usage, showing that e-commerce has become a regular part of digital consumer behavior.
2. Nearly half of the respondents (47.62%) are somewhat aware of cybersecurity, while a smaller proportion reported being very familiar with it. This suggests that although awareness exists, knowledge depth can still be improved.

3. 47.62% of respondents have occasionally received suspicious or fraudulent messages, reflecting the prevalence of phishing attempts and scam links targeting online shoppers.
4. Phishing attacks were identified as the most common perceived threat (47.62%), followed by payment fraud, data breaches, and identity theft. This highlights phishing as the dominant risk affecting consumer trust.
5. UPI/mobile wallet payments were the most preferred method (52.38%), indicating a strong shift toward digital and contactless transactions. Debit/credit card usage and Cash on Delivery were comparatively lower.
6. 38.10% of participants were neutral about the security of e-commerce platforms, suggesting that trust in platform security mechanisms is present but not fully assured.
7. The most critical cybersecurity improvement areas identified by respondents were:

- Consumer Awareness (30.95%)
- Stronger Authentication (21.42%)
- Encrypted Payment Security (19.04%)
- Security Audits & Monitoring (16.66%)
- Transparent Breach Reporting (11.90%)

8. A notable percentage (38.10%) would immediately stop using an e-commerce platform in case of a major data breach, indicating that cybersecurity incidents directly influence user retention and brand reputation.

VI. CONCLUSION

1. This study highlights the increasing significance of cybersecurity in e-commerce platforms as digital transactions become an essential part of consumer life. The survey findings reveal that although users actively engage in online shopping and prefer secure digital payment methods such as UPI and mobile wallets, they continue to face cybersecurity risks, particularly phishing attempts and fraudulent messages. The level of cybersecurity awareness among users is moderate, indicating the need for continuous security education and responsible online behavior.Phishing was identified as the most dominant threat, demonstrating that cybercriminals are increasingly exploiting social engineering techniques to target consumers. Additionally, a considerable number of respondents expressed neutral confidence regarding the security of e-commerce platforms, emphasizing the need for stronger authentication practices, improved encryption, and transparent communication when breaches occur. The study further confirms that cybersecurity incidents directly influence user trust and can lead to the immediate discontinuation of platform usage.Overall, the research concludes that enhancing cybersecurity in e-commerce requires a combination of advanced security technologies, robust payment protection, continuous monitoring, and consumer awareness programs. Platforms that prioritize these measures are more likely to build trust, protect customer data, and ensure safe and reliable online transactions.

VII. REFERENCES

1. Alshamrani, A. (2020). Cybersecurity challenges in e-commerce: A review. *International Journal of Advanced Computer Science and Applications, 11*(5), 45–53.
2. Hassan, A., & Hijazi, R. (2019). Enhancing e-commerce security using encryption and authentication. *International Journal of Computer Science and Information Security, 17*(5), 120–127.
3. IBM Security. (2021). *Cost of a data breach report*. IBM Corporation. Laudon, K. C., & Traver, C. G. (2018). *E-commerce: Business, technology, society* (14th ed.). Pearson.
4. OWASP Foundation. (2021). *OWASP Top 10: The ten most critical web application security risks*. Verizon. (2022). *Data breach investigations report (DBIR)*. Verizon Enterprise.