Educational Administration: Theory and Practice
2024, 30(1), 2018-2022
ISSN: 2148-2403
https://kuey.net/

Research Article

Adoption Of Online Payment Services Based On Perceived Risk And Customer Awareness

Anjali Yadav[1*], Dr. Arvind Kumar[2], Prof. V.K. Gangal[3]

[1*]Research Scholar in the Department of Management, Dayalbagh Educational Institute (Deemed to be University) Agra.
[2]Supervisor, the Department of Management, Dayalbagh Educational Institute (Deemed to be University) Agra.
[3]Cosupervisor, Dean, Faculty of Commerce, Dayalbagh Educational Institute (Deemed to be University) Agra.

Citation: Anjali Yadav et al. (2024), Adoption Of Online Payment Services Based On Perceived Risk And Customer Awareness, Educational Administration: Theory and Practice, 30(1), 2018-2022
Doi: 10.53555/kuey.v30i1.6830

ARTICLE INFO

ABSTRACT

The information technology has led to significant growth in the usage of online payments in recent years. The perceived risk and customer awareness have an impact on the online payment options available. This study analyses a theoretical relationship between perceived risk and consumers' awareness of adopting online payments. To evaluate a different of hypotheses aimed at analysing the distinctive features of each aspect and its impact on the perceived risks, a questionnaire with 45 respondents were administered. This study shows a significant relationship between consumer awareness, security risks and privacy risks in the adoption of online payment.

Keywords: Adoption, Online Payment Services, Perceived Risk, Customer Awareness

Introduction:

The development of Internet payments has improved people's quality of life and given businesses ongoing advantages in reaching clientele. Information tailored to each user individually. Smartphones are increasingly being used for online payments, and this trend is only going to grow. This type of online payment includes using websites or applications to buy things on a tablet, or smartphone, or even by employing near-field communications. Researchers have studied if customers are incorporating online payment systems into their everyday routines as well as their perception of risks and consumer awareness affects their usage patterns **Hossain, Md. A. (2019).**

Online payment refers to the purchase of products, services, and content via wireless devices without regard to time or location constraints. Online payments will continue to be a popular way for businesses and individuals to conduct secure electronic business transactions. Any payment in which a mobile device is used to start, approve, and validate a commercial transaction is referred to in this study as an online payment, or e-payment. Online payments are practical and convenient, and they are a logical progression of electronic payments. Researchers and practitioners who are particularly interested in online payment systems can all benefit greatly from a better understanding of the key factors underlying online users' intention user's intention to use online payment because systems, software, supporting service providers, financial institutions, trusted third parties **Kim et al (2010).**

Perceived risk in online payment

It is important to remember that different types of risk could be perceived significantly from one another and have various consequences while researching the idea of consumers' perceived risk in diverse industries. This is because different types of risk might have distinct causes and conditions.

Here are a few concerns regarding the security and privacy of information technology users. Concerns about consumer privacy are not new. Complaints over the government's and companies' use of personal data have been present for years among consumers. Several laws protecting privacy have been passed as a result of their action and worry. As more and more individuals utilize the Internet's information resources and the general public has become more tech-savvy, the problem of consumer privacy is becoming more and more significant. One of the primary excuses given by web users for doing online transactions is security concerns. Payment fraud is a serious issue for consumers, even though most of the media coverage regarding Internet security has concentrated on the possible threats to customers who use credit cards to make purchases electronically. Apart

from technological disruptions and break-ins, security dangers also include identity theft, impersonation, and stalking, which are grave concerns that everyone should be aware of. The hacking of computers is yet another major issue. Hacking is a behaviour that can be harmful or innocuous **Udo, G. J. (2001).**
When users exchange information on social networks or applications, the necessity for privacy-awareness-raising techniques becomes more pressing. To reduce the negative impacts of making an online payment by raising user knowledge of the discrepancy between users' intended and real audiences.

Literature Review

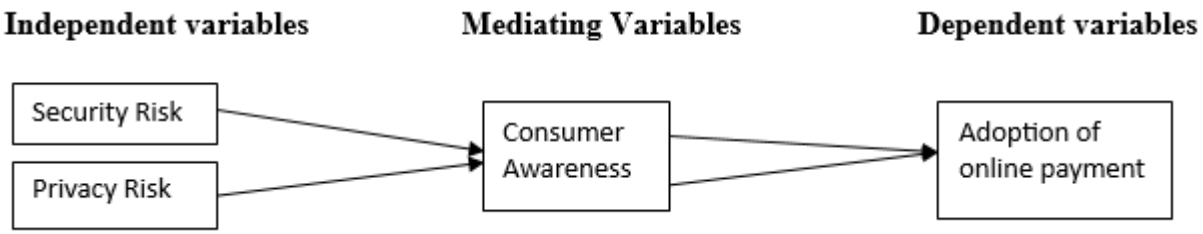
Security risk on online Payment

This article examines the security concerns surrounding online payments in China, focusing on transaction fraud and information leaks. It highlights the growing issue and its impact on client confidence, highlighting the need for strategic recommendations to address these security issues and promote e-commerce growth **(Zhang, C et al 2012).** Modern business is made more convenient and efficient by the use of electronic payment solutions that improve security. Research indicates that multi-factor authentication systems provide more security features **(Aigbe. P. and Akpojaro. J., 2014).** Online payment security threats include identity theft, data breaches, and cyberattacks. A thorough analysis of these risks is crucial for establishing robust security measures. In particular, Near Field Communication (NFC) technology is examined concerning the perceived security and reliability of mobile payments. Nonetheless, its applicability is restricted to a particular Middle Eastern nation. Cross-cultural studies should be a part of future studies **(Almaiah. M.A. et al., 2022).**

Privacy risk on online payment

Studies reveal that the absence of security controls by e-service providers results in breaches of privacy and improper usage of customer data. Privacy risk evaluations by consumers are impacted by issues related to security and dependability. Adoption of e-services is hampered by privacy risks, although this can be lessened by consumers' favourable opinions of website usability and company reliability. Internet service providers need to come up with fresh ideas to combat privacy threats **(Featherman et al 2010).** Despite privacy and convenience issues looks at a supply chain where an e-tailer sells through both an internet website and mobile applications. It focuses on the best ways to promote the product in each channel **(Choi, T. M. 2021).** Internet-based payment systems are systems or networks that let people and companies send and receive money online. Credit/debit card payments, digital wallets, cryptocurrency, and online banking services are just a few of the systems that these technologies and processes cover **(Sahi A, Khalid H et al 2022).**

Conceptual Framework of Online Payment



Research Methodology

Online payment, consumer awareness of security risks, and privacy risks are among the topics covered in a questionnaire designed to evaluate the study model and test the theoretical approaches. To fit the final questionnaire with the context of online payment, the researcher chose questionnaire items based on consumer behaviour and perceived risk. Measures of perceived risk and consumer awareness are taken from the research. A five-point Likert scale, with 1 denoting strongly disagree and 5 denoting strongly agree, is used to evaluate each item. Every measurement construct was implemented in the current research as an indicative concept. A survey has been carried out to explore the relationship between security and privacy concerns and how it relates to consumers' knowledge of online payment options. Survey responses have been requested from 45 participants.

Data Analysis

Forty-five people in all took part in the study and completed the questionnaire. Additionally, we tested our hypotheses and calculated reliability and validity, correlation, regression and factor analysis, frequencies and descriptive study Cronbach's alpha α using the Statistical Package for the Social Sciences (SPSS) software.

Reliability

Cronbach's alpha (α) is a reliability measure that runs from 0 to 1 although some professionals consider a value between 0.6 and 0.8 to be acceptable. Table 1 displays the Cronbach's alpha (α) of each measurement in the

survey; a value of 0.770 indicates that the research measurements are reliable. This reliability assessment was done to confirm the internal consistency of the measurements of the proposed model.

Table 1 Reliability statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. of items
0.770	0.770	4

Descriptive Statistics

Table 2 shows data collected from 45 participants in the study to look at their opinions on online payment, consumer awareness, privacy risk, and security risk. The findings indicated that there were differences of 6, 3, 5, and 4 between the highest and minimum responses for each of these variables. In particular, 3, 1, 2, and 2 were the lowest values recorded for security risk, privacy risk, consumer awareness, and online payment, respectively; 9, 4, 6, and 6 were the highest values The average values were calculated as follows: 5.5111, 1.8222, 3.7111, and 3.4889 for security risk, privacy risk, consumer awareness, and online payment, respectively. The dispersion across the datasets was evaluated using the standard deviation (SD), which yielded variance values of 1.65999, 0.74739, 1.30771, and 1.19891 for online payment, security risk, privacy risk, and consumer awareness, in that order.

Additionally, the distributions of responses for consumer awareness, security risk, privacy risk, and online payment were found to have right-skewed features, as shown by the positive skewness values. Furthermore, platykurtic behaviour was seen in these reactions. In contrast to a positive kurtosis value, which denotes a wider tail in their distributions, the negative kurtosis values linked to security risk, consumer awareness, and online payment suggest a shorter tail.

Table 2 Statistics

	SR	OP	AW	PR
No.	45	45	45	45
Valid missing	0	0	0	0
Mean	5.5111	3.4889	3.7111	1.8222
Mode	5.00	2.00	3.00	2.00
Std. deviation	1.65999	1.19891	1.30771	.74739
Skewness	.401	.193	.375	.647
Std. error of skewness	.354	.354	.354	.354
Kurtosis	-.465	-1.232	-.884	.238
Std. Error of Kurtosis	.695	.695	.695	.695
Minimum	3.00	2.00	2.00	1.00
Maximum	9.00	6.00	6.00	4.00

Output Of SPSs

Hypothesis testing

The problem is investigating the relationship between security risk, privacy risk, consumer awareness and online payment. Using Pearson's correlation coefficient, mean values, standard deviations, and correlations between study dimensions were taken into consideration for assessing research hypotheses. We computed these metrics using all 45 individuals' replies

H_1: Online payments and the variable security risk are correlated. So there is a positive significant relationship between security risk and online payment

Security risk and online payment

Pearson correlation of security risk and online payment was found to be low positive and statistically significant ($R=.408$, $p<0.05$). Hence H_1 was supported this shows that an increase in security risk behaviour would lead to a higher online payment in the followers.

Privacy risk and online payment

H_2: Similarly, we associate online payment with variable privacy risk. So there is a significant positive relationship between privacy risk and online payment.

The Pearson correlation analysis found a statistically significant and somewhat favourable link between privacy risk and online payment ($R = 0.679$, $p < 0.001$). As a result, hypothesis H_2, which postulates that participants' higher online payment is correlated with their increasing privacy risk behaviour, was supported.

Consumer awareness and online payment adoption

H_3: Additionally, a correlation has been shown between online payment and customer awareness. There is a positive mediating significant relationship between consumer awareness and online payment.

The computed correlation coefficient (r) between online payment adoption and consumer awareness was found to be 0.571, suggesting a somewhat favourable relationship between the two variables. Given that the computed p-value is less than 0.001, the association is statistically significant. Thus, it follows that a rise in consumer awareness is probably going to be associated with a rise in the use of online payments. Consequently, the results support hypothesis H_3.

A simple mediation analysis conducted using ordinary least square path analysis was found for the hypothesis that a positive relation significantly mediated the relationship between consumer awareness and online payment.

Table 3 Correlation

	SR	OP	CA	PR
SR	1	.408	.446	.679
OP	.408	1	.571	.505
CA	.446	.571	1	.458
PR	.679	.505	.458	1

Regression analysis

Table 4Regression Result

Model	R	R Square	Adjusted Square	R Std. Error of the estimate
1	.513	.263	.228	1.05350

a.Predictors: (Constant), SR, PR

As indicated in Table no. 4 Researcher can see that R- the square value is 0.263, which means that our independent variable i.e. perceived risk causes a 26.3% change in the dependent variable i.e. online payment adoption.

Table no.5 ANOVA

Model		Sum of Square	df	Mean Square	F	Sig.
1	Regression	16.630	2	8.315	7.492	.002
	Residual	46.615	42	1.110		
	Total	6/3.244	44			

a. Dependent Variable: OP
b. Predictors: (Constant) SR, PR

In Table No. 5 ANOVA results show that the p-value is .002 which is less than 0.05, hence we say that there is a significant relationship between independent security risk, privacy risk and online payment adoption.

Table no. 6 Coefficients

		Unstandardized Coefficients		Standardized Coefficient		
Model		B	Std. Error	Beta	t	Sig.
1	Constant	1.771	.552		3.211	.003
	SR	.087	.130	.121	.671	.506
	PR	.678	.290	.423	2.342	.024

a. Dependent variable: OP

The coefficient findings are shown in Table 6, where the beta values for privacy risk and security risk are 0.423 and 0.121, respectively. These figures show that an increase of 0.121 and 0.423 units results from a unit increase in the independent variables, security risk and privacy risk, respectively. The uptake of online payments is the dependent variable. Furth more, a significant correlation is indicated by the positive beta values between online payment uptake, privacy risk, and security risk. It follows that the adoption of online payment rises in proportion to increases in security and privacy risk, which are estimated to be 0.121 and 0.423 units higher, respectively.

Results and discussions

Using the SPSS macro developed by Hayes (2022), a basic mediation analysis using ordinary least square path analysis revealed evidence in favour of the hypothesis that consumer awareness significantly mediates the relationship between security risk and privacy risk with the adoption of online payments.

The data shown in Figure 1 and Table 6 indicates a significant correlation between security risk and customer knowledge (α = 0.352). Additionally, the use of online payments is favourably correlated with consumer awareness (b = 0.445). Based on 5000 bootstrap resamples, a bootstrap confidence interval for the indirect impact (ab = 0.156) showed that the interval (0.149 to 0.197) completely surpassed zero, suggesting that consumer knowledge mediates the relationship between security risk and the adoption of online payments. In a similar vein, there was a positive correlation between privacy risk and customer awareness (α = 0.8011) and online payment uptake (b = 0.394). Once more, based on 5000 bootstrap resamples, a bootstrap confidence interval for the indirect impact (ab = 0.315) revealed that the interval (0.197 to 0.721) was completely above zero, showing consumer awareness as a mediating factor in the association between privacy risk and online payment acceptance.

These results highlight the critical role that consumer knowledge plays as a mediator in the dynamics between security risk and privacy risk with the adoption of online payments, providing insightful information that may help improve online payment practices.

Conclusion

Perceived risk and client knowledge are two important elements that affect the adoption of online payment systems. Consumers' perception of risk is shaped by their worries about security, privacy, and fraud. However, these worries have been lessened by developments in encryption technology, strong authentication procedures, and regulatory frameworks, which have increased customer trust. Another important element is customer knowledge, as this may boost confidence and enable well-informed decision-making. Education on the advantages, features, and security aspects of different payment systems is available. Adoption rates can be further increased by resolving misunderstandings and boosting digital literacy. Businesses and financial institutions need to make investments in technology advancements, security protocols, and awareness campaigns in order to create an atmosphere that is favourable to the acceptance of online payments.

References

1. Acharya, B. (2017). Privacy and security risks on online payment. ORF ISSUE BRIEF, 177, 1–6.
2. Choi, T. M. (2021). Mobile-App-Online-Website Dual Channel Strategies: Privacy Concerns, E-Payment Convenience, Channel Relationship, and Coordination. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(11), 7008–7016. https://doi.org/10.1109/TSMC.2019.2961979
3. Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. Journal of Services Marketing, 24(3), 219–229. https://doi.org/10.1108/08876041011040622.
4. Hossain, Md. A. (2019). Security perception in the adoption of mobile payment and the moderating effect of gender. PSU Research Review, 3(3), 179–190. https://doi.org/10.1108/prr-03-2019-0006
5. Kim, C., Mirusmonov, M., & Lee, I. (2010). An empirical examination of factors influencing the intention to use mobile payment. Computers in Human Behaviour, 26(3), 310–322. https://doi.org/10.1016/j.chb.2009.10.013
6. Udo, G. J. (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. In Information Management and Computer Security (Vol. 9, Issue 4, pp. 165–174). https://doi.org/10.1108/EUM0000000005808.
7. Neama, G., Alaskar, R., & Alkandari, M. (2016). Privacy, security, risk, and trust concerns in e-commerce. ACM International Conference Proceeding Series, 04-07-January-2016. https://doi.org/10.1145/2833312.2850445
8. Sahi, A. M., Khalid, H., Abbas, A. F., Zedan, K., Khatib, S. F. A., & Amosh, H. al. (2022). The Research Trend of Security and Privacy in Digital Payment. In Informatics (Vol. 9, Issue 2). MDPI. https://doi.org/10.3390/informatics9020032