

Cyber Security Issues Affecting the Users' Willingness to Use E-Banking: A Case of Nepalese Commercial Banks

Sulav Raj Joshi*

Abstract

This study examines the cyber security issues affecting the user willingness to use e-banking in Nepalese commercial banks. Willingness to use e-banking is selected as the dependent variable. Similarly, security and privacy concerns, fear of identity theft, fear of identity fraud, lack of trust and ease of use are selected as the independent variables. This study is based on primary data with 124 observation. To achieve the purpose of the study, structured questionnaire is prepared. The correlation coefficients and regression models are estimated to test the significance and importance of different factors influencing e-banking users in Nepalese commercial banks.

The study showed that security and privacy concerns has a positive impact on willingness to use e-banking. It means that increase in security and privacy concerns leads to increase in willingness to use e-banking. Similarly, fear of identity theft has a negative impact on willingness to use e-banking. It indicates that decrease in fear of identity theft leads to increase in willingness to use e-banking. Moreover, fear of identity fraud has a negative impact on willingness to use e-banking. It means that decrease in fear of identity fraud leads to increase in willingness to use e-banking. Likewise, lack of trust has a negative impact on willingness to use e-banking. It shows that decrease in lack of trust leads to increase in willingness to use e-banking. Similarly, ease of use has positive impact on willingness to use e-banking. It shows that higher the ease of use, higher would be the willingness to use e-banking

Keywords: security and privacy concerns, fear of identity theft, fear of identity fraud, lack of trust, ease of use, willingness to use e-banking.

1. Introduction

Internet banking (or E-banking) means any user with a personal computer and a browser can get connected to his bank's website to perform any of the virtual banking functions (Sharma, 2011). The internet banking enables one to buy and sell without physical cash, make deposits, transfer, pay bills, etc. with ease (Adewale, 2014). Similarly, e-banking applications, which include automated teller machines (ATM), telephone banking, mobile banking, digital television, debit and credit cards, internet banking, etc., have become one of the main battlefields of the banking industry (Atay and Apak, 2013). Likewise, Traditional banking used to deal with customers in person and was confined to services that could only be availed by having the physical

* Mr. Joshi is a Freelance Researcher, Kathmandu, Nepal.

presence of customers (Dua and Upadhyaya, 2022). However, technological advancement has led to a change in how the banking sector operates.

Cyber security is the protection of internet-connected systems, including hardware, software, and data, from cyber-attacks (Tyagi, 2019). Likewise, perceived identity theft is described as one of the several dimensions of cyber-security threats. This occurs when the individual is perceived that his/her identity (such as name, address, mobile number, etc.) could be stolen by the third party in a transaction regarding any related e-business (Lai *et al.*, 2012). Identity fraud is defined as the broad criminal use of false identifiers and false identification documents. Identity theft is a term used to categorize the fraudulent use of an individual's personal information for criminal purposes and without their agreement (Reyns, 2013). Moreover, Identity theft a growing problem which affects individuals all over the world (Reyns and Henson, 2016). Similarly, the criminal use of false identifiers and false identification documents is an integral part of many crimes committed by global criminal groups, including drug traffickers, gun runners, cyber criminals, and terrorists (Wilcox and Regan, 2002). Trust plays a large role in determining consumers' initial and continued use of the e-banking service (Suh and Han, 2002). The study found that trust not only effects intent to use e-banking but trust in e-banking has also been found to be an antecedent to commitment to e-banking (Kassim and Abdulla, 2006; Vatanasombut *et al.*, 2008). Likewise, banks are recommended to find a way to increase user trust by offering their users a range of the latest and the best security technologies in order to encourage them to accept the e-banking system and gain the user trust (Ataya *et al.*, 2019).

In online business trust, security and safety are the most challenging issues for the banks. Besides them, to build and retain the customers' trust will also become a future challenge for banks especially in internet banking (Aladwani, 2001). Similarly, majority of the customers hesitate to use internet banking services because of security and privacy issues (Lee and Turban, 2001). Furthermore, Ramayah and Ignatius (2005) found that usefulness, ease of use and awareness are not only the factors that affect the intention to use online banking system. Mannan and Van Oorschot (2008) investigated that online banking is one of the most sensitive tasks performed by general Internet users. The study found that the security settings of systems is used for sensitive online transactions and the discussion on real-world system security and user responsibilities. Similarly, Polasik and Piotr Wisniewsk (2009) investigated that identify empirically the factors underlying the decision to adopt online banking in Poland. The study found that the useful insights are

also provided with regard to market segmentation, security and strategies fostering the acceptance of online banking. Likewise, Vrîncianu and Popa (2010) concluded that the current global recession is likely to increase the frequency of internal fraud and security breaches.

Huang *et al.* (2011) showed that people's compliance to security practices, such as setting strong passwords for IT systems, can be enhanced by changing their perceived knowledge, severity and possibility, while changing their perceived knowledge and severity is most effective. Likewise, Twum and Ahenkora (2012) found that the internet banking security strategy may consider the generation gap in adoption and should continuously aim at securing customers' trust of the providers' online brand's security, including the provision of security information and education. Bashir and Madhavaiah (2014) investigated that the determinants of young consumers' intention to use Internet banking services in India. The study concluded that the bank practitioners should focus on increasing usefulness of Internet banking system and devise trust building strategies that would reduce consumers' perceived risk and attract them to use Internet banking. Similarly, Kassim and Ramayah (2015) found that the factors that allows Internet banking providers to enhance the services in the most effective and efficient way to increase bank business in the long run and encourage their bank customers to continue using Internet banking.

Aboobucker and Bao (2018) found that the country contributes to the advancement of Internet banking acceptance and offers some useful insights to researchers, practitioners and policy makers on how to enhance Internet banking acceptance for country similar in context. Moreover, Eleyan *et al.* (2022) concluded that the raise of the customer awareness to avoid victims of cyber security issues and minimize the loss of data and money. Jordan *et al.* (2018) investigated that the online activities are present in almost every aspect of people's daily lives. The study found that the impact of fear of identity theft and perceived risk on online purchase intention can be helpful for online sellers, because with these findings they can manage this fear and perceived risk to increase online purchase intention and address the risks accordingly. Moreover, Jibril *et al.* (2020) investigated that the e-banking transactions have focused more on motivational factors that trigger the intention to accept and use the e-banking transaction, rather than the de-motivational factors that propel the action. The study concluded that the impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana.

Wang *et al.* (2020) found that the lack of advanced technologies to prevent and address cyber security breaches appear to be the primary factors

that have reduced cyber security capability in our sample of banks. Likewise, Muhammad *et al.* (2021) concluded that the privacy and security are critical aspects in Islamic banking operation, and Islamic banking should take proactive measures to ensure that privacy and security in internet banking are at an optimal level. Fatmawati *et al.* (2023) concluded that the understanding of perceived usefulness, ease of use, security, and consumer attitude on behavioral intentions in mobile banking. Moreover, Purnamasari *et al.* (2023) found that the privacy, security, trust has a simultaneous and partial effect on the intention to transact online at Bank BCA Bandung. Likewise, Gomes *et al.* (2022) investigated that the internet brought a new revolution to the financial sector and it has changed the way of operations in the last two decades. The study found that the number of cyber security issues in internet banking in India and the consumer's awareness of these issues and preventive measures used by them.

In the context of Nepal, Khatri and Upadhyaya-Dhungel (2013) concluded that customers education level, security and privacy concerns, theft of passwords were identified as the major challenges faced by the bank regarding the development of their online facilities. Similarly, Shah (2015) found that the challenges for the development of e-banking, its impact of infrastructural barriers, legal and security barriers and management-banking barriers on the development of e-banking in Nepal. Likewise, Dangol and Kauish (2019) concluded that the study concluded that the more experience with cyber-fraud incidents customers have, the more likely they will not commit transactions in e-commerce. Moreover, Mastran (2021) concluded that the Nepalese banking industry should invest on adopting the most secured and trustworthy e-banking system and educating customers on the use and importance of e-banking regularly.

The above discussion shows that the empirical evidences vary greatly across the studies on the cyber security issues affecting the users' willingness to use e-banking in commercial banks. Though there are above mentioned empirical evidences in the context of other countries and in Nepal, no such findings using more recent data exist in the context of Nepal. Therefore, in order to support one view or the other, this study has been conducted.

The main purpose of the study is to analyze the cyber security issues affecting the users' willingness to use e-banking in Nepalese commercial banks. Specifically, it examines the impact of security and privacy concerns, fear of identity theft, lack of trust and ease of use on willingness to use e-banking in Nepalese commercial banks.

The remainder of this study is organized as follows. Section two describes the sample, data and methodology. Section three presents the empirical results and the final section draws the conclusion.

2. Methodological aspects

The study is based on the primary data. The data were gathered from 124 respondents through questionnaire. The respondents' views were collected on security and privacy concerns, fear of identity fear, fear of identity theft, lack of trust, ease of use and willingness to use e-banking. The study used descriptive and casual comparative research design.

The model

The econometric models used in this study tries to explain the relationship between selected variables and willingness to use e-banking in Nepal. This study uses least square regression model to test which of the hypothesis are consistent with data. As each hypothesis in this study imply signed relationship, regression model may help to indicate which of the hypotheses are generally consistent or inconsistent with the data.

In this model, the dependent variable is WEB indicated by Willingness to use e-banking. The independent variables are security and privacy concerns, fear of identity theft, fear of identity fraud, lack of trust and ease of use. The model is presented as:

$$WUE = \beta_0 + \beta_1 SPC + \beta_2 FIT + \beta_3 FIF + \beta_4 LOT + \beta_5 EOU + e$$

Where,

WUE = Willingness to use e-banking

SPC = Security and Privacy Concerns

FIF= Fear of Identity Fraud

FIT = Fear of Identity Theft

LOT= Lack of Trust

EOU= Ease of Use

Security and privacy concerns was measured using a 5-point Likert scale where respondents were asked to indicate the responses using 1 for strongly agree and 5 for strongly disagree. There are 5 items and sample items include "I don't think e-banking has enough safeguards to make me feel comfortable using it to transact personal business", "Electronic banking is insecure for transaction data and privacy" and so on. The reliability of the items was measured by computing the Cronbach's alpha ($\alpha = 0.658$).

Fear of identity theft was measured using a 5-point Likert scale where the respondents were asked to indicate the responses using 1 for strongly agree and 5 for strongly disagree. There are 5 items and sample items include “My identity will be stolen if I using electronic banking services”, “Having my online identity stolen through e-banking is a severe problem for me” and so on. The reliability of the items was measured by computing the Cronbach’s alpha ($\alpha = 0.658$).

Fear of identity fraud was measured using a 5-point Likert scale where the respondents were asked to indicate the responses using 1 for strongly agree and 5 for strongly disagree. There are 5 items and sample items include “My credit card details can be used illegally via the Internet”, “My personal information provided for e-banking could be misused.” and so on. The reliability of the items was measured by computing the Cronbach’s alpha ($\alpha = 0.762$).

Lack of trust was measured using a 5-point Likert scale where the respondents were asked to indicate the responses using 1 for strongly agree and 5 for strongly disagree. There are 5 items and sample items include “The internet banking website doesn’t keeps it promises and commitment”, “The internet banking website is not trustworthy”, and so on. The reliability of the items was measured by computing the Cronbach’s alpha ($\alpha = 0.688$).

Ease of use was measured using a 5-point Likert scale where the respondents were asked to indicate the responses using 1 for strongly agree and 5 for strongly disagree. There are 5 items and sample items include “Internet banking is user friendly and flexible in use”, “The internet enables customers to access the banks website 24/7”, and so on. The reliability of the items was measured by computing the Cronbach’s alpha ($\alpha = 0.686$).

Willingness to use e-banking was measured using a 5-point Likert scale where the respondents were asked to indicate the responses using 1 for strongly agree and 5 for strongly disagree. There are 5 items and sample items include “I would use electronic banking services for purchasing a product/service”, “Given the chance, I would try to buy items online via electronic banking”, and so on. The reliability of the feature was measured by computing the Cronbach’s alpha ($\alpha = 0.732$).

The following section describes the independent variables used in this study along with hypothesis formulation.

Security and privacy concern

Online banking brings many benefits to the banking industry but also creates a significant opportunity for cybercrime offenders (Eleyan *et al.*,

2022). Similarly, Ataya and Ali (2019) argued that despite the endless number of benefits from electronic banking, there are many security concerns related to trust and privacy, which significantly impact customers' acceptance of the adoption and the use of electronic banking services. Likewise, Polasik (2009) argued that the security and privacy risk of online transactions significantly impact online banking adoption. Furthermore, Nguyen *et al.* (2014) argued that security and trust remarkably impact customers' intention to use e-banking. Moreover, Wessels and Drennan (2010) concluded that customers' perceived risk has the most crucial influence on the acceptance of mobile banking. The study showed that customers' perceived security and privacy risk have the highest impact on their behaviour toward accepting any e-banking system. Based on it, the study develops the following hypothesis:

H₁: There is a positive relationship between security and privacy concerns and willingness to use e-banking.

Fear of identity theft

Online identity theft is a growing problem which affects individuals all over the world (Reyns and Henson, 2016). Similarly, the perceived risk is a significant factor influencing attitude towards intention to continue using Internet banking in Malaysia (Kassim and Ramayah, 2015). Likewise, identity theft happens when personal information (such as name, address, mobile number, credit card number, etc.) is accessed by someone else without your explicit permission (Lai *et al.*, 2012). Furthermore, identity theft is a type of cybercrime in which hackers attempt to access crucial personal data such as PAN numbers, debit/credit card numbers, and other associated information to impersonate someone and profit off their identity (Gomes *et al.*, 2022). Moreover, Jibril *et al.* (2020) stated that perceived online identity theft generates a "fear of reputational damage," "fear of financial loss," and "security and privacy concern" and negatively affects the intention to engage in e-banking transactions. Based on it, the study develops the following hypothesis:

H₂: There is a negative relationship between fear of identity theft and willingness to use e-banking.

Fear of identity fraud

Identity fraud is defined as the broad criminal use of false identifiers and false identification documents. The criminal use of false identifiers and false identification documents is an integral part of many crimes committed by global criminal groups, including drug traffickers, gun runners, cyber criminals, and terrorists (Wilcox and Regan, 2002). Similarly, the types of

fraud that are commonly experienced by financial institution include sales fraud, purchase fraud, cheque payment fraud and ATM fraud (Benjamin, 2011). Likewise, users may not know that a fraud has been committed until they see an account they did not open on their credit report or until a debt collector contacts them for payment (Rachel Kim, 2009). Furthermore, Onu *et al.* (2017) defined electronic banking frauds as frauds associated with electronic banking perpetrated using ATM, POS, internet and mobile banking platforms. Moreover, identity fraud occurs when criminals take illegally obtained personal information and misuse it for their financial gain by making fraudulent purchases or withdrawals, creating false accounts, or attempting to obtain services such as employment or healthcare (Rachel Kim, 2009). Based on it, the study develops the following hypothesis:

H3: There is a negative relationship between fear of identity fraud and willingness to use e-banking.

Lack of trust

Chen and Barnes (2007) stated that trust substantially plays an important role on online purchasing intent, web site loyalty, and internet banking commitment, electronic banking adoption. Similarly, customer trust is a significant component impacting the growth of online banking (Suh and Han, 2003). Likewise, Mwesigwa and Nkundabanyanga (2011) stated that organizations acting business online must boost trust rapidly in order to succeed. Furthermore, Kassim and Abdulla (2006) argued that trust plays an important role in expanding and keeping successful relationships in the financial tasks sector because many of the activities are complicated and there is an online relationship. Moreover, Sohrabi *et al.* (2013) found that trust, security and costs have significant and positive relationship with customers' adoption of online banking in Malaysia. Based on it, the study develops the following hypothesis:

H4: There is a negative relationship between lack of trust and willingness to use e-banking.

Ease of use

Perceived ease of use relates to the degree to which individuals believe that using a particular system would require no effort (Davis, 1989). Similarly, the ease of use and accessibility has a positive impact on internet banking services (Poon, 2008). Likewise, ease of use is the factor that contributed to the acceptance of the internet banking services among customers and as well as with other factors such as enjoyment, information on internet banking and quality of the internet connection (Pikkarainen *et al.*, 2004). Furthermore,

information technologies that are easy to use will be less threatening to the individual (Moon and Kim, 2001). The study also found that ease of use positively correlates with use of customer technologies, such as computer software (Davis, 1989). Moreover, the usefulness and ease of use have been found to have a strong influence on the use of electronic banking services (Gefen and Keil, 1998). Based on it, the study develops the following hypothesis:

H₅: There is a positive relationship between ease of use and willingness to use e-banking.

3. Results and discussion

Correlation analysis

On analysis of data, correlation analysis has been undertaken first and for this purpose, Kendall’s Tau correlation coefficients along with means and standard deviations have been computed, and the results are presented in Table 1.

Table 1

Kendall’s Tau correlation coefficients matrix

This table presents Kendall’s Tau coefficients between dependent and independent variables. The correlation coefficients are based on 145 observations. The dependent variable is WUE (Willingness to use e-banking). The independent variables are SPC (Security and privacy concerns), FIT (Fear of identity theft), FIF (Fear of identity fraud), LOT (Lack of trust) and EOU (Ease of use).

Variables	Mean	S.D.	WUE	SPC	FIT	FIF	LOT	EOU
WUE	1.908	0.642	1					
SPC	2.472	0.640	0.046	1				
FIT	2.477	0.543	-0.008	0.398**	1			
FIF	2.471	0.535	-0.112	0.320**	0.423**	1		
LOT	2.504	0.612	-0.119	0.437**	0.477**	0.525**	1	
EOU	2.180	0.516	0.256**	0.226**	0.248**	0.321**	0.191	1

Note: The asterisk signs (**) and (*) indicate that the results are significant at one percent and five percent levels respectively.

Table 1 shows the Kendall’s Tau correlation coefficients of dependent and independent variables. The study indicates that security and privacy concerns is positively correlated to the willingness to use e-banking indicating that security and privacy concerns increases the willingness to use e-banking. Likewise, fear of identity theft is negatively correlated to the willingness to use e-banking. This implies that decrease in fear of identity theft leads to the increase in the willingness to use e-banking. Similarly, fear of identity

fraud is negatively correlated to the willingness to use e-banking. It indicates that higher the fear of identity fraud, lesser will be the willingness to use e-banking. However lack of trust is also negatively co-related related to the willingness to use e-banking. It indicates that lesser the lack of trust, higher the willingness to use e-banking. Moreover, ease of use is positively correlated to the willingness to use e-banking that indicates that increase in ease of use leads to the increase in the willingness to use e-banking.

Regression analysis

Having indicated the Kendall's Tau correlation coefficients, the regression analysis has been carried out and the results are presented in Table 2. More specifically, it presents the regression results of security and privacy concerns, fear of identity theft, fear of identity fraud, lack of trust and ease of use on willingness to use e-banking in Nepalese commercial banks.

Table 2

Estimated regression result willingness to use e-banking, security and privacy concerns, fear of identity theft, fear of identity fraud, lack of trust and ease of use provided by e-banking users of Nepalese commercial banks

The results are based on 124 observations using linear regression model. The model is $WUE = \beta_0 + \beta_1 SPC + \beta_2 FIT + \beta_3 FIF + \beta_4 LOT + \beta_5 EOU + \varepsilon$ where the dependent variable is WUE (Willingness to use e-banking). The independent variables are SPC (Security and privacy concerns), FIT (Fear of identity theft), FIF (Fear of identity fraud), LOT (Lack of trust) and EOU (Ease of use).

Model	Intercept	Regression coefficients of					Adj. R_bar ²	SEE	F-value
		SPC	FIT	FIF	LOT	EOU			
1	1.807 (10.828) **	0.041 (0.627)					-0.005	0.464	0.394
2	1.883 (9.628) **		-0.010 (0.130)				-0.008	0.464	0.017
3	1.689 (8.586) **			-0.089 (1.139)			0.002	0.462	1.298
4	1.685 (0.089)				-0.089 (1.313)		0.006	0.461	1.724
5	1.256 (7.332) **					0.299 (3.912) **	0.104	0.438	15.301
6	1.837 (8.806) **	0.051 (0.657)	-0.089 (0.241)				-0.013	0.465	0.224
7	1.717 (7.494) **	0.43 (0.559)	-0.086 (0.826)	-0.121 (1.253)			-0.008	0.464	0.673
8	1.722 (7.519) **	0.43 (0.210)	-0.128 (1.147)	-0.69 (0.645)	-0.116 (1.067)		-0.007	0.464	0.790
9	1.327 (5.531) **	0.000 (0.004)	-0.163 (1.535)	-0.129 (0.182)	-0.138 (1.342)	0.314 (3.842) **	0.097	0.439	3.657

Notes:

- Figures in parenthesis are t-values.
- The asterisk signs (**) and (*) indicate that the results are significant at one percent and five percent level respectively.
- Willingness to use e-banking is the dependent variable.

The regression results show that the beta coefficients for security and privacy concerns are positive with the willingness to use e-banking. It indicates that security and privacy has positive impact on the willingness to use e-banking. This finding is consistent with the findings of Wessels and Drennan (2010). Likewise, the beta coefficients for fear of identity theft are negative with the willingness to use e-banking. It indicates that fear of identity theft have negative impact on the willingness to use e-banking. This finding is consistent with the findings Gomes *et al.*, (2022). In addition, the beta coefficients for fear of identity fraud are negative with willingness to use e-banking. It indicates that fear of identity fraud has a negative impact on the willingness to use e-banking. This result is consistent with the findings of Rachel Kim (2009). Further, the beta coefficients for lack of trust are negatively related with the willingness to use e-banking. It indicates that lack of trust has a negative impact on the willingness to use e-banking. This finding is consistent with the findings of Chen and Barnes (2007). Moreover, the beta coefficient for ease of use are positive with the willingness to use e-banking which indicates that ease of use has positive impact on the willingness to use e-banking. This result is consistent with the findings of (Daniel, 1999).

4. Summary and conclusion

E-banking is a broad term that describes the various banking products and services requiring digital, internet, and mobile technology. E-banking applications, which include automated teller machines (ATM), telephone banking, mobile banking, digital television, debit and credit cards, internet banking, etc., have become one of the main battlefields of the banking industry. Internet banking (or E-banking) means any user with a personal computer and a browser can get connected to his bank's website to perform any of the virtual banking functions. Cyber security is the protection of internet-connected systems, including hardware, software, and data, from cyber-attacks.

This study attempts to examine the cyber security issues affecting the users' willingness to use e-banking in Nepalese commercial banks. The study is based on primary data with 124 observations.

The major conclusion of this study is that higher the security and concerns, ease of use higher would be the willingness to use e-banking. The result shows that security and privacy concerns and ease of use are positively correlated to the willingness to use e-banking. The study also shows that fear of identity fraud, fear of identity theft and lack of trust are negatively correlated to willingness to use e-banking. The study also concludes that the most influencing factor is ease of use followed by ease of use that explains the

willingness to use e-banking.

References

- Aboobucker, I., and Y. Bao, 2018. What obstruct customer acceptance of internet banking? Security and privacy, risk, trust and website usability and the role of moderators. *The Journal of High Technology Management Research* 29(1), 109-123.
- Adewale, A., A.S. Ibunni, J. Badejo, and T. Odu, 2014. Biometric enable e-banking in Nigeria management and customers' perspectives. *Journal of Information and Knowledge Management* 4(11), 23- 28.
- Aladwani, A. M., 2001. Online banking: A field study of drivers, development challenges, and expectations. *International Journal of Information Management* 21(3), 213-225.
- Atay, E., and S. Apak, 2013. An overview of GDP and internet banking relations in the European Union versus China. *Procedia-Social and Behavioral Sciences* 99(3), 36-45.
- Ataya, M. A. M., and M. A. Ali, 2019. Acceptance of website security on e-banking. A review. In *2019 IEEE 10th Control and System Graduate Research Colloquium* 2(3), 201-206
- Bashir, I., and C. Madhavaiah, 2014. Determinants of young consumers' intention to use internet banking services in India. *Vision* 18(3), 153-163.
- Benjamin, O.A., and B.S. Samson, 2011. Effect of perceived inequality and perceived job insecurity on fraudulent intent of bank employees in Nigeria. *Europe's Journal of Psychology* 7(1), 99-111.
- Chen, Y. H., and S. Barnes, 2007. Initial trust and online buyer behavior. *Industrial Management and Data Systems* 107(7), 21-36.
- Dangol, S., and S. Kautish, 2019. IT security related issues and challenges in electronic payment system in Nepal: A study from customer's perspective. *LBEF Research Journal of Science, Technology and Management* 1(2), 85-103.
- Davis, F. D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly* 13(3), 319-340.
- Dua, S., and A. Upadhyaya, 2022. A study on analyzing awareness towards demographics of the e-banking customers. *Effulgence-A Management Journal* 20(1)1-11.
- Eleyan, D. E. R. A. R., R. A. S. H. E. E. D. Yousef, and A. M. N. A. Eleyan, 2022. Assessment of cybersecurity awareness among e-banking in Palestine-empirical study from customer's perspective. *Journal of Theoretical and Applied Information Technology* 100(16), 1-11.
- Fatmawati, I., D.A. Zulfanti, N. Aini, and F. Tsani, 2023. Young customers'

- perception of Sharia financial services mobile-banking and behavioral intention consequences. In digitalization: *Opportunities and Challenges for Business* 2(22), 116-125.
- Gefen, D., and M. Keil, 1998. The impact of developer responsiveness on perceptions of usefulness and ease of use: An extension of the technology acceptance model. *ACM SIGMIS Database: The Database for Advances in Information Systems* 29(2), 35-49.
- Giri, S., and S. Shakya, 2020. High risk of cybercrime, threat, attack and future challenges in Nepal. *International Journal of Computer Sciences and Engineering* 8(2), 46-51.
- Gomes, L., A. Deshmukh, and N. Anute, 2022. Cyber security and internet banking: Issues and preventive measures. *Journal of Information Technology and Sciences* 8(2), 31-42.
- Huang, D. L., P. L. P. Rau, G. Salvendy, F. Gao, and J. Zhou, 2011. Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies* 69(12), 870-883.
- Jibril, A. B., M. A. Kwarteng, R. K. Botchway, J. Bode, and M. Chovancova, 2020. The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business and Management* 7(1), 1-23.
- Kassim, N. M., and T. Ramayah, 2015. Perceived risk factors influence on intention to continue using internet banking among Malaysians. *Global Business Review* 16(3), 393-414.
- Kassim, N. M., and A. K. M. A. Abdulla, 2006. The influence of attraction on internet banking: An extension to the trust-relationship commitment model. *International Journal of Bank Marketing* 24(6) 424-442.
- Khatri, J. R., and K. Upadhyaya, 2013. Internet banking in Nepal: Use and challenges. *Banking Journal* 3(2), 57-77.
- Lai, F., D. Li, and C. T. Hsieh, 2012. Fighting identity theft: The coping perspective. *Decision Support Systems* 52(2), 353-363.
- Lee, M. K., and E. Turban, 2001. A trust model for consumer internet shopping. *International Journal of Electronic Commerce* 6(1), 75-91.
- Moon, J. W., and Y. G. Kim, 2001. Extending the tam for a world-wide-web context. *Information and Management* 38(4), 217-230.
- Mwesigwa, R., and S. K. Nkundabanyanga, 2011. Consumer, attitude, trust, perceived risk and internet banking adoption in Uganda. *Journal of Business and Economics* 2(5), 405-416.
- Nguyen, L., T. Singh, and D. Nguyen, 2014. Effect of trust on customer intention to

- use electronic banking in Vietnam. *Journal of Business and Policy Research* 9(2), 19–41.
- Onu, F. U, C. V. Umeakuka, and S. E. Eneji, 2017. Computer based forecasting in managing risks associated with electronic banking in Nigeria. *Journal of Innovative Research and Advanced Studies* 4(3), 390-396.
- Pikkarainen, T., K. Pikkarainen, H. Karjaluoto, and S. Pahnla, 2004. Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet Research* 14(3), 224-235.
- Polasik, M., and T. Wisniewski, 2009. Empirical analysis of internet banking adoption in Poland. *International Journal of Bank Marketing* 27(1), 32-52.
- Poon, W. C., 2008. Users' adoption of e-banking services: The Malaysian perspective. *Journal of Business and Industrial Marketing* 23(1), 59-69.
- Purnamasari, E., A. A. Bakri, and E. C. Mayndarto, 2023. The impact of privacy, security, and trust on online transaction intentions. *International Journal of Economics and Management Research* 2(1), 215-222.
- Ramayah, T., and J. Ignatius, 2005. Impact of perceived usefulness, perceived ease of use and perceived enjoyment on intention to shop online. *ICFAI Journal of Systems Management* 3(3), 36-51.
- Reyns, B. W., 2013. Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency* 50(2), 216-238.
- Sathye, M., 1999. Adoption of internet banking by Australian consumers: An empirical investigation. *International Journal of Bank Marketing* 17(7), 324-334.
- Shah, K. K. (2015). Electronic banking: Its use and challenge in Nepal academic voices: *A Multidisciplinary Journal*, 5(15), 9-15.
- Sharma, H., 2011. Bankers' perspectives on e-banking. *Global Journal of Research in Management* 1(1), 71-85.
- Sohrabi, M., J. Y. M. Yee, and R. J. Nathan, 2013. Critical Success Factors for the Adoption of e-Banking in Malaysia. *International Arab of Journal E-Technology* 3(2), 76-82.
- Suh, B., and I. Han, 2002. Effect of trust on customer acceptance of internet banking. *Electronic Commerce Research and Applications* 1(3), 247-263.
- Twum, F., and K. Ahenkora, 2012. Internet banking security strategy: Securing customer trust. *Journal of Management and Strategy* 3(4), 78-83.
- Tyagi, S., 2019. Cybercrime overwhelming online banking: A project management approach's alternative. *PM World Journal* 8(5), 1-21.
- Vatanasombut, B., M. Igbaria, A. C. Stylianou, and W. Rodgers, 2008. Information systems continuance intention of web-based applications customers: The case

- of online banking. *Information and Management* 45(7), 419-428.
- Vrîncianu, M., and L. A. Popa, 2010. Considerations regarding the security and protection of e-banking services consumers' interests. *The Amfiteatru Economic Journal* 12(28), 388-403.
- Wang, V., H. Nnaji, and J. Jung, 2020. Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, 62(15), 1-39.
- Wessels, L., and J. Drennan, 2010. An investigation of consumer acceptance of m-banking. *International Journal of Bank Marketing* 28(7), 547-568.
- Willox, N. A. and T. Regan, 2002. Identity fraud: Providing a solution. *Journal of Economic Crime Management* 1(1), 1-15.