Our Heritage

ISSN: 0474-9030
Vol-68-Issue-1-January-2020

Customers Perception Of Mobile Banking Threat And Security Issues

Gayathri.S & Buvaneswari.PS.

#Research Scholar, Department of Commerce, University of Madras, Chennai, Tamil Nadu, India

# Assistant Professor, Department of Commerce, University of Madras, Chennai, Tamil Nadu, India

[1] s.gayathri918@gmail.com, +91 98841 17291

[2] cvcpsb@gmail.com, +91 94441 90128

Abstract

Mobile payment is an alternative for cash, check, or credit cards. These technologies have enabled a broad range of new functionalities, supporting various mobile financial services, such as bill payment, account transfers, person to person transfers, proximity payments at the point of sale, remote payments to purchase goods and services, location-based services, mobile marketing, ticketing, discounts, or coupons, etc. In spite of all the benefits, the adoption or usage of mobile banking is at a lower phase due to threats and security issues. Fear of hacking on Customer personal information acts as a hindrance in usage on mobile banking applications the banking must take initiative by educating customers regarding various kinds of threat and security issues. Thus this study aims to identify the threat which hampers the customer in using mobile banking application.

Keywords: security, threats, mobile banking

1. Introduction

The role of technology particularly in the banking sector in today’s cashless world has brought about a foremost change in the activities of the customers. It facilitates the customer to enjoy the service they require with a more flexible choice and increased efficiency and effectiveness of service providers (Pampallis&bond, 2000). Since the bank aims to move towards global standards, the provision of alternative delivery channels like biometric ATMs, contactless payments, low-cost bill payment systems, and mobile banking applications has become routine in banks. Customers are well versed in technologies and carry out their transactions through mobile banking applications. Mobile banking allows customers to eliminate the need to use cash (Pham &

Ho, 2015), offering convenience and speed (Teo, Tan, Ooi, Hew, & Yew, 2015), performance and transfer of secure information between devices, from single or individual transactions to environment with high volume of payments (Leong, Hew, Tan, & Ooi, 2013).

Mobile banking applications are enjoying tremendous growth in India (Merritt, 2011). Mobile banking improves the bank's service and improves customer relationships and satisfaction. Globally, millions of consumers are already using a wide array of mobile devices to conduct banking - and millions more are expected to go mobile in the coming months. But with that growth comes a whole new set of threats which has reduced the adoption and usage rate of mobile banking .the commonly known threats of mobile banking are mobile malware, third-party apps, unsecured Wi-Fi networks, risky consumer behavior, etc. The mobile malware mainly includes Trojans, rootkits and viruses. Many of mobile malware are variants of existing malware that affect computers and traditional online banking. Some common malware affecting mobile bank apps include Zitmo, Banker, Perkel/Hesperbot, Wrob, Bankum, ZertSecurity, DroidDream and Keyloggers(Webroot, 2014; Shih et al., 2008). Cybercriminals have been refining this malware to target mobile devices for accessing the bank accounts.

The other important threat in mobile banking applications is third party applications on mobile devices which could secretly tamper an existing banking app that is already in the mobile device and steal account information. There are many fake banking applications that claim to be official on the third-party app marketplace. Cybercriminals also often offer a downloadable update for the banking apps on third-party app websites. These fake apps or fake app updates contain mischievous codes to steal the users' account information (Huang, 2015). Banks are taking numerous initiatives to minimize the security risks of a mobile banking application, they suggest that the customers should download apps or update app only from their official sources or trusted app stores and need to install reputable mobile antivirus products to protect their mobile devices against malware attack. Effective antivirus should be selected such that the mobile antivirus products don't bring down the performance and erroneously blocking valid programs on mobile devices. It is also recommended to the customer that If they notice something suspicious with their mobile banking applications, they should contact immediately to their bank to block their account temporarily until the issue is solved. The adoption of security software along with good security

ISSN: 0474-9030
Vol-68-Issue-1-January-2020

behavior will substantially lower the security risk

2. Literature review

Author	Findings
Mei-Ling Yao *et al* (2018)	Explored on malware detection technology regarding mobile banking applications, and identified that the majority of Smartphone holders do not have any mobile security applications and are prone to malware threats.
Isis Chong *et al* (2018)	Focused on hackers and cyber security issues of a mobile banking application, and identified that the customers with a lack of security software installed in their mobile were facing the problem of hackers and security issues.
Mansi Bosmia (2017)	The different threats and vulnerabilities hindering the customers in using the mobile banking application were studied and was identified that the new solutions for specific threats are a vulnerability, which will increase trust boundaries of mobile banking transactions.
Jie Guo (2015)	explore the use of mobile devices to access electronic payment services and electronic banking, and identified that development of various security, trust and network algorithms based on software and physical tokens can be used in various payment scenarios.
Mihail Cocosila & Houda Trabesi (2016)	risk of mobile banking adoption was studied and identified that the malware and phishing is the common threat faced by the customer while carring out their transaction hrough mobile banking application

3. Scope of the study:

The study identifies various threats and security issues of mobile banking applications which act as a hindrance to the adoption of mobile banking applications. despite being tech-savvy banking customers are hesitant about adopting mobile banking applications due to these security and trust issues .thus the aim of this article is to focus on awareness of various threats affecting mobile banking applications and problems faced by the customer in the adoption of mobile banking application.

4. Research methodology

The study determines the threat and security issues of mobile banking application which hinders the customers in using the application .the study is empirical in nature as customers are chosen randomly to elicit information

Table 2 Research Methodology

Materials and method	Description
Research design	Survey
Study place	Chennai
Sample size	200
Sample technique	Convenience sampling
Data collection	Questionnaire
Measures and scale	Likert’s scale
Stastical tools	Frequency,ANOVA,Chi Square
Software used	SPSS,AMOS

5. OBJECTIVES OF THE STUDY:

* To explore the awareness of security and privacy issues in M- banking applications.

*To investigate the relationship between demographic variables and various threats of mobile Bankingapplication

6. Analysis And Interpretation

Table 3 Demographic Profiles Of The Respondents

Table 3
Profile Of The Respondents

Demographic Variable	Classification	Frequency N= 200	Percentage
Gender	Male	119	59.5
	Female	81	40.5
Age	21-30	190	95.0
	31-40	4	2.0
	41-50	4	2.0
	50 Above	2	1.0
Education	HSC	11	5.5
	UG	126	63.0
	PG	36	18.0
	Professional	27	13.5
Monthly Income	Below 20000	4	2.0
	21000- 30000	189	94.5
	31000-40000	6	3.0
	41000-50000	1	.5
	Above 50000	4	2.0

Source: Primary data

The above table also shows that the customers of the mobile banking app users were male of the age group of 21-30 with UG qualification. *Jaafar&, Zafar (2017).*also highlighted that the majority of mobile banking application users were male who was graduates employed in the age group 21-30. The study by *Hashita 2015* also supported our findings that the majority of the male respondents belonging to the age group of 21-30 were using mobile banking app services.

Table 4 AWARENESS LEVEL OF THE RESPONDENTS ON VARIOUS THREATS

Table 4 Awareness level of the respondents		
	Frequency	Percent
yes	123	61.5%
no	77	38.5%

Primary data

61.5%) of the customers have stated that they are aware of various threats and security issues of mobile banking application, whereas 38.5% of customers have stated that they are not aware of threats and security issues of mobile banking application .as banks are taking various initiatives to create awareness among the customers regarding the various threats and security issues of mobile banking application. banks must educate the customer regarding biometrics which enhances existing authentication, Transport Layer Security (TLS) protocol combined with a proposed trust negotiation method, which authenticates the client, the mobile device used in accessing the bank account information, and the server etc to eliminate the fraudulent practice *Fatima (2011), Elkhodr, Shahrestani and Kourouche (2012).*

Table 5 RESPONDENTS OPINION ON VARIOUS THREATS of MOBILE BANKI9NG

Table 5 Threats of mobile banking		
	Frequency	Percent
Malware	120	60.0
Privacy violation	28	14.0
Hardware or OS vulnerability	37	18.5
SMS vulnerability	15	7.5

Primary data

The frequency of the MBA threat is revealed in the above Table 5. The majority of the respondents have stated that they are affected by the MALWARE threat **wich** damages devices, steals data, and causes a mess. Viruses, Trojans, spyware, and ransomware are among the different kinds of malware. *Economic* Times of India 2019 highlighted that the malware steals the credentials and money from users' bank accounts around 30,000 in the first quarter of 2019, up from 18,500 in the previous quarter, with a growth of over 60 percent.

Table 6 Chi-square test for association between gender and education qualification of customers and various threats of Mobile Banking Application

		Malware	Privacy violation	Hardware or OS vulnerability	SMS vulnerability	Chi-Square	P-value
Gender	Male	71.4 57.5%	16.7 50.0%	22.0 64.9%	8.9 80.0%	4.306	.030
	Female	48.6 42.5%	11.3 50.0%	15.0 35.1%	6.1 20.0%		
AGE	21-30	114.0 97.5%	2.4 0.0%	2.4 2.5%	1.2 0.0%	39.476	.000
	31-40	26.6 89.3%	.6 10.7%	.6 0.0%	.3 0.0%		
	41-50	35.2 94.6%	.7 2.7%	.7 2.7%	.4 0.0%		
	50 Above	14.3 86.7%	.3 0.0%	.3 0.0%	.2 13.3%		
Education Qualification	HSC	1.5 10.7%	17.6 57.1%	5.0 14.3%	3.8 17.9%		.044
	UG	75.6 64.2%	6.6 5.0%	21.6 14.2%	16.2 16.7%		

	PG	2.0 2.7%	23.3 73.0%	6.7 21.6%	5.0 2.7%	17.335	
	Professional	.8 6.7%	9.5 40.0%	2.7 46.7%	2.0 6.7%		

Primary data

The table above reveals the association between the demographic and various threats of mobile banking applications. Male customers of age group between 21-30 with ug qualification reveals that malware is the threat they frequently overcome while using their mobile banking application which is followed by Privacy violation, Hardware or OS vulnerability, SMS vulnerability.according to the report of *economic times 2019* revealed that around 58.4 percent of all mobile banking customers affected by Asacub malware.according to the report of *economic times of India 2016 highlighted* threats such as malware, Privacy violation, Hardware or OS vulnerability, SMS vulnerability affects the customer by requesting upfront payment as an investment, This transferring of funds could lead to criminal misdemeanors.

Table 7 Mean and standard deviations of mobile banking application threat

Threats	Mean	Std. Deviation
Phishing	14.6650	3.48763
Malware	14.6500	3.62813
Hacking	11.2150	2.49799
Social-networking	19.0150	3.89366

The mean and standard deviation of the table reveals to us that malware threat affects customers frequently followed by phishing, social networking and hacking. Phishing involves installing 'malware' or 'spyware' that reads sensitive client information including client details, passwords and PINs at the point of contact on the channel. The fraudulent practice also is done through social networking site as customers view their bank accounts and perform transactions via the social network *SISA 2017*

Conclusion

The 'security and privacy' issues act as a major roadblock in the adoption of M-banking application services. These issues have brought down the usage.it has become important for banks to educate their customers regarding various threats and security issues of mobile banking application. The banks stated adopting security features of M-banking application portals which helps the bankers to make their online portals more secure by implanting the advanced security and privacy features in their online portals. Banks also started upgrading their online portal to 256-bit Secure Socket Layer from 128-bit Security Socket Layer And a Multi-Factor Authentication (MFA)is also adopted by few banks such that it strengthens security at login by using an additional form of authentication beyond the standard username and password. Despite all these efforts, it has become important for the bank to identify the most common threat and security issues hindering the customer. This study determines the threat and awareness level of the customer regarding various threats. it was identified that Malware is the most commonly known threat faced by customer while using the mobile banking application. Thus the bank must concentrate on these issues and educate the customer regarding the precaution, thus which will increase the customer base.

. Reference

- Alghazo, Jaafar & Kazimi, Zafar (2017). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. 1-6. 10.1109/ICETAS.2017.8277910.
- Economictimes.indiatimes.com/articleshow/55113849.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- Elkhodr, M., Shahrestani, S., and Kourouche, K. 2012. "A proposal to improve the security of mobile banking applications", In ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on (pp. 260-265). IEEE.
- Fatima, A. 2011. "E-banking security issues–Is there a solution in biometrics", in Journal of Internet Banking and Commerce, 16(2): 2011-08.
- https://www.sisainfosec.com/blogs/cyber-security-risks-social-media-banking/

- Huang, S. 2015. “The South Korean Fake Banking App Scam”, Retrieved on Feb 02, 2015, at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-thesouth-korean-fake-banking-app-scam.pdf

- Isis Chong, Aiping Xiong, 2018 Human Factors in the Privacy and Security of the Internet of Things https://doi.org/10.1177/1064804617750321

- Mei-Ling.Y.A.O. Chuang,M.C.Chun-Cheng,H.S.U: the kano model analysis of features of mobile bankingnapplications,comput secur, 78,336-346(2018)

- Shih, D. H., Lin, B., Chiang, H. S., and Shih, M. H. 2008. “Security aspects of mobile phone virus: a critical survey”, in Industrial Management & Data Systems, 108(4), 478-494.

- Singh, S., Srivastava, V., and Srivastava, R. K. 2010. “Customer acceptance of mobile banking: A conceptual framework”, in Sies journal of management, 7(1), 55-64. Webroot. 2014. “The risks & rewards of mobile banking apps”, Retrieved on Feb 22, 2015