Cybercrime – Factors Influencing the Adoption and Use of Electronic Financial Services in Tanzania

Violete Rwezaura
and
Tumsifu Elly
elly@udbs.udsm.ac.tz

Abstract

This study was conducted to determine cybercrime-factors influencing the adoption and use of electronic financial transactions in Tanzania. Specifically the study aimed at determining the cybercrime-factors influencing the adoption and use of online banking services, mobile money transfer and mobile banking services. The study followed a survey strategy whereby a semi structured questionnaire was used to collect data from 200 respondents in Dar es Salaam. Data analysis was carried out using descriptive and factor analyses. Findings show that personal information-security, online frauds and service reliability in that order of importance are the factors influencing the adoption and use of online banking services, additionally, mobile fraud and service security, personal information security and service reliability in that sequence of importance are the most important factors influencing the adoption and use of mobile money transfer while personal information security and online frauds, service reliability and mobile bank fraud and environmental crimes in that sequence of importance are important factors in the adoption and use of mobile banking services. From the findings, respondents ranked the factors differently for the various electronic payment services. The study concludes that cybercrime-factors influencing the adoption and use of electronic transactions are ranked differently based on a particular

electronic service in order. Thus, the weight attached to each factor differs depending on the type of the electronic service. It is recommended that services providers should assign appropriate weight for each factor based on the type of service offered be it, online banking services, mobile money transfer and/or mobile banking services in order to create a positive image to the customers.

Key words: *Online/ internet banking; Mobile money transfer (MMT); Mobile banking*

Introduction

The information revolutions coupled with strategic use of the internet, has exposed a number of relatively open societies to dangers of cybercrime (Smith, 2004). The expansion of internet is opening up many new opportunities for criminals to exploit online vulnerabilities and commit cybercrime acts (Sand, 2007). Most forms of crime now involves technology in some way, whether through the use of cell phones and text messages or more novel applications of technology to commit crimes that are not otherwise possible outside of digital devices (Holt, 2013) .According to Thomas & Loader (2000) cybercrime involves computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Holt (2013) defined cybercrime as crimes which the perpetrator uses special knowledge of cyberspace.

Electronic financial transactions(E-Finance) use electronic means to exchange information, to transfer signs, representations of value, and to execute transactions in commercial environment (Glaessner, Kellermann, & McNevin, 2002). Electronic finance uses four channels for derivery of financial services including internet, telephone, mobile and ATMs (Zekos,

2004). E-finance delivers services, namely e- fund transfer, e-data interchange, e-benefit transfers and e-trade confirmations (Kellermann, 2002).

According to Jaishankar, (2008), Cyber crime is most harmful in the banking and financial industries, where computers are used to send and receive funds and where thousands of business transactions are processed every day . This is due to the fact that, technology has been a business driver (Chavan, Aggarwal, Bajaj, & Agrawal, 2012) and has been facilitating delivery of banking services to masses by changing the way of functioning of financial institutions as they gain efficiency, outreach and spread.

The use of electronic means is widespread in both developed and developing countries. Such use of the modern technology has always overtake theories and knowledge that describe them (Elly, 2010). There is therefore knowledge gap on what really influence the adoption of such high-tech related services. Some studies have discussed about the adoption and use of online related services, for example, Riyadhi, Islam & Hoque, (2009) studied about the development of electronic financial services in developing countries, a study which did not look at how cybercrime influence their adoption and use.

Additionally, Kavishe and Elly, (2008) profiled the electronic payment methods in use in Tanzania and the user perceptions and use of the same. This study did not address the cybercrime factors influencing the adoption and use of e-financial transactions. Ondiege, (2010) studied on mobile banking in Africa, mobile telephone penetration and the opportunity they offer to serve the unbanked Africans but the study did not touched anything on cybercrime, while FITSP (2013) established the use , barriers and opportunities of mobile banking in Tanzania. There is still a knowledge gap on the cybercrime factors influeincing the adoption and use ofelectronic financial transactions in the Tanzania context.

Theoretical Bases

Routine activity theory

The routine activity theory, essentially, explains how crime occurs with the convergence of three elements which are motivated offender, suitable target and absence of capable guardianship. When these three elements converge in time and space, crime occurs. In other words, when the motivated offender comes in contact with the suitable target in the absence of a capable guardian that could potentially prevent the offender from committing crime, crime occurs (Cohen & Felson, 1979). In the context of e-based financial transactions the theory offers a lot in terms of the way users and service providers alike are exposed into various crime position.

Lifestyle Exposure Theory

Different lifestyles expose people to different situations and some lifestyles may bring people into more crime-prone situations in which people are exposed to higher risk of victimization. (Hindelang, et al., 1978). It is central to Hindelang's argument that people who have different demographic and socioeconomic characteristics, related to age, sex, marital status, family income, and race, may have different role expectations and structural constraints that affect lifestyle choices available to individuals, such as where they live, with whom they associate, or how they are entertained, which in turn expose individuals to different risks of victimization (Hindelang, et al., 1978). This risk propensity in the context of e-financial transactions tend to increase even as users of these services are of differing background in terms of education, knowledge and experience, internet and mobile which all add to how, when and where they use the services.

Application of Routine activity theory and Lifestyle Exposure Theory to the study

Alshalan (2006), applying routine activities theory to cybercrime, argues that people who use the Internet more often are more likely to be a suitable

target that might come across a motivated offender in the absence of guardianship in the cyberspace

Some online activities, such as downloading freeware programs or visiting file sharing web sites, create higher risk of victimization than other online activities such as checking emails or visiting online news channels. (Choi, 2008; Moitra, 2005; Yar, 2005, 2006). Hence, a better understanding of victimization in cyberspace requires knowledge of online lifestyles of individuals.

In that sense, both routine activity theory and lifestyle exposure theory are useful in understanding cybercrime victimization in a society in which people's everyday routine activities have dramatically changed with the advent of computer technologies and increased use of the Internet, (Alshalan, 2006; Grabosky, 2001; Yar, 2005).

Space transition theory

Space Transition Theory is an explanation about the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyberspace (Jaishankar 2008). It involves the movement of persons from one space to another (e.g., from physical space to cyberspace and vice versa). Space transition theory argues that, people behave differently when they move from one space to another.

Identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime; Criminal behavior of offenders in cyberspace is likely to be imported to physical space which, in physical space may be exported to cyberspace as well; Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape; Strangers are likely to unite together in cyberspace to commit crime in the physical space and associates of physical space are likely to unite to commit crime in cyberspace; Persons from closed society are

more likely to commit crimes in cyberspace than persons from open society; The conflict of Norms and Values of physical Space with the Norms and Values of cyberspace may lead to cyber crimes (Jaishankar, 2007).

Application of space transition theory

This theory will very much be applicable in investigating the issues of online financial fraud and computing environment crimes in online banking; Mobile financial fraud and mobile environment crimes in mobile money transfer; Mobile-banks financial fraud and banking/mobile environment crime in mobile banking.

Empirical Bases

Cybercrime on MMT, online banking and mobile banking

The number of mobile banking users continues to grow globally. In turn, organizations are adding new functionality to the mobile channel and seeing an increase in mobile transaction volume. According to Gartner, (2009), global mobile transaction volume and value is expected to have an average 42% annual growth between 2013 and 2016. As users continue to move more of their daily lives to their mobile device, it is only expected that cybercriminals will do the same and direct more attacks at this growing channel.(Juniper Research, 2013: Gartner, 2009)

According to Trendlabs (2012) vishing (phishing by phone) and smishing (phishing by SMS/text message) are two of the more common attacks we see today that exploit the mobile device. These phishing alternatives are becoming more popular by cybercriminals as witnessed by fraud as a service vendors in the underground readily offering services such as SMS blasting applications and SMS spoofing services designed to send short messages to potential victims and direct them to fraudulent phone numbers, this service offers the ability to conceal the cybercriminal's true phone number, replacing it with an alpha-numeric name.

As mobile vulnerabilities increase, so do opportunities for cybercrime,

and while not as prevalent as it is online, fraud will continue to intensify in the mobile channel through socially engineered attacks on users and mobile apps will increasingly be exploited as a means to launch phishing and Trojan attacks,(RSA , 2013 pg3)

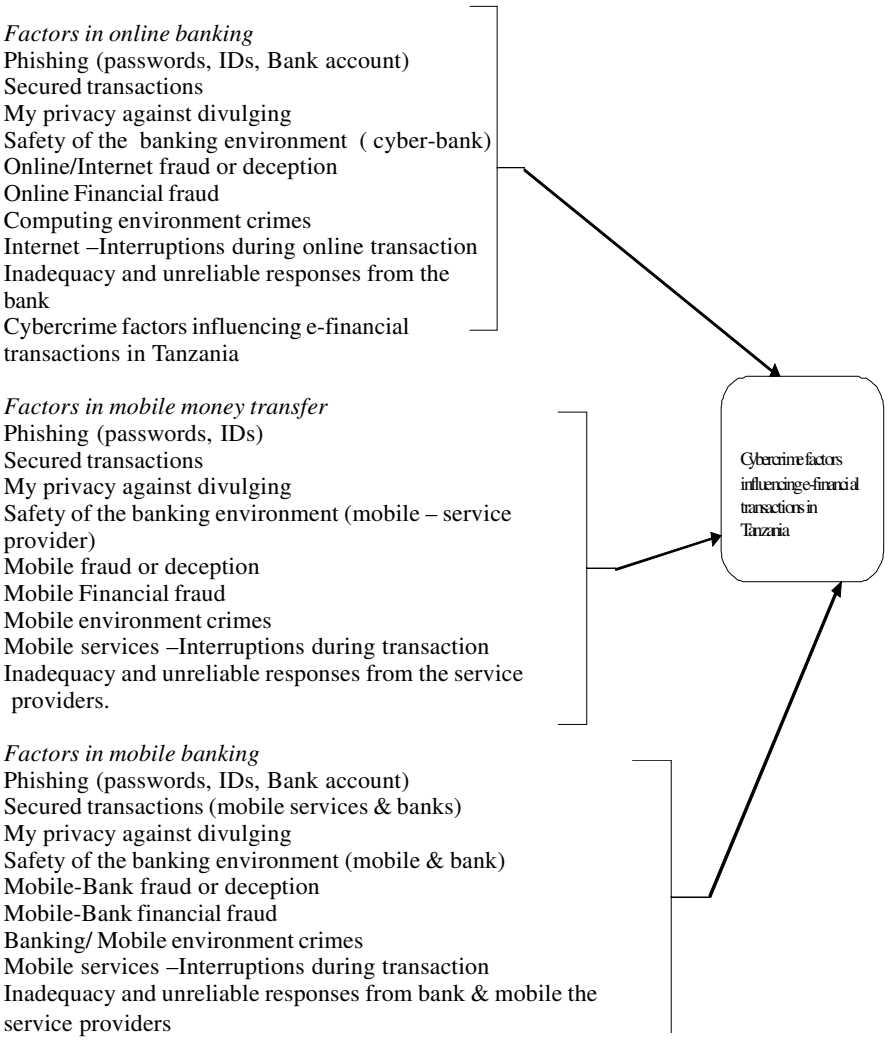
Arumuga perumal, (2006), FC-ISAC, (2012), Loucif Kharouni (2012), Chavan, Aggarwal, Bajaj & Agrawal, (2012), and (Cheng & Ma, 2009) talked about cybercrime on online/internet banking. According to Chavan, Aggarwal, Bajaj & Agrawal, (2012), the fast development of network communication has led to the expansion of Information technology which in turn led to the influence of access control system in IT sectors and banking sectors. In banking sector Information Technology has led to the improvement of customer services but on the other side it faces the major problem of network insecurity which to banks is a result of fraud.

Cheng & Ma, (2009) identified two types of bank fraud being internal and external fraud. Internal fraud is widely associated with internet bank theft as it involves the attempts to acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

To Arumuga perumal, (2006) the most dangerous fraud that causes in day to day banking activity is phishing, a criminal activity using social engineering techniques where by phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. According to Perumal, the more recent phishing attempts targets the customers of banks and online payment services.

FC-ISAC, 2012 did a research on current state cybercrime and found a new trend in which cyber criminal actors are using spam and phishing e-mails, keystroke loggers, and Remote Access Trojans (RAT) to compromise financial institution networks and obtain employee login credentials. The stolen credentials are used to initiate unauthorized wire transfers overseas.

Conceptual Framework



Methodology

A semi structured questionnaire was administered to 200 people who use online e-financial transactions in Dar es Salaam. Respondents were obtained through non probability sampling where by a convenience sampling technique was used. The respondent were thus picked conveniently as they were ready and had experience in e-transactions.

Data was analyzed following factor analysis where Kaiser-Meyer-Olkin (KMO) was used to measure the sampling adequacy of 200 respondents while Bartlett's test of Sphericity was used to identify statistical significance, at P< 0.005. The value of each eigenvalue was greater than 1 and all factors loading were above 0.5 statistical significance.

Findings

Distribution of respondents by age

Findings show that majority of the respondents (55%) had age falling between 18-30 years. Above 30 years were (31%) and below 18 years were (14%) as shown in table 1.1 below.

Table 1.1: *Distribution of Respondents by Age*

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	Under 18	28	14.0	14.0	14.0
	18 up to 30	110	55.0	55.0	69.0
	Above 30	62	31.0	31.0	100.0
	Total	200	100.0	100.0	

Source: *Field Data (2013)*

Distribution of the Respondents by their Occupation

Findings show that majority of the respondents (30%) were self employed, followed by those who were working or engaged in formal employment (26%) and 24% was unemployed. These can be found in table 1.2 below.

Table 1.2: *Distribution of Respondents by Occupation*

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	Working/Employed	52	26.0	26.0	26.0
	Studying	40	20.0	20.0	46.0
	Self employed	60	30.0	30.0	76.0
	Unemployed	48	24.0	24.0	100.0
	Total	200	100.0	100.0	

Source: *Field Data (2013)*

Distribution of Respondents by Gender

Findings shows that, gender distribution of the respondents was fairly equal as there were about 52% males and 48 % female as shown in Table 1.3.

Table 1.3: *Distribution of Respondents by Gender*

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	Male	97	48.5	48.5	48.5
	Female	103	51.5	51.5	100.0
	Total	200	100.0	100.0	

Source: *Field Data (2013)*

Respondents Distribution by Education

Majority of the respondents (36%) had secondary education. About (30%) had primary education, (23%) and (11%) had degree and certificates as being shown in the table 1.4 below.

Table 1.4: *Respondents Distribution by Education*

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	Secondary education	72	36.0	36.0	36.0
	Degree	46	23.0	23.0	59.0
	Certificate	22	11.0	11.0	70.0
	Others(Primary level)	60	30.0	30.0	100.0
	Total	200	100.0	100.0	

Source: *Field Data (2013)*

4.3 Prevalence of Cybercrime based on their Forms

The study aimed to establish the prevalence of cybercrime based on their forms. As shown in table1.1 below, cash transfer had the highest frequency (62%), followed by hacking "illegal intrusion in the computer system/ theft of information from computer system" (31%), phishing (19%) and intentional damage (4%). However, (73%) of respondents have not experienced intentional damage, while (57%) of respondents indicated that hacking was not prevalent and (40%) respondents have not encountered phishing.

Table1.1: *Forms/ means of Cybercrime and Frequencies of Occurrence*

Forms of cybercrime	*Highly prevalent (%)*	*Prevalent (%)*	*Not prevalent (%)*
Phishing (online trafficking of false identity information.)	19	41	40
Hacking (illegal intrusion and theft of data in the computer system)	31	11	57
Intentional damage (hired to damage by competing industries)	4	23	73
Cash transfer	62	34	4

Source: *Field Data (2013)*

Cybercrime factors influencing the adoption and use of online banking in Tanzania

Factor analysis was run to test the underlying factors that influence the adoption and use of online banking. The KMO value was 0.638 showing the data was adequate for factor analysis see table 1.2 below. Additionally, Bartlett's test of Sphericity was statistically significance at P< 0.000, thus the data was adequate.

Table 1.2: *KMO and Bartlett's Test*

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.638
Bartlett's Test of Sphericity	Approx. Chi-Square	582.111
	Df	36
	Sig.	.000

SSource: *Field Data*

After testing the adequacy of data, factor analysis was conducted using Maximum Likelihood and varimax rotation with Kaiser Normalisation.The value of each eigenvalue is greater than 1.0see table 1.3; the factor loadings after varimax rotation are greater than 0.5; The variance explained by all factors (66.6%) is greater than 40 percent. Thus extracted variance explained the factors influencing the adoption.

Table 1.3: *Total Variance Explained*

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.122	34.692	34.692	3.122	34.692	34.692	2.465	27.385	27.385
2	1.735	19.274	53.966	1.735	19.274	53.966	1.774	19.716	47.102
3	1.140	12.668	66.634	1.140	12.668	66.634	1.758	19.532	66.634
4	.935	10.384	77.018						
5	.670	7.450	84.468						
6	.465	5.166	89.633						
7	.393	4.369	94.003						
8	.305	3.386	97.389						
9	.235	2.611	100.000						

Extraction Method: Principal Component Analysis

As shown in table 1.3 above, three factors were extracted. These factors together explain about 67% of the total variance extracted. Rotated matrix table 1.4 shows these factors. The first group of variables is secured transaction (0.807), privacy against divulging (0.806), phishing-Personal Identity information confidentiality (0.741) as well as Safety of the banking environment (matching cyber&bank) (0.719). This group was labeled as "**personal information-security**" The group explains 27% variance extracted.

The second group of the factors consists of three variables namely online financial fraud (0.925), online /internet fraud or deception (0.683) and computing environment crimes (0.563) which tighter explain about 20% of the explained variance. The group could be labeled as "**online frauds**".

The third group consists of interruption of internet or transactions (0.848) and unreliable responses (0.811). These two variables could be named as "**service reliability**" together they explain about 20% of the variance explained. Therefore factors influencing the adoption and use of online

banking are personal information-security, online frauds and service reliability in that order of importance.

Table 1.4: *Rotated Component Matrix on the Adoption and Use of Online Banking*

Factors	*Component*		
	1	*2*	*3*
Secured transaction	.807		
My privacy against divulging	.806		
Phishing-Personal Identity information confidentiality(passwords, IDs, Bank account)	.741		
Safety of the banking environment (matching the two, Cyber-bank)	.719		
Online financial fraud		.925	
Online/ internet fraud or Deception		.683	
Computing environment crimes		.563	
Internet/ interruptions during online transactions			.848
Inadequacy and unreliable responses from the bank			.811

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
A Rotation converged in 5 iterations.

Cybercrime Factors Influencing the Adoption and Use of Mobile Money Transfer

The second objective was to find out cybercrime factors influencing the adoption and use of Mobile Money Transfer in Tanzania. Table 1.5 shows that, KMO test revealed a value of 0.615, while the Bartlett's test of Sphericity reached statistical significance at $p< 0.000$. These two parameters indicate satisfactory data requirement for factor analysis.

Table 1.5: *KMO and Bartlett's Test*

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.615
Bartlett's Test of Sphericity	Approx. Chi-Square	677.978
	Df	36
	Sig.	.000

Source: *Field Data (2013)*

Table 1.6: T*otal Variance Explained*

Component	*Initial Eigenvalues*			*Extraction Sums of Squared Loadings*			*Rotation Sums of Squared Loadings*		
	Total	*% of Variance*	*Cumula-tive %*	*Total*	*% of Variance*	*Cumula-tive %*	*Total*	*% of Variance*	*Cumula-tive %*
1	2.835	31.505	31.505	2.835	31.505	31.505	2.650	29.446	29.446
2	2.125	23.611	55.115	2.125	23.611	55.115	2.304	25.604	55.050
3	1.260	14.003	69.118	1.260	14.003	69.118	1.266	14.069	69.118
4	.928	10.311	79.429						
5	.620	6.888	86.317						
6	.442	4.909	91.226						
7	.367	4.075	95.302						
8	.242	2.685	97.986						
9	.181	2.014	100.000						

Extraction Method: Principal Component Analysis

As observed in table 1.6 above, three extracted factors explains about (69.119%) of total variance extracted. Table 1.7 below summarizes the rotated factor matrix the first group has four factors which are mobile fraud/ deception (0.876), Mobile financial fraud (0.836), Safety of service provider environment (0.738) and Mobile environment crimes (0. 627). This group could be labeled as **"mobile fraud and service security**" the group explains 29% variance extracted.

The second group of factors consist three variables; secured transactions (0.911), Mobile privacy against divulging (0.872), Phishing-Personal identity information confidentiality (0.811) which together explains about 26% of the variance extracted. This group can be labeled as **"concern about personal security of information**"

The third group consists of Mobile services-interruptions during transactions (0.756) and Inadequacy and unreliable responses from service providers (0.736). These two variables explains the variance of 14% and can be named **"service reliability**" therefore, factors influencing the adoption and use of mobile money transfer are **"mobile fraud and service security, personal information security**" and **service reliability in that sequence of their importance.**

Table1.7: *Rotated Factor Matrix on the Adoption and Use of Mobile Money Transfer*

	Component		
	1	*2*	*3*
Mobile fraud/ deception	.876		
Mobile financial fraud	.836		
Safety of service provider environment	.738		
Mobile environment crimes	.627		
Secured transactions		.911	
My privacy against divulging		.872	
Phishing-Personal identity information confidentiality		.811	
Mobile services-interruptions during transactions			.756
Inadequacy and unreliable responses from service providers			.736

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
A Rotation converged in 4 iterations.

Cybercrime Factors Influencing the Adoption and Use of Online Banking

KMO test revealed in this third objective had a value of 0.751, the Bartlett's test of Sphericity reached statistical significance (0.000) as summarized in table 1.8 the below.

Table 1.8: *KMO and Bartlett's Test*

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.751
Bartlett's Test of Sphericity	Approx. Chi-Square	652.631
	Df	36
	Sig.	.000

Source: *Field Data (2013)*

Table 1.8: *Total Variance Explained*

Component	*Initial Eigenvalues*			*Extraction Sums of Squared Loadings*			*Rotation Sums of Squared Loadings*		
	Total	*% of Variance*	*Cumulative %*	*Total*	*% of Variance*	*Cumulative %*	*Total*	*% of Variance*	*Cumulative %*
1	3.245	36.051	36.051	3.245	36.051	36.051	3.151	35.011	35.011
2	1.938	21.528	57.579	1.938	21.528	57.579	1.735	19.279	54.290
3	1.118	12.424	70.002	1.118	12.424	70.002	1.414	15.712	70.002
4	.751	8.340	78.342						
5	.638	7.090	85.433						
6	.416	4.624	90.056						
7	.371	4.117	94.174						
8	.306	3.399	97.573						
9	.218	2.427	100.000						

Extraction Method: Principal Component Analysis

The factors extracted together explain about 70% of total variance as it is well seen in table 1.8 above. Findings are being summarized in table 1.9 below. The first group of variables is, secured transactions (Between mobile services and banks) (0.893), privacy against divulging (0.844), phishing-

Personal Identity information confidentiality (passwords, IDs and Bank account) (0.839), Banking/Mobile environment crimes (0 .778) and Mobile service providers-banks fraud or deception (0 .569). This group could be named **"personal information security and online frauds"** and have extracted variance of more than 35%.

The second group of factors consists of two variables; Inadequacy and unreliable responses from the bank (0.893) and Mobile services / bank services – interruptions during transaction (0.869). These two factors contain the variance of 19% and can be called **"service reliability"**

The last group consists of Mobile –banks fraud (0.812) and Bank/ mobile environment crimes (0.720). These two variables explain the variance of 15% and can be named **mobile bank fraud and environmental crimes.**

Thus, factors influencing the adoption and use of mobile banking in Tanzania are **personal information security and online frauds, service reliability** and **mobile bank fraud and environmental crimes in that series of importance.**

Table 1.9: *Rotated Factor Matrix on the Adoption and Use of Online Banking*

	Component		
	1	*2*	*3*
Secured transactions (Between mobile services and banks)	.893		
My privacy against divulging	.844		
phishing-Personal Identity information confidentiality(passwords, IDs and Bank account)	.839		
Banking/Mobile environment crimes	.778		
Mobile service providers-banks fraud or deception.	.569		
Inadequacy and unreliable responses from the bank		.893	
Mobile services / bank services – interruptions during transaction		.869	
Mobile –banks fraud			.812
Bank/mobile environment crimes			.720

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
A Rotation converged in 5 iterations

Summary of the Findings

Factors influencing the adoption and use of online financial transactions in Tanzania *a are summarized in shown in table 1.10*

Table 1.10: *Summary of the Findings*

Ranking	*Online banking*	*Mobile money transfer*	*Mobile banking*
1	Personal information security	Mobile fraud and service security	Personal information security and online frauds.
2	Online frauds	Concern about personal security of information.	Service reliability
3	Service reliability	Service reliability	Mobile banking and environmental crimes

Source: *Field Data (2013)*

Conclusion

The conclusion on the objectives is drawn from the findings of the study which shows that, personal information-security, online frauds and service reliability in that order of importance, are the factors influencing the adoption and use of online banking services. Additionally, mobile fraud and service security, personal information security and service reliability in that sequence of their importance are the most important factors influencing the adoption and use of mobile money transfer (MMT). While personal information security and online frauds, service reliability and mobile bank fraud and environmental crimes in that sequence of importance are important in the adoption and use of mobile banking services. From the findings respondents ranked the factors differently for the various electronic payment services as summarised in the model figure 1.1 below.

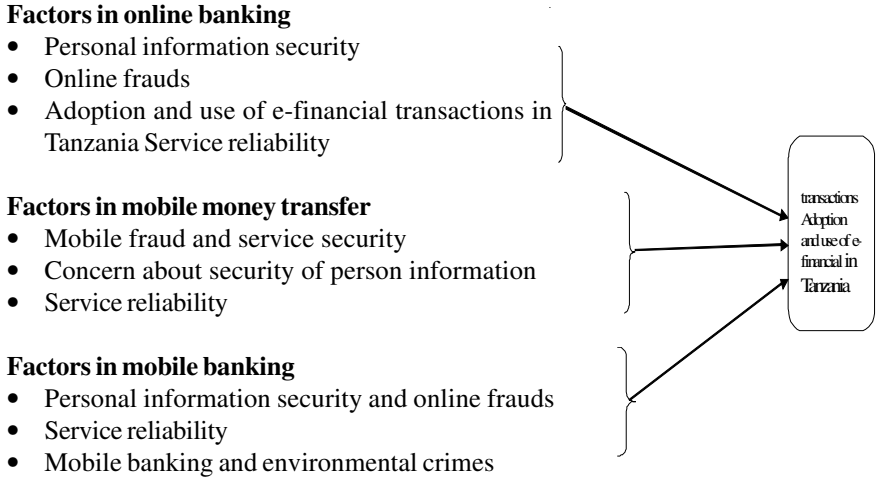


Fig. 1.1: *Modeling Cybercrime-factors Influencing the Adoption of Electronic Financial Transactions in Tanzania*

The study concludes that cybercrime factors influencing the adoption and use of electronic transactions are ranked differently based on a particular electronic service in order. Thus, the weight attached to each factor differs depending on the type of the electronic service. It is recommended that services providers should assign appropriate weight for each factor based on the type of service offered. in further studies, research should be done on the financial impact of the cybercrime to the users of e-financial transactions.

References

Bossler, A. M., & Holt, T. J. (2012). International Journal of Police strategies & management. *Patrol officers' perceived role in responding to cybercrime*.

Cheng, H., & Ma, L. (2009). white collar crime and criminal justice system;government response to bank fraud and corruption in China. *journal of financialcrime*.

Holt, T. J. (2013). *cybercrime and chriminological theory, fundamental reeding on hacking, pyracy,theft and harrassment.* Cognella Inc.

ICT policy. (2007). *Tanzania Information and communication technology ICT policy for basic education.*

MacConnel. (2000). *cybercrime and purnishment.*

Muthukumaran. (2008). *cybercrime scenario in India; criminal investigation departmentreview*.

Purkait, S. (2012). Information management and computer security. *Phishing counter measures and their effectiveness - literature review.*

Sain, H., Lao, Y. S., & Panda, T. C. (2012). *cyber-crimes and their impacts; A review*.

Wada, F., Longe, O., & Danquah, P. (2012). Journal of Internet Banking and Commerce. *Actions speaks louder than words-understandind cyber criminal behaviours using chriminological theories*.

Cohen, L.E. & Felson, M. (1979). Social Change and Crime Rsye Trends: A Routine Activite Approach. America Sociological Review, 44(4).588-608.

Hindelang, M.J., Gottfredson, M.R., & Garofalo, J. (1978). Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization. Cambridge , M,A: Balliger Publishing Company.

Choi, K.S., (2008) Computer Crime Victimization and Integrated theory: An Empirical Assessment. International Journal of Criminology, 2(1), 308-333.

Felson, M. (1998). Crime and everyday life (2nd Ed). Thousand Oaks, Clif: Pine Forge Press.

Goodman,M.D., & Brenner, S.W. (2002). The emerging Consensus on Criminal Conduct in Cyberspace. International Journalof Law and Information Technology.

Grabosky, P.N., & Smith, R. (2001). Telecommunication Fraud in the Digital age:The convergence of Technologies. In D.S. Wall(Ed.), Crime and the Internet . London and Newyork: Routledge, Taylor and Francis Group.

Alshalan, A. (2006). Cybercrime Fear and Victimization: An analysis of a National survey. Mississippi State University, Mississippi.

Saunders, M. et al (2009). Research Methods for Business Students, (5th Ed), Pearson Education Ltd.

Kothari, C.R (2009).Research Methodology Methods and Techniques, New Delhi.

Elly, T and Kavishe, V. (2008). The users Perception on electronic Payment Systems in Tanzania. Operations Research Society of Eastern Africa (RSEA).