Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2022 Proceedings | SIG GlobDev - Global Development

Aug 10th, 12:00 AM

Examining the Effect of Security Behavior on the Continuance Use of Mobile Money Services in Ghana: A protection Motivation Perspective

Adiata Borresa Seini
SD Dombo university of business and integrated development studies, adiataborresa@gmail.com

Ibrahim Osman Adam
University for Development Studies, ioadam@ubids.edugh

Muftawu Dzang Alhassan
SD Dombo University of Business and Integrated Development Studies, mdalhassan@ubids.edu.gh

LOUIS NOUTERAH
University of Business and Integrated Development Studies, louisnouterah@gmail.com

Follow this and additional works at: https://aisel.aisnet.org/amcis2022

Recommended Citation

Seini, Adiata Borresa; Adam, Ibrahim Osman; Alhassan, Muftawu Dzang; and NOUTERAH, LOUIS, "Examining the Effect of Security Behavior on the Continuance Use of Mobile Money Services in Ghana: A protection Motivation Perspective" (2022). *AMCIS 2022 Proceedings*. 4.
https://aisel.aisnet.org/amcis2022/sig_globdev/sig_globdev/4

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Examining the Effect of Security Behavior on the Continuance Use of Mobile Money Services in Ghana: A protection Motivation Perspective

Emergent Research Forum (ERF)

Adiata Borresa Seini
SD Dombo University of Business and Integrated Development Studies, Wa, Ghana
adiataborresa@gmail.com

Ibrahim Osman Adam
University for Development Studies, Tamale, Ghana
ioadam@uds.edu.gh

Muftawu Dzang Alhassan
SD Dombo University of Business and Integrated Development Studies, Wa, Ghana
mdalhassan@ubids.edu.gh

Louis Nouterah
SD Dombo University of Business and Integrated Development Studies, Wa, Ghana
louisnouterah@gmail.com

Abstract

Mobile Money Services are essential for dealing with transactions in today's digital economy. The use of mobile money services is an essential contributor to financial inclusion and economic development in developing countries. Unfortunately, the service has become a platform for fraud and other risky online activities. It is therefore imperative for users to rely on behaviors that protect their mobile money wallets in order to continuously use the service. However, there is no empirical evidence on this in the literature. This study therefore intends to investigate the effects of user security behaviors on the continuance use of mobile money services in Ghana. To do this, our study seeks to develop a conceptual model based on the protection motivation theory and validate it using survey data from mobile money users in Ghana and structural equation modelling. Findings from this study are intended to make major contributions to research, practice and policy.

Keywords

security behavior, continuance use, mobile money services, protection motivation.

Introduction

Mobile payment services are expanding owing to the increasing adoption and use of mobile devices among customers in both developed and developing nations (Baabdullah, Alalwan, Rana, Kizgin, & Patil, 2019; Narteh, Yeboah-Asiamah, & Mackin, 2022). This is because digitalization has increased inclusive innovations in dealing with transactions, especially with the unbanked (Chipere, 2018) who rely so much on mobile money (MoMo) services. The term MoMo (also referred to as mobile payment) defines a system

in which mobile terminals (such as mobile phones) are used to pay bills, commodities, and services (Dahlberg, Mallat, Ondrus, & Zmijewska, 2008).

The development of the mobile payment services industry, spearheaded by simple payment services, is recognized as the fastest expanding financial technology (FinTech) service sector in emerging nations (Kim, Choi, Park, & Yeon, 2016). Payment services, such as MoMo, Mobile Banking, and Internet banking, have helped to redefine the delivery of payment services in the financial services sectors in Ghana (Alhassan, Kolog, & Boateng, 2020). The use of MoMo continues to grow in Ghana. However, in recent years, this growth ecosystem faces key challenges such as the high prevalence of MoMo fraud, unsolicited electronic communications (UECs) to subscribers and the security of devices.

Despite these challenges, extant research has only examined the role of MoMo in promoting financial and digital inclusion (Ahmad, Green, & Jiang, 2020; Lashitew, van Tulder, & Liasse, 2019). There is lacking empirical evidence on how MoMo users engage in secure behaviors to protect their MoMo wallets in order to continuously use MoMo services. The existence of MoMo fraud activates the need for users to adopt behaviors that protects their MoMo funds from fraudsters in order to continuously use the service. An empirical analysis into these effects may enable MoMo service providers to formulate policies that will help protect users MoMo wallets from fraudulent activities. This study therefore aims to examine the effects of user security behavior on their continuance use of MoMo services in Ghana. To do this, the study relies on the Protection Motivation Theory as the theoretical lens and survey data from MoMo users in Ghana. Partial Least Squares – Structural Equation Modelling will be adopted to analyze survey data gathered., Our study therefore seeks to answer the following question:

RQ. What is the effect of security-related behavior on the continuance use of MoMo services in Ghana?

In the ensuing sections, the theoretical foundation of the study is presented. This is followed by the development of the hypotheses based on our research model. The methodology, the expected contribution and the conclusion follows respectively.

Theoretical Foundation

Protection Motivation Theory (PMT) is used to explain people's protective responses when they are presented with threats (Rogers, 1975, 1983). It is a general theory of motivation that explains individuals' actions in times of threats. The assumptions of PMT are that when confronted with a threat(s), he or she experiences two cognitive processes. These are: threat appraisal and coping appraisal. Threat appraisal involves a process of analysing (1) perceived threat vulnerability, and (2) perceived threat severity. Coping appraisal, on the other hand, involves evaluating (1) the efficacy of the potential adaptive responses to a threat (response efficacy); (2) the ability to successfully carry out the recommended responses (self-efficacy); and (3) the response costs associated with the engagement in an adaptive coping strategy.

PMT has been adapted and applied in different contexts. The PMT was developed to better investigate how people adopt health-protective behaviors (Prentice-Dunn & Rogers, 2001). However, it has now been applied to behaviours outside of a health context such as parenting (Campis, PrenticeDunn, & Lyman, 1989), tourism (Horng, Hu, Teng, & Lin, 2014), information security (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014), and disaster preparedness (Bubeck, Wouter Botzen, Laudan, Aerts, & Thieken, 2017). It has also been touted as an effective theory for understanding and promoting engagement in pro environmental behaviours (Cismaru et al., 2011; Nelson et al., 2011; Pronello & Gaborieau, 2018).

Information Systems research, for example, the PMT has been used to investigate information security behaviours (Hassandoust & Techatassanasoontorn, 2018; Yang et al., 2020). Studies in this area show how users engage in secure behaviours to protect their data and information from intruders (Duke Giwah, 2019). However, in order to accommodate a wide range of applications in the usage of PMT to handle a variety of difficulties, the theory has been expanded with other components to provide some perspectives and understanding of phenomena other than information security behavior (Aurigemma & Mattson, 2018; Ifinedo, 2012; Thompson, McGill, & Wang, 2017; Verkijika, 2018). In the context of Information Systems security research, PMT has been widely used in threat response studies. These previous studies influenced

our research on the use of MoMo services and the fear of breaching user information when using MoMo services and the motivation to continue using the services despite the threats. In this study, PMT is used as the theoretical lens for the conceptual model presented in Figure 1 below.

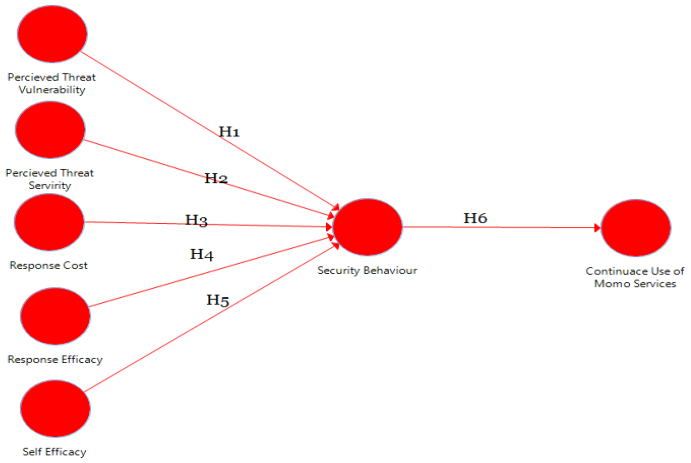

Figure 1: Research Model and Hypotheses

Hypotheses Development

Perceived threat Vulnerability and security behaviour

PMT suggests that threat vulnerability, also plays a significant role in the determination of protective security behavior and influences behavioral intent in a similar manner (Warkentin et al., 2016) Perceived threat is defined in this study as the likelihood that malicious threat will cause individuals to be concerned (Al-Sharafi et al., 2021) in other words the degree of harm caused by the unhealthy behaviour is referred to as perceived threat vulnerability. Given the context of ongoing protective security actions, we anticipate that as threat vulnerability perceptions increase, so will one's intent to continue engaging in protective security behaviours and continuance use mobile money services.

H_1: As perceived threat vulnerability increases, one's security behaviour to continue to engage in mobile money services also increases.

Perceived threat severity and security behaviour

According to PMT, a second threat dimension, threat severity is an important factor in determining the impact of security behavior, and it also influences behavioral intent. (Boss et al., 2015) Perceived threat severity also represent beliefs about the extent of harm that will be caused by a negative behavior (Gaube et al., 2019) Given the context of ongoing protective security actions, we anticipate that as threat severity perceptions increase, so will one's intent to continue engaging in protective security behaviours and continue to use mobile money services. This leads us to the hypothesis that:

H_2: As perceived threat severity increases, one's security behaviour to continue to engage in mobile money services also increases.

Response Cost and Security Behaviour

As the cost or effort required to perform the actions increases, so does one's security behaviour in continuing to use mobile money services. People are less likely to engage in the behaviour if they believe the costs of using mobile money services are prohibitively expensive (Fischer-Preßler et al., 2021). But the zeal to engage and continue to use the mobile money services increases response cost thereby also increasing mobile money services. We, therefore, hypothesise that:

H_3: As response cost increases, one's security behaviour to continue to engage in mobile money services also increases.

Response Efficacy and Security Behaviour

The belief that the adaptive response (i.e., the use of security checks) will be effective in protecting someone is referred to as perceived response efficacy (Boss et al. 2015). Response efficacy, according to PMT, influences protection motivation behaviour (Maddux and Rogers 1983; Rogers 1983). A protective behaviour attempts to provide an acceptable level of protection against threats. Thus, within the context of protection motivation, as one's perceptions of the efficacy of engaging in secure behaviour improve, so do the one's intent to continue engaging in secure behaviour (Warkentin et al., 2016) and may continue to use mobile money service. It is therefore hypothesized that:

H_4: As response efficacy increases, one's security behaviour to continue to engage in mobile money services also increases

Self-Efficacy and Security Behavior

Self-efficacy refers to people's belief in their ability to use protective measures to protect themselves (Boss et al. 2015). Self-efficacy of an individual's evaluation of his/her ability to cope and avert the potential loss or damage from the threat determines coping appraisal (Upadhyay et al., 2022) Individuals are more likely to engage in the behaviour if they are confident in their ability to carry out protective actions effectively and those actions are not difficult (Fischer-Preßler et al., 2021). Self-efficacy has been found to have a positive effect on IS retention in IS security behaviour (Warkentin et al., 2016). However, one's ability and behaviour towards the usage of mobile money services despite security breaches and the ability to continuously protect themselves show as self-efficacy increases, one's security behaviour to continue to engage in mobile money services also increases. It is therefore hypothesized that:

H_5: As self-efficacy increases, one's security behaviour to continue to engage in mobile money services also increases

Security Behavior and Continuance Use.

In technology adoption, security behaviour adoption has been theorized to influence actual usage behaviour (Lai, 2017). Security behaviour is a measure kept in place to protect one from threats involved in the use of mobile money services. In addition, there is a link between behavioural intention and actual behaviour (Warkentin et al., 2016). Consistent with the findings of an earlier study, continuation intention is found to be significantly related to security behaviour. As a result, we propose the following hypothesis:

H_6: As security behaviour increases, one's continuance use of mobile money services increases.

Proposed Research Methodology

The study will adopt a quantitative methodology. A survey instrument will be developed to collect data from MoMo users in Ghana. This is due to the wealth of available data in the country with high mobile payment usage and frequent fraudulent events to which users may have been exposed to.

Due to the disperse nature of respondents, a convenience sampling technique will be adopted to recruit respondents for the study. It is key to state that the intended target population for this study will be users of MoMo services in Ghana. Google forms will be relied on to administer the survey instrument to respondents.

There will be two parts to the survey instrument. Part 1 will collect information on respondents' demographic features, while Part 2 will include statements that will aid in the gathering information on threat and coping appraisals users adopt to secure their mobile money wallets to continuously use mobile

money services. The responses will be measured using Likert scales, which are effective in measuring research statements (Babbie, 1990; Churchill, 1979).

The study intends to adapt measurement items for previous studies (Kim et al., 2021). Measurement items for security behaviour will be adapted from (Malinga & Maiga, 2020) Items for threat and coping appraisal will be adapted from Liang and Xue (2010) and Tsai, Jiang, Alhabash, Larose, Rifon and Cotten (2016). Measurement items for the continuance use of mobile payment services will be drawn from Shao, Zhang and Guo (2019).

The data collected will be analyzed using Partial Least Squares – Structural Equation Modeling (PLS-SEM). PLS-SEM is a causal-predictive model that emphasizes prediction when estimating statistical models with structures that are intended to provide causal explanations (Hair, Risher, Sarstedt, & Ringle, 2019). The rationale for using the PLS-SEM approach stems from the fact that a single stage-based SEM approach can measure the linear relationships between the variables in the research model (Sim et al., 2014). Using the PLS-SEM approach, the study's sample size will be '10 times' the construct with the maximum number of measurement items (Hair, Ringle, & Sarstedt, 2011).

Expected Contribution

The findings of this study are expected to make several contributions to theory and practice in area of mobile payment services. This study is unique in that it intends to rely on the PMT to examine how MoMo users adopt threat and coping appraisals to engage in secure behaviors that protect their MoMo wallets from fraudsters in order to continuously use MoMo services. This will enable service providers to develop polices that will protect users MoMo wallets from fraudulent activities. Some of these polices may be targeted towards educating users on safe practices they should adopt in their use of MoMo services to protect their MoMo wallets from fraud.

Conclusion

In conclusion, this study will investigate the effects of security behavior on the continuance use of MoMo services in Ghana. A conceptual model will be developed based on the PMT and validated using data survey data from MoMo users in Ghana and PLS-SEM. It is intended that several interesting findings will emerge from the study. We aim to empirically confirm that the existence of MoMo fraud trigger users to evaluate their vulnerability to fraud attacks as well as the severity of fraud attacks to their MoMo wallets and financial information. This enables them to adopt secure that protects their MoMo wallets from fraudsters. Individuals' appraisal of fraud vulnerability and severity will also lead to their reliance on coping mechanisms that enable them to develop secure behaviors to continuously use MoMo services despite the existence of fraud.

REFERENCES

Ahmad, Green, and Jiang. 2020. "Mobile money, financial inclusion and development: A review with reference to African experience". *Journal of economic surveys*, (34:4), pp. 753-792.

Alhassan, Kolog, and Boateng. 2020. "Effect of gratification on user attitude and continuance use of mobile payment services: a developing country context". *Journal of Systems and Information Technology*.

Aurigemma, and Mattson. 2018. "Exploring the effect of uncertainty avoidance on taking voluntary protective security actions". Computers and Security, (73), pp. 219-234.

Baabdullah, Alalwan, Rana, Kizgin, and Patil. 2019. "Consumer use of mobile banking (M-Banking) in Saudi Arabia: Towards an integrated model". *International Journal of Information Management*, (44), pp. 38-52.

Chipere. 2018. "Virtual currency as an inclusive monetary innovation for the unbanked poor". *Electronic Commerce Research and Applications*, (28), pp. 37-43.

Dahlberg, Mallat, Ondrus, and Zmijewska. 2008. "Past, present and future of mobile payments research: A literature review". *Electronic Commerce Research and Applications*, (7:2), pp. 165-181.

Ifinedo. 2012. "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory". *Computers & Security*, (31:1), pp. 83-95.

Kim, Choi, Park, and Yeon. 2016. "The adoption of mobile payment services for Fintech". *International Journal of Applied Engineering Research,* (11:2), pp. 1058-1061.

Lashitew, van Tulder, and Liasse. 2019. "Mobile phones for financial inclusion: What explains the diffusion of mobile money innovations?" *Research Policy*, (48:5), pp. 1201-1215.

Narteh, Yeboah-Asiamah, and Mackin. 2022. "Analysis of young banked and unbanked customers' usage, satisfaction, trust and loyalty for mobile money services in Ghana". *International Journal of Business and Systems Research,* (16:1), pp. 40-64.

Odoom, and Kosiba. 2020. "Mobile money usage and continuance intention among micro enterprises in an emerging market–the mediating role of agent credibility". *Journal of Systems and Information Technology*.

Rogers. 1975. "A protection motivation theory of fear appeals and attitude change". *The journal of psychology*, (91:1), pp. 93-114.

Rogers. 1983. "Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation". *Social psychophysiology*: *A sourcebook*, pp. 153-176.

Thompson, McGill, and Wang. 2017. "Security begins at home: Determinants of home computer and mobile device security behavior". *Computers & Security*, (70), pp. 376-391.

Verkijika. 2018. "Understanding smartphone security behaviors: an extension of the protection motivation theory with anticipated regret". Computers & Security, (77), pp. 860-870.