INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

International Journal of Information and Decision Sciences

ISSN online: 1756-7025 - ISSN print: 1756-7017
https://www.inderscience.com/ijids

Cybersecurity antecedents of trust: toward OPS adoption in Jordan

Yazan Alshboul, Nareman Al.Hamouri

DOI: 10.1504/IJIDS.2023.10054769

Article History:

Received:	22 August 2020
Last revised:	03 December 2020
Accepted:	21 December 2020
Published online:	20 March 2023

Cybersecurity antecedents of trust: toward OPS adoption in Jordan

Yazan Alshboul* and Nareman Al.Hamouri

Department of Information Technology,
Yarmouk University,
P.O. Box 566, 21163, Irbid, Jordan
Email: Yazan.shboul@yu.edu.jo
Email: Naremanmazen92@gmail.com
*Corresponding author

Abstract: Online services such as online banking, particularly, the online payment system (OPS), plays an important role in modern life. In developing countries, there is a kind of resistance to adopting OPSs. Therefore, more focus is needed to understand the behaviour toward OPS, especially in developing countries. This paper integrates the trust model and the theory of planned behaviour and addresses the antecedents of the trust factor in the context of OPSs. Particularly, it focuses on the cybersecurity factors as antecedents to the trust model. We tested our model empirically using data gathered from 200 participants who use eFawateercom system, an online payment system used in Jordan. The results showed that cybersecurity factors like systems security, privacy, and reliability play an essential role in affecting users' trust, which has a crucial impact on the attitude toward OPS adoption. This article concluded with implications for academia and practitioners.

Keywords: online payment system; OPS; cybersecurity factors; trust; privacy; security; reliability.

Reference to this paper should be made as follows: Alshboul, Y. and Al.Hamouri, N. (2023) 'Cybersecurity antecedents of trust: toward OPS adoption in Jordan', *Int. J. Information and Decision Sciences*, Vol. 15, No. 1, pp.73–93.

Biographical notes: Yazan Alshboul is an Assistant Professor in Department of Information Technology and Coordinator of the Cybersecurity Program at Yarmouk University. He earned his PhD in Information Systems/Information Assurance and Security from Dakota State University in the USA. His research interest is in cybersecurity and data analysis.

Nareman Al.Hamouri has graduated from Yarmouk University in Management Information Systems – master program from Yarmouk University. She earned her Bachelor's in MIS from Yarmouk University. Her research interest is in technology acceptance.

1 Introduction

In the last decades, there is a rising diffusion of banking services through the internet (Laukkanen, 2007). There are different online banking services such as online payment

systems (OPSs), e-commerce services, e-shopping, and e-government. The proliferation of technology such as internet and mobile applications facilitates OPS usage, payment processing devices, and mobile payment (Baptista and Oliveira, 2015; Bezhovski, 2016; Aboobucker and Bao, 2018). As a consequence of the proliferation and development of ICT industry, business models have changed to meet this technology advancement including but not limited to internet and mobile banking services (Riffai et al., 2012; Martins et al., 2014; Baptista and Oliveira, 2015; Wang and Alshboul, 2015; Yang et al., 2015; Shaikh et al., 2017; Aboobucker and Bao, 2018). Internet banking is the using of information systems to deliver banking services to customers (Daniel, 1999). There is a strong association between internet and mobile banking services with the growth of banking industry (Sinha and Mukherjee, 2016).

OPS is one of the results of internet banking which refers to the process of performing different payments using internet and information systems (Yang et al., 2015; Shaikh et al., 2017). OPS play an essential role in the growth of e-commerce industry. It provides easy, cost effective, and less time-consuming ways to pay than the traditional payment processes (Daniel, 1999; Yang et al., 2015; Bezhovski, 2016). OPS has proven its ability to deliver secure, safe, confidential, and reliable services (Yang et al., 2015). It can provide 24/7 service availability and safe efforts and time for the customers (Shaikh et al., 2017; Aboobucker and Bao, 2018).

In fact, the future of the e-commerce industry, especially in developing countries, depends on the success of integrating e-business models and OPS. This integration depends on the security and effectiveness of OPS (Yang et al., 2015). The prosperity of e-commerce and OPS rely on people adoption of internet banking, particularly, using OPS to make payments.

The adoption and acceptance rate to OPS is still not satisfactory despite the proliferation of technology devices, such as PC, laptop, mobile, and tablets (Yiu et al., 2007; Akturan and Tezcan, 2012; Zhou, 2012, 2013; Malaquias and Hwang, 2016). Therefore, it is important to study the factors that influence consumers' behaviour toward OPS and the drivers that lead consumers to accept and pay online.

In the context of online shopping, internet banking, and e-commerce, different factors influence people adoption toward using these technologies, including but not limited to security, trust, perceived risks, perceived usefulness, and ease of use. Table 1 shows a summary of these factors and the corresponding articles.

There are some similarities between e-commerce, services, and OPS. Each of these domains is relying on the internet, software applications, and technology devices to complete the required task. Therefore, we assume that similar factors will also impact the behaviour of using OPS and internet banking in general.

Trust is one of the main factors that influence people behaviour when it comes to using internet banking (Hoffman and Lawson-Jenkins, 2006; Lai et al., 2011). There is a large body of research that addressed the importance of trust on OPS adoption (Kim and Benbasat, 2006; Yang et al., 2015; Rouibah et al., 2016; Salloum and Al-Emran, 2018). In this term, AlAdwani (2001) argued that trust and computer security are among the challenges of internet banking, including OPS. Zhou (2012) discussed the importance of building initial trust as a first step toward the adoption of internet banking. In the developing country context, trust also plays an essential role in OPS adoption (Malaquias and Hwang, 2016; Rouibah et al., 2016; Sharma et al., 2017).

Table 1 Some factors addressed in similar domains

Articles	*Addressed factors*	*Domain*
Dinev and Hart (2006)	Perceived privacy, trust	E-commerce
Featherman et al. (2006)	Perceived risk, ease of use	E-commerce
Bélanger and Carter (2008), Malaquias and Hwang (2016), Rouibah et al. (2016)	Trust, perceived risk	E-government, mobile payment, e-commerce
Lopez-Nicolas and Molina-Castillo (2008), Martins et al. (2014)	Perceived risk	E-commerce
Kim and Benbasat (2006), Wang et al. (2015), Cao et al. (2018)	Trust	E-commerce, mobile banking
Choshin and Ghaffari (2017)	Security, trust	E-commerce
Roy et al. (2017)	Perceived risk, perceived usefulness	Internet banking

Jordan, one of the developing countries in middle-east, has invested in an online payment system called eFawateercom (Madfooatcom, 2014). Despite the huge amount of investments in the internet banking industry in Jordan, the adoption of online banking services is still not satisfactory (Alalwan et al., 2018). Al-Rfou (2013) conducted a statistical study that shows a low rate of internet banking adoption. Only less than 19% of banks' customers in Jordan have accessed online banking services (Al-Rfou, 2013). Some users debated security issues as a reason not to use internet banking. Reluctance of users toward internet banking negatively impacts the growth of OPS and turns the investment in this industry to be pointless.

Accordingly, this paper focuses on the antecedents of trust toward using OPS in the developing country context. Particularly the cybersecurity antecedents, which includes systems security, privacy, and reliability. Another construct, social influence, is also considered in this study. Therefore, the main goal of this research is to understand what are the factors that affect individuals' trust to use OPS. We developed a behavioural model combining the theory of planned behaviour and the trust model to explain the relationship of the trust model and the intention to use OPS (Ajzen, 1991; Mayer et al., 1995; Pavlou, 2003; Lai et al., 2011). Furthermore, we study the effect of self-efficacy and perceived usefulness on the attitude to use OPS (Ajzen, 1991).

The proposed model is addressing the following research questions:

1 Does security and privacy factors affect users' trust?

2 Does the trust model have an influence on the OPS adoption?

The rest of this paper is organised as follows: Section 2 discusses the literature review related to this study. Section 3 explains the proposed research model. Sections 4 and 5 discussed the research methodology and results. Section 7 concludes the article.

2 Literature review

There are many studies that addressed the factors that are influencing the adoption and acceptance of internet banking and OPS. Ofori et al. (2017) relied on the institutional

trust theory to understand the factors that affect continuance intention towards internet banking. Using a questionnaire of 481 internet banking users in Ghana, they found that privacy and security concerns, information quality, and service quality have a significant impact on trust and satisfaction.

Yang et al. (2015) addressed the influence of the elements of perceived risk and trust on the behaviour of using OPS. They proposed a model based on theory of reasoned action (TRA), TPB, technology acceptance model (TAM), and DTPB. Their model was empirically tested using questionnaire data of 870 respondents from China. Their findings argued that building trust is an essential element toward the adoption of online banking (Yang et al., 2015).

Using the diffusion of innovation theory and the TAM, Estrella-Ramon et al. (2016) studied the impact of customers' offline transaction behaviour on the adoption of online banking. Particularly, they discussed the impact of loyalty and cross-buying behaviour on the adoption. They argued that the offline behavioural pattern is associated with the online adoption where customers of higher periodicity of interactions and convenience with bank services adopt the online banking faster (Estrella-Ramon et al., 2016). Yu et al. (2015) argued that trust is associated with internet banking and is affected by trustworthiness and its relative factors. They empirically demonstrated the significant impact of trusting beliefs of consistency, integrity, and shared values on trustworthiness (Yu et al., 2015).

Pavlou (2003) conducted a study that intended to understand the acceptance of e-commerce by consumers. His study applied the TAM, and the TRA to construct its model. Furthermore, the study suggested some drivers related to the process of conducting online transactions by consumers (Pavlou, 2003). The proposed model of Pavlou includes trust and perceived risk as they give some uncertainty for the e-commerce transactions. Their main construct was consumer intention to an online transaction. The model was tested using data from two empirical studies with a sample of 258 studies and online consumers. Their findings indicated that trust and perceived risk are direct antecedents for the intention to transact. They also found that ease of use and perceived usefulness have a considerable impact on the intentions of the transaction. Furthermore, trust has an indirect impact through perceived usefulness, perceived ease of use, and perceived risk (Pavlou, 2003).

Nguyen and Huynh (2018) investigated the impact of perceived risk and trust on the users' behaviour toward online payment systems. They tested their proposed model using 200 questioners, where the results confirmed the rule of perceived risk and trust on the adoption of OPS (Nguyen and Huynh, 2018). In the context of internet-based organisational systems, Lai et al. (2011) examined the factors of the trust model toward internet-based systems adoption in organisations. They investigated five factors, namely reliability and availability, usability, audit and verification mechanisms, and interoperability. However, their study unexpectedly found that security is an insignificant factor to trust concepts (Lai et al., 2011). Therefore, more investigations are needed to provide a better understanding of this issue.

Yousafzai et al. (2003) addressed the impact of the element of trust on perceived risk, which turns to influence the intention to use internet banking services. They proposed a conceptual model of trust in the context of internet banking services, where two antecedents of trust are discussed in their model: perceived security and perceived privacy (Yousafzai et al., 2003). However, this paper provides a coherent framework of the trust model with internet-banking without testing the proposed model empirically.

Perceived security and privacy were also discussed as antecedents to trust in the context of trusting websites (Flavián and Guinalíu, 2006). Casaló et al. (2007) addressed the trust model on online banking. They analysed perceived website security and privacy, usability, and reputation on consumer trust in the context of internet banking. Their analysis shows perceived security and privacy play a significant role in developing trust of online banking users (Casaló et al., 2007). However, their study focused on general internet banking and not specifically investigating their research phenomena in the context of online payment systems.

In the context of mobile payment within the restaurant industry, Khalilzadeh et al. (2017) extended the unified theory of acceptance and use of technology (UTAUT) and TAM and proposed a model that identify the drivers of using mobile banking technology (Khalilzadeh et al., 2017). Using a questionnaire of 412 restaurant customers, the analysis results demonstrated the significant role of risk, security, and trust on customers' behavioural intentions (Khalilzadeh et al., 2017).

Carter et al. (2011) investigated the impact of six factors on the intention of taxpayers toward adopting e-file systems. The suggested model combined UTAUT model with trust, security, and efficacy factors. The analysis of questionnaire data of 304 US taxpayers showed that three factors from the UTAUT model play a significant role in predicting taxpayers' e-filing intentions. Furthermore, the results also confirmed the significant impact of personal factors, web-specific self-efficacy, and perceived security control toward the intentional behaviour of using e-file systems (Carter et al., 2011).

In the context of the e-payment system in developing countries, Rouibah (2012) examined the causes and consequences of trust in OPS. Rouibah (2012) proposed a theoretical model including five variables: personal innovativeness, internet experience, familiarity, the presence of the third-party seal, and propensity to trust. He investigated how these variables influence consumer intention to use online payment through three mediation variables (perceived trust, perceived risk, and perceived enjoyment). The analysis of 350 participants of the study showed the notable role of the exogenous variables on the intention to use OPS through the mediation variables (Rouibah, 2012).

3 Research model and hypotheses

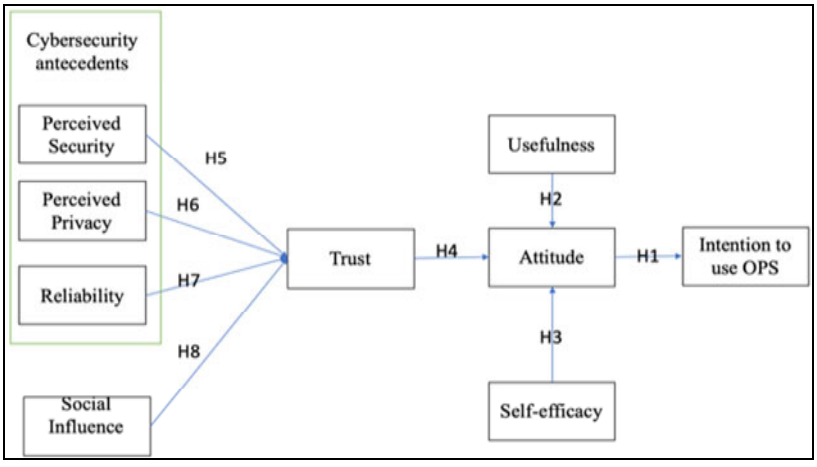
In this research, we build a research model based on the generic trust model (Mayer et al., 1995; Hoffman and Lawson-Jenkins, 2006; Costante et al., 2011; Wang et al., 2015; Yu et al., 2015), cybersecurity aspects (Casaló et al., 2007), and the theory of planned behaviour (Ajzen, 1991).

As the goal is to study the drivers of OPS adoption, the theory of planned behaviour explains how the attitudes toward OPS adoption influence users' intention to adopt the technology (Ajzen, 1991; Bulgurcu et al., 2010). In the context of internet banking, trust plays a significant role in changing users attitudes toward internet banking adoption, which leads to influence their adoption behaviour (Costante et al., 2011; Malaquias and Hwang, 2016; Rouibah et al., 2016; Abdul-Hamid et al., 2019). However, there is still a need to understand the drivers toward building trust in the internet banking context, particularly OPS.

The proposed model clarifies the interaction between the cybersecurity antecedents of trust, including perceived security and privacy, and reliability. Cybersecurity attacks and threats are deemed as one of the barriers to accept technology, especially those related to

financial services (Barney and Hansen, 1994; Mcallister, 1995; Flavián and Guinalíu, 2006; Kim et al., 2008; Alshboul and Streff, 2017) Furthermore, the model investigated the role of social influence on users trust toward using internet banking. Figure 1 shows the proposed research model.

Figure 1 Research model (see online version for colours)



3.1 Attitude relationship with intention to use OPS

According to The TRA and the theory of planned behaviour, there is an approved relationship between users' attitude and their intention to behave (Ajzen, 1991). There are many studies in different contexts that confirmed the significant relationship between the attitude toward the technology or services and the intention to use or adapt it. Such context includes information security policy compliance (Bulgurcu et al., 2010), internet banking adoption (Lee, 2009), mobile banking adoption (Akturan and Tezcan, 2012). Therefore, it is evident that attitude has a direct effect on the intention to behave, and we hypothesise that:

H1 Attitude toward OPS has a positive impact on the intention to use the OPS.

3.2 Usefulness and self-efficacy effect on attitude

Perceived usefulness is defined as the individual's perception of the benefits of using new technology, including the performance and productivity improvement (Davis, 1989). In the context of our study, perceived usefulness will improve the consumer's attitude toward OPS. According to Koenig-Lewis et al. (2010), perceived usefulness, compatibility, and risk are significant drivers of mobile banking adoption.

Self-efficacy is defined as the individual's beliefs about their ability and capabilities to do, perform, produce, and learn (Bandura, 1994). In the context of our study, self-efficacy is defined as the' individuals' beliefs in their ability to use online payment systems (Milne et al., 2000). Hsia et al. (2014) found that computer self-efficacy is one of the significant drivers in employees' e-learning systems in high-tech companies. We, therefore, propose the following hypotheses:

H2 Perceived usefulness of OPS users has a positive impact on the attitude toward OPS.

H3 Self-efficacy of OPS users has a positive impact on the attitude toward OPS.

3.3 Trust influence on individual's attitude

Trust is one of the main drivers influencing people behaviour toward using technology. It plays a significant role in encouraging the use of internet banking (Hoffman and Lawson-Jenkins, 2006; Lai et al., 2011). There is a large body of research that confirmed the essential role of trust on using OPS (Kim and Benbasat, 2006; Yang et al., 2015; Rouibah et al., 2016; Salloum and Al-Emran, 2018). Ofori et al. (2017) relied on the institutional trust theory to understand the factors that affect continuance intention towards internet banking. Their findings approved the strong relationship between trust and continuance intention to adopt internet banking (Ofori et al., 2017). AlAdwani (2001) argued that internet security and customer distrust are among the top ranked challenges of internet banking. Zhou (2012) discussed the importance of building initial trust as a first step toward the adoption of internet banking. He investigated the role of quality in building trust to use mobile banking (Zhou, 2012). In the developing country context, different studies approved trust role in encouraging OPS adoption (Malaquias and Hwang, 2016; Rouibah et al., 2016; Sharma et al., 2017). Based on the above argument, we hypothesise that:

H4 Users' trust in OPS has a positive impact on the attitude toward using OPS.

3.4 Cybersecurity antecedents of trust

With the proliferation of internet technologies in different industries, including the banking industry, cybersecurity threats are raised as barriers to using internet technology. Cybersecurity threats and attacks play in increasing role in minimising trust toward using advanced technology (Hoffman and Lawson-Jenkins, 2006). Some cybersecurity-related factors like reliability and availability, audit and verification mechanisms show a significant impact on the trust of using internet-based systems (Costante et al., 2011; Lai et al., 2011). Hoffman et al. proposed four facets of trust's antecedents, namely: security, usability, privacy, reliability (Hoffman and Lawson-Jenkins, 2006). Aleroud et al. (2020) confirmed the relationships between the risks of security and privacy on trust-related issues.

3.4.1 Perceived security

Perceived security refers to the user's subjective appraisal of the security level of an online payment system (Kathrin et al., 2006; Gao et al., 2017). In the context of this paper, perceived security refers to the degree to which people believe that their interaction with OPS is secure. Perceived security is one of the significant factors that influence users' trust in technology in general (Hoffman and Lawson-Jenkins, 2006; Aleroud et al., 2020), e-commerce (Pavlou, 2003), e-government (Lai et al., 2011), and e-banking (Khalilzadeh et al., 2017; Fan et al., 2018). Security is crucial in users' trusting that information systems will perform their intended and requested functions (Hoffman and Lawson-Jenkins, 2006). When users' perceived security is high, this leads to lower

the perceived risk of using information technology and increasing the level of trust (O'Reilly and Finnegan, 2005; Lai et al., 2011; Fan et al., 2018).

In a similar way, the user's perceived security plays an important role in increasing or decreasing users' trust toward OPS adoption. Based on the arguments above, we propose the following hypothesis:

H5 Perceived security of OPS has a positive impact on users' trust in OPS.

3.4.2 Perceived privacy

Perceived privacy refers to the degree to which users believe that their personal data will be protected and only authorised people can process and work with it (Casaló et al., 2007). It also indicates that personal data being processed within safety measures and data confidentiality assurance that includes legal grounds, anonymisation techniques, and good privacy practices (Hoffman and Lawson-Jenkins, 2006; Casaló et al., 2007). In this paper, we refer to perceived security as the degree to which people believe that their personal data protected from disclosure to the public and only authorised people can work with it during the interaction with the online payment systems.

The growing capacity of information systems, particularly, financial information systems like OPS, plus its complexity have made privacy as one of the important issues (Shin, 2010). How personal information is being gathered, stored, processed, and transferred in an online environment is becoming a major obstacle to the proliferation of online systems (Flavián and Guinalíu, 2006; Shin, 2010; Johnson et al., 2018; Aleroud et al., 2020). It is important for any online service provider to assure data privacy as it increases users trust (Bart et al., 2005). Based on the above arguments, we propose that:

H6 Perceived privacy of OPS has a positive impact on users' trust in OPS.

3.4.3 Reliability

Reliability is one of the cybersecurity attributes and refers to the capability of a system to perform consistently and precisely what it is expected to do (Hoffman and Lawson-Jenkins, 2006). Reliability is used to prevent and detect the error faults of systems and try to correct them (Lai et al., 2011). The reliability of the website is measured in terms of credibility and consistency of online service, which leads to customer loyalty. If a website is considered reliable, it instils trust in consumers and therefore motivates them to deal with a reliable vendor (Sahney et al., 2013). When an unexpected system error or failure occurs, it will negatively affect users' trust in the information systems. Therefore, we hypothesise that:

H7 Reliability of OPS has a positive impact on users' trust in OPS.

3.5 Social influence

Social influence refers to the influence of the social networks on the individual's thoughts, actions, and reactions (Lu et al., 2005). In sociology, social network effects have been used to explain and understand a variety of organisational behaviour phenomena (Krackhardt and Porter, 1985). Support from other influential has an important impact on individual decisions. Thus, an individual trust in new technology is

influenced by other trusted individuals (such as family and friends) who already using the same technology before (Ryan et al., 2011).

When an individual thinks that there are trusted people who believe that the adoption of new technology has positive results, he tends to adopt the same opinion and share the same convictions (Venkatesh et al., 2000). Other studies also refer to the important role of social influence on the decision to use online and mobile banking systems (Tan et al., 2014; Chaouali et al., 2016; Hwang et al., 2016). Therefore, we hypothesise that:

H8 Social influence of OPS has a positive impact on users' trust in OPS.

4 Data collection and research methodology

The data collection was conducted in Jordan, targeting adults who have one or more banking accounts in Jordan's banks that provide internet and mobile banking services, particularly through eFawateercom system. Questionnaire instruments were developed based on the literature and modified based on the study context. All the constructs of the model are reflective. Then it is translated into the Arabic language by a professional translator, since Arabic is the main language used in Jordan. To ensure the content validity of the survey, three IS assistant and associate professors have reviewed the questionnaire, then we considered their feedback. We also did a pilot study to make sure that the questions were appropriate; our pilot sample was MIS master students.

Two hundred twelve individuals participated in our study. Twelve copies were removed because they have missing data. Table A3 shows descriptive statistics of the collected data.

The sample includes about 41% men, and most of the participants' ages are less than 40. Most of the participants have higher education degrees and work in different industries with different income levels.

5 Data analysis and results

In order to evaluate the proposed hypotheses in the research model, we used structural equation modelling-partial least square (SEM-PLS). According to Hair et al. (2009, 2016), the process of evaluating this kind of research model using PLS includes two phases: measurement model and structural model evaluation.

5.1 Measurement model evaluation

The first step toward model assessment is to assess the quality of the research instruments used in the study (Hair et al., 2016). There are few tests to assess the quality of the measurement, including: internal consistency test or (composite reliability), convergent validity, and discriminant validity (Hair et al., 2016). To assess the internal consistency, we used the following tests: Cronbach's alpha, composite reliability, and Fornell-Larcker test. Table 2 presents the test results of Cronbach's alpha, composite reliability. Values of greater than 0.7 are considered satisfied and greater than 0.5 are accepted (Hair et al., 2009, 2016). The results show that most of the values are greater than 0.7, with only one

(self-efficacy – 0.576) is less than 0.7 but greater than 0.5. However, CR is greater than 0.7. So, the result is satisfactory and accepted.

Table 2 The result of composite reliability

Construct	*Cronbach's alpha*	*Composite reliability*	*AVE*
Attitude	0.804	0.884	0.719
Intention	0.879	0.925	0.805
Perceived privacy	0.765	0.850	0.587
perceived security	0.766	0.848	0.585
perceived usefulness	0.791	0.864	0.614
Reliability	0.794	0.866	0.619
Self-efficacy	*0.576*	0.781	0.553
Social influence	0.796	0.864	0.615
Trust	0.835	0.890	0.671

Table A3 in shows the results of Fornell-Larcker test. This test compares the square root of the AVE values with the construct correlations, which should be greater than the correlation with constructs (Hair et al., 2009, 2016). The results indicated that internal consistency is achieved.

We also assessed the convergent validity. Convergent validity assesses the degree to which the construct instruments correlate positively with the constructs by assessing the factor loadings (Hair et al., 2009, 2016). Factor loadings of values greater than 0.7 are considered satisfied, and values between 0.4 and 0.7 are considered accepted if the cross-loading with other constructs is low (Hair et al., 2009, 2016). Table A1 shows that most of the measurement instruments are loading highly to their constructs with values greater than 0.7. However, there are some instruments (SC1, SE3, SI2) less than 0.7, but they are greater than 0.5. Furthermore, Table A2 shows that their cross-loading values with other constructs are low. Therefore, we keep all the measurements values.

Finally, we also assessed the cross-loading. Constructs' instruments must have loading to their constructs higher than the loadings with other constructs (Hair et al., 2009, 2016). Table A2 shows that all the instruments passed the cross-loading test. Therefore, we did not remove any instruments and keep them in our analysis.

5.2 Structural model evaluation

The second phase in the process of model assessment is to assess the structural model. The structural model evaluation assesses the power of the model to predict the dependent variables and the significance of the relationships (hypotheses) in the model (Hair et al., 2009, 2016). There are three main tests toward structural model evaluation: hypotheses significant test, path coefficients, and the coefficient of determination (Hair et al., 2009, 2016).

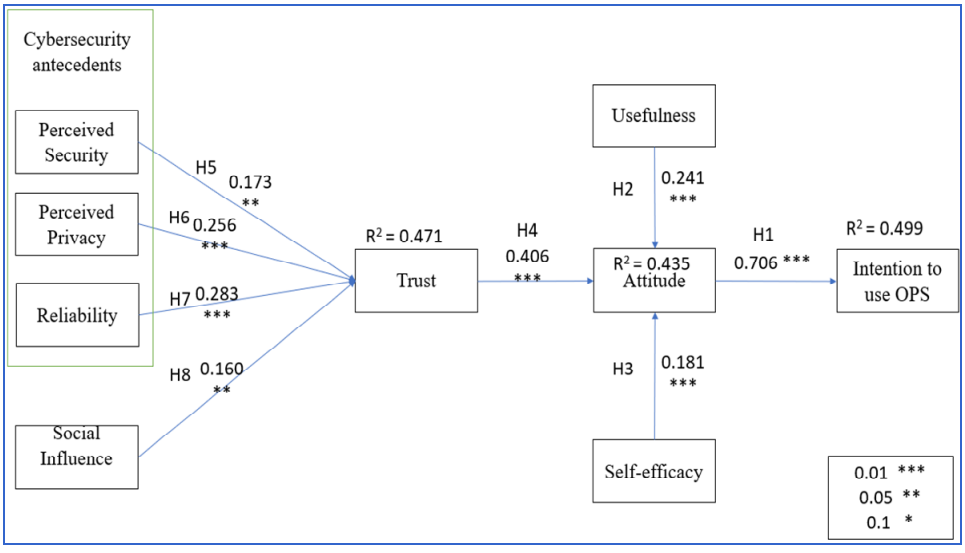
The hypotheses significant test examined the t-values computed by the bootstrapping method. T-values are examined at three significance values 0.1, 0.05, and 0.01, where t-values should be equal or greater than the critical value for each level, which is consecutively 1.65, 1.96, and 2.57. Usually, a t-value at significance level 0.05 is used where t-value should be 1.96 or greater to be considered satisfactory (Hair et al., 2009,

2016). In our analysis, all of the hypothesis' paths t-values are greater than 1. 96, which indicates that all hypotheses are supported at 0.05 level. Table 3 shows the t-test results.

Table 3 Path coefficients T-test

Hypothesis		*T-value*	*Decision*
H1	TRUST -> ATT	6.121	Supported
H2	PS -> TRUST	2.055	Supported
H3	PR -> TRUST	3.495	Supported
H4	SI -> TRUST	2.945	Supported
H5	RELI -> TRUST	3.622	Supported
H6	SE -> ATT	3.233	Supported
H7	PU -> ATT	3.748	Supported
H8	ATT -> INT	17.791	Supported

Figure 2 Analysis of research model (see online version for colours)



The second and third steps of structural model evaluation are to examine the path coefficients between constructs and the coefficient of determination (R^2). Path coefficients with high values indicate a strong association between constructs (Hair et al., 2016). R^2 refers to the amount of variance in the dependent variables, which is explained by independent (external) variables. According to Hair et al. (2016) R^2 values of 0.25, 0.5, and 0.75 respectively described as weak, moderate, and substantial. Figure 2 shows the analysis results of the proposed research model.

The results of the structural model assessment indicate that the survey data analysis is consistent with the proposed research model and confirms all the proposed hypotheses. Figure 2 confirms the arguments that cybersecurity-related constructs have a positive impact on trust toward using OPS in Jordan, particularly eFwateercom system. Perceived privacy and reliability have a greater influence on trust than perceived security with path coefficients of 0.256 and 0.283 consecutively at the significance level 0.01. Furthermore,

the trust construct has a very positive influence on attitude toward using eFwatercom system with greater impact than usefulness and self-efficacy. This result supports the argument that trust is an essential factor (maybe the most influential driver) when it comes to using an online payment system.

6 Discussion

Our theoretical model demonstrates the importance of cybersecurity factors on an individual's trust to explain online payment systems behaviour (Hoffman and Lawson-Jenkins, 2006; Lai et al., 2011). The theoretical model integrates the generic trust model and the theory of planned behaviour (Ajzen, 1991; Mayer et al., 1995; Costante et al., 2011).

6.1 Main findings

The research model explains 49.9% of the variation in the intention to use OPS. Our model revealed that cybersecurity factors have a crucial role in the acceptance of using OPS, where they have a significant impact on the trust factor, which is the most influential driver toward the individual's attitude to OPS adoption. This finding is consistent with Hoffman and Lawson-Jenkins (2006) argument about the significant role of cybersecurity-related factors on trust.

The result of the significant impact of reliability is consistent with the findings of Lai et al. (2011), where he examined the role of reliability of trust factor in the context of internet-based inter-organisational systems. However, unlike their finding that the security factor is an insignificant driver to trust factor (Lai et al., 2011), our study finds that perceived security is a significant driver to trust at the 0.05 significant levels with path coefficient (0.173) and t-value 2.05. One reason for that difference is the context, where their context was internet-based inter-organisational systems, and our context is the OPS, which is associated with financial systems. Gao et al. (2017) found that when people perceived higher security of the payment system, they are more likely to use it. Their result is consistent with our findings. Our finding also confirms the importance of security of mobile payment systems (Kathrin et al., 2006; Khalilzadeh et al., 2017; Fan et al., 2018).

Our study finds that protecting personal information privacy is a significant factor toward the trust of OPS. We find that perceived privacy has a significant impact on the trust factor with a t-value equal to 3.495 at significance level 0.01 and with a path coefficient (0.256). The result of this research model is consistent with the argument about the importance of privacy when it comes to trust in internet banking (Yousafzai et al., 2003; Bart et al., 2005; Flavián and Guinalíu, 2006; Casaló et al., 2007; Shin, 2010; Ofori et al., 2017; Johnson et al., 2018). Furthermore, the study supports the argument that the reliability of systems is an important driver to increase users' trust. Our results show that the reliability factor has a significant impact on trust factor with a t-value equal to 3.622 at significance level 0.01 and with a path coefficient (0.283). This result confirms the finding that reliability instils trust in consumers and therefore motivates them to deal with a reliable vendor (Sahney et al., 2013). The results show that perceived privacy and reliability has more impact on trust than perceived security.

Our study suggests that the high social influence of OPS can attain high users' trust in OPS. The result shows that the social influence-trust relationship is significant at the 0.05 level with a path coefficient equal to (0.160). Our result is consistent with the argument that an individual trust in new technology is influenced by other important people (such as family and friends) who already using the same technology before (Ryan et al., 2011).

Our study argues the significant influence of trust on people behaviour. The results show that the trust factor has a higher impact on the user's attitude toward using OPS than other factors like self-efficacy and usefulness. The importance of the trust factor, particularly, with OPS adoption, raises the attention to focus on trust when it comes to using related financial systems. This is consistent with the argument that building the initial trust is the first step toward the adoption of internet banking (Zhou, 2012).

6.2 Theoretical implication

This study proposed a theoretical framework that holds a new dimension by the integration between the generic trust model and the theory of planned behaviour (Ajzen, 1991; Costante et al., 2011). This theoretical framework contributes to supporting the empirical evidence about the significant impact of trust on internet banking, particularly, OPS adoption.

Furthermore, the proposed theoretical framework shed light about the importance of cybersecurity factors and their association with the trust factor, particularly, when dealing with online financial systems like OPS. From a theoretical perspective, our findings revealed that cybersecurity-related factors should be considered as the main drivers to change people behaviour, particularly when it comes to technologies over the internet.

Nowadays, cybersecurity threats and attacks threaten the adoption of using online technology (Hoffman and Lawson-Jenkins, 2006). The findings of our study revealed the significant role of cybersecurity-related factors on people trust to adopt OPS, particularly in the developing country environment. Therefore, more efforts are needed to understand how to develop the trust of OPS by focusing on the cybersecurity-related factors.

6.3 Practical implication

Our study provides online banking service providers with a deep understanding of the factors influencing the adoption of internet banking in general. Our findings lend themselves to several practical implications. First, since the findings revealed the significant role of cybersecurity-related factors on trust toward OPS adoption, there is a need to take all cybersecurity measures that prevent security attacks and mitigate security risks. Second, top management in the banking industry needs to pay more attention to its security policy as a first step to start a comprehensive cybersecurity program which helps to increase trust level.

Third, information officers at IT departments should be involved in the process of building trust by assuring to customers that all security controls are taken to protect the security of systems. They need to show that they are applying up to date technologies to protect systems and users' data. Fourth, top management needs to make sure that their security policy and controls are complying with security and privacy regulations, which help increasing the trust level. They need to ensure that they are following the latest security standards. Fifth, it is quite important to periodically review and assess the cybersecurity program and share it with customers. Furthermore, there is a need to create

cybersecurity awareness and training materials to educate OPS users about how to stay safe and secure while using the system. As revealed by our study, practitioners need to investigate the factors that may negatively impact trust level and work to mitigate their effects.

7 Conclusions

This study investigated people behaviour toward using online payment systems. The results of our study demonstrate the role of trust in using online banking services. The trust factor has a high impact on the attitude toward the adoption of online payment systems. Therefore, the proposed model addressed the antecedents of trust. The study examined the role of cybersecurity factors in influencing users' trust toward using internet banking, particularly the online payment system. The proposed model demonstrated the significant role of cybersecurity antecedents, including perceived security, perceived privacy, and reliability, on users' trust. Furthermore, the study integrates the trust model with the theory of planned behaviour.

References

Abdul-Hamid, I.K. et al. (2019) 'Customers' perceived risk and trust in using mobile money services-an empirical study of Ghana', *International Journal of e-Business Research*, Vol. 15, No. 1, pp.1–19, DOI: 10.4018/IJEBR.2019010101.

Aboobucker, I. and Bao, Y. (2018) 'What obstruct customer acceptance of internet banking? Security and privacy, risk, trust and website usability and the role of moderators', *Journal of High Technology Management Research*, Vol. 29, No. 1, pp.109–123, Elsevier, DOI: 10.1016/j.hitech.2018.04.010.

Ajzen, I. (1991) 'The theory of planned behavior', *Orgnizational Behavior and Human Decision Processes*, Vol. 50, pp.179–211.

Akturan, U. and Tezcan, N. (2012) 'Mobile banking adoption of the youth market: perceptions and intentions', *Marketing Intelligence and Planning*, Vol. 30, No. 4, pp.444–459, DOI: 10.1108/02634501211231928.

Aladwani, A.M. (2001) 'Online banking: a field study of drivers, development challenges, and expectations', *International Journal of Information Management*, Vol. 21, pp.213–225, DOI: 10.1086/209413.

Alalwan, A.A. et al. (2018) 'Examining factors influencing Jordanian customers' intentions and adoption of internet banking: extending UTAUT2 with risk', *Journal of Retailing and Consumer Services*, Vol. 40, pp.125–138, Elsevier Ltd., August 2017, DOI: 10.1016/j.jretconser.2017.08.026.

Aleroud, A. et al. (2020) 'An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities', *Journal of Information Security and Applications*, Vol. 55, p.102614, Elsevier Ltd., DOI: 10.1016/j.jisa.2020.102614.

Al-Rfou, A.N. (2013) 'The usage of internet banking evidence from Jordan', *Asian Economic and Financial Review*, Vol. 3, No. 5, pp.614–623.

Alshboul, Y. and Streff, K. (2017) 'Beyond cybersecurity awareness: antecedents and satisfaction', in *ACM International Conference Proceeding Series*, DOI: 10.1145/3178212.3178218.

Bandura, A. (1994) 'Self-efficacy', *Encyclopedia of Human Behavior*, Vol. 4, pp.71–81, Academic Press, New York.

Baptista, G. and Oliveira, T. (2015) 'Understanding mobile banking: the unified theory of acceptance and use of technology combined with cultural moderators', *Computers in Human Behavior*, Vol. 50, pp.418–430, DOI: 10.1016/j.chb.2015.04.024.

Barney, J.A.Y. and Hansen, M.H. (1994) 'Trustworthiness as a source of competitive advantage', *Strategic Management Journal*, Vol. 15, No. S1, pp.175–190.

Bart, Y. et al. (2005) 'Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study', *Journal of Marketing*, Vol. 69, No. 4, pp.133–152, DOI: 10.1509/jmkg.2005.69.4.133.

Bélanger, F. and Carter, L. (2008) 'Trust and risk in e-government adoption', *Journal of Strategic Information Systems*, Vol. 17, No. 2, pp.165–176, DOI: 10.1016/j.jsis.2007.12.002.

Bezhovski, Z. (2016) 'The future of the mobile payment as electronic payment system', *European Journal of Business and Management*, Vol. 8, No. 8, pp.127–132.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly*, Vol. 34, No. 3, pp.523–A7.

Cao, X., Yu, L., Liu, Z., Gong, M. and Adeel, L. (2018) 'Understanding mobile payment users' continuance intention: a trust transfer perspective', *Internet Research*, Vol. 28, No. 2.

Carter, L. et al. (2011) 'The role of security and trust in the adoption of online tax filing', in *Transforming Government: People, Process and Policy*, Vol. 5, No. 4, pp.303–318.

Casaló, L.V., Flavián, C. and Guinalíu, M. (2007) 'The role of security, privacy, usability and reputation in the development of online banking', *Online Information Review*, Vol. 31, No. 5, pp.583–603, DOI: 10.1108/14684520710832315.

Chaouali, W., Ben Yahia, I. and Souiden, N. (2016) 'The interplay of counter-conformity motivation, social influence, and trust in customers' intention to adopt internet banking services: the case of an emerging country', *Journal of Retailing and Consumer Services*, Vol. 28, pp.209–218, Elsevier, DOI: 10.1016/j.jretconser.2015.10.007.

Choshin, M. and Ghaffari, A. (2017) 'An investigation of the impact of effective factors on the success of e-commerce in small- and medium-sized companies', *Computers in Human Behavior*, Vol. 66, pp.67–74, Elsevier Ltd., DOI: 10.1016/j.chb.2016.09.026.

Costante, E., Den Hartog, J. and Petkovic, M. (2011) 'On-line trust perception: what really matters', *Proceedings – 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011*, pp.52–59, DOI: 10.1109/STAST.2011.6059256.

Daniel, E. (1999) 'Provision of electronic banking in the UK and the Republic of Ireland', *International Journal of Bank Marketing*, Vol. 17, No. 2, pp.72–83, DOI: 10.1108/02652329910258934.

Davis, F.D. (1989) 'Perceived ease of use, and user acceptance of information technology', *MIS Quarterly*, Vol. 13, No. 3, pp.319–340.

Dinev, T. and Hart, P. (2006) 'An extended privacy calculus transactions model for e-commerce transactions', *Information Systems Research*, Vol. 17, No. 1, pp.61–80, DOI: 10.1287/isre.l060.0080.

Estrella-Ramon, A., Sánchez-Pérez, M. and Swinnen, G. (2016) 'How customers' offline experience affects the adoption of online banking', *Internet Research*, Vol. 26, No. 5, pp.1072–1092, DOI: 10.1108/IntR-03-2015-0092.

Fan, J. et al. (2018) 'Understanding users' attitude toward mobile payment use: a comparative study between China and the USA', *Industrial Management and Data Systems*, Vol. 118, No. 3, pp.524–540, DOI: 10.1108/IMDS-06-2017-0268.

Featherman, M.S., Valacich, J.S. and Wells, J.D. (2006) 'Is that authentic or artificial? Understanding consumer perceptions of risk in e-service encounters', *Information Systems Journal*, Vol. 16, No. 2, pp.107–134, DOI: 10.1111/j.1365-2575.2006.00211.x.

Flavián, C. and Guinalíu, M. (2006) 'Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site', *Industrial Management & Data Systems*, Vol. 106, No. 5, pp.601–620, DOI: 10.1108/02635570610666403.

Gao, F., Rau, P.L.P. and Zhang, Y. (2017) 'Perceived mobile information security and adoption of mobile payment services in China', *International Journal of Mobile Human Computer Interaction*, Vol. 9, No. 1, pp.45–62, DOI: 10.4018/IJMHCI.2017010104.

Hair, J. et al. (2009) *Multivariate Data Analysis*, 7th ed., Prentice Hall.

Hair, J. et al. (2016) *A Primer on Partial Least Squares – Structural Equation Modeling (PLS-SEM)*, 2nd ed., April, SAGE Publications, Inc.

Hoffman, B.L.J. and Lawson-Jenkins, K. (2006) 'Trust beyond security: an expanded trust model', *Communication of the ACM*, Vol. 49, No. 7, pp.94–101.

Hsia, J.W., Chang, C.C. and Tseng, A.H. (2014) 'Effects of individuals' locus of control and computer self-efficacy on their e-learning acceptance in high-tech companies', *Behaviour and Information Technology*, Vol. 33, No. 1, pp.51–64, DOI: 10.1080/0144929X.2012.702284.

Hwang, Y., Al-Arabiat, M. and Shin, D.H. (2016) 'Understanding technology acceptance in a mandatory environment: a literature review', *Information Development*, Vol. 32, No. 4, pp.1266–1283, DOI: 10.1177/0266666915593621.

Johnson, V.L. et al. (2018) 'Limitations to the rapid adoption of M-payment services: understanding the impact of privacy risk on M-payment services', *Computers in Human Behavior*, Vol. 79, pp.111–122, Elsevier BV, DOI: 10.1016/j.chb.2017.10.035.

Kathrin, L., Pousttchi, K. and Wiedemann, D.G. (2006) 'Security issues in mobile payment from the customer viewpoint', in *Proceedings of the 14th European Conference on Information Systems (ECIS 2006)*, Göteborg, Schweden 2006, pp.S.1–11.

Khalilzadeh, J., Ozturk, A.B. and Bilgihan, A. (2017) 'Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry', *Computers in Human Behavior*, Vol. 70, pp.460–474, Elsevier Ltd., DOI: 10.1016/j.chb.2017.01.001.

Kim, D. and Benbasat, I. (2006) 'The effects of trust-assuring arguments on consumer trust in internet stores: application of Toulmin's model of argumentation', *Information Systems Research*, Vol. 17, No. 3, pp.286–300, DOI: 10.1287/isre.1060.0093.

Kim, D.J., Ferrin, D.L. and Rao, H.R. (2008) 'A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents', *Decision Support Systems*, Vol. 44, No. 2, pp.544–564, DOI: 10.1016/j.dss.2007.07.001.

Koenig-Lewis, N., Palmer, A. and Moll, A. (2010) 'Predicting young consumers' take up of mobile banking services', *International Journal of Bank Marketing*, Vol. 28, No. 5, pp.410–432, DOI: 10.1108/02652321011064917.

Krackhardt, D. and Porter, L. (1985) 'When friends leave: a structural analysis of the relationship between turnover and stayers' attitudes', *Administrative Science Quarterly*, June, Vol. 30, No. 2, pp.242–261.

Lai, I.K.W., Tong, V.W.L. and Lai, D.C.F. (2011) 'Trust factors influencing the adoption of internet-based interorganizational systems', *Electronic Commerce Research and Applications*, Vol. 10, No. 1, pp.85–93, Elsevier BV, DOI: 10.1016/j.elerap.2010.07.001.

Laukkanen, T. (2007) 'Internet vs mobile banking: comparing customer value perceptions', *Business Process Management Journal*, Vol. 13, No. 6, pp.788–797, DOI: 10.1108/14637150710834550.

Lee, M.C. (2009) 'Factors influencing the adoption of internet banking: an integration of TAM and TPB with perceived risk and perceived benefit', *Electronic Commerce Research and Applications*, Vol. 8, No. 3, pp.130–141, Elsevier BV, DOI: 10.1016/j.elerap.2008.11.006.

Lopez-Nicolas, C. and Molina-Castillo, F.J. (2008) 'Customer knowledge management and e-commerce: the role of customer perceived risk', *International Journal of Information Management*, Vol. 28, No. 2, pp.102–113, DOI: 10.1016/j.ijinfomgt.2007.09.001.

Lu, J., Yao, J.E. and Yu, C.S. (2005) 'Personal innovativeness, social influences and adoption of wireless internet services via mobile technology', *Journal of Strategic Information Systems*, Vol. 14, No. 3, pp.245–268, DOI: 10.1016/j.jsis.2005.07.003.

Madfooatcom (2014) *eFwatercom, Madfooatcom for Electronic Payments* [online] https://www.efawateercom.jo/Portal/About (accessed 27 February 2020).

Malaquias, R.F. and Hwang, Y. (2016) 'An empirical study on trust in mobile banking: a developing country perspective', *Computers in Human Behavior*, Vol. 54, pp.453–461, Elsevier Ltd., DOI: 10.1016/j.chb.2015.08.039.

Martins, C., Oliveira, T. and Popovič, A. (2014) 'Understanding the internet banking adoption: a unified theory of acceptance and use of technology and perceived risk application', *International Journal of Information Management*, Vol. 34, No. 1, pp.1–13, DOI: 10.1016/j.ijinfomgt.2013.06.002.

Mayer, R.C. et al. (1995) 'An integrative model of organizational trust', *The Academy of Management Review*, Vol. 20, No. 3, pp.709–734.

Mcallister, D.J. (1995) 'Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations', *The Academy of Management Journal*, Vol. 38, No. 1, pp.24–59.

Milne, S., Sheeran, P. and Orbell, S. (2000) 'Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory', *Journal of Applied Social Psychology*, Vol. 30, No. 1, pp.106–143, DOI: 10.1111/j.1559-1816.2000.tb02308.x.

Nguyen, T.D. and Huynh, P.A. (2018) 'The roles of perceived risk and trust on e–payment adoption', in *International Econometric Conference of Vietnam*, pp.397–420, DOI: 10.1007/978-3-319-73150-6.

O'Reilly, P. and Finnegan, P. (2005) 'Performance in electronic marketplaces: theory in practice', *Electronic Markets*, Vol. 15, No. 1, pp.23–37, DOI: 10.1080/10196780500035175.

Ofori, K.S. et al. (2017) 'Examining customers' continuance intentions towards internet banking usage', *Marketing Intelligence and Planning*, Vol. 35, No. 6, pp.756–773, DOI: 10.1108/MIP-11-2016-0214.

Pavlou, P.A. (2003) 'Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model', *International Journal of Electronic Commerce*, Vol. 7, No. 3, pp.101–134.

Riffai, M.M.M.A., Grant, K. and Edgar, D. (2012) 'Big TAM in Oman: exploring the promise of on-line banking, its adoption by customers and the challenges of banking in Oman', *International Journal of Information Management*, Vol. 32, No. 3, pp.239–250, Elsevier Ltd., DOI: 10.1016/j.ijinfomgt.2011.11.007.

Rouibah, K. (2012) 'Trust factors influencing intention to adopt online payment in Kuwait', in *Proceedings of the Southern Association for Information Systems Conference*, Atlanta, GA, USA.

Rouibah, K., Lowry, P.B. and Hwang, Y. (2016) 'The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: new perspectives from an Arab country', *Electronic Commerce Research and Applications*, Vol. 19, pp.33–43, DOI: 10.1016/j.elerap.2016.07.001.

Roy, S.K. et al. (2017) 'Predicting internet banking adoption in India: a perceived risk perspective', *Journal of Strategic Marketing*, Vol. 25, Nos. 5–6, pp.418–438, Routledge, DOI: 10.1080/0965254X.2016.1148771.

Ryan, R.M. et al. (2011) 'Motivation and autonomy in counseling, psychotherapy, and behavior change: a look at theory and practice 1ψ7', *The Counseling Psychologist*, Vol. 39, No. 2, pp.193–260, DOI: 10.1177/0011000009359313.

Sahney, S., Ghosh, K. and Shrivastava, A. (2013) 'Conceptualizing consumer 'trust' in online buying behaviour: an empirical inquiry and model development in Indian context', *Journal of Asia Business Studies*, Vol. 7, No. 3, pp.278–298, DOI: 10.1108/JABS-Jul-2011-0038.

Salloum, S.A. and Al-Emran, M. (2018) 'Factors affecting the adoption of e-payment systems by university students: extending the tam with trust', *International Journal of Electronic Business*, Vol. 14, No. 4, pp.371–389, DOI: 10.1504/ijeb.2018.10019536.

Shaikh, A.A., Hanafizadeh, P. and Karjaluoto, H. (2017) 'Mobile banking and payment system: a conceptual standpoint', *International Journal of e-Business Research*, Vol. 13, No. 2, pp.14–27, DOI: 10.4018/IJEBR.2017040102.

Sharma, S.K. et al. (2017) 'A multi-analytical model for mobile banking adoption: a developing country perspective', *Review of International Business and Strategy*, Vol. 27, No. 1, pp.133–148, DOI: 10.1108/RIBS-11-2016-0074.

Shin, D.H. (2010) 'The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption', *Interacting with Computers*, Vol. 22, No. 5, pp.428–438, Elsevier BV, DOI: 10.1016/j.intcom.2010.05.001.

Sinha, I. and Mukherjee, S. (2016) 'Acceptance of technology, related factors in use of off branch e-banking: an Indian case study', *Journal of High Technology Management Research*, Vol. 27, No. 1, pp.88–100, Elsevier BV, DOI: 10.1016/j.hitech.2016.04.008.

Tan, G.W.H. et al. (2014) 'Predicting the drivers of behavioral intention to use mobile learning: a hybrid SEM-neural networks approach', *Computers in Human Behavior*, Vol. 36, pp.198–213, Elsevier Ltd., DOI: 10.1016/j.chb.2014.03.052.

Venkatesh, V., Davis, F.D. and College, S.M.W. (2000) 'Theoretical acceptance extension model: four longitudinal field studies', *Management Science*, Vol. 46, No. 2, pp.186–204.

Wang, S.W., Ngamsiriudom, W. and Hsieh, C.H. (2015) 'Trust disposition, trust antecedents, trust, and behavioral intention', *Service Industries Journal*, Vol. 35, No. 10, pp.555–572, DOI: 10.1080/02642069.2015.1047827.

Wang, Y. and Alshboul, Y. (2015) 'Mobile security testing approaches and challenges', *2015 First Conference on Mobile and Secure Services (MOBISECSERV) IEEE*, pp.1–5, DOI: 10.1109/MOBISECSERV.2015.7072880.

Yang, Q. et al. (2015) 'Exploring consumer perceived risk and trust for online payments: an empirical study in China's younger generation', *Computers in Human Behavior*, Vol. 50, pp.9–24, Elsevier Ltd., DOI: 10.1016/j.chb.2015.03.058.

Yiu, C.S., Grant, K. and Edgar, D. (2007) 'Factors affecting the adoption of internet banking in Hong Kong-implications for the banking sector', *International Journal of Information Management*, Vol. 27, No. 5, pp.336–351, DOI: 10.1016/j.ijinfomgt.2007.03.002.

Yousafzai, S.Y., Pallister, J.G. and Foxall, G.R. (2003) 'A proposed model of e-trust for electronic banking', *Technovation*, Vol. 23, No. 11, pp.847–860, DOI: 10.1016/S0166-4972(03)00130-5.

Yu, P.L., Balaji, M.S. and Khong, K.W. (2015) 'Building trust in internet banking: a trustworthiness perspective', *Industrial Management and Data Systems*, Vol. 115, No. 2, pp.235–252, DOI: 10.1108/IMDS-09-2014-0262.

Zhou, T. (2012) 'Understanding users' initial trust in mobile banking: an elaboration likelihood perspective', *Computers in Human Behavior*, Vol. 28, No. 4, pp.1518–1525, Elsevier Ltd., DOI: 10.1016/j.chb.2012.03.021.

Zhou, T. (2013) 'An empirical examination of continuance intention of mobile payment services', *Decision Support Systems*, Vol. 54, No. 2, pp.1085–1091, Elsevier BV, DOI: 10.1016/j.dss.2012.10.034.

Appendix

Table A1 Factor loading

Construct	*Indicator*	*Factor loading*
Attitude (at)	AT1	0.762
	AT2	0.890
	AT3	0.886
Intention (in)	Int1	0.897
	Int2	0.908
	Int3	0.887
Perceived privacy (pr)	PR1	0.724
	PR2	0.791
	PR3	0.835
	PR4	0.706
Perceived usefulness (pu)	PU1	0.737
	PU2	0.797
	PU3	0.777
	PU4	0.822
Reliability (r)	RE1	0.732
	RE2.	0.847
	RE3	0.795
	RE4	0.767
Perceived security (sc)	Sec1	*0.623*
	Sec 2	0.775
	Sec 3	0.779
	Sec 4	0.862
Self-efficacy (se)	SE1	0.832
	SE 2	0.839
	SE 3	*0.513*
Social influence (sl)	SI1	0.754
	SI 2	*0.691*
	SI 3	0.880
	SI 4	0.799
Trust (tr)	Tr1	0.843
	Tr 2	0.823
	Tr 3	0.856
	Tr 4	0.749

Table A2 Cross-loading

	ATT	*INT*	*PR*	*PU*	*RELI*	*PS*	*SE*	*SI*	*TRUST*
at1	0.762	0.467	0.397	0.434	0.510	0.350	0.282	0.307	0.410
at2	0.890	0.636	0.383	0.390	0.500	0.491	0.303	0.443	0.528
at3	0.886	0.671	0.430	0.480	0.516	0.515	0.410	0.357	0.552
in1	0.637	0.897	0.382	0.377	0.503	0.451	0.404	0.458	0.496
in2	0.610	0.908	0.434	0.437	0.521	0.506	0.402	0.484	0.557
in3	0.653	0.887	0.531	0.538	0.564	0.565	0.381	0.477	0.573
pr1	0.393	0.362	0.724	0.332	0.390	0.370	0.258	0.213	0.368
pr2	0.340	0.425	0.791	0.367	0.354	0.445	0.349	0.287	0.402
pr3	0.387	0.433	0.835	0.370	0.310	0.487	0.279	0.299	0.486
pr4	0.335	0.304	0.706	0.461	0.258	0.446	0.225	0.187	0.345
pu1	0.373	0.332	0.406	0.737	0.343	0.385	0.280	0.332	0.386
pu2	0.375	0.356	0.349	0.797	0.377	0.380	0.253	0.289	0.435
pu3	0.366	0.418	0.367	0.777	0.303	0.361	0.216	0.204	0.397
pu4	0.474	0.460	0.420	0.822	0.453	0.463	0.278	0.359	0.414
r1	0.394	0.422	0.309	0.305	0.732	0.396	0.235	0.462	0.415
r2	0.513	0.511	0.369	0.421	0.847	0.485	0.356	0.427	0.476
r3	0.546	0.469	0.349	0.392	0.795	0.442	0.396	0.359	0.419
r4	0.426	0.453	0.312	0.376	0.767	0.427	0.416	0.451	0.492
sc1	0.293	0.220	0.356	0.257	0.272	0.623	0.254	0.256	0.282
sc2	0.382	0.378	0.361	0.453	0.409	0.775	0.347	0.358	0.376
sc3	0.394	0.487	0.369	0.341	0.481	0.779	0.311	0.363	0.402
sc4	0.532	0.562	0.601	0.475	0.500	0.862	0.410	0.461	0.567
se1	0.360	0.381	0.260	0.251	0.320	0.352	0.832	0.303	0.263
se2	0.280	0.303	0.372	0.246	0.357	0.340	0.839	0.263	0.224
se3	0.219	0.289	0.170	0.245	0.345	0.289	0.513	0.270	0.265
sl1	0.226	0.331	0.163	0.225	0.343	0.250	0.249	0.754	0.263
sl2	0.359	0.400	0.207	0.308	0.408	0.403	0.293	0.691	0.272
sl3	0.383	0.461	0.262	0.325	0.470	0.425	0.301	0.880	0.467
sl4	0.378	0.443	0.351	0.328	0.458	0.414	0.328	0.799	0.435
tr1	0.508	0.509	0.442	0.408	0.455	0.487	0.204	0.344	0.843
tr2	0.495	0.553	0.419	0.461	0.470	0.483	0.273	0.371	0.823
tr3	0.502	0.499	0.453	0.407	0.482	0.437	0.282	0.448	0.856
tr4	0.429	0.413	0.416	0.429	0.479	0.408	0.338	0.413	0.749

Table A3 'Descriptive statistics of participants'

	Categories	*Frequency*	*%*
Gender	Male	84	41.8
	Female	116	57.7
Age	18–30	114	56.7
	31–40	52	25.9
	41–50	25	12.4
	More than 50	9	4.5
Education	Secondary and less	17	8.5
	Diploma	27	13.4
	BA	119	59.2
	MA	28	13.9
	PhD	9	4.5
Industry type	Financial	26	12.9
	Educational	53	26.4
	Telecommunications	28	13.9
	Commercial	25	12.4
	Other	68	33.8
Income	More than 1000	27	13.4
	750–1,000	36	17.9
	749–501	39	19.4
	280–500	55	27.4
	Less than 250	43	21.4

Table A4 The result of Fornell-Larcker criterion

	ATT	*INT*	*PR*	*PS*	*PU*	*RELI*	*SE*	*SI*	*TRUST*
ATT	*0.848*								
INT	0.706	*0.897*							
PR	0.474	0.502	*0.766*						
PS	0.541	0.566	0.572	*0.765*					
PU	0.512	0.503	0.494	0.511	*0.784*				
RELI	0.597	0.591	0.426	0.557	0.477	*0.787*			
SE	0.396	0.441	0.363	0.441	0.329	0.449	*0.744*		
SI	0.437	0.527	0.327	0.484	0.382	0.541	0.374	*0.784*	
TRUST	0.591	0.604	0.528	0.555	0.520	0.576	0.333	0.481	*0.819*