







“Enhancing the public value of mobile fintech services through cybersecurity awareness antecedents: A novel framework in Jordan”

AUTHORS Hasan Alhanatleh 
Amineh Khaddam 
Farah Abudabaseh 
Mahmoud Alghizzawi 

Amro Alzghoul 


ARTICLE INFO Hasan Alhanatleh, Amineh Khaddam, Farah Abudabaseh, Mahmoud Alghizzawi and Amro Alzghoul (2024). Enhancing the public value of mobile fintech services through cybersecurity awareness antecedents: A novel framework in Jordan. *Investment Management and Financial Innovations*, 21(1), 417-430. doi:[10.21511/imfi.21\(1\).2024.32](https://doi.org/10.21511/imfi.21(1).2024.32)

DOI [http://dx.doi.org/10.21511/imfi.21\(1\).2024.32](http://dx.doi.org/10.21511/imfi.21(1).2024.32)

RELEASED ON Friday, 22 March 2024

RECEIVED ON Wednesday, 17 January 2024

ACCEPTED ON Tuesday, 12 March 2024


LICENSE This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

JOURNAL "Investment Management and Financial Innovations"

ISSN PRINT 1810-4967

ISSN ONLINE 1812-9358

PUBLISHER LLC “Consulting Publishing Company “Business Perspectives”

FOUNDER LLC “Consulting Publishing Company “Business Perspectives”


NUMBER OF REFERENCES

64


NUMBER OF FIGURES

2


NUMBER OF TABLES

3

© The author(s) 2024. This publication is an open access article.



BUSINESS PERSPECTIVES



LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine
www.businessperspectives.org

Received on: 17th of January, 2024

Accepted on: 12th of March, 2024

Published on: 22nd of March, 2024

© Hasan Alhanatleh, Amineh Khaddam, Farah Abudabaseh, Mahmoud Alghizzawi, Amro Alzghoul, 2024

Hasan Alhanatleh, Ph.D, Assistant Professor, Business Faculty, Amman Arab University, Jordan.

Amineh Khaddam, Ph.D, Associate Professor, Business Faculty, Amman Arab University, Jordan.

Farah Abudabaseh, Master, Lecturer, King Abdullah II School of Engineering, Princess Sumaya University for Technology, Jordan.

Mahmoud Alghizzawi, Ph.D, Assistant Professor, Business Faculty, Applied Science Private University, Jordan.

Amro Alzghoul, Ph.D., Assistant Professor, Business Faculty, Amman Arab University, Jordan. (Corresponding author)



This is an Open Access article, distributed under the terms of the [Creative Commons Attribution 4.0 International license](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

Conflict of interest statement:

Author(s) reported no conflict of interest

Hasan Alhanatleh (Jordan), Amineh Khaddam (Jordan), Farah Abudabaseh (Jordan), Mahmoud Alghizzawi (Jordan), Amro Alzghoul (Jordan)

ENHANCING THE PUBLIC VALUE OF MOBILE FINTECH SERVICES THROUGH CYBERSECURITY AWARENESS ANTECEDENTS: A NOVEL FRAMEWORK IN JORDAN

Abstract

The study aimed to link cybersecurity awareness and its antecedents to discover the level of public value of using mobile financial services from the perspective of 'citizens in the government context in Jordan. The quantitative approach was customized to serve the purposes of this study. A convenience sampling method was used based on 550 e-survey Jordanians from whom data were collected. A total of 449 responses were used in the analysis process. A structural equation model was specified to evaluate the developed research model. The results revealed that all hypotheses are accepted at less than $P < 0.001$, cybersecurity awareness and predictions of financial services systems play a significant role in determining the use of financial services systems and generating the value of using financial services. Moreover, combining cybersecurity awareness with public value theory is an important approach to measure the performance of government institutions, especially in the financial services industry. Therefore, these results can be used to develop financial services and meet Jordanians' requirements. Therefore, providing well-understood dimensions that influence the value of microfinance service use among Jordanians is a necessary process that probably ensures long-term sustainability of microfinance services. Finally, future efforts can explore the benefits and challenges of adopting digital transformation technologies in the public sector and financial services. Furthermore, the term government resilience is likely provided new insights to enhance public administration performance based on technology trends. Digital transformation, integrating government flexibility with the existing research model may influence the overall value of Mobile Fintech Services in Jordan.

Keywords

fintech, cybersecurity awareness, Public Value Theory, mobile fintech services, public institutions, social media, intention to use, government

JEL Classification

G23, O33, L86, M15

INTRODUCTION

As modernized technology, mobile apps have become an essential platform worldwide. Smartphones and their apps have been utilized in various settings such as government services, agency offices, learning, and amusement. The revolutions of technology and the coronavirus have changed the shape of services presented by public institutions and the private sector, where programming companies have increased their production of mobile apps. The organization's performance in employing smartphone technology has noticeably witnessed a high growth indicator in recent years (Halim et al., 2023). The digital platforms, tablets, and smart devices have compelled users to accomplish their daily sensitive and considerable activities, putting them easily attacked from several

internal and external sources. However, the resources of attack can be classified into several types: technical or user misuse of mobile technology (Alqahtani, 2022). Through this, users will be exposed to earnest risks such as accessing personal information easily and misappropriating secure data.

Recently, threats to cybersecurity have been considered a critical issue that plays a significant role in the continued use of technology (Ulven & Wangen, 2021). However, awareness regarding cyber security crimes is supposed to have a capacity for increasing the use of emerging digital technologies. If the users have sufficient information about several types of cybersecurity and how to secure their smartphones, they will increase their awareness of using specific technology. However, determining the degree of users' awareness is influenced by multiple determinants (Aljeaid et al., 2020). In the last period of time, the public administration of Jordan has provided additional financial services through the application of fintech platforms to present financial services depending on mobile app technology for citizens of Jordan. Measuring the performance of public institutions' services using mobile apps has become a contemporary setting that globally earns the attention of scholars, academics, and specialists (Twizeyimana & Andersson, 2019). There is an appeal in the literature review for reinforcing the performance of public institutions' services through applying several approaches and theories like public value theory (Alhanatleh et al., 2022). However, connecting the antecedents of cybersecurity awareness and the public value of MFS usage based on citizens' experiences in Jordan may provide new insights to measure the degree of MFS use and the performance of public institutions using MFS. Based on the above, this study seeks to contribute to financial services contexts, to bridge the public value gap for financial services and mobile government. The study highlights the importance of linking cybersecurity awareness to MFS and its predecessors in terms of using MFS to estimate and enhance the performance of government institutions in Jordan. The combination of cybersecurity awareness, the use of MFS terminology and the theory of public value and its dimensions is considered a new theoretical and practical base for all partners working with MFS in the sector government in Jordan.

1. LITERATURE REVIEW

The public value theory was first introduced by Moore and Moore (1995) to generate value for residents. As an emergent framework regarding public administration services, public value theory has been introduced for diverse purposes. First, Alford and O'flynn (2009) indicate that public value is a manner for assessing and administering government services for its partners. According to several models, government activity should switch from being reactive to being collaborative and consultative, with citizens being considered equal contributors (Stoker, 2006). In terms of m-government, Perera et al. (2017) have claimed that m-government aims to empower the mobile technology forces to allow citizens to perform their practices based on mobile apps of government services. However, there have been several arguments for identifying the attributes of public value. Kelly et al. (2002) have argued that improving the features of outcome, trust, and services is the basic line to public administration for generating

the value of government services. Additional argument, enhancing the quality of electronic and mobile services of public institutions is considered critical to investigate how residents view and estimate the services of public institutions depending on quality dimensions (services, information, and systems) for measuring the performance of public institutions as proposed by Alnaser et al. (2022), Alghizzawi et al. (2023), and Omar et al. (2011). Scott et al. (2016) confirmed that the public value of government services is created by improving three characteristics: efficiency, effectiveness, and social value, while government leaders should always seek to reinforce the services matching these categories. The public value established relies on the interactions between public institutions and engaged stakeholders to design and deliver services to citizens in accordance with their needs, tendencies, and valuable outcomes (Ansell & Torfing, 2021). The current study has followed Scott's and his colleague's approach to determine the public value of the fintech services mobile app presented by public institutions.

According to Moore and Moore (1995) and Scott et al. (2016), the public value of efficiency measures is based on cost, time, and communication. The plurality of investigations indicates that using the capabilities of information and communication technology reduces the cost of gathering and accessing public organizations' information. As a second attribute of public value theory, the public value of effectiveness is defined as the level of government services fulfilling an expected result. The public value of effectiveness consists of three major attributes: convenience, ease of information retrieval, and personalization, which play an essential role in generating the value of public services in a government context. As the last attribute of the public value theory, the public value of social value is defined as the residents' perspectives toward the benefits provided by using mobile apps of government institutions, measuring based on trust, well-unforcedness, and participation dimensions. Digitalization has influenced several portions of mobile app services and financial services using digital transformation technologies, which indicates employing these technologies to change the social-technical process to stimulate the connectivity of people, companies, industries, and communities (Alnaser et al., 2023; Dhar & Stein, 2017; Limna et al., 2023; Yang et al., 2023). Fintech is defined as "Financial sector innovations involving technology-enabled business models that can facilitate disintermediation; revolutionize how existing firms create and deliver products and services; address privacy, regulatory and law-enforcement challenges; provide new gateways for entrepreneurship; and seed opportunities for inclusive growth". However, due to rapid growth in digital industries, fintech services have been presented through various platforms, such as electronic, mobile apps, and fintech block-chain as a service for serving several sectors like banks, organizations, and government. Adopting the contemporary technology of fintech services has also been targeted at facilitating consumer transactions. In terms of the current study, Alhanatleh et al. (2022) describe MFS as accomplishing financial transactions through mobile technology and its channels, where users of mobile fintech can send and receive money while having the advantages of mobility. The adoption or use of fintech services has been the trend of many businesses to examine users' behavior toward accepting or rejecting

fintech services (Shaikh et al., 2020). However, investigating the factors that influence the use of fintech services is considered a critical process for improving and developing fintech services (Khuong et al., 2022). Recently, the government of Jordan has established the eFAWATEERcom mobile app, which is incredibly well-liked there and helps Jordanians process, store, and manage their financial services (Carlin et al., 2017; Rahi et al., 2023). However, little effort has been considered to measure the effectiveness of using fintech mobile apps provided by the government and its affected variables, especially in Middle Eastern countries such as Jordan, as asserted by (Alhanatleh et al., 2024 b; Ediagbonya & Tioluwani, 2023).

Nevertheless, many people are still under the hazard of information security from a tremendous domain of threats. Thus, cybersecurity awareness is indispensable for reducing risks and threats to the public (Zwilling et al., 2022) and still needs to be expanded to increase the degree of public awareness regarding cybersecurity (de Bruijn & Janssen, 2017). Lenhart et al. (2007) define cybersecurity as the "protection of computerized information, processing systems and the data they contain and process." Ergen et al. (2021) considered cybersecurity awareness the initial phase to overcome cyberattacks that can be realized as the degree of information, experiences, and knowledge users have regarding the cyber threats facing their companies, systems, and even themselves. In their influential empirical work, Mohammed and Bamasoud (2022) confirmed that enhancing the rate of users' cybersecurity awareness is considered important to minimize the risks and threats of cyber. In this way, users improve the level of protection and privacy associated with significant information. It has been advocated that human factors are considered the main reason causing security threats, where human factors depict their daily reactions and activities within an information system circumference, while the irresponsible acts of users are classified as the primary cause of security risks (Donalds & Osei-Bryson, 2020).

Cybersecurity awareness has been introduced to decrease the possibility of hacking users' information. It is critical to provide a comprehensive overview of the variables that positively affect cybersecurity awareness (Al_Kasasbeh et al., 2023;

Ifinedo, 2012; Siponen et al., 2014). According to Alqahtani (2022), users' cybersecurity awareness is impacted by increasing their experience and knowledge regarding password security factor, social media factor, and browser security factor. Kovačević et al. (2020) investigated the most dominant factors influencing cybersecurity awareness to reduce the cyber risks of digital citizens. The results of this systematic review study uncovered that knowledge and experiences are the most influential determinants identifying the cybersecurity behavior, especially on smartphones and mobile apps. Similar, Simonet and Teufel (2019) confirmed that the strategies should concentrate on providing sufficient knowledge, well-understanding, and well-experienced engagement with cyber vulnerabilities and threats for users rather than fear. Moreover, Mai and Tick (2021) supported that knowledge of individuals' cybersecurity awareness is confirmed depending on four critical dimensions, which are password security usage matters, malware matters, social engineering risks, and online scam matters. In addition, Limna et al. (2023) conducted empirical evidence in the context of mobile apps, and it has been disclosed that cybersecurity knowledge plays a considerable role in identifying the rate of cybersecurity awareness among users of mobile apps. Rising cybersecurity knowledge and skills among users is a substantial determinant influencing the degree of cybersecurity awareness regarding cyber fear. In the current study, several prior factors affecting cybersecurity awareness have been employed to discover the citizens' point of view toward using MFS in Jordan. Carefully, cybersecurity password security and social engineering threats have been proposed as attendances to measure the residents' cybersecurity awareness of using MFS in Jordan. Establishing a new theoretical framework for discovering the rate of MFS usage to measure the level of public value of using MFS is considered a major novelty of the current research.

As a first important antecedent of cybersecurity awareness, Hadnagy (2010) defines social engineering threats as "any act that influences a person to take an action that may or may not be in their best interest" (Aldawood & Skinner, 2018). Social engineering can be materialized through simple or complex methods. The offensive attacks of social engineering can occur through emails or repre-

sentation via phone calls. However, organizations and public sector institutions have sought to enhance their employees' and residents' realization of social engineering attacks through continuous training and education (Pósa & Grossklags, 2022). Furthermore, *password security* is considered a primary determinant for identifying cybersecurity awareness, defined as a secret combination of numbers, characters, words, and special symbols utilized to permit to access electronic or digital information systems (Knight-McCord et al., 2016). Citizens protect themselves in information systems depending on shaping passcodes. However, they form their own passcodes in two ways, either simple or strong passcodes (Wash et al., 2016). Based on empirical evidence, Alqahtani (2022) uncovered that changing the passwords of users grounded on a complex approach increases the degree of their cybersecurity awareness. Finally, *social media* is a considerable determinant affecting cybersecurity awareness. Sharing, accessing, and distributing users' information through interactions with others is a behavior allowed by the social media platform through non-direct (Creevey et al., 2022). In this way, information on social media platforms could be easily stolen due to unacceptable acts such as sharing the location, publishing private photos, and distributing private information. Alqahtani (2022) emphasized that interactions and dealing in an unclear information technology environment bring cyber threats, where positive acts across social media provide users with a high level of cybersecurity awareness

Creating cybersecurity awareness among users assists in producing productivity systems such as mobile apps, MFS, and electronic and digital payment services and provides a high level of economic growth in developed and developing nations (Chang & Coppel, 2020). The role of cybersecurity awareness is represented in the behavior and attitude of users toward adopting or using new technology (Calderwood & Popova, 2019). Positively aware users can determine the degree of use of mobile services by public institutions, as empirically examined in the government sector (Alhanatleh et al., 2022; Rahi et al., 2023). In the setting of MFS, users decide to download, have, and use MFS depending on their awareness and knowledge of its benefits, risks, and threats, as confirmed by (Reddick & Zheng,

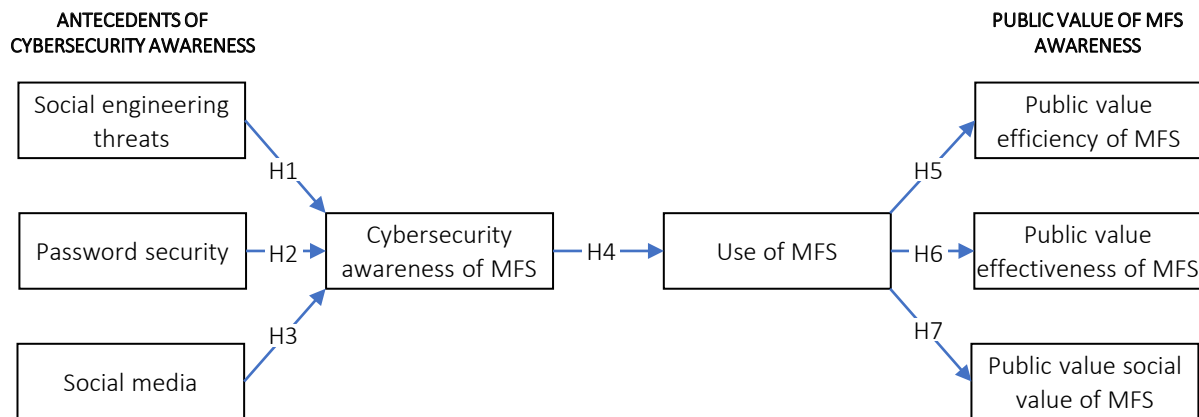


Figure 1. The developed model of the current research

2017). Corresponding to the prior description, the current study argues that cybersecurity awareness will determine the acts and behaviors of citizens to use MFS in Jordan. As a result, the following hypothesis will aim to discover the rate of citizens' cybersecurity awareness when using MFS in Jordan:

The use of MFS is considered a key factor in enhancing the overall public value of financial services, as outlined in the Information Success Model (McLean, 2018). Scott et al. (2016) initially instituted the developed theoretical framework for connecting the intention to use specific technology to public value theory in government service settings, relying on three primary attributes: efficiency, effectiveness, and social value. The empirical evidence confirmed that citizens' intention to use mobile services in the government sector is critical in generating or growing public value efficiency, public value effectiveness, and public value social value (Alhanatleh et al., 2022). To fulfill the objectives of this study, the use of MFS depending on cybersecurity awareness and its priors would provide new insights to create public value efficiency, public value effectiveness, and public value social value among public institutions from citizens' perspectives

According to above above-mentioned justifications, the following hypotheses will target at identifying the level of public value of using the MFS among citizens of Jordan:

H1: Social engineering threats will positively affect Cybersecurity Awareness of MFS.

H2: Password security will positively affect Cybersecurity Awareness of MFS.

H3: Social media will positively affect Cybersecurity Awareness of MFS.

H4: Cybersecurity Awareness of MFS will positively affect MFS usage.

H5: MFS usage will positively increase Public value efficiency of MFS.

H6: MFS usage will positively increase Public value effectiveness of MFS.

H7: MFS usage will positively increase Public value social value of MFS.

Therefore, in accordance with the overall above-mentioned justifications, Figure 1 clarifies the variables and hypotheses of the present study.

2. METHOD

This paper used a quantitative method to look at the role of social engineering threats, password security, and social media on cybersecurity awareness of MFS, the effect of cybersecurity awareness of MFS and its priors on MFS usage, and the effect of MFS usage on public value dimensions (efficiency, effectiveness, and social value) among Jordanians. The quantitative design has been approached by executing several stages. First, conducting an inclusive literature review in the field of public value. Next, establishing a well-justified

conceptual framework connecting the MFS with public value theory. After that, choosing a proper sample for gathering the data from the target population. Afterwards, employing the analysis software to provide the results. Lastly, discussing the findings of this study compared with prior investigations. To empirically estimate the model of the present study, an electronic (e)-survey was conducted using the Google Drive platform. To access the identified sample of this study to fill out the e-survey, Jordanians were invited to participate in the survey through various social media channels, such as Facebook and WhatsApp. As Mou et al. (2017) suggested, the convenience sampling method was used to make collecting data easier, taking into account things like cost-effectiveness, ease of access for Jordanian people, and quick response retrieval.

The questionnaire for this study consisted of three layers of constructs: exogenous factors (social engineering threats, password security, and social media), mediation variables (cybersecurity awareness of MFS and MFS usage), and endogenous factors (public value dimensions). The survey items have been measured in accordance with related investigations for explaining the Jordanians' perspectives about the public value of using MFS. In terms of adopting the exogenous factors, social engineering threats with six items, password security with eight items, and social media with five items have been evaluated and adapted from Mai and Tick (2021). Regarding the mediation factor, cybersecurity awareness of MFS has been evaluated and developed with four items, as in Limna et al. (2023). Moreover, the intention to use MFS has been measured with four items from Alodat et al. (2022). Finally, the endogenous factors (public value dimensions) have been evaluated with 19 items, as in Alhanatleh et al. (2022). The measure of a five-point Likert has gradually been scaled for the survey items in the current study from "1 = strongly disagree" to "5 = strongly agree." The population of this study was Jordanians who use eFAWA-TEERcom app and the Amman Stock Exchange app mobile app to accomplish their financial transactions. Therefore, the number of MFS users cannot be computed for calculating the sample size to serve the data collection stage. Sitthipon et al. (2022) indicated that if the study population is unknown, 385 users of MFS are appropriate

to gather data from the target population. The e-survey was deployed to 550 citizens in Jordan. The total number of retrieved questionnaires was 460. The total number of responses used in the analysis process was 449 due to the use of several statistical techniques for preparing data, such as missing response values, outliers, and others. However, Hair et al. (2019) noted that 449 responses are qualified to fulfill the data analysis process. The data collection stage was held on May 16 and took three weeks to complete.

3. RESULTS

IBM-SPSS-AMOS version 22 has been the tool for analysis and providing results of the developed hypotheses regarding the current study due to its capabilities in supporting a high-quality rate of accuracy for retrieving results, as noted by Hair et al. (2007). Sarstedt et al. (2020) state that confirmatory factor analysis (CFA) and SEM have been allocated as approaches for measuring the model and providing the results of this study. Depending on Hermida (2015), CFA measurements have been implemented by subjecting all items' constructs to a CFA test for estimating the reliability and validity (convergent validity, composite reliability, and discriminant validity) of the sophisticated model. Initially, Raza and Awang (2021) noted that confirming the factor loading of items' constructs (threshold value $\geq .60$) and estimating covariance correlation (threshold value $\leq .85$) among all model constructs is considered the primary stage in terms of measuring reliability and validity. Afterward, the evaluation of model fit can be affirmed in accordance with multiple indicators. Awang (2018) confirmed the satisfied values of model fit indices: (CMIN/DF indicator < 5 is approved or < 3 is exemplary), (GFI, NFI, CFI, AGFI, and TLI indices $\geq .85$ are approved or $\geq .90$ are exemplary), and (RMSEA < 0.08 is approved). Accordingly, the results of CFA uncovered that the model of the current study has provided an ideal fit (CMIN/DF = 2.385, GFI = 0.851, NFI = 0.854, CFI = 0.909, AGFI = 0.827, TLI = 0.901, and RMSEA = 0.056). After that, Composite reliability (CR) and Average Variance extracted (AVE) mechanisms were employed to evaluate the convergent validity and composite reliability of the model constructs. Raza and Awang (2021) confirmed that when the

CR value ($\geq .60$) and AVE value ($\geq .50$), the measurements of convergent validity and composite reliability can be confirmed. In addition, the mean and standard deviation tests have been utilized to ensure the normality of the data distribution. The findings in Table 1 confirm that the data were normally distributed, and the convergent validity and composite reliability assessments were successfully emphasized.

Lastly, Dijkstra and Henseler (2015) stated that the baseline for evaluating discriminant validity is that the computed square root of AVEs regarding the model constructs (in bold font) should be higher than the absolute values of AVEs regarding the inter-correlations. As presented in Table 2, the assessments of discriminant validity have been confirmed by vigorous guidance to estimate this study's SEM.

Table 1. Composite reliability and convergent validity of constructs' study

Model constructs	Items	Factor loading	CR	AVE	Mean	Std
Social engineering threats	SET1	0.785	0.933	0.698	2.316	0.815
	SET2	0.889				
	SET3	0.823				
	SET4	0.794				
	SET5	0.851				
	SET6	0.865				
Password security	PWS1	0.786	0.928	0.619	2.378	0.844
	PWS2	0.915				
	PWS3	0.846				
	PWS4	0.759				
	PWS5	0.858				
	PWS6	0.731				
	PWS7	0.594				
	PWS8	0.764				
Social media	SM1	0.802	0.869	0.570	3.091	0.974
	SM2	0.805				
	SM3	0.780				
	SM4	0.696				
	SM5	0.684				
Cybersecurity Awareness of MFS	CAR1	0.758	0.810	0.520	3.102	0.913
	CAR2	0.842				
	CAR3	0.626				
	CAR4	0.635				
MFS use	MIU1	0.577	0.855	0.601	1.949	0.670
	MIU2	0.785				
	MIU3	0.885				
	MIU4	0.819				
Public value efficiency	PEY1	0.689	0.874	0.538	2.425	0.746
	PEY2	0.813				
	PEY3	0.650				
	PEY4	0.695				
	PEY5	0.808				
	PEY6	0.732				
Public value effectiveness	PES1	0.788	0.928	0.649	3.112	1.014
	PES2	0.824				
	PES3	0.698				
	PES4	0.810				
	PES5	0.837				
	PES6	0.845				
	PES7	0.828				
Public value social value	PSV1	0.724	0.848	0.528	2.776	0.836
	PSV2	0.812				
	PSV3	0.732				
	PSV4	0.670				
	PSV5	0.686				

Table 2. Discriminant validity assessment

Constructs	1	2	3	4	5	6	7	8
Password security	0.787							
Social engineering threats	0.089	0.835						
Social media	0.514	0.215	0.755					
Cybersecurity Awareness of MFS	0.413	0.217	0.499	0.721				
MFS use	0.061	0.773	0.187	0.251	0.775			
Public value efficiency	0.436	0.099	0.549	0.433	0.180	0.734		
Public value effectiveness	0.387	0.292	0.750	0.445	0.327	0.615	0.806	
Public value social value	0.485	0.085	0.542	0.452	0.194	0.529	0.544	0.726

After measuring the CFA criteria, all imputed factors of this study have been subjected to the SEM test, targeted to estimate the findings of the hypotheses results. Figure 2 and Table 3 demonstrate that all developed hypotheses have been provided empirical support (H1 – H7). In more detail, the results of the present study confirmed that Social engineering threats directly and significantly influence Cybersecurity Awareness of MFS among citizens of Jordan ($\beta = .142, p = .001$), and Social engineering threats elucidate R2 (cybersecurity awareness of MFS) = 12.6% of the variance, meaning that H1 is empirically evaluated. Moreover, the findings revealed that Password security has a direct, positive, and significant effect on Cybersecurity Awareness of MFS among citizens of Jordan ($\beta = .235, p = .000$), and Password security clarifies R2 (cybersecurity awareness of MFS) = 21.7% of the variance, meaning that H2 is empirically confirmed. In addition, the findings revealed that Social media directly and positively influences Cybersecurity Awareness of MFS among citizens of Jordan ($\beta = .393, p = .000$), and Social media explains R2 (cybersecurity awareness of MFS) = 41.9% of the

variance, meaning that H3 is empirically ensured. Besides, the results disclosed that Cybersecurity Awareness of MFS has a direct and considerable influence on MFS use among citizens of Jordan ($\beta = .210, p = .000$), and Cybersecurity Awareness of MFS explains R2 (MFS use) = 28.6% of the variance, meaning that H4 is empirically affirmed. Next, the findings confirmed that MFS use has a direct and considerable effect on Public value efficiency among citizens of Jordan ($\beta = .223, p = .000$), and MFS use explicates R2 (Public value efficiency) = 20% of the variance, meaning that H5 is empirically affirmed. The findings also asserted that MFS use has a direct and considerable effect on Public value effectiveness among citizens of Jordan ($\beta = .535, p = .000$), and MFS use explicates R2 (Public value effectiveness) = 35.4% of the variance, meaning that H6 is empirically affirmed. Finally, the outcomes uncovered that MFS use has a direct and considerable effect on Public value social value among citizens of Jordan ($\beta = .267, p = .000$), and MFS use explicates R2 (Public value social value) = 21.4% of the variance, meaning that H7 is empirically affirmed.

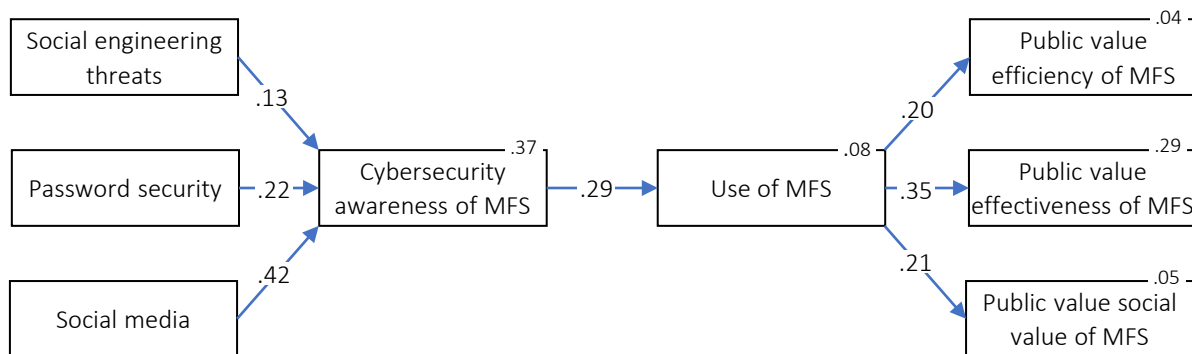


Figure 2. The retrieved graphic of the model hypotheses results (SEM)

Table 3. Results of the study hypotheses

Hypothesis	Coefficient Estimates	S.E.	t- Statistics	P
Social engineering threats → Cybersecurity Awareness of MFS	0.142	0.043	3.272	0.001
Password security → Cybersecurity Awareness of MFS	0.235	0.049	4.805	***
Social media → Cybersecurity Awareness of MFS	0.393	0.043	9.054	***
Cybersecurity Awareness of MFS → MFS use	0.21	0.033	6.309	***
MFS use → Public value efficiency	0.223	0.052	4.326	***
MFS use → Public value effectiveness	0.535	0.067	7.999	***
MFS use → Public value social value	0.267	0.058	4.644	***

4. DISCUSSION

The current paper aimed to develop a novel conceptual framework that integrates cybersecurity awareness and public value theory depending on the use of MFS in fintech settings among Jordanian citizens. This paper has empirically confirmed the potential predictors influencing cybersecurity awareness of MFS, MFS use, and ultimately, public value dimensions in Jordan. As the first hypothesis mentioned in this study, the outcomes of this article uncover that social engineering threats are considered a major factor in deciding the level of Jordanian citizens' cybersecurity awareness of MFS. This explains that Jordanian residents have increased their cybersecurity awareness of MFS since they know various types of social engineering risks. Policymakers, managers, and leaders of mobile fintech government services could prepare and provide sufficient training regarding the recent potential social engineering threats for citizens, which is considered successful planning for increasing the degree of their cybersecurity awareness of MFS. The first hypothesis results align with similar investigations in the relevant literature (Aldawood & Skinner, 2018; Pósa & Grossklags, 2022). The results of the second hypothesis confirm that password security is considered a pivotal variable that critically influences cybersecurity awareness of MFS among citizens of Jordan. As a result, citizens' cybersecurity awareness of MFS has increased since they realize how to keep their passwords secure, form a sturdy password for MFS, and do not share their personal information and password applications with others. However, government managers are responsible for increasing residents' behavior toward dealing with formulating their passwords in the MFS context. The empirical results of the second hypothesis are in touch with prior studies (Alqahtani, 2022; Wash et al., 2016). In terms of the third hypothesis

of the present study, the findings disclose that social media is considered a highly influential variable among others affecting citizens' cybersecurity awareness of MFS in Jordan. This explains that cybersecurity awareness of MFS has been raised among citizens of Jordan, since they are perceived about their behavior and activities of using social media platforms. Hence, public administration managers could prepare comprehensive guidance regarding the risks and threats of social media technologies for citizens. The results of the third hypothesis are similar to previous investigations (Alqahtani, 2022; Creevey et al., 2022).

In addition, the findings of the fourth hypothesis confirm that cybersecurity awareness of MFS and its predictors play an essential role in determining the level of MFS use among citizens of Jordan. This means that highly aware citizens have the strength to identify the degree of MFS usage in Jordan. Accordingly, high-level citizens' cybersecurity awareness of MFS will encourage them to download MFS on their smartphones and accomplish their financial transactions depending on MFS in Jordan. In addition, the citizens of Jordan decided that using MFS brings numerous benefits, such as cost-effectiveness, ease of use, speed of services, and low risks. However, increasing the degree of cybersecurity awareness and its antecedents will support a strong attitude and behavior toward using MFS among Jordanians. Hence, public institutions in Jordan must prepare proper planning and training to elevate the level of citizens' cybersecurity awareness of MFS toward attacks, threats, and risks. Moreover, developers and designers should pay attention to social engineering threats, password security, and social media dimensions in the development process of MFS that could decrease the potential cybersecurity threats using MFS. In this way, continuous development of MFS will make public organizations safer regarding cyber-

security attacks and provide the maximum rate of MFS ease of use among Jordanians. The findings of the fourth hypothesis are in touch with similar research findings in the literature review (Alhanatleh et al., 2022; Alhanatleh et al., 2024). Regarding the fifth hypothesis, the outcomes of this article ensure that MFS use can generate public value efficiency among Jordanians. This elucidates that using the capabilities of MFS reinforces reducing the cost and time for collecting and accessing the information and financial services of public institutions in Jordan. In addition, the capabilities of MFS communication assist in accomplishing financial transactions for Jordanians. The empirical evidence of the fifth hypothesis results is linked with prior investigations (Bannister & Connolly, 2014). Relying on the sixth hypothesis mentioned, the findings of this study indicate that MFS use aids in creating public value effectiveness among citizens of Jordan, meaning that the public institutions fulfill the foreseeable outcomes of residents of Jordan. Increasing the convenience, ease of information retrieval, and personalization of MFS will generate or maximize the public value effectiveness among Jordanian citizens. The results of the sixth hypothesis are in line with similar studies (Kernaghan, 2013; Schryen, 2013). Finally, the findings of the seventh hypothesis confirm that MFS use assists in creating or maximizing the public value of social value among Jordanians, clarifying using MFS with high-quality trust, well-unforcedness, and participation attributes aims to enhance the degree of public value of social value and gain benefits among Jordanian citizens. As a result, creating public value of MFS among Jordanians requires strong planning for the sustainability of MFS through reinforcing the present financial service and suggesting mandatory financial services in terms of the requirements of citizens. Government leaders and managers could

seek to adopt the latest trends in information technology (such as artificial intelligence, blockchain technology, and big data) to increase the public value of using MFS among Jordanians. The findings of the seventh hypothesis are in touch with prior research (Jiao et al., 2017).

Finally, the study possesses certain limits and areas for future investigations that contribute to advancing knowledge and understanding in the field of the present study. Firstly, the results of the current study require generalization. To do so, conducting the same model in several sectors could provide new insights and the ability to publicize the outcomes. Besides, maximizing the sample size requires deeply understanding the factors influencing the public value of using MFS. Secondly, adding other dimensions to the study model could potentially provide another perspective for measuring public institutions' performance and ensuring MFS's sustainability. Thirdly, investment in digitalization is considered a future trend in the public and private sectors. The future effort regarding the area of the present study could conduct quantitative and qualitative investigations to explore the benefits and challenges of adopting digital transformation technologies (block-chain, artificial intelligence, big data analytics, and Internet of things) in the public sector and MFS. In addition, the government agility idiom expects to provide new insights to reinforce public administration performance based on the trends of digital transformation technologies. Integrating government agility with the current research model may affect the public value of MFS in Jordan. Finally, measuring the mediation role of the cybersecurity awareness of MFS and MFS use could explain the citizens' behavior and attitude toward increasing or generating MFS's public value among Jordan's public institutions.

CONCLUSION

By connecting the elements of public value theory with the cybersecurity awareness of Mobile Fintech services and its precursors, this work is an early attempt to obtain insight into the performance processes of public institutions. The sophisticated conceptual model of the recent study has been estimated to measure the performance of public institutions from citizens' points of view regarding Mobile Fintech services. Connecting the cybersecurity awareness of Mobile Fintech services and public value theory has been considered a primary theoretical contribution that feeds the relevant literature regarding the field of this study. This study has discovered that social engineering threats,

password security, and social media factors can evaluate the degree of citizens' cybersecurity awareness of Mobile Fintech services in Jordan. Moreover, the findings have revealed that cybersecurity awareness of Mobile Fintech services and its predictors positively and significantly affect the use of Mobile Fintech services among citizens of Jordan. Therefore, the public value of using Mobile Fintech services can be generated among Jordanians. Moreover, the contribution of research on financial services, cybersecurity, and public value theory to measure the performance of public institutions depends on citizens' information and knowledge about the use of Mobile Fintech services in Jordan. The statistical findings of the recent manuscript have empirically affirmed the connection between cybersecurity awareness of Mobile Fintech services usage and its predictors with the dimensions of public value theory in the government sector. The outcomes of this study confirmed that social engineering threats, password security, and social media factors support powerful statistical evidence to increase citizens' cybersecurity awareness of Mobile Fintech services and eventually affect Mobile Fintech services usage.

Moreover, the findings asserted that cybersecurity awareness of Mobile Fintech services, depending on its antecedents and MFS use, provides empirical support for the public value determinants (efficiency, effectiveness, and social value) of citizens in Jordan. However, the primary difference between this paper and previous research is that it has statistically confirmed the link between cybersecurity awareness of Mobile Fintech services and public value theory based on citizens' viewpoints in Jordan. Therefore, the confirmed results of this article could be utilized as a valuable reference for government managers and leaders, designers, developers, stockholders, and policymakers in the domain of government services and the public value realm in Jordan. In addition, the results may be employed in terms of the Mobile Fintech services development and sustainability, meeting Jordanians' requirements, needs, and specifications. Consequently, presenting inclusive and well-understood dimensions that influence the public value of using Mobile Fintech services among Jordanians is a necessity process that expects to provide long-term Mobile Fintech services sustainability. Finally, the growth in digitalization has offered an alternative approach to evaluating the performance of public institutions and adding value to citizens in accordance with the big-data realm, artificial intelligence technology, block-chain technology, and its services platform, the technologies of the virtual world and virtual reality, and the internet of things platform.

AUTHOR CONTRIBUTIONS

Conceptualization: Hasan Alhanatleh, Amineh Khaddam, Farah Abudabaseh, Mahmoud Alghizzawi, Amro Alzghoul.

Data curation: Hasan Alhanatleh, Amineh Khaddam, Mahmoud Alghizzawi, Amro Alzghoul.

Formal analysis: Hasan Alhanatleh, Farah Abudabaseh.

Funding acquisition: Farah Abudabaseh, Mahmoud Alghizzawi.

Investigation: Hasan Alhanatleh, Amineh Khaddam, Mahmoud Alghizzawi.

Methodology: Hasan Alhanatleh, Amineh Khaddam, Amro Alzghoul.

Project administration: Mahmoud Alghizzawi, Amro Alzghoul.

Resources: Amineh Khaddam, Farah Abudabaseh.

Software: Hasan Alhanatleh, Farah Abudabaseh.

Supervision: Hasan Alhanatleh, Amineh Khaddam, Amro Alzghoul.

Validation: Hasan Alhanatleh, Amineh Khaddam, Farah Abudabaseh, Amro Alzghoul.

Visualization: Hasan Alhanatleh, Farah Abudabaseh, Amro Alzghoul.

Writing – original draft: Hasan Alhanatleh, Amineh Khaddam, Farah Abudabaseh, Mahmoud Alghizzawi, Amro Alzghoul.

Writing – review & editing: Hasan Alhanatleh, Amro Alzghoul.

REFERENCES

1. Al-Okaily, M., Al Natour, A. R., Shishan, F., Al-Dmour, A., Alghazzawi, R., & Alsharairi, M. (2021). Sustainable FinTech innovation orientation: a moderated model. *Sustainability*, 13(24), 13591. <https://doi.org/10.3390/su132413591>
2. Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62-68. <https://doi.org/10.1109/TALE.2018.8615162>
3. Alford, J., & O'flynn, J. (2009). Making sense of public value: Concepts, critiques and emergent meanings. *International Journal of Public Administration*, 32(3-4), 171-191. <https://doi.org/10.1080/01900690902732731>
4. Alghizzawi, M., Attar, R. W., Alhanatleh, H., Alnawafleh, H., Tahat, K., & Tahat, D. N. (2023). Digital Ads via Smart Phones and Purchase Intent. *2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, 1-7. <http://dx.doi.org/10.1109/SNAMS60348.2023.10375452>
5. Alhanatleh, H., Khaddam, A., & Abousweilem, F. (2022). Mobile government public value model for assessing the public institution's services: evidence through the context of Jordan. *International Journal of Data and Network Science*, 6(4), 1295-1308. <http://dx.doi.org/10.5267/j.ijdns.2022.6.005>
6. Alhanatleh, H., Alghizzawi, M., Alhawamdeh, Z., Alkhlaifat, B., Alabaddi, Z., & Al-Kasasbeh, O. (2024 b). Public value of using fintech services' mobile applications: Citizens' perspective in a Jordan setting. *Uncertain Supply Chain Management*, 12(2), 1317-1330. <http://dx.doi.org/10.5267/j.uscm.2023.11.005>
7. Aljeaid, D., Alzhrani, A., Alrougi, M., & Almalki, O. (2020). Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. *Information*, 11(12), 547. <https://doi.org/10.3390/info11120547>
8. Al_Kasasbeh, O., Khasawneh, O., & Alzghoul, A. (2023). The Real Effects of Fintech on the Global Financial System. *International Journal of Professional Business Review*, 8(3), e01725-e01725. <https://doi.org/10.26668/business-review/2023.v8i3.1725>
9. Alnaser, A. S., Theep, K. A., & Alhanatleh, H. (2022). Do e-government services affect Jordanian customer loyalty? *Marketing i Menedžment Inovacij*, 2, 17-30. Retrieved from https://essuir.sumdu.edu.ua/bitstream-download/123456789/88295/1/Alnaser_mmi_2_2022.pdf;jsessionid=4813A5090006C1CD4DCFFC7AA20725FD
10. Alnaser, F., Rahi, S., Alghizzawi, M., & Ngah, A. H. (2023). Does Artificial Intelligence (Ai) Boost Digital Baking User Satisfaction? Integration of Expectation Confirmation Model and Antecedents of Artificial Intelligence Enabled Digital Banking. *Integration of Expectation Confirmation Model and Antecedents of Artificial Intelligence Enabled Digital Banking*. <https://doi.org/10.1016/j.heliyon.2023.e18930>
11. Alodat, A. Y., Salleh, Z., Hashim, H. A., & Sulong, F. (2022). Corporate governance and firm performance: Empirical evidence from Jordan. *Journal of Financial Reporting and Accounting*, 20(5), 866-896. <https://doi.org/10.1108/JFRA-12-2020-0361>
12. Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12(5), 2589. <https://doi.org/10.3390/app12052589>
13. Ansell, C., & Torfing, J. (2021). Co-creation: The new kid on the block in public governance. *Policy & Politics*, 49(2), 211-230. <http://dx.doi.org/10.1332/030557321X16115951196045>
14. Awang, P. (2018). *Pendekatan Mudah SEM (Structural Equation Modeling)*. MPWS Rich Resources. Retrieved from <https://eprints.uniswa.edu.my/3865/>
15. Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. *Government Information Quarterly*, 31(1), 119-128. <http://dx.doi.org/10.1016/j.giq.2013.06.002>
16. Calderwood, F., & Popova, I. (2019). Smartphone cyber security awareness in developing countries: A case of Thailand. *International Conference on Emerging Technologies for Developing Countries. Emerging Technologies for Developing Countries*, 79-86. http://dx.doi.org/10.1007/978-3-030-05198-3_7
17. Carlin, B., Olafsson, A., & Pagel, M. (2017). *FinTech Adoption Across Generations: Financial Fitness in the Information*. Retrieved from <https://www.nber.org/papers/w23798>
18. Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security*, 97, 101959. <https://doi.org/10.1016/j.cose.2020.101959>
19. Creevey, D., Coughlan, J., & O'Connor, C. (2022). Social media and luxury: A systematic literature review. *International Journal of Management Reviews*, 24(1), 99-129. <https://doi.org/10.1111/ijmr.12271>
20. de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1-7. <https://doi.org/10.1016/j.giq.2017.02.007>
21. Dhar, V., & Stein, R. M. (2017). FinTech platforms and strategy. *Communications of the ACM*, 60(10), 32-35. <http://dx.doi.org/10.1145/3132726>
22. Dijkstra, T. K., & Henseler, J. (2015). Consistent partial least

- squares path modeling. *MIS Quarterly*, 39(2), 297-316. <http://dx.doi.org/10.25300/MISQ/2015/39.2.02>
23. Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51, 102056. <https://doi.org/10.1016/j.ijinfomgt.2019.102056>
 24. Ediagbonya, V., & Tioluwani, C. (2023). The role of fintech in driving financial inclusion in developing and emerging markets: issues, challenges and prospects. *Technological Sustainability*, 2(1), 100-119. <https://doi.org/10.1108/TECHS-10-2021-0017>
 25. Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is it possible to change the cyber security behaviours of employees? Barriers and promoters. *Academic Journal of Interdisciplinary Studies*, 10(4), 210. <https://doi.org/10.36941/ajis-2021-0111>
 26. Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.
 27. Hair, J. F., Money, A. H., Samouel, P., & Page, M. (2007). Research methods for business. *Education + Training*. <https://doi.org/10.1108/et.2007.49.4.336.2>
 28. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2-24. <https://doi.org/10.1108/EBR-11-2018-0203>
 29. Halim, S. B. K., Osman, S. B., Al Kaabi, M. M., Alghizzawi, M., & Alrayssi, J. A. A. (2023). The Role of Governance, Leadership in Public Sector Organizations: A Case Study in the UAE. In *Digitalisation: Opportunities and Challenges for Business* (Vol. 2, pp. 301-313). Springer. http://dx.doi.org/10.1007/978-3-031-26956-1_30
 30. Hermida, R. (2015). The problem of allowing correlated errors in structural equation modeling: concerns and considerations. *Computational Methods in Social Sciences*, 3(1), 5-17. Retrieved from <https://econpapers.repec.org/article/ntuntcmss/vol3-iss1-15-005.htm>
 31. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95. <https://doi.org/10.1016/j.cose.2011.10.007>
 32. Jiao, Y., Jo, M.-S., & Sarigöllü, E. (2017). Social value and content value in social media: Two paths to psychological well-being. *Journal of Organizational Computing and Electronic Commerce*, 27(1), 3-24. <https://doi.org/10.1080/10919392.2016.1264762>
 33. Kelly, G., Mulgan, G., & Muers, S. (2002). *Creating public value*. London: Cabinet Office. Retrieved from <https://cdi.mecon.gov.ar/bases/docelec/dp4080.pdf>
 34. Kernaghan, K. (2013). Changing channels: Managing channel integration and migration in public organizations. *Canadian Public Administration*, 56(1), 121-141. <https://doi.org/10.1111/capa.12006>
 35. Khuong, N. V., Phuong, N. T. T., Liem, N. T., Thuy, C. T. M., & Son, T. H. (2022). Factors Affecting the Intention to Use Financial Technology among Vietnamese Youth: Research in the Time of COVID-19 and Beyond. *Economies*, 10(3), 57. <https://doi.org/10.3390/economies10030057>
 36. Knight-McCord, J., Cleary, D., Grant, N., Herron, A., Lacey, T., Livingston, T., & Emanuel, R. (2016). What social media sites do college students use most. *Journal of Undergraduate Ethnic Minority Psychology*, 2(21), 21-26. Retrieved from https://juempyschology.com/wp-content/uploads/2022/08/Knight-McCord-et-al_JUEMP_2016.pdf
 37. Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access*, 8, 125140-125148. <https://doi.org/10.1109/ACCESS.2020.3007867>
 38. Lenhart, A., Madden, M., Macgill, A. R., & Smith, A. W. (2007). *Teens and social media: The use of social media gains a greater foothold in teen life as they embrace the conversational nature of interactive online media*. Washington, DC: Pew Internet & American Life Project. Retrieved from https://books.google.com.au/books/about/Teens_and_Social_Media.html?id=88-htgAACAAJ&redir_esc=y
 39. Limna, P., Kraiwanit, T., Siripipattanakul, S., Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand. *International Journal of Computing Sciences Research*, 7, 1133-1151. <http://dx.doi.org/10.25147/ijcsr.2017.001.1.123>
 40. Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, 18(8), 67-89. Retrieved from https://acta.uni-obuda.hu/Mai_Tick_115.pdf
 41. McLean, G. (2018). Examining the determinants and outcomes of mobile app engagement - A longitudinal perspective. *Computers in Human Behavior*, 84, 392-403. <https://doi.org/10.1016/j.chb.2018.03.015>
 42. Mohammed, M., & Bamasoud, D. M. (2022). The Impact of Enhancing Awareness of Cyber-security on Universities Students: A Survey Paper. *J. Theor. Appl. Inf. Technol.*, 100. Retrieved from <https://www.jatit.org/volumes/Vol100No15/19Vol100No15.pdf>
 43. Moore, M. H., & Moore, M. H. (1995). *Creating public value: Strategic management in government*. Harvard University Press.
 44. Mou, J., Shin, D.-H., & Cohen, J. (2017). Understanding trust and perceived usefulness in the consumer acceptance of an e-service: A longitudinal investigation. *Behaviour & Information Technology*, 36(2), 125-139. <http://dx.doi.org/10.1080/0144929X.2016.1203024>

45. Omar, K., Scheepers, H., & Stockdale, R. (2011). *How mature is Victorian local e-government: an overall view*. Retrieved from <https://core.ac.uk/reader/301352810>
46. Perera, S., Sandhu, S. K., & Soosay, C. (2017). Investigating the impact of agility and resilience on sustainable supply chains. *Academy of Management Proceedings*, 2017(1), 12682. Retrieved from <http://dx.doi.org/10.5465/AMBPP.2017.12682abstract>
47. Pósa, T., & Grossklags, J. (2022). Work experience as a factor in cyber-security risk awareness: A survey study with university students. *Journal of Cybersecurity and Privacy*, 2(3), 490-515. <https://doi.org/10.3390/jcp2030025>
48. Rahi, S., Alghizzawi, M., Ahmad, S., Munawar Khan, M., & Ngah, A. H. (2021). Does employee readiness to change impact organization change implementation? Empirical evidence from emerging economy. *International Journal of Ethics and Systems*, ahead-of-p(ahead-of-print). <https://doi.org/10.1108/IJOES-06-2021-0137>
49. Rahi, S., Alghizzawi, M., & Ngah, A. H. (2022). Factors influence user's intention to continue use of e-banking during COVID-19 pandemic: the nexus between self-determination and expectation confirmation model. *EuroMed Journal of Business*, ahead-of-print(ahead-of-print). <https://doi.org/10.1108/EMJB-12-2021-0194>
50. Raza, I., & Awang, Z. (2021). Knowledge-sharing practices in higher educational institutes of Islamabad, Pakistan: an empirical study based on theory of planned behavior. *Journal of Applied Research in Higher Education*, 13(2), 466-484. <http://dx.doi.org/10.1108/JARHE-03-2020-0068>
51. Reddick, C. G., & Zheng, Y. (2017). Determinants of citizens' mobile apps future use in Chinese local governments: An analysis of survey data. *Transforming Government: People, Process and Policy*, 11(2), 213-235. <https://doi.org/10.1108/TG-11-2016-0078>
52. Sarstedt, M., Ringle, C. M., & Hair, J. F. (2020). Handbook of Market Research. In *Handbook of Market Research* (Issue September). <https://doi.org/10.1007/978-3-319-05542-8>
53. Schryen, G. (2013). Revisiting IS business value research: what we already know, what we still need to know, and how we can get there. *European Journal of Information Systems*, 22(2), 139-169. <https://doi.org/10.1057/ejis.2012.45>
54. Scott, M., DeLone, W., & Golden, W. (2016). Measuring eGovernment success: a public value approach. *European Journal of Information Systems*, 25, 187-208. <http://dx.doi.org/10.1057/ejis.2015.11>
55. Shaikh, I. M., Qureshi, M. A., Noordin, K., Shaikh, J. M., Khan, A., & Shahbaz, M. S. (2020). Acceptance of Islamic financial technology (FinTech) banking services by Malaysian users: an extension of technology acceptance model. *Foresight*, 22(3), 367-383. <https://doi.org/10.1108/FS-12-2019-0105>
56. Simonet, J., & Teufel, S. (2019). The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. IFIP International Conference on ICT Systems Security and Privacy Protection. *ICT Systems Security and Privacy Protection*, 194-208. http://dx.doi.org/10.1007/978-3-030-22312-0_14
57. Siponen, M., Mahmood, M. A., & Pahnla, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217-224. <https://doi.org/10.1016/j.im.2013.08.006>
58. Sitthipon, T., Limna, P., Jaipong, P., Siripipattanakul, S., & Auttawechasakoon, P. (2022). Gamification predicting customers' repurchase intention via e-commerce platforms through mediating effect of customer satisfaction in Thailand. *Review of Advanced Multidisciplinary Sciences, Engineering & Innovation*, 1(1), 1-14. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080558
59. Stoker, G. (2006). Public value management: A new narrative for networked governance? *The American Review of Public Administration*, 36(1), 41-57. <https://doi.org/10.1177/0275074005282583>
60. Twizeyimana, J. D., & Andersson, A. (2019). The public value of E-Government—A literature review. *Government Information Quarterly*, 36(2), 167-178. <https://doi.org/10.1016/j.giq.2019.01.001>
61. Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, 13(2), 39. <https://doi.org/10.3390/fi13020039>
62. Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 175-188. Retrieved from <https://www.use-nix.org/system/files/conference/soups2016/soups2016-paper-wash.pdf>
63. Yang, J., Wang, K., Luo, F., & Wen, F. (2023). AC Network-Constrained Peer-to-Peer Electricity Market Model in Low-voltage Power Distribution Networks. *International Journal of Electrical Power & Energy Systems*, 154, 109428. <https://doi.org/10.1016/j.ijepes.2023.109428>
64. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82-97. <http://dx.doi.org/10.1080/08874417.2020.1712269>