Exploring the Link Between Cashless Society and Cybercrime in Indonesia

Kemal Farouq Mauladi
Fakultas Teknik, Universitas Islam Lamongan

I Made Laut Mertha Jaya
Fakultas Ekonomi dan Bisnis, Universitas Mahakarya Asia

Miguel Angel Esquivias
Faculty of Economics and Business, Universitas Airlangga

Abstract: This study examines whether the rise in cybercrime activity in Indonesia is associated with the perceived benefits, convenience, and risk of a cashless society. In doing so, we apply Structural Equation Modelling (SEM) to a total sample of 200 Indonesian respondents who have been victims of cyber fraud. The results indicate that the high cybercrime rate, including phishing, distributed denial-of-service (DDoS), and social engineering, is positively associated with the perceived benefits and risks of transacting online. The rise in cases of DDoS can particularly be linked to consumers' increasing perceptions of convenience in undertaking cashless transactions. The findings suggest that more stringent cyber law enforcement needs to be implemented. Digital technologies will continue to improve, and more consumers will do transactions digitally. With increasing volumes of cashless transactions, the risk of cyber attacks will likely increase. Stakeholders need to strengthen data privacy and provide a secure environment for customers. International cooperation should be promoted through the establishment of virtual world law as economic activities and cybercrime risks now become borderless.

Keywords: cybercrime, fraud, cashless society, fintech, digital economy

Introduction

Developments in science and technology have brought tremendous benefits to civilization. Jobs that previously required considerable physical strength are increasingly replaced by automated systems (Dwivedi *et al.*, 2021;Malesev & Cherry, 2021;Trinugroho *et al.*, 2017). Similarly, new technologies are applied to business activities to enhance the consumer experience (Wohllebe *et al.*, 2021). Rapid incorporation of technologies in new business

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

models is likely to encourage the use of digital means by consumers and businesses (Tee & Ong, 2016). However, as more consumers embrace digital transactions, the risk of exposure to cybercrime may also increase. Criminal activities target Internet users through hacking, cracking, and cyber terrorism. Not surprisingly, cybercrime rates have increased substantially in the last decade (Kemp, Miró-Llinares & Moneva, 2020).

Fraud cases are increasingly reported worldwide (Ajayi, 2016;Hidayati *et al.*, 2021;Nawang, 2017), with victims reaching millions of Internet users (Hill & Marion, 2016). In the United Kingdom, a third of the total crimes (nearly 3.8 million in 2019) are related to online activities, according to the Crime Survey of England and Wales (Office for National Statistics, 2022). In the United States, cybercrime increased by almost 69% in 2019, with losses equivalent to US$4.2 billion, a figure three times larger than that for 2018 (Economist, 2021). Cybercrime has expanded in both advanced and developing countries (Ajayi, 2016; Lubis & Handayani, 2022; Nawang, 2017). In Indonesia, the number of cases is the second highest globally, after Japan. Akamai International (2013), a security threat report, showed that Indonesia ranked first in the list of countries at risk of increased cyber-attack. Internet users in Indonesia reached more than 202 million in 2021, equivalent to nearly 73% of the population (http://www.datareportal.com). Still, awareness among business people and the general public about the risk of cybercrimes remains low.

Based on the traffic anomaly data reported by the National Cyber and Crypto Agency (Indonesia), throughout 2020, Indonesia experienced more than 495 million cyber anomalies, which is a 41% increase from 2019 (BSSN, 2020), with trojans becoming the most frequent cyber threat. From the same report, nearly 2,550 cases of email phishing were detected, 79,439 accounts experienced data breaches, and 9,749 sites experienced web defacement. Educational-related resources saw the largest number of cases in Indonesia in 2020, likely due to remote schooling due to the COVID19 pandemic. Meanwhile, from January to July 2021, traffic anomalies/cyber threats reached 741.4 million, with the most frequent being malware, distributed denial-of-service (DDoS), and trojans. Increasingly, cyber attackers demand ransom and cause data leaks.

In Indonesia, most cybercrime cases are data hacking, often caused by Internet users' ignorance and carelessness (Lubis & Handayani, 2022). According to data from the Indonesian National Police (POLRI), from April 2020 to July 2021, at least 937 cases of cybercrime were reported, with the highest involving provocative/hate content (473 cases), fraud (259 cases), and pornographic content (82 cases). Other types of cybercrime in Indonesia include phishing — i.e., stealing consumer data such as user identification, passwords, and personal details — and DDoS — i.e., attacks on servers aimed at disturbing network resources and machines — or website hijacking through web defacement (Ajayi,

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

2016;Hidayati *et al.*, 2021; Kemp, Miró-Llinares & Moneva, 2020). Pirated software and user ignorance facilitate such cybercrimes (Hidayati *et al.*, 2021; Nawang, 2017).

Companies in Indonesia have been accelerating their digitalization strategies, such as by implementing e-commerce, expanding social networks and digital infrastructure (Kusmiarto *et al.*, 2021; Mihardjo *et al.*, 2019; Nasution *et al.*, 2020). Digitalization is reshaping customer behaviour by increasing the perceived benefits, convenience, and risks when transacting online (Dwivedi *et al.*, 2021). Non-cash payments are becoming more common among Indonesians (Salman & Saleem, 2017; Tee & Ong, 2016; Trinugroho *et al.*, 2017). In 2021 alone, digital financial transactions in Indonesia increased by more than 45%, with e-money expanding by nearly 50% (Bank Indonesia, 2021). However, this expansion was not accompanied by security system improvements, which leaves users vulnerable to cybercrimes Astuti, 2020; Hidayati *et al.*, 2021). Moreover, digital mastery among business players and consumers remains low, and they are not fully aware of privacy issues and security threats Kusmiarto *et al.*, 2021; Nasution *et al.*, 2020).

In Indonesia, the number of fraud cases has increased in the last decade along with the rapid technological progress, growth in numbers of financial applications (Suryono, Budi & Purwandari, 2021), expansion of super apps (Fauzi & Sheng, 2020), and other advances in digitalization (Esquivias *et al.*, 2020). The Indonesian authorities have started cyber patrols to minimize cybercrime, but fraud remains pervasive. Prabowo (2012) points out that fraud prevention related to credit card services is ineffective due to poor mechanisms for collecting, managing, and distributing data. Kusmiarto *et al.* (2021) pointed out how government agencies lack cybersecurity strategies, privacy protection, and cyber resilience, suggesting that they are not ready for digital transformation.

In the banking industry, Purwanegara, Apriningsih & Andika (2014) noted that regulations and protection for consumers in Indonesia are low. However, in recent years, financial authorities in Indonesia have paid more attention to, and deployed resources for, data protection, privacy frameworks, and more stringent digital finance regulations (Lubis & Handayani, 2022; Suryono, Budi & Purwandari, 2021). These efforts are expected to enhance the perceived safety in digital transactions (Ruiz-Real *et al.*, 2021).

This study examines whether the increasing cybercrime rate for phishing, DDoS, and social engineering is linked to consumers' perceived benefits, convenience, and risks of cashless transactions. To test our research hypotheses, we used the results from a survey of 200 users of cashless services in 2021. In the analysis, we used a Structural Equation Model (PLS-SEM) to test whether consumer perception of i) benefits, ii) convenience, and iii) risk determines or influences cybercrime.

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

As the cashless society in Indonesia is still young (Esquivias *et al.*, 2020), we aim to show whether the expansion of digital activities and changes in consumers' perceptions can be associated with an increase in cybercrime. This study offers a unique contribution because access to cybercrime data in Indonesia is difficult to achieve. Moreover, the data collection period covers the COVID19 pandemic, when online activities were peaking due to the strict containment measures imposed on citizens. Cyber security shapes consumers' trust and determines the future of digital businesses. Since it could also threaten a country's stability, governments need to play an active role in cyber security and develop protection policies for businesses and consumers.

Earlier studies on the cashless economy in Indonesia have examined digital financial practices (Suryono, Budi & Purwandari, 2021), the links between cashless transactions and financial inclusion (Bayero, 2015), digital competencies and cashless transactions (Salman & Saleem, 2017), cashless payments, economic growth (Tee & Ong, 2016), and consumers' digital readiness for digital finance (Trinugroho *et al.*, 2017). However, little research has examined the link between cashless transactions and cybercrime. We aim to fill this gap.

The remainder of this paper is structured as follows. Section 2 presents the literature review. Section 3 outlines the methodology. Section 4 shows the results and discussion. Section 5 concludes the discussion and outlines the limitations of the study.

Literature Review and Hypothesis Development

Most social and economic activities today are assisted by technology. Digital technologies are not only for communicating and interacting, but are also an integral part of business activities (Abad-Segura *et al.*, 2020; ACFE, 2018; Njanike, Mutengezanwa & Gombarume, 2011; Suryono, 2019; Teja, 2017). Worldwide, a transition towards a digital economy is taking place, with the increasing use of e-money and digital transactions referred to as the cashless society.

Cybercrime in the era of a cashless society

Benefits

Cashless transactions have become increasingly common in the digital era (Malesev & Cherry, 2021; Ruiz-Real *et al.*, 2021; Thaichon, Soutar & Weaven, 2021), including in Indonesia with its rapid development of digital infrastructure. Cashless transactions are supported by an entire ecosystem that includes regulators, financial institutions, device manufacturers, retailers, sellers, and consumers (Tee & Ong, 2016; Trinugroho *et al.*, 2017). A cashless society, if well-orchestrated, offers many advantages for consumers (Trinugroho *et al.*, 2017).

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

Benefits for consumers are revealed in the simplification of transactions when using digital money (Chang *et al.*, 2016). In the context of the COVID19 pandemic, such benefits were evident, as digital money became a very helpful means of transacting when governments imposed restrictions on physical mobility. Besides, a number of consumers opted for digital transactions during the pandemic as a prevention measure against COVID19. As individuals increase the frequency of digital payments, and as more businesses provide cashless channels to consumers, the perception of the benefits of cashless transactions is likely to improve (Fauzi & Sheng, 2020).

Convenience

A cashless society results in improved convenience for businesses, consumers, and regulators (Bayero, 2015; Hidayati *et al.*, 2021; Tee & Ong, 2016). Increasingly, consumers find digital money convenient to access as more financial institutions provide digital payment systems, and more businesses accept digital transactions. As markets achieve network scale, the frequency in use of digital money increases, and so consumers' perceptions of the convenience of using cashless means of payment may also rise. Similarly, the greater the use of digital payments, the greater the proficiency in the use of cashless transactions, and the simpler it becomes to use digital money. Besides, companies have improved app interfaces and made instructions for using digital payments clear and understandable, raising consumers' perceptions of the convenience of using digital money (Kusmiarto *et al.*, 2021). Additionally, marketing campaigns by digital money providers (Dwivedi *et al.*, 2021) and businesses adopting digital payments may have contributed to increased public awareness of the suitability of electronic payments for daily life (Mieseigha & Ogbodo, 2013; Tee & Ong, 2016).

Risk

Users may perceive current technologies as increasingly sophisticated (Kuzmin & Menisov, 2021; Suryono, Budi & Purwandari, 2021). As digital technologies become more refined and integrated, they may increase perceptions of their increasing safety (Bayero, 2015; Hidayati *et al.*, 2021; Tee & Ong, 2016). Besides, the government's security regulations are active in preventing potential crime taking place (Hidayati *et al.*, 2021; Honigsberg, 2020; Laut & Narsa, 2021), with efforts to improve the security of fintech services (Suryono, Budi & Purwandari, 2021). On the business side, new technologies supporting cashless services are migrating to new technologies (e.g., blockchain and cloud computing) to keep consumer and business data safe (Hidayati *et al.*, 2021). As consumers feel more confident in the use of technologies, governments are active in regulatory action, and businesses provide more secure systems for consumers, so it is likely that consumers' perceptions of protection in digital environments strengthen.

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

Apart from this, as consumers become more familiar with apps and digital platforms (Almunawar, Anshari & Lim, 2020), the perception of safe navigation on digital platforms may increase. Similarly, as more providers offer digital alternatives and businesses promote cashless transactions, consumers may feel that online transactions are increasingly regulated and protected by state laws. Consumers may then associate lower risk with use of digital payments as the entire digital ecosystem comes to rely more on cashless transactions.

However, public awareness of the importance of handling data safely is vital for lowering the risk of cyber fraud (Purwanegara, Apriningsih & Andika, 2014). If public awareness about data security is low, cyber criminals may find loopholes to carry out crime at large scale (Putnam & Elliott, 1999). If consumers' perceptions of safety are high, but awareness of cyber risk is low, criminals may feel encouragement to employ cyber activities to commit fraud (Archer, 2012). While the risk of crime can be reduced if collaboration between the government, fintech owners, and the community is optimized (Choi, 2021; Kemp, Miró-Llinares & Moneva, 2020), that does not always happen.

Crime threat

Although countries have been progressively linked and become interdependent on digital technologies, the downside is the accompanying increasing incidence of cyber fraud (Hidayati *et al.*, 2021; Kemp, Miró-Llinares & Moneva, 2020; Nawang, 2017). Although the cashless society offers increasing benefits, convenience, and safety for users, it may also open prospects for new types of crime assisted by the Internet. As consumers rely more on digital transactions for daily life, cybercrime is on the ascent. In criminology, the rise of cyber fraud can be explained using the institutional anomie theory (IAT), economic factor theory, or ecological criminology theory.

Anomie refers to a deregulated condition. Rapid and gripping social changes are difficult to navigate (Dearden, Parti & Hawdon, 2021). Conventional norms will blur and disappear as new prospects for development appear (Messner & Rosenfeld, 2012). Anomie occurs in modern society when achieving material success is all that matters. People who have achieved high status or cultural goals are celebrated by the community. Some people may use non-legitimate means to achieve material success (Hövermann, Groß & Messner, 2016). As new technologies expand the borders within which market transactions can take place, new digital environments offer loopholes for individuals to illegitimately profit from unknown or unregulated environments. New technologies are not entirely understood by regulators, business, and consumers.

Another driver of crime is economic inequality (Atems, 2020), which arises in societies with uneven income distribution, or in dense populations due to urbanization, among other factors.

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

Tight economic competition, high unemployment, and gaps in labour skills (Muryani *et al.*, 2021) often push people to look for ways to get by, which sometimes includes committing crimes (Honigsberg, 2020; Smith, 2010; Svabova *et al.*, 2020). The technical complexity of digital transactions, the lack of awareness of consumers about cyber risk, and the lack of digital savviness of the general public may induce individuals to engage in illicit activities. Studies by Campaniello, Gray & Mastrobuoni (2016), Li *et al.* (2019) and Sugiharti *et al.* (2022) suggest that economic development and a rise in income level can be accompanied by growing levels of crime.

We argue that increasing information and telecommunication services, broader access to digital services, and a higher economic level in Indonesia may have encouraged the use of digital technologies among its citizens. As more Indonesians are using digital devices and awareness of the way cybercrime operates is low, it is likely that more space for cybercrime exists. Some of these cybercrimes include phishing, vishing, data breaches, hacking, cyber fraud, identity theft, spamming, cyber stalking, and cyberbullying, among others. However, the three largest cybercrimes reported in Indonesia can be grouped into phishing, distributed denial-of-service (DDoS), and social engineering.

Building on the above literature, three hypotheses are proposed:

H1: Cybercrime related to phishing is positively associated with perceived benefits, convenience, and risk in a cashless society.

H2: Cybercrime related to DDoS is positively associated with perceived benefits, convenience, and risk in a cashless society.

H3: Cybercrime related to social engineering is positively associated with perceived benefits, convenience, and risk in a cashless society.

Research Method

After reviewing the existing literature, this study enquires whether customer perceptions (of benefits, of convenience, and of risk) influence cybercrime. The response variable is cybercrime or fraud (y), which is defined as phishing ($y1$), DDoS ($y2$), and social engineering ($y3$). That is, the model takes the functional relationship of the following form:

$y1$ (phishing) = f(benefits, convenience, risk)

$y2$ (DDoS) = f(benefits, convenience, risk)

$y3$ (social engineering) =f(benefits, convenience, risk).

This research uses data collected through questionnaires. The questionnaires were distributed to 200 victims of cybercrime. As a reference point, the victims of cybercrime in Indonesia

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

reached 3,130 cases in 2020, as reported by the Directorate of Cybercrime (Bareskrim), the Indonesian National Police. The questionnaire covers demographic data (i.e., age, gender, education, location), digital transaction experience, and the perceived benefits, convenience, and risks for digital consumers.

We also propose three blocks of questions to identify whether users have experienced phishing, DDoS, or social engineering. The questionnaire uses a 5-point Likert scale: strongly disagree, disagree, somewhat agree, agree, and strongly agree (Likert, 1932). The operational definitions of the variables are presented in Table 1.

Table 1. Variables' operational definitions and measurements

No.	Variable	Operational Definition	Indicator
1.	Cybercrime (Fraud)	A criminal activity performed through a digital device or computer network as a means, tool, or target (Hidayati *et al.*, 2021).	Phishing DDoS Social engineering
2.	Cashless society	Society brought about by behavioural shifts marked by changes in payment instruments from cash to non-cash (Trinugroho *et al.*, 2017).	Perceived benefits Perceived convenience Perceived risks

This study uses the Structural Equation Modelling (SEM) based on variance as an analytical method. The research data was analyzed using Smart PLS, verified in three stages: measuring the outer model; evaluating the structural model; and testing the research hypothesis.

Results

The analysis starts with the respondents' profiles, then continues with validity and reliability tests and the results from the SEM. The respondents' profiles include gender, age, education, and cybercrime experience. The descriptive respondent profiles are shown in Figure 1.

The SEM test results are as follows. The dimensions are considered reliable if they have a composite reliability value (ρc) above 0.7 (Table 2). The outer model test measures a construct by evaluating the composite reliability value (ρc). Table 3 displays the calculations using composite reliability (ρc).

Table 2. Research Instruments' validity and reliability test results

Variable	Dimension	Items	Correlation (r)		Coefficient	
			r	Status	Alpha	Status
Cybercrime (Fraud) (X1)	Phishing	PH01 – Phishing email or website	0.525	valid	0.827	reliable
		PH02 – Data Scam	0.899	valid		
		PH03 – Fake Accounts Ads	0.937	valid		
		PH04 – Malware (i.e., trojan)	0.934	valid		
	DDoS	DD05 – Freezing, Changing IP Address	0.944	valid	0.865	reliable
		DD06 –Internet bandwidth Attack	0.575	valid		
		DD07 – CPU Overload	0.940	valid		

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

Variable	Dimension	Items	Correlation (r)		Coefficient	
			r	Status	Alpha	Status
		DD08 – Unauthorized System Updates	0.943	valid		
	Social engineering	SE09 – Baiting	0.788	valid	0.813	reliable
		SE10 – Spam and unofficial emails	0.766	valid		
		SE11 – Hack of email, social media and dishonestly used	0.869	valid		
		SE12 – Scams (SMS, Data, mail)	0.783	valid		
Cashless society (Y)	Perceived benefits	PM13 – Effective transactions	0.954	valid	0.873	reliable
		PM14 – Helpful	0.951	valid		
		PM15 – Frequent Use	0.950	valid		
		PM16 – Higher advantages over cash	0.559	valid		
	Perceived convenience	PK17 – Easy to Use	0.961	valid	0.851	reliable
		PK18 – Wider Access and Acceptance	0.961	valid		
		PK19 – Increasingly simple use	0.406	valid		
		PK20 – Easily Available – compatible	0.961	valid		
	Perceived risks	PR21 – Feel Payments are Safe	0.799	valid	0.772	reliable
		PR22 – Protection by state laws	0.777	valid		
		PR24 – Good and Safe Experience	0.741	valid		
		PR24 – Lower Risk than cash	0.771	valid		

Source: Questionnaire data, 2021.

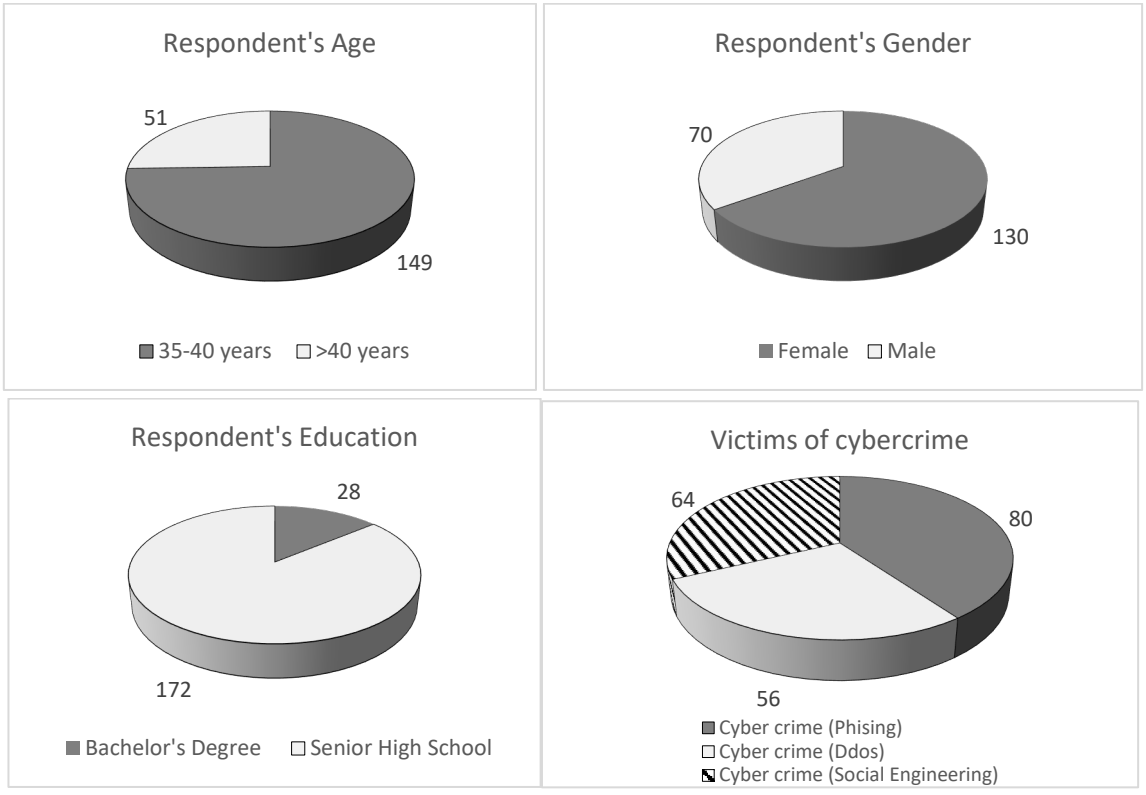

Figure 1. Characteristics of respondents (Source: Questionnaire, 2021)

The calculations that have been carried out find that the R-Square value for the cybercrime variable is greater than 0.2, so the latent predictor has a considerable influence on the structural level. Furthermore, the structural model is evaluated using R-Square for the

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

dependent construct, following the Stone-Geisser Q-Square test for predictive relevance. The inner structural model was also assessed by looking at the Q-Square predictive relevance. The following is the result of the Q-Square calculation.

$$Q2 = 1- (0.968)(0.939)(0.829)$$
$$= 1- 0.753 = 0.246$$

The calculation results show Q-Square value >0, so the model can be considered as having a relevant predictive value.

Table 3. Composite reliability calculation results

Dimension	Composite Reliability	R-Square
Cybercrime (fraud)-Phishing	0.907	0.968
Cybercrime (fraud)-DDoS	0.923	0.939
Cybercrime (fraud)-Social Engineering	0.878	0.829
Cashless society (Benefits)	0.926	-
Cashless society (Convenience)	0.912	-
Cashless society (Risk)	0.848	-

Source: Smart PLS, 2021.

Testing of research hypotheses

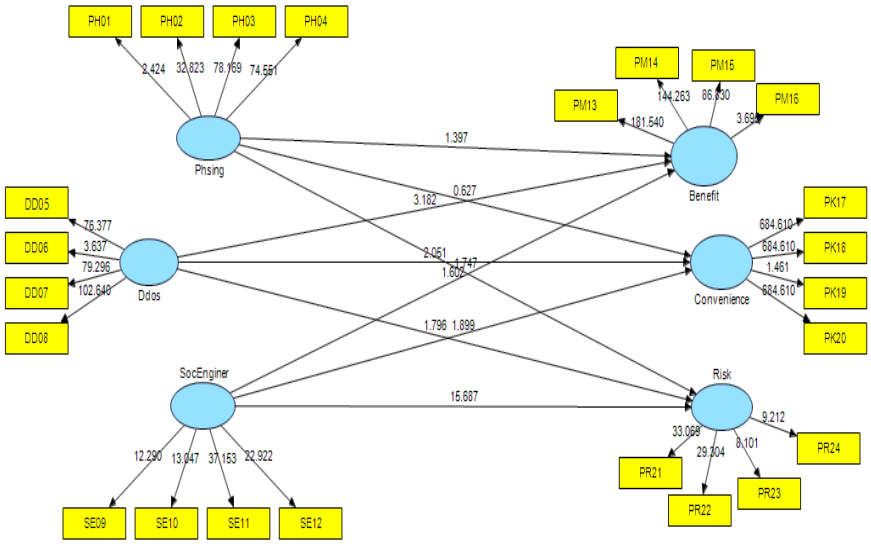

Figure 2. Empirical framework and Data Test Results (Source: Smart PLS, 2021)

Figure 2 depicts the path analysis framework, where we hypothesised that increasing levels of cybercrime (i.e., proposed as phishing, DDoS, and social engineering) are influenced by the growing perception of benefits, convenience, and perception of risk in cashless transactions. Phishing crimes are proxied by four types of phishing, as indicated in Table 2 and depicted in Figure 2 as PH01, PH02, PH03, and PH04. A similar approach follows when asking respondents to identify attacks in the fashion of DDoS (DD05–DD08), and social engineering (SE09–SE12). Similarly, respondents are asked to identify perceptions of the degree of

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

benefits (PM13–PM16), convenience (PK17–PK20), and risk (PR21–PR24) associated with a cashless society.

The hypothesis testing compares the t-count value with the t-table value. If the t-count value is greater than the t-table value, then the relationship between the variables is significant and can be analyzed further. With sample data size 200, the value of the t table (α=5%) obtained was 1,652, and the value of the t table (α=10%) was 1,285. The results of hypothesis testing are presented in Table 4.

Table 4. Hypothesis Testing Results

Hypothesis				coef. Path	t count
	Cybercrime (fraud)-Phishing	→	Cashless society (Benefits)	0.542	1,505**
H1	Cybercrime (fraud)-Phishing	→	Cashless society (Convenience)	0.676	0.672
	Cybercrime (fraud)-Phishing	→	Cashless society (Risk)	0.548	1,752*
	Cybercrime (fraud)-DDoS	→	Cashless society (Benefits)	0.524	3,434*
H2	Cybercrime (fraud)-DDoS	→	Cashless society (Convenience)	0.668	2,199*
	Cybercrime (fraud)-DDoS	→	Cashless society (Risk)	0.559	1,809*
	Cybercrime (fraud)-Social Engineering	→	Cashless society (Benefits)	0.052	1,652*
H3	Cybercrime (fraud)-Social Engineering	→	Cashless society (Convenience)	0.083	1,939*
	Cybercrime (fraud)-Social Engineering	→	Cashless society (Risk)	0.054	17,540*

* Significant at the 5% level. ** Significant at the 10% level.

We proceeded with the hypothesis testing results displayed in Table 4. For each type of cybercrime, we tested three sub-hypotheses related to behavioural aspects of the cashless economy, i.e., the perceived benefits, convenience, and risks.

1a. Perceived benefits (cashless society) have a positive and significant effect on phishing, which means that perpetrators (phishing) take advantage of the increasing perceived benefits of consumers who see cashless transactions as helpful, advantageous, and effective when conducting digital payments. As digital services continue to improve and expand, authorities need to pay closer attention to the risks, as consumers may experience increasing exposure to cybercrime in the form of phishing.

1b. Perceived convenience of digital transactions does not have a significant effect on Phishing. This suggests that cybercrime in the form of phishing does not rise along with the rise in users' perceived convenience.

1c. Perceived risk of digital technologies has a positive and significant effect on phishing. Users' perceived safety is high when they think that the risks of doing an online transaction are low. Phishing takes advantage of this. The absence of safety measures, low awareness of risks, and overconfidence of digital consumers may trigger more phishing activities. The results align with those of earlier studies (Choo, 2011; Nawang, 2017; Purwanegara, Apriningsih & Andika, 2014). Trinugroho *et al.* (2017) argue that

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

regulations should focus on raising users' awareness about risks, especially among ordinary users who often cannot detect them.

2a-b. The perceived benefits and convenience of cashless transactions have positive and significant effects on DDoS. As digital platforms become more sophisticated and financial providers offer more variety of services, users may perceive higher benefits in using such platforms. As consumers increasingly perceive digital services as helpful, advantageous, and efficient, DDoS crime rises.

Unlike phishing, some degree of cooperation is needed for DDoS to happen — e.g., downloading an app, opening and replying to an email, clicking on ads, and providing information to a false source. Consumers' increasing perception of the convenience of digital transactions may encourage them to blindly follow instructions — clicking and downloading quickly when prompted. Once in, criminals interfere and flood the systems, weaken the networks, drain resources, disrupt transactions, block gateways, slow access, steal users' databases, etc. This result is in line with that of a previous study by Dwivedi *et al.* (2021).

2c. Perceived risks have a positive and significant effect on DDoS. The claimed improvements in digital infrastructure (Bayero, 2015), advances in applications (Wang & Ong, 2019; Wohllebe *et al.*, 2021), more 'secure' sites, and 'stricter' regulatory efforts, can shape the perception of low risks among consumers (Aaron, Rivadeneyra & Sohal, 2017; Archer, 2012; Suryono, Budi & Purwandari, 2021). As consumers perceive lower risk in the use of cashless transactions, they provide data more widely when doing digital transactions. However, a higher perception of safety makes consumers more vulnerable to cyberattacks, as it can trigger crime in the form of DDoS. This suggests the need to strengthen the data privacy policy (Lubis & Handayani, 2022) and encourage firms to improve the safety of their services.

Users of e-money in Indonesia were less than 1% of individuals in 2016. However, by 2020, this number had risen to 11.7%. As more users are employing digital payments, greater safety is needed to protect consumers and firms.

3a-b. Perceived benefits and convenience of cashless transactions have a positive and significant effect on social engineering. This means that criminals profit from the rise of perceived benefits and convenience by maliciously acting against consumers' interests in the form of social engineering. Social engineering often employs social media, emails, messaging services, and other means to manipulate users and extract sensitive information from consumers. As cybercrime becomes more sophisticated, the faking of accounts, falsifying of news, and messages from illegitimate sources become increasingly difficult to spot. This type of fraud multiplies with the rapid growth in

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

numbers of social media users, super apps, and other digital interactions experienced in Indonesia.

The regulations governing social media are still few, allowing cybercriminals to engage in malicious actions shaped through human interaction on the Internet. Digital marketing and social applications now offer more benefits for businesses and consumers (Dwivedi *et al.*, 2021; Wohllebe *et al.*, 2021), so social engineering will continue to expand.

3c. Perceived risk has a positive and significant effect on Social Engineering, which means that cybercrime relies on lower perception of risks. The difference is that social engineering may also include that for political purposes, conflicts, violence, chaos, or other sources of social disturbances employing manipulation tactics to influence consumers. Digital readiness among Indonesians is low (Kusmiarto *et al.*, 2021; Nasution *et al.*, 2020; Trinugroho *et al.*, 2017), and the findings suggest the need to tighten regulations, update privacy policies, and promote cyber security protocols to protect consumers.

Discussion

The findings of this research contribute to the literature of the cashless society in Indonesia by providing empirical evidence on the link between cybercrime and consumer perceptions. Our results use primary data collected during the COVID19 pandemic. The findings show that the shift towards a cashless economy has threats and challenges. Perpetrators of cyber crimes will continue to find loopholes in digital systems to take advantage of the rising numbers of digital ecosystems. Authorities need to tighten regulations, and international cooperation may also be required in dealing with cyber security threats (Ajayi, 2016; Aviles, Sitorus & Trujillo Tejada, 2019).

Startups in Indonesia are flourishing, banks are developing cashless services, national authorities are promoting more use of e-money, and super apps are expanding rapidly (Almunawar, Anshari & Lim, 2020; Fauzi & Sheng, 2020). To facilitate the thriving of digital businesses, and to guarantee digital users' safety, government regulations and mechanisms to monitor, prevent, and prosecute cyber crime need to be in place (Choo, 2011). Research in China (Chang *et al.*, 2016), Europe (Kemp, Miró-Llinares & Moneva, 2020), and other countries (Tee & Ong, 2016) has shown that providing safe regulatory frameworks can substantially influence the adoption of digital services.

The expansion of digital business in Indonesia needs to be supported with a more secure environment by strengthening digital readiness (Nasution *et al.*, 2020), improving digital

Copyright © 2022
http://doi.org/10.18080/jtde.v10n3.533

strategy (Mihardjo *et al.*, 2019), increasing digital infrastructure (Kusmiarto *et al.*, 2021), and providing a more comprehensive regulatory framework (Suryono, Budi & Purwandari, 2021).

Although the number of consumers using the Internet for financial transactions in Indonesia is relatively low (around 14% of the total users), it is rapidly increasing. The use of e-money increased from less than 5% in 2018 to 11.7% in 2020. Digital transactions increased by nearly 45% and e-money use by 50% during the first year of the COVID19 pandemic. With the containment measures to minimize the virus spread, users relied much more on online transactions. Consumer behaviour is likely to remain after the COVID19 pandemic, suggesting that the more consumers use digital apps, the more they perceive the benefits, which may trigger more cyber-criminal activities.

Conclusions

This study examines the relationship between cybercrime and cashless transactions. We used data from a survey of 200 respondents in 2021 to test a set of hypotheses relating to cybercrime and perceived benefits, convenience, and risks using Structural Equation Modelling (SEM). The results show that cybercriminals benefit from the increasingly perceived benefits, convenience, and safety of cashless transactions. Cybercrime in the form of phishing, DDoS, and social engineering is triggered by the perceived benefits, convenience, and risks associated with a cashless society. DDoS and social engineering are also positively and significantly associated with the perceived benefits of digital transactions. As social media, super apps, digital banking, and other digital services become increasingly popular and part of daily life, new security frameworks are needed to protect users' safety. Cybercrime is becoming more sophisticated, taking advantage of consumers' growing interest in using cashless services. We envisage that cybercrime targeting devices, the Internet, and digital technologies will expand as technological development and cashless transactions grow. The data suggests that consumers may not be aware of the risks associated with cybercrime and that the rapid growth of digital technologies will put them at higher risk. Most cybercrimes most likely go unreported, as the survey indicates that most individuals suffer from cybercrime or are exposed to it.

Acknowledgments

This work was supported by Universitas Airlangga, Surabaya, Indonesia, through Hibah "Riset Mandat 2022".

Copyright © 2022

References

Aaron, M., Rivadeneyra, F., & Sohal, S. (2017). *Fintech: Is This Time Different?: A Framework for Assessing Risks and Opportunities for Central Banks*. Bank of Canada. https://doi.org/10.34989/sdp-2017-10

Abad-Segura, E., González-Zamar, M. D., López-Meneses, E., & Vázquez-Cano, E. (2020). Financial Technology: Review of trends, approaches and management. *Mathematics*, *8*(6), 1–36. https://doi.org/10.3390/math8060951

Akamai International. (2013). Akamai's State of the Internet. [online] Available at: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q4-2013state-of-the-internet-connectivity-report.pdf [accessed 16.02.2022]

ACFE. (2018). Global Study on Occupational Fraud and Abuse. *Association of Certified Fraud Examiners*, *10*, 80.

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1–12. https://doi.org/10.5897/jiis2015.0089

Almunawar, M. N., Anshari, M., & Lim, S. A. (2020). Customer acceptance of ride-hailing in Indonesia. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/JSTPM-09-2019-0082

Archer, N. (2012). Consumer identity theft prevention and identity fraud detection behaviours. *Journal of Financial Crime*. https://doi.org/10.1108/13590791211190704

Astuti, S. A. (2020). Era disrupsi teknologi 4.0 dan aspek hukum perlindungan data hak pribadi. *PAJOUL (Pakuan Justice Journal Of Law)*, *01*(01), 1–32.

Atems, B. (2020). Identifying the Dynamic Effects of Income Inequality on Crime. *Oxford Bulletin of Economics and Statistics*, *82*(4), 751–782. https://doi.org/10.1111/obes.12359

Aviles, A. M., Sitorus, D., & Trujillo Tejada, V. P. (2019). *Advancing Digital Financial Inclusion in ASEAN: Policy and Regulatory Enablers*. The World Bank. http://documents.worldbank.org/curated/en/856241551375164922/Advancing-Digital-Financial-Inclusion-in-ASEAN-Policy-and-Regulatory-Enablers

Bank Indonesia (2021), Retrieved from Financial Statistics. https://www.bi.go.id/en/statistik/ekonomi-keuangan/ssp

Bayero, M. A. (2015). Effects of Cashless Economy Policy on Financial Inclusion in Nigeria: An Exploratory Study. *Procedia - Social and Behavioral Sciences*, *172*, 49–56. https://doi.org/10.1016/j.sbspro.2015.01.334

BSSN, 2020. Retrieved from https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Campaniello, N., Gray, R., & Mastrobuoni, G. (2016). Returns to education in criminal organizations: Did going to college help Michael Corleone? *Economics of Education Review*, *54*, 242–258. https://doi.org/10.1016/j.econedurev.2016.03.003

Chang, Y., Wong, S. F., Lee, H., & Jeong, S. P. (2016). What motivates Chinese consumers to adopt FinTech services: A regulatory focus theory. *Proceedings of the 18th Annual*

Copyright © 2022

International Conference on Electronic Commerce: E-Commerce in Smart Connected World, 1–3. https://doi.org/10.1145/2971603.2971643

Choi, K. (2021). The Driving Force Behind Cybercrime: Cyber Resilience and Cybercriminology. *Journal of Contemporary Criminal Justice*, *37*(3), 308–310. https://doi.org/10.1177/10439862211001631

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. https://doi.org/10.1016/j.cose.2011.08.004

Dearden, T. E., Parti, K., & Hawdon, J. (2021). Institutional Anomie Theory and Cybercrime—Cybercrime and the American Dream, Now Available Online. *Journal of Contemporary Criminal Justice*, *37*(3), 311–332. https://doi.org/10.1177/10439862211001590

Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A. S., Kumar, V., Rahman, M. M., Raman, R., Rauschnabel, P. A., Rowley, J., Salo, J., Tran, G. A., & Wang, Y. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management*, *59*(June 2020), 102168. https://doi.org/10.1016/j.ijinfomgt.2020.102168

Esquivias, M. A., Sugiharti, L., Jayanti, A. D., Purwono, R., & Sethi, N. (2020). Mobile Technologies, Financial Inclusion and Inclusive Growth in East Indonesia. *Journal of Telecommunications and the Digital Economy*, *8*(2), 123–145. https://doi.org/10.18080/jtde.v8n2.253

Economist, 2021. Retrieved from https://www.economist.com/international/2021/05/06/new-technology-has-enabled-cyber-crime-on-an-industrial-scale

Fauzi, A. A., & Sheng, M. L. (2020). Ride-hailing apps' continuance intention among different consumer groups in Indonesia: The role of personal innovativeness and perceived utilitarian and hedonic value. *Asia Pacific Journal of Marketing and Logistics*. https://doi.org/10.1108/APJML-05-2019-0332

Financial Inclusion Insights (2021). Retrieved from http://fii-website.staging.interactive.columnfivemedia.com/blog.php?country=37

Hidayati, A. N., Riadi, I., Ramadhani, E., & Amany, S. U. Al. (2021). Development of conceptual framework for cyber fraud investigation. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, *7*(2), 125–135. https://doi.org/10.26594/REGISTER.V7I2.2263

Hill, J. B., & Marion, N. E. (2016). *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. Praeger Security International.

Honigsberg, C. (2020). Forensic Accounting. *Annual Review Of Law and Social Science*, 423–431. https://doi.org/10.1016/B978-0-12-382165-2.00218-X

Hövermann, A., Groß, E. M., & Messner, S. F. (2016). Institutional imbalance, integration into Non-economic institutions, and a marketized mentality in Europe: A multilevel, partial elaboration of Institutional Anomie Theory. *International Journal of Comparative Sociology*, *57*(4), 231–254. https://doi.org/10.1177/0020715216667452

Copyright © 2022

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3), 293–312. https://doi.org/10.1007/s10610-020-09439-2

Kusmiarto, K., Aditya, T., Djurdjani, D., & Subaryono, S. (2021). Digital Transformation of Land Services in Indonesia: A Readiness Assessment. *Land*, *10*(2), 120. https://doi.org/10.3390/land10020120

Kuzmin, V., & Menisov, A. (2021). An approach to identifying threats of extracting confidential data from automated control systems based on internet technologies. *Business Informatics*, *15*(3), 35–47. https://doi.org/10.17323/2587-814X.2021.3.35.47

Laut, I. M. M. J., & Narsa, I. M. (2021). The Importance of Forensic Tax and Accounting Knowledge to Prevent Fraud in New Normal Era. *Journal of Hunan University (Natural Sciences)*, *48*(2), 101–112.

Li, J., Wan, G., Wang, C., & Zhang, X. (2019). Which indicator of income distribution explains crime better? Evidence from China. *China Economic Review*, *54*, 51–72. https://doi.org/10.1016/j.chieco.2018.10.008

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*.

Lubis, M., & Handayani, D. O. D. (2022). The relationship of personal data protection towards internet addiction: Cyber crimes, pornography and reduced physical activity. *Procedia Computer Science*, *197*, 151–161. https://doi.org/10.1016/j.procs.2021.12.129

Malesev, S., & Cherry, M. (2021). Digital and Social Media Marketing — Growing Market Share for Construction SMEs. *Construction Economics and Building*, *21*(1), 65–82. https://doi.org/10.5130/AJCEB.v21i1.7521

Messner, S. F., & Rosenfeld, R. (2012). *Crime and the American dream*. Cengage Learning. https://doi.org/10.4135/9781446270097

Mieseigha, E. G., & Ogbodo, U. K. (2013). An empirical analysis of the benefits of cashless economy on Nigeria's economic development. *Research Journal of Finance and Accounting*, *4*(17), 11–16.

Mihardjo, L. W. W., Sasmoko, Alamsjah, F., & Elidjen. (2019). Digital transformation: A transformational performance-based conceptual model through co-creation strategy and business model innovation in the Industry 4.0 in Indonesia. *International Journal of Economics and Business Research*, *18*(3), 369–386. https://doi.org/10.1504/IJEBR.2019.102736

Muryani, Esquivias, M. A., Sethi, N., & Iswanti, H. (2021). Dynamics of Income Inequality, Investment, and Unemployment in Indonesia. *Journal of Population and Social Studies*, *29*, 660–678. https://doi.org/10.25133/JPSSv292021.040

Nasution, R. A., Arnita, D., Rusnandi, L. S. L., Qodariah, E., Rudito, P., & Sinaga, M. F. N. (2020). Digital mastery in Indonesia: The organization and individual contrast. *Journal of Management Development*, *39*(4), 359–390. https://doi.org/10.1108/JMD-03-2019-0081

Nawang, N. I. (2017). Combating anonymous offenders in the cyberspace: An overview of the legal approach in Malaysia. *2017 2nd International Conference on Anti-Cyber Crimes,*

Copyright © 2022

ICACC 2017, August 1996, 13–18. https://doi.org/10.1109/Anti-Cybercrime.2017.7905255

Njanike, K., Mutengezanwa, M., & Gombarume, F. B. (2011). Internal Controls in Ensuring Good Corporate Governance in Financial Institutions. *Annals of the University of Petrosani - Economics*, *11*(1), 187–196.

Office for National Statistics. (2022). Crime in England and Wales: year ending March 2022. Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2022

Prabowo, H. Y. (2012). A better credit card fraud prevention strategy for Indonesia. *Journal Of Money Laundering Control*. https://doi.org/10.1108/13685201211238034

Purwanegara, M., Apriningsih, A., & Andika, F. (2014). Snapshot on Indonesia Regulation in Mobile Internet Banking Users Attitudes. *Procedia - Social and Behavioral Sciences*, *115*, 147–155. https://doi.org/10.1016/j.sbspro.2014.02.423

Putnam, T. L., & Elliott, D. D. (1999). To Cyber Crime. *Terrorism*, 35–67.

Ruiz-Real, J. L., Uribe-Toril, J., Torres, J. A., & Pablo, J. D. E. (2021). Artificial intelligence in business and economics research: Trends and future. *Journal of Business Economics and Management*, *22*(1), 98–117. https://doi.org/10.3846/jbem.2020.13641

Salman, M., & Saleem, I. (2017). Role of digital competence in cashless economy. *IOSR Journal of Business and Management (IOSR-JBM)*, *19*(11), 49–53. https://doi.org/10.9790/487X-1905064953

Smith, R. G. (2010). *Identity theft and fraud*. In Jewkes & Yar (Eds.), *Handbook of internet crime*. Routledge.

Sugiharti, L., Esquivias, M. A., Shaari, M. S., Agustin, L., & Rohmawati, H. (2022). Criminality and Income Inequality in Indonesia. *Social Sciences*, 11(3), 142. https://doi.org/10.3390/socsci11030142

Suryono, R. R. (2019). Financial Technology (Fintech) Dalam Perspektif Aksiologi. *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *10*(1), 52. https://doi.org/10.17933/mti.v10i1.138

Suryono, R. R., Budi, I., & Purwandari, B. (2021). Detection of fintech P2P lending issues in Indonesia. *Heliyon*, *7*(4), e06782. https://doi.org/10.1016/j.heliyon.2021.e06782

Svabova, L., Kramarova, K., Chutka, J., & Strakova, L. (2020). Detecting earnings manipulation and fraudulent financial reporting in Slovakia. *Oeconomia Copernicana*, *11*(3), 485–508. https://doi.org/10.24136/OC.2020.020

Tee, H.-H., & Ong, H.-B. (2016). Cashless payment and economic growth. *Financial Innovation*, *2*(1), 4. https://doi.org/10.1186/s40854-016-0023-z

Teja, A. (2017). *Indonesian Fintech Business: New Innovations or Foster and Collaborate in Business Ecosystems? 2. Literature Study and Hypothesis Development*. *10*(1), 10–18. https://doi.org/10.12695/ajtm.2017.10.1.2

Thaichon, P., Soutar, G., & Weaven, S. (2021). Guest Editorial: Technologies and Relationship Marketing. *Australasian Marketing Journal*, *29*(2), 109–110. https://doi.org/10.1177/1839334921994387

Copyright © 2022

Trinugroho, I., Sawitri, H. S. R., Toro, M. J. S., Khoiriyah, S., & Santoso, A. B. (2017). How Ready Are People for Cashless Society? *Jurnal Keuangan Dan Perbankan*, *21*(1), 105–112. https://doi.org/10.26905/jkdp.v21i1.1231

Wang, G., & Ong, Y. B. O. (2019). Analysis the use of P2P lending mobile applications in Indonesia. *Journal of Physics: Conference Series*, *1367*(1), 012006. https://doi.org/10.1088/1742-6596/1367/1/012006

Wohllebe, A., Hübner, D. S., Radtke, U., & Podruzsik, S. (2021). Mobile apps in retail: Effect of push notification frequency on app user behavior. *Innovative Marketing*, *17*(2), 102–111. https://doi.org/10.21511/im.17(2).2021.10

Copyright © 2022