

Cyber Crime and The Use of Internet Banking in The Community of Denpasar City

Desak Made Sukarnasih¹, Desak Ayu Sriary Bhegawati²

¹Universitas Pendidikan Nasional Denpasar, Indonesia

²Universitas Mahasaraswati Denpasar, Indonesia

Correspondent: desak.bhegawati@gmail.com²

Received : May 23, 2023

Accepted : July 19, 2023

Published : July 31, 2023

Citation: Sukarnasih, D, M., & Bhegawati, D, A, S. (2023). Cyber Crime Use of Internet Banking in Denpasar City Community. Ijomata International Journal of Management, 4(3), 318-328.
<https://doi.org/10.52728/ijjm.v4i3.804>

ABSTRACT: The three objectives of this study were to determine: 1) the effects of internet banking on cybercrime in Denpasar City; 2) the effects of consumer protection for users of internet banking facilities on cybercrime in Denpasar; and 3) the effects of both the use of internet banking and consumer protection for users of internet banking facilities on cybercrime in Denpasar. This is a quantifiable research with population comprising the residents of Denpasar. The information was collected through a survey with 150 respondents using an unintentional selection technique. To evaluate the data collection, the traditional premise test, the multiple linear regression analysis, the coefficient of determination test (R^2), and the hypothesis test (F-test and t-test) were all implemented. The outcome demonstrates: 1) The use of internet banking positively impacts cybercrime in Denpasar. 2) Consumer protection for users of internet banking facilities positively impacts cybercrime in Denpasar. 3) The use of internet banking positively impacts both consumer protection for users of internet banking facilities and cybercrime in Denpasar.

Keywords: Cyber Crime, Customer Protection, Internet Banking Facility



This is an open access article under the CC-BY 4.0 license

INTRODUCTION

In this globalization era, business competition among organizations is getting tougher. Companies must create high-quality products in order to compete. Various new business opportunities, including the increased internet-based business operations have been developed by utilizing sophisticated technological advances. The creation of the necessary goods and services is greatly influenced by the technological advances in all aspects of human life. The internet is one of the most modern innovations ever invented. In Banking sector, for instance, the implementation of technological advances has greatly contributed to the improved qualities and services, one of which is the use of internet. Digital-based accounting information systems will undoubtedly be affected by the growth and increasing use of the internet (Fletcher & Griffiths, 2020; Iivari et al., 2020; Klein & Todesco, 2021; Sun & Guo, 2022). The improvement of the performance of banking

itself is achieved in the banking industry through the creation of digitally-based financial information systems. Internet banking, which is commonly used for both internal and external financial requirements, was made possible by the technological integration of accounting information systems. The availability of online banking services has improved relationships among not only the existing banks, but also among clients and customers. Nevertheless, the easy access of online banking can lead to a number of risks, one of which is cybercrime. It is detected that cybercrime is impacted by the massive use of online commerce and transactions. The more consumers using online financial services, the more likely the cybercrime occurs ([Alshurideh, 2022](#)). Hence, banks should ensure the security for clients who use online banking services for various transactions.

Today's technology utilizes a lot of internet usage. The banking industry has adapted to the emergence of internet technologies. One of the latest developments in bank services, internet banking, has shifted the banking industry's business strategy from human-based technology to information-based technology. Currently, it is impossible to separate technology from people's life, particularly while pandemic was intensifying. In fact, the early 2022 pandemic has triggered the increasing use of internet for both personal and professional lives. As pandemic is waning technology serves as a basic requirement ([Jashinsky et al., 2021](#); [Partelow et al., 2023](#); [Pekkola et al., 2021](#); [Venkatesh, 2020](#)). Before the pandemic and the rise of technology, most financial transactions were carried out conventionally. Overtime, spurred on by a pandemic, an increasing number of banking institutions are implementing and improving their services by creating new innovation: internet banking services. Internet banking is a strategy in Banking businesses to meet the demands of the modern society for the practical yet useful services. Technology is indeed a vital necessity in pandemic situations ([Naeem & Ozuem, 2021](#)). When a number of financial transactions were still carried out manually, technology then took over the business activities and became intensified during and after the epidemic. It is a common practice in banking institutions to adopt and improve their services by providing new innovations, such as internet banking services. Therefore, the availability of Internet banking is considered crucial in response to the demands of modern society for practical and useful services, and becomes one of the banking strategies in order to compete ([Hassan & Farmanesh, 2022](#); [Pai et al., 2022](#)).

The banking business centers offer clients the online banking services with legal guarantees in two different ways, both implicitly and explicitly ([Rodrigues et al., 2022](#)). The Bank of Indonesia with its regulation No. 9/15/PBI 2007 emphasized the instructions for institutions on how to secure their information system technology. The laws issuance is to safeguard customers from cybercrime when using online banking services, as the activity has an impact on cybercrime ([Hasbullah, 2022](#)). Cybercrime is triggered by easy access to online banking and a weak security system for customers. Trojan horses and man-in-the-middle attacks are two types of threats to people who use and provide internet banking, and this is caused by poor security service. Attackers perform man-in-the-middle assaults by building a website and convincing users to join. Trojan horses are fake programs used for malicious reasons and inserted into frequently used programs. Since they are hidden, Trojan horses differ from other harmful viruses ([Ngo et al., 2020](#)). To prevent this from recurring, it is suggested that the Bank of Indonesia carry out evaluation system regarding the banks transactions within a specific time frame in the form of bank supervision ([Irawati et al., 2019](#); [Khan et al., 2015](#); [Okafor et al., 2020](#); [Pantea et al., 2014](#)). Currently, the online banking

system in Denpasar has experienced a hacking threat. As reported by the Financial Services Authority (OJK), 300 customers suffered losses with a total of IDR 130 billion in 2017. In addition, more than 100 clients of three prominent Indonesian banks whose accounts compromised had filed grievances to OJK in 2018. The total losses amounted to IDR 2 billion. It is detected that a virus is inserted by a hacker for the purpose of stealing the money. Every time an online financial service is accessed, the virus is activated. In response to the ongoing matters, OJK requested that banks improve the IT security.

Compared to other routes, Internet banking offers a cost-effective alternative, which is the lowest in percentage, as the operating costs can be reduced up to 79 percent. The availability of online banking services has made a variety of conveniences possible, including the flexibility and simplicity with which transactions may now be conducted between banks and their clients, banks and its businesses, banks to other banks, and clients to clients (Giri et al., 2017; Usman et al., 2020). Customers will find it simpler to execute financial operations without direct visit to the bank. The ease to the different internet banking features access is granted. Internet banking, supported by a robust cyber security system, offers rapid, convenient, and safe access to banking operations with computer networks, in addition to the numerous services previously mentioned. This helps guarantee the privacy and security of clients' data and financial transactions. Additionally, the availability of online banking allows banks to offer better services by speeding up service, broadening the scope of services, and reaching more people with various financial activities (Javaid et al., 2022). Bench Council Transactions on Benchmarks, Standards and Evaluations are the hazards associated with utilizing internet banking, despite the ease it offers clients. Numerous legal infractions involving the personal data of customers are among the possible risks to take. Banks customers who utilize online banking are prone to financial risks in addition to concerns relating to personal data (Qi et al., 2020). Perpetrators of banking crimes impacted the use and users of online banking. This typical criminal act referred to as "cyber crime," and involves the use of sophisticated information technology and computers by offenders in the commission of crimes including terrorism and money laundering. It is apparent that Indonesia is one of the countries having been affected by the intensified cybercrimes. According to Danuri and Suharnawi (2017), Indonesia becomes the world's top two significant targets of internet criminal assaults and is a nation with the highest risk of information technology security attacks.

The Technology Acceptance Model (TAM) is a hypothesis about the usage of information technology systems that is extremely influential and frequently used to explain why different people accept the use of different IT systems. The Theory of Reasoned Action (TRA) model, which was created by Fishbein and Ajzen, is the theory of reasoned action that the TAM model is based on (Jogiyanto, 2007). This theory seeks to identify the behaviors that computer users exhibit. According to Kamus Besar Bahasa Indonesia (an Indonesian dictionary), *method of use* is a process that involves the use of a certain thing. Internet banking is a bank feature added to the Banks websites which functions not only to provide information about their products or services but also to allow customers to access their accounts, transfer money, and buy financial products and services online (online banking transactions). (Adiandari et al., 2020). McKeown defines information technology as any technology used to produce, store, modify, or utilize information in various forms. Information technology is a generic term that refers to any technology that aids in the generation, manipulation, storage, communication, and/or transmission of information.

Information and communication technology is sometimes defined as everything that facilitates the collection, the processing, the retrieval, the transmission, the delivery, and the information reception ([Chen, 2022](#))

Internet banking is the only banking service that utilizes communication and information technology, including mobile banking (transactions using a handphone), SMS banking, and telephone banking ([Ghelani et al., 2022](#)). Consumer protection is a strategy used to build consumer confidence and comfort while doing online transactions. Another viewpoint, however, holds that all efforts made by specific financial institutions are directed toward protecting the interests of their customers ([Park & Kim, 2020](#)). The following are the service facilities offered: Inter-account transfers, domestic interbank transfers, and planned transfer lists are examples of fund transfers. The payments for bills such as Telkom (Home Telephone Services) and CDMA phones, GSM phones, internet, cable TV, credit cards, power, installments, insurance, education, airfare, and other transactions ; purchases, such as credit for CDMA and GSM phones, tickets, and time deposits; Account and credit card information which includes savings and current accounts, balances, transaction history, a list of accounts, deposit accounts, loan accounts, and Visa card information; Check status, SMS notification service, interest rate information, and exchange rate information are a few examples of available service facilities ([Zhai et al., 2019](#)). According to ([Drew, 2020](#); [Franjić, 2020](#); [Piasecki et al., 2021](#)), "cybercrime" is any kind of computer networks use for motives of crimes and/or high-tech crimes by abusing the ease of digital technology. Cybercrime is a recent phenomenon in crime as a direct impact of the development of information technology. Moreover, it is a type of crime related to the utilization of unlimited information technology and has strong characteristics with technological engineering that relies on a high level of security and credibility of information submitted and accessed by internet customers ([Drew, 2020](#)).

METHOD

When a survey for this study was conducted, it was reported by denpasarkota.go.id that there were an estimation of 176,156 population living in Denpasar City . Using the accidental sampling approach, 150 respondents made up the sample size. A quantitative data is employed and the primary data served as the source of the study. The data collection method was through the distribution of a questionnaire to the residents of South Denpasar, whereas the validity and the reliability tests were conducted to determine whether or not the assertions on the questionnaire were true. Furthermore, the classical assumption testing, the multiple linear regression analysis, the coefficient of determination testing (R²), the F-testing, and t-testing are the analysis approaches. Since the sig value for each variable in this study was less than 0,05, all variables were considered valid, and passed the validity test. It may be deduced that this research instrument is dependable and has passed the reliability test since the Cronbach's alpha value of all independent and dependent variables is above 0,6.

The one-sample Kolmogorov-Smirnov test technique yielded a normality test result of 0,973 and an Asym. Sig (2-tailed) of 0,300. The significance value of 0,300 > 0,05 (5%), indicates that the data in this study are regularly distributed data, thus the conclusion drawn is that the data employed

in the regression equation are normally distributed data. The independent variables for both Internet Banking Users and Customer Protection of Internet Banking Facility Users had significant values of 0,210 and 0,053, respectively, this is in line with the heteroscedasticity test. All significant values of the variables exceed the level of significance, which is 5% (0,05). Therefore, it may be stated that this regression model does not exhibit heteroscedasticity symptoms. The tolerance value for the two independent variables is 0,994, which is more than or equal to 0,10, and the VIF coefficient for the two independent variables is 1,006 (10). Hence, it can be concluded that there are no multicollinearity issues with the regression equation used in this work.

RESULTS AND DISCUSSIONS

By assessing the coefficient of determination, F statistical value, and t statistical value, the model feasibility test demonstrates the precision of the sample regression function in the calculation of the accrual value. The adjusted R square is used to measure the coefficient of determination. The following table shows the findings of the coefficient of determination analysis:

Table 1 Coefficient of Determination Test Results

Model	R	R Square	Adjusted R Square	Std.Error of the Estimate
1	0,783	0,769	0,754	2,5759

Source: Data processed (2023)

The Adjusted R Square (R^2) value of 0,754 demonstrates the variable contribution of Internet Banking Users and Customer Protection of Internet Banking Facility Users. This indicates that the variance in Internet Banking Users and Customer Protection of Internet Banking Facility Users may account for 22,80% of the variation in cybercrime, while the remaining 77,20% is explained by other factors and variables outside this study model.

Table 2 F Test Results (Simultaneous test)

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	204,537	2	104,312	14,415	0,000
Residual	624,126	147	5,621		
Total	828,663	149			

Source: Data processed (2023)

By comparing the significance threshold of 0,05, the F test is used. H1 is rejected if the probability value is greater than 0,05 but acceptable if it is less than 0,05. The following table shows the

outcomes of the F statistical test. The F-test value of 14,415 with a significance of 0,000 indicates that the standard of financial reporting at LPDs in Denpasar City is concurrently influenced by leadership ethics, supervisory body functions, work experience, and the degree of accounting comprehension. When there are several independent variables and more than one dependent variable in a regression equation, the term "multiple linear regression" is used. According to (Sugiyono, 2017), this analytical method is utilized to ascertain the relationship between the independent and dependent variables.

Table 3 Multiple Linear Regression Test Results

Model	Non-standardized Coefficients		Standardized Coefficients	t	Sig
	B	Std Error	Beta		
Constant	6,734	2,924		1,827	0,000
Internet usage Banking	0,023	0,038	0,202	2,413	0,009
Customer Protection	0,325	0,065	0,440	5,223	0,000

Source: Data processed (2023)

$$\text{Cyber Crime} = 6,734 + 0,023 \text{ Internet usage Banking} + 0,325 \text{ Customer Protection} + e_i \dots (1)$$

The impacts of Internet Banking Use on cybercrime in Denpasar Community

From the study findings, it is emphasized that the use of Internet banking has a substantial favorable impact on cybercrime in Denpasar. This is demonstrated by the statistical analysis of Internet banking usage, which has a coefficient value of 0,023 (positive) and a significant probability value of 0,009 less than 0,05. Consequently, it may be said that H1 in this investigation is accepted. The use of Internet banking has a substantial impact on cybercrime due to a number of factors. Additionally, the increase of cybercrime in financial sectors occur, not only because of the emergence of sophisticated apps but also because of the conventional and ineffective transaction methods. Trenn utilizes the increased financial transactions, which contributes to an increase in cybercrime in this sector (Okpa et al., 2020). Banking cybercrime has intensified through the ever increasing use of complex applications. In addition, the massive use of mobile wallets has an impact on the rising trend of using financial transactions features (Jameel & Alheety, 2022) and this reflects customers' perceptions and behavioral intentions regarding mobile banking usage. In 2022, the International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT) IEEE highlighted such issues. Since payments may now be done online through mobile banking, internet banking, and internet banking, payment transactions that are conducted by the general public will no longer be carried out conventionally (Thirupathi et al., 2019). Today, payments are mostly made online through ATMs, convenience shops that accept such payments, mobile banking, internet banking, and ATMs (Yadav & Shaikh, 2023). The

various payment options is a result of the increasing number of people utilizing mobile wallets. Today, instead of going to certain public services to pay the bills and to purchase necessities, people make payments online using the available payment facilities and providers. As a consequence, cybercrimes will be detected as common and unavoidable occurrences. The findings of this study emphasized that there is a greater danger of crimes in financial institutions than in other organizations ([Akartuna et al., 2022](#)). The more clients or customers access internet banking services, the bigger the chances for cyber perpetrators to commit crimes. Given that the current era is the digital era, a growing number of individuals are taking advantage of their knowledge of technology, yet, others abusing it in various ways. The findings of H1 are consistent with the number of earlier researches, including the studies conducted by ([Ali, 2019](#)) and ([Abbas et al., 2023](#)).

The Impacts of Customer Protection For Internet Banking Users towards Cyber Crime in the Community of Denpasar

Based on the findings, it can be concluded that cybercrime in Denpasar has been significantly and positively impacted by the protection for the users of internet banking facility. This is demonstrated by the statistical analysis of the Protection of Internet Banking Facility for the users, which has a coefficient value of 0,325 and a significant probability value of 0,000 which is less than 0,05. As a result, it can be stated that H2 in this investigation is valid. Customers Protection on the use of Internet Banking facility has a significant and positive Impact on Cybercrime. With the increasing awareness from customers and the efforts from the banks to maintain the confidentiality of any information pertaining to depositors and their savings, such crimes can be minimized. The term "bank secrecy," which refers to all information pertaining to depositors and their deposits, also covers all details pertaining to individuals and organizations that obtain the supply of services and services in the transportation of money. The terms and conditions section with all the rights and duties of the parties, primarily banks and consumers, and are legally competent to ensure the complete security for the users of internet banking applications. The bank prioritizes the rights of the bank and the duties of the customer rather than the rights of the customer and the obligations of the bank itself in the explanation of these terms and conditions, which is a typical agreement signed in by the business actor or bank ([Shokuhi et al., 2019](#)). It is crucial to further discuss about customer protection in future studies, especially the legal protection as it is the right of customers to have a sense of security from cybercrime threats, to ensure that there are no longer errors made by both the customers and the bank, and so forth. Hence, the findings of H2 in this study are consistent, and in line with the results from the earlier researches conducted by ([Setiawati et al., 2019](#)) and ([Hatta et al., 2018](#)).

Furthermore, from the study findings, cybercrime in Denpasar is significantly reduced if customers are protected when using internet banking services. This is demonstrated by statistical analysis with a coefficient value of 14,415 and a significant probability value of 0,000 less than 0,05. Therefore, it may be emphasized that H3 in this study is acknowledged. The use of Internet banking and the customer protection for users of Internet banking facility have a positive impact on the reduced cybercrime. In practice, cybercrime must be prevented by ensuring the safety and security of transaction data against any intervention, tapping, or theft from anybody ([Liyanaarachchi et al., 2021](#)). It is also necessary to secure the data and information of bank clients who use internet

banking services. If governed by rules or regulations, the protection of transaction data and consumers will be more effective and the legal force can be set up clearer.

CONCLUSIONS

It can be inferred from this study that the protection towards the users of Internet banking has a substantial impact on a reduced cybercrime in the Denpasar community. This is proven by the findings of the data analysis and the results of the discussion. In fact, conventional ways of purchasing and paying items have gradually been replaced by online transactions, be it via mobile banking, internet banking, ATMs, and convenience stores with such facilities. Consequently, the transactions triggers the prevalence of cybercrime. Cybercrime rates in Denpasar community has gradually declined, and this can be realized since a better customer protection for users of internet banking facilities is implemented. Moreover, the Bank secrecy that refers to all information pertaining to depositors and their deposits as well as to individuals and companies that seek the provision of services in the transportation of money should be well-maintained. In Denpasar region itself, the use of Internet banking supported by the customer protection for the users has significantly lowered the cybercrime rates. The success of cybercrime prevention can be supported through the safety of bank transactions and the security from tampering, tapping, or theft. Hence, Banks should ensure stricter supervision to combat cybercrime. To enhance the quality of future research, it is also advised that study variables be added so as to address other issues of legal or governmental protection, in addition to the security and consumer protection.

REFERENCES

- Abbas, T., Officer, S., Affairs, C., Limited, A. S., Arif, K., & Lumpur, K. (2023). End-users. In *Perception of Cybercrimes towards E-banking Adoption and Retention* (Vol. 1, pp. 89–97). <https://doi.org/10.31645/JISRC.23.21.1.10>
- Adiandari, A., Winata, H., Fitriandari, M., & Hariguna, T. (2020). Improving the quality of Internet banking services: An implementation of the quality function deployment (QFD) concept. *Management Science Letters*, *10*(5), 1121–1128.
- Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting and Social Change*, *179*, 121632.
- Ali, L. (2019). Cyber crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC). *The Journal of Developing Areas*, *53*(1).
- Alshurideh, M. (2022). Does electronic customer relationship management (E-CRM) affect service quality at private hospitals in Jordan? *Uncertain Supply Chain Management*, *10*(2), 325–332.
- Chen, X. (2022). Machine learning approach for a circular economy with waste recycling in smart cities. *Energy Reports*, *8*, 3127–3140.

- Danuri, M., & Suharnawi. (2017). Trend Cyber Crime Dan Teknologi Informasi Di Indonesia. *Informasi Komputer Akuntansi Dan Manajemen*, 13(2), 55–65.
- Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 6(1), 17–33. <https://doi.org/10.1108/JCRPP-12-2019-0070>
- Fletcher, G., & Griffiths, M. (2020). Digital transformation during a lockdown. *International Journal of Information Management*, 55. <https://doi.org/10.1016/j.ijinfomgt.2020.102185>
- Franjić, S. (2020). Cybercrime is very dangerous form of criminal behavior and cybersecurity. *Emerging Science Journal*, 4, 18.
- Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. *American Journal of Information Science and Technology*, 6(3), 52–63.
- Giri, R. R. W., Santoso, B. R., Mustikasari, A., & Bratawisnu, M. K. (2017). *Consumer perceptual mapping towards e-banking channel:(A study of bank BRI customer in Indonesia* (pp. 1–4).
- Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology*, 16(2), 119–130.
- Hassan, H., & Farmanesh, P. (2022). Customer adoption of self-service technologies in Jordan: Factors influencing the use of Internet banking, mobile banking, and telebanking. *Management Science Letters*, 12(3), 193–206.
- Hatta, M., Rajamanickam, R., Abdullah, D., Hartono, H., Bunga, M., Adji, H. S., & Rianita, D. (2018). Efforts to overcome cyber crime actions in Indonesia. *Journal of Physics: Conference Series*, 1114(1), 12081.
- Iivari, N., Sharma, S., & Ventä-Olkkonen, L. (2020). Digital transformation of everyday life – How COVID-19 pandemic transformed the basic education of the young generation and why information management research should care? *International Journal of Information Management*, 55. <https://doi.org/10.1016/j.ijinfomgt.2020.102183>
- Irawati, N., Maksum, A., Sadalia, I., & Muda, I. (2019). Financial performance of Indonesian's banking industry: the role of good corporate governance, capital adequacy ratio, non performing loan and size. *International Journal of Scientific and Technology Research*, 8(4), 22–26.
- Jameel, A. S., & Alheety, A. S. (2022). Customers' perceptions and behavioral intentions regarding mobile banking usage. *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 189–194.
- Jashinsky, T. L., King, C. L., Kwiat, N. M., Henry, B. L., & Lockett-Glover, A. (2021). Disability and COVID-19: Impact on workers, intersectionality with race, and inclusion strategies. *The Career Development Quarterly*, 69(4), 313–325. <https://doi.org/10.1002/cdq.12276>
- Javaid, M., Haleem, A., Pratap, R., Suman, R., & Khan, S. (2022). BenchCouncil Transactions on Benchmarks, Standards and Evaluations Review article A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, 2(3), 100073. <https://doi.org/10.1016/j.tbench.2022.100073>
- Jogiyanto. (2007). *Sistem informasi keperilakuan (Revisi)*. Andi Offset.

- Khan, K., Nouman, M., & Imran, M. (2015). Determinants of financial performance of financial sectors (An assessment through Economic value added. *Institute of Business and Management Sciences*, 1–32.
- Klein, V. B., & Todesco, J. L. (2021). COVID-19 crisis and SMEs responses: The role of digital transformation. *Knowledge and Process Management*, 28(2), 117–133.
- Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2021). Market-oriented corporate digital responsibility to manage data vulnerability in online banking. *International Journal of Bank Marketing*, 39(4), 571–591.
- Naeem, M., & Ozuem, W. (2021). Journal of Retailing and Consumer Services The role of social media in internet banking transition during COVID-19 pandemic : Using multiple methods and sources in qualitative research. *Journal of Retailing and Consumer Services*, 60(October 2020), 102483. <https://doi.org/10.1016/j.jretconser.2021.102483>
- Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious software threats. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 793–813).
- Okafor, L. E., Bhattacharya, M., & Apergis, N. (2020). Bank credit, public financial incentives, tax financial incentives and export performance during the global financial crisis. *World Economy*, 43(1), 114–145. <https://doi.org/10.1111/twec.12848>
- Okpa, J. T., Ajah, B. O., & Igbe, J. E. (2020). Rising trend of phishing attacks on corporate organisations in Cross River State, Nigeria. *International Journal of Cyber Criminology*, 14(2), 460–478.
- Pai, C.-K., Wu, Z.-T., Lee, S., Lee, J., & Kang, S. (2022). Service Quality of Social Media-Based Self-Service Technology in the Food Service Context. *Sustainability (Switzerland)*, 14(20). <https://doi.org/10.3390/su142013483>
- Pantea, M., Gligor, D., & Anis, C. (2014). Economic determinants of Romanian firms' financial performance. *Procedia-Social and Behavioral Sciences*, 124, 272–281. [org/10.1016/j.sbspro.2014.02.486](https://doi.org/10.1016/j.sbspro.2014.02.486).
- Park, H., & Kim, J. D. (2020). Transition towards green banking: role of financial regulators and financial institutions. *Asian Journal of Sustainability and Social Responsibility*, 5(1), 1–25.
- Partelow, S., Fujitani, M., Williams, S., Robbe, D., & Saputra, R. A. (2023). Disaster impacts, resilience, and sustainability opportunities for Gili Trawangan, Indonesia: transdisciplinary reflections following COVID-19. *Disasters*, 47(2), 499–518. <https://doi.org/10.1111/disa.12554>
- Pekkola, E., Siekkinen, T., Kujala, E.-N., Kanninen, J.-P., & Laihonen, H. (2021). An assessment of COVID-19's impact on Finnish University Leadership. *Knowledge Management Research and Practice*, 19(4), 510–516. <https://doi.org/10.1080/14778238.2021.1906773>
- Piasecki, S., Urquhart, L., & McAuley, P. D. (2021). Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards. *Computer Law and Security Review*, 42. <https://doi.org/10.1016/j.clsr.2021.105542>
- Qi, S., Jin, K., Li, B., & Qian, Y. (2020). The exploration of internet finance by using neural network. *Journal of Computational and Applied Mathematics*, 369, 112630.

- Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, 60, 101616.
- Setiawati, A. P., Susetyorini Susetyorini, U. E., Rusdiyanto, R., Astanto, D., Ulum, B., Khadijah, S. N., & Umanailo, M. C. B. (2019). The Role Of Customer Service Through Customer Relationship Management (CRM) To Increase Customer Loyalty And Good Image. *International Journal of Scientific and Technology Research*, 8(10), 2004–2007.
- Shokuhi, A., Ali, S., & Chashmi, N. (2019). Formulation of Bank Melli Iran Marketing Strategy Based on Porter ' S Competitive Strategy Formulation of Bank Melli Iran Marketing Strategy Based on Porter ' S. *Journal of Business-to-Business Marketing*, 0(0), 1–7. <https://doi.org/10.1080/1051712X.2019.1603421>.
- Sugiyono. (2017). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta.
- Sun, S., & Guo, L. (2022). Digital transformation, green innovation and the Solow productivity paradox. *PLoS ONE*, 17(7 July). <https://doi.org/10.1371/journal.pone.0270928>
- Thirupathi, M., Vinayagamoorthi, G., & Mathiraj, S. (2019). *Effect Of Cashless Payment Methods : A Case Study Perspective Analysis*.
- Usman, O., Monoarfa, T., & Marsofiyati, M. (2020). E-Banking and mobile banking effects on customer satisfaction. *Accounting*, 6(6), 1117–1128.
- Venkatesh, V. (2020). Impacts of COVID-19: A research agenda to support people in their fight. *International Journal of Information Management*, 55. <https://doi.org/10.1016/j.ijinfomgt.2020.102197>
- Yadav, P., & Shaikh, I. (2023). Measuring financial resilience with consumer sentiment data from India. *International Journal of Bank Marketing*, 41(5), 1083–1103.
- Zhai, Y., Chen, K., Zhou, J. X., Cao, J., Lyu, Z., Jin, X., Shen, G. Q. P., Lu, W., & Huang, G. Q. (2019). Advanced Engineering Informatics An Internet of Things-enabled BIM platform for modular integrated construction : A case study in Hong Kong. *Advanced Engineering Informatics*, 42(September), 100997. <https://doi.org/10.1016/j.aei.2019.100997>