Macrothink Institute™

Business and Management Horizons
ISSN 2326-0297
2023, Vol. 11, No. 2

Understanding Cyber Threats Vulnerability of Future Victimization in Fintech

Nurul Arinah Bazilah Bakari

Faculty of Accountancy, Universiti Teknologi MARA, Kampus Puncak Alam, Selangor, Malaysia

E-mail: arinahbazilah12@gmail.com

Intan Salwani Mohamed (Corresponding Author)

Accounting Research Institute, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia

E-mail: intan838@uitm.edu.my

Siti Nur Shuhada Nazuri

Faculty of Business management, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia

E-mail: shuhada1705@gmail.com

Received: Oct. 17, 2023 Accepted: Nov. 23, 2023 Published: Dec. 20, 2023

doi:10.5296/bmh.v11i1.21543 URL: https://doi.org/10.5296/bmh.v11i1.21543

Abstract

Individuals' participation in online activities is expanding, and the number of businesses moving to online operations is increasing, raising the possibility that they will become victims of cybercrime. Vulnerability in a technological system refers to any flaw or weak point within a technology or network that could be used to inflict damage or give an attacker unauthorized control. On the other hand, victimization results from intentional actions by an individual or organization to exploit, harm, or unlawfully gain access to another's assets or possessions. This research seeks to evaluate the future vulnerability of private sector employees to cybercrime when using FinTech. This study was conducted using an approach drawing from victimization theory. The study focuses on three primary factors influencing vulnerability: the economic shutdown, income inequality, and reliance on technology. The

primary method for gathering data in this study was through questionnaire surveys, specifically distributed among service sector employees in Malaysia. Findings from this study show that economic shutdown (ES) due to COVID-19 and income inequality (II) have a significant positive relation with the vulnerability of future victimization in FinTech. However, reliance on technology does not significantly influence the vulnerability of future victimization in FinTech. This research contributes to the expanding body of knowledge regarding risk factors associated with future victimization in FinTech. The findings benefit companies and individuals, offering insights into areas that should be fortified to decrease vulnerability.

Keywords: vulnerability, victimization, FinTech, cybercrime, service sector

1. Introduction

1.1 Introduction to Financial Technology (FinTech)

In the rapidly evolving landscape of technological adoption, digital transformation has introduced two pivotal concepts: digitization and digitalization. The former involves converting analogue data into digital format, enabling storage within computer systems. Conversely, digitalization harnesses digital information and technologies processed by computers to facilitate instantaneous data processing and process optimization (Lachvajderová & Kadarova, 2021). Amidst this context, Financial Technology (FinTech) emerges as a vast domain encompassing diverse financial services and technological endeavours, ranging from mobile payments, peer-to-peer lending, and crowdfunding to blockchain, cryptocurrencies, and robo-investing (Goldstein, Jiang, & Karolyi, 2019). As Goh (2019) outlines, the years spanning from 2016 to 2018 witnessed remarkable growth in transaction value per capita, soaring from RM550,703.00 to RM668,785.00. Concurrently, e-payment transactions surged from 97.5 percent to 124.6 percent. This era of technological advancement and shifting consumer behaviours has given rise to novel business solutions and market prospects within FinTech as technology intertwines with global societal trends.

In alignment with the Malaysia Fintech Report (2022), online payments and e-wallets stand out as pivotal players, accounting for 19% of the FinTech landscape in a nation with a population of 32.7 million and an internet penetration rate of 84.2%. Simultaneously, online banking penetration reached 126.2%, while smartphone adoption was 76.4%. Notably, the FinTech sector burgeoned from 2020 to 2022, propelled by the COVID-19 pandemic and the resultant implementation of the Movement Control Order, accelerating the shift towards digital interactions. As the Malaysia Fintech Report (2022) highlighted, the average number of e-wallet payment transactions per capita surged beyond pre-Covid levels, reaching 64.5% in 2021 (Chart 1). Over 7.2 billion electronic payment (e-payment) transactions were conducted in Malaysia within a year, marking a substantial 30% year-on-year growth. Over the past decade, the ascent and acceptance of digital payments in Malaysia took on a new dimension during the COVID-19 pandemic, solidifying the transition to a cashless society. The number of FinTech enterprises in Malaysia surged to 294 in 2022 (Figure 1), reflecting the inevitable trend of heightened mobile banking use and increased adoption of cashless payment methods in tune with the evolving daily routines of consumers in the “new normal.”

As financial technology (FinTech) rapidly shifts towards digital platforms, keeping up with the changing trends and the associated risks of cyber threats is crucial. Bissell and Ponemon (2019) discovered that cybercrimes are changing for three reasons. The first reason is the shift in targets. As more and more people move their important information online during digitalization, criminals find it easier to steal this valuable information. The most significant and rapidly increasing cybercrime is information theft, which is the costliest type of loss. The second reason involves the ever-changing methods used by cybercriminals. While sensitive data remains a prime target, theft is not always the end goal. The third reason is the evolving techniques cybercriminals employ. They adapt their attack strategies to keep up with technological advancements and growth. They increasingly use tactics like phishing and

insider attacks to exploit the human element, often the weakest link in security. These cybercrimes encompass a range of activities, such as attacks on computer systems and data, identity theft, distribution of inappropriate images involving children, fraud in online marketplaces, targeting the financial sector on the Internet, and spreading computer viruses.

The recent years have witnessed a significant transformation in the financial services landscape, driven by technological advancements and expanded global regulations. These changes have emerged in response to banking crises and compliance failures. This shift has coincided with the rise of financial technology, commonly referred to as FinTech, which prioritizes user experiences, efficiency, and adaptability as its core principles.

This period of change has seen a proliferation of companies introducing innovative approaches to revolutionize financial behaviours and experiences. Particularly notable are advancements in areas such as mobile payments, peer-to-peer lending, money transfers, crowdfunding, wealth management, digital currencies, and e-wallets. The emergence of the COVID-19 pandemic in early 2020 prompted the widespread adoption of digital technologies as people embraced social isolation measures and remote work. However, this also inadvertently created a fertile ground for cybercrime, exposing individuals to a heightened risk of falling victim to large-scale cyberattacks (Europol, 2020). Transitioning to remote work brought challenges, including lax implementation of robust cybersecurity measures among home-based professionals. Issues like inadequate user verification protocols, improper communication of sensitive company information with unauthorized family members, and the reuse of passwords for work purposes became prevalent. In 2020, a study by Ipsos found that 65 percent of Malaysians claimed to be working from home as a response to the pandemic, surpassing the global average of 52 percent. The survey encompassed 12,823 online workers aged 16 to 74 across 28 countries, highlighting the pandemic's influence on the workforce.

While the growth of FinTech is to be applauded, there are also significant financial crime dangers. Financial crimes have begun to be committed due to the exploitation of FinTech's quick financial services. Businesses were compelled to take steps to prevent financial crimes such as money laundering, terrorist funding, corruption, and bribery by committing crimes through quick and easy solutions supplied by financial technology companies. The biggest question is: Is financial fraud becoming a bigger or smaller problem over time? Con artists are known to feed on user fear and bewilderment during the COVID-19 outbreak, resulting in a surge in fraud. According to Bissell and Ponemon (2019), 1,000 cyberattacks identified malware as the most common attack overall, and the most expensive to resolve in many countries, and people-based attacks show some of the largest increases over the year, which seems to be a major worry when people continue to be the weakest point in cybersecurity defending.

According to Free Malaysia Today (2021), the Malaysian police's Commercial Crime Investigation Department (CCID) recorded 15,935 online deception and fraud cases, resulting in losses of nearly RM380 million in the initial nine months of 2021. These cases include the African and Macau Scam, fake loans, investment fraud, and e-commerce scams. Financial

fraud victims face monetary losses and often experience significant emotional distress and other non-monetary consequences (Button et al., 2010; Financial Industry Regulatory Authority, 2015). Research has extensively examined financial fraud types like Ponzi schemes, pyramid investments, and hedge fund-related frauds, which have shaken the financial realm in recent decades (Davis & Wilson, 2011; Bollen & Pool, 2012; Amoah, 2018). Despite authorities' efforts to prevent these frauds over time, fraudsters have evolved their tactics, employed new channels and targeted different segments of the population to perpetrate novel forms of financial fraud.

CCID's deputy director, Muhammed Hasbullah Ali, in a 2021 press statement, expressed deep concern over the statistics, revealing that many individuals in Malaysia still fall prey to deceptive scams. Human error stands out as a leading factor in most cybersecurity incidents. Hackers have exploited human mistakes to gain access to vital information and secure networks on numerous occasions. According to IBM's Cyber Security Intelligence Index Report, 95 percent of cybersecurity breaches stem from human error. Furthermore, as highlighted in IBM's Cost of a Data Breach Report 2020, cyber breaches caused by human error incur an average cost of $3.33 million. Hence, it is imperative to research further to understand the issues. This involves raising awareness, addressing underlying causes, enhancing the capabilities of local actors in the FinTech ecosystem, and empowering communities to reduce information imbalances among Malaysians, making them less susceptible to victimization through FinTech.

1.2 Objectives of Study

This research aims to assess the vulnerability of future victimization of private sector employees toward cybercrime while using FinTech. The detailed objectives of this study are as follows:

1) To analyze the relationship between the economic shutdown due to COVID-19 and the vulnerability of future victimization in FinTech.

2) To examine the relationship between income inequality and the vulnerability of future victimization in FinTech.

3) To explore the relationship between the reliance on technology and the vulnerability of future victimization in FinTech.

To attain the research objectives as stated above, this study employs the Vulnerability Theory to address gaps in the existing literature about the vulnerability of future victimization of Malaysia's private sector employees toward cybercrime while using FinTech. During the COVID-19 pandemic, wherein all sectors were mandated to transition to remote work, the policy has increased cyber-attacks. This has heightened the vulnerability of many to technological threats, particularly within the FinTech. Notably, there has been a lack of research examining the vulnerabilities associated with potential victimization in FinTech within the Malaysian context, prompting this study to focus on this overlooked area. The service sector is crucial due to its heightened vulnerability following the government's movement control order (MCO). The findings from this study can be pivotal in determining if

there is a relationship between economic shutdown, income inequality and reliance on technology, as seen in prior studies.

This study examines three independent variables: economic shutdown, income inequality, and reliance on technology. These variables are assessed concerning the dependent variable, vulnerabilities of future victimization in FinTech. The focus of this research is on employees within the service sector. Comprehensive data regarding the number of service sector employees in Malaysia has been obtained from credible resources, specifically the Department of Statistics Malaysia (DOSM). The research design section provides an in-depth presentation and discussion on the overall service sector in Malaysia. The results of this research emphasize the threats of cyber-attacks, like ransomware, and suggest practical solutions sourced from academic literature. These solutions will assist the service sector in enhancing data security and strengthening cybersecurity systems. A proactive approach, such as performing scheduled penetration testing, can bolster cyber defences and safeguard confidential information. This study also sheds light on crucial factors affecting human vulnerability data that were previously overlooked by previous research.

2. Literature Review and Hypotheses Development

2.1 Vulnerability and Future Victimization in FinTech

The concept of vulnerability surpasses various scientific domains and pertains to an array of potentially risky situations. Vulnerability is characterized as the qualities that render one susceptible to the possibility and potential of experiencing fear from an unknown origin. Physical vulnerability, as outlined by Skogan and Maxfield (1981), is described as the ease of access for assault or offences, the lack of ability to resist such attacks, and the exposure to physical and emotional trauma in the event of an attack. They indicate a further aspect of social vulnerability; victimization's social and financial implications are heavier.

Cybercrime can negatively affect a person's mental health by causing emotional distress, physical injury, and financial loss. There are generally three components to the cost of victimization: physical injury, monetary loss, and emotional distress. Prior victimization has accurately predicted future victimization (Lynch et al., 2002). The effect of prior victimization on the likelihood of future victimization is extensive and multifaceted. According to Kadoya et al. (2021), financial illiteracy and lack of awareness are the most prevalent characteristics in victim profiles for financial fraud. These are the most notable key contributors to fraudulent financial vulnerability, given that substantial financial literacy is linked to human choice's sophisticated intellectual ability, which enables individuals "to judge and evaluate products and services that have been offered to them." Risk-takers who made high-risk purchases were even more susceptible to adverse effects (Federal Trade Commission, 2019).

FinTech denotes using advanced technologies within business models to profit from the underlying record and telecommunications in accessing financial services (Nicoletti, 2017). Financial crime encompasses deceiving, defrauding, and manipulating individuals to attain financial or asset-related gains by concealing illicit monetary operations or equity

investments. According to the US Department of Justice (2022), fraud involves manipulating individuals by presenting pledges, services, or monetary advantages lacking substance. Financial crime is commonly utilized to obfuscate unlawful activities such as deception, cybercrime, misappropriation of funds, terrorist funding, corruption and bribery, manipulation of markets, and insider trading.

As stipulated by Malaysia's legal framework, all actions enlisted within the 'Second Schedule of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2010' are classified as financial crimes. With the development of technology and the automation of financial dealings, financial fraud has evolved into a more technologically adept and less discernible form. The emergence of Financial Crime 4.0, together with the relentless expansion of digital technology and the shift towards online platforms, has inaugurated a new era of fraudulent practices characterized by the absence of geographical boundaries. According to Grima et al. (2020), the term Financial Crime 4.0 encapsulates the transformative progression of fraud. It represents a sweeping trend of immense risk, encompassing the heightened intricacy and escalated volume of nascent financial crimes arising from hyperconnectivity and data inundation within today's Industry 4.0, commonly known as the Age of the Connected World.

As postulated by Fineman (2008), vulnerability theory is built upon acknowledging diverse factors, including physically or mentally detrimental events beyond individuals' control. Human reliance on and integration within social interactions and institutions throughout various social roles and events over time give rise to vulnerability. This dependence assumes two forms: inevitable and derivative. Inevitable dependency pertains to the need for care during specific biological and developmental life stages, while derivative dependency emerges when individuals care for those intrinsically reliant on them. The global embrace of Fintech, notably in developing nations, is propelled by an underserved demand for financial services, fostering its widespread adoption (Frost, 2020). Despite its potential to enhance financial inclusion, the increasing reliance on daily technological use raises concerns. This approach identifies four fundamental dimensions: universality, constancy, complexity, and particularity (Fineman, 2010). Vulnerability research predominantly draws from two previous research (Skogan & Maxfield, 1981), each possessing essential theoretical underpinnings that may not be immediately apparent. The fundamental premise is that specific individuals (the elderly, women, minorities, and the economically disadvantaged) are (passively) more vulnerable to crime and, thus, fearful. Skogan and Maxfield (1981) stated that physical vulnerability encompasses susceptibility to assault, incapacity to counteract attacks, and exposure to traumatic physical (and potentially psychological) consequences when victimized. They also described socially vulnerable individuals as perennially menaced by victimization due to their identity. Another feature of social vulnerability they highlight is the heightened social and economic impact of victimization on such vulnerable populations. Killias (1990) agreed with Skogan and Maxfield (1981) on the physical elements engendering vulnerability to crime. Most of Skogan and Maxfield's social vulnerability concept finds expression in Killias' notion of "situational factors," wherein residing in high-crime areas exposes vulnerable individuals to risks.

Without individual causal factors or environmental adversities, "vulnerability" lacks relational significance. However, practical criminal investigations are rarely devoid of environmental challenges and victim resistance. Personal vulnerability takes on a relational dimension where environmental hardships intersect with vulnerability attributes delineated by the expanded vulnerability approach (openness, controllability, and consequences). Illustrated through instances presented by Loewenstein et al. (2001), it is asserted that risk perception arises from a synergy of preventative actions, emotional arousal, and individual and contextual determinants. The technique of generalization, wherein diffuse fears are projected onto criminal contexts, aligns with this notion of vulnerability, consequently magnifying awareness of environmental adversity when perceived through the prism of vulnerability. Figure 1 shows the general flow of the Vulnerability Model.

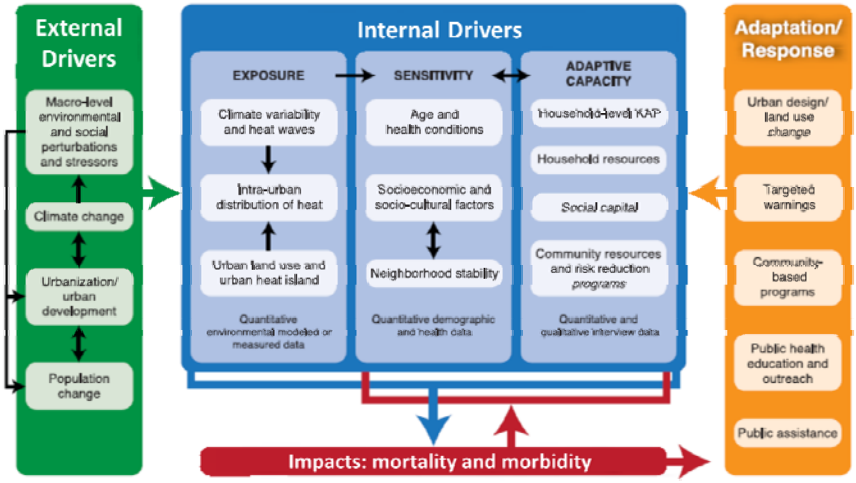

Figure 1. General Flow of Vulnerability Model

Figure 2 presents the theoretical framework illustrating the relationship between three key determinants toward the vulnerability of future victimization in FinTech (VFVF).

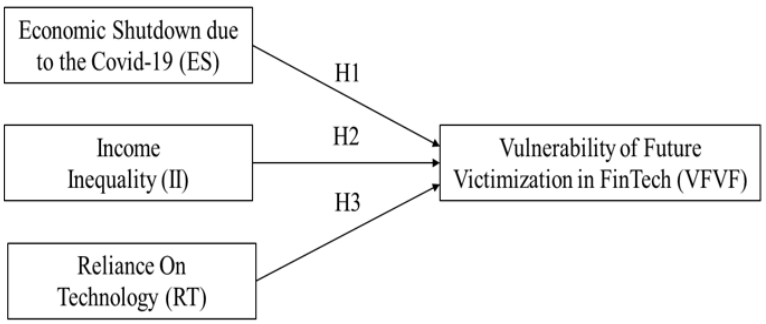

Figure 2. Theoretical Framework

2.2 Hypotheses Development

2.2.1 Economic Shutdown due to the COVID-19 (ES)

The COVID-19 pandemic has highlighted how people, the global community, and economic gains are interconnected, particularly concerning healthcare, inequality, environmental decline, and the stability of the global economy. It brought to light vulnerabilities in the financial system, including issues related to supply chains, labour markets, credit ratings, and liquidity. There is a rising concern about the future robustness of the finance system in light of these challenges. Therefore, a significant shift from in-person to online modes occurred in both personal and professional realms. The pandemic precipitated a significant health and financial crisis and transformed work cultures. In Malaysia, the government implemented various stages of movement control orders (MCO, CMCO, and RMCO) throughout 2020 to curb the spread of the virus. Some of these restrictions were reintroduced later in the year due to a resurgence in cases. These measures, combined with the global economic downturn and disruptions in international trade, severely impacted the country's economy. A significant 52% of Malaysians worked from home.

However, this massive online transition increased vulnerabilities to cyber-attacks. The surge in the use of remote access tools heightened the risk of cyber breaches and other financial crimes (Crisanto and Prenio, 2020). Financial institutions became primary targets, experiencing a higher rate of cyber-attacks than other sectors. Apart from healthcare, the financial sector witnessed the highest number of pandemic-related cybercrimes, with phishing attacks utilizing the crisis as bait to deceive victims (Checkpoint Risk Intelligence, 2020). Accordingly, the following hypotheses were suggested.

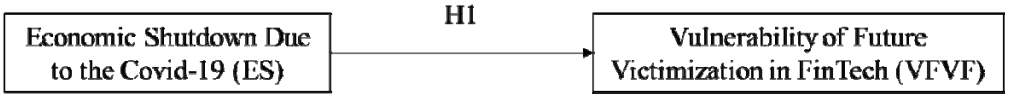

Figure 3. Hypothesis 1 (H1)

$H_0$1: The economic shutdown due to COVID-19 does not have a significant positive relation with the vulnerability of future victimization in FinTech.

H_A1: The economic shutdown due to COVID-19 has a significant positive relation with the vulnerability of future victimization in FinTech.

2.2.2 Income Inequality (II)

"Income inequality" refers to the difference in discretionary income within a year, encompassing various income sources like wages, self-employment, and assets. This is adjusted for taxes and social security payments. COVID-19's impact on household income in Malaysia during 2020 is presented in the Household Income Estimates and Poverty Incidence Report, Malaysia, 2020. Primary sources of income, paid work and self-employment,

declined by -16.1% and -9.7%, respectively, leading to a -10.3% decrease in average monthly family income to RM7,089 from RM7,901 in 2019. Job loss, reduced work hours, and long-term unemployment due to skills contributed to this decline. The unemployment rate rose from 3.5% in Q1 2019 to 4.5% in May 2021. Unemployed individuals increased by 12.4% over fourteen months to 728.1 thousand in May 2021. Consequently, the unemployment rate dropped to 3.9% in March 2021, but the mean monthly household income fell by 11.3% in 2019 compared to the previous year, reaching RM5,209 in 2020. Household income distribution by decile shifted towards lower income percentiles as many households experienced decreased income.

Ehrlich (1973) emphasized crime literature's significance, reviving interest in criminal justice. They established that income inequality influences crime patterns, prompted. Many economists believe rising inequality makes solving issues like poverty and crime harder, endangering democratic capitalism. The connection between economic inequality and crime rates is supported by both economics and criminology. Crime causes loss of assets, life, and emotional distress. According to the United Nations, the number of victims of property crime varied by country, e.g., 14.8% in New Zealand and 3.4% in Japan (Imrohoroglu et al., 2006). Madden and Chiu (1998) noted that income inequality affects the likelihood of property crime. Teles (2004) suggested that fiscal and monetary policies influence crime.

Choe (2008) contradicted this by finding no significant link between crime rates, including violent and property crime, and wealth disparity. Mehanna (2004) supported this, concluding that income inequality insignificantly affects crime in a study spanning 1959 to 2001. Magnus and Matz (2008) further distinguished permanent and transitory income effects. They found that while a rise in permanent income inequality significantly increases total and property crimes, transitory income inequality has minimal impact, diverging from typical aggregated measurements. Brush (2007) analyzed US counties cross-sectionally and over time, yielding conflicting results: income inequality relates to crime in cross-sectional analysis but inversely in time series. Habibullah and Law (2007) used Malaysia's Vector Error Correction Model (VECM), indicating an unclear connection between crime and real per capita income, financial access, or interest rates. Consequently, the following hypotheses were proposed:

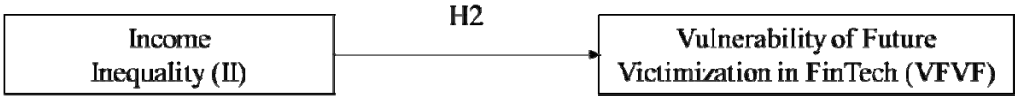

Figure 4. Hypothesis 2 (H2)

$H_0$2: Income inequality does not have a significant positive relation with the vulnerability of future victimization in FinTech.

H_A2: Income inequality has a significant positive relation with the vulnerability of future

victimization in FinTech.

2.2.3 Reliance on Technology (RT)

The evolution of high-end cybercriminals parallels advanced IT corporations, using cloud-based apps, artificial intelligence (AI), Software-as-a-Service, and encryption. Cybercriminals exploit weak user precautions and tech vulnerabilities, quickly analyze targets, and automate software and profit. FinTech, a comprehensive term, pertains to financial services provided through technical solutions via the Internet and mobile apps. Its beginnings can be dated to the early 1990s (Arner et al., 2016). FinTech services have the potential to enhance users' financial experiences by digitizing lending, investing, insurance, financial advice, and more. FinTech refers to tech-based financial services like digital lending, investing, and insurance. Subcategories of FinTech include PayTech (digital payments), LendTech (streamlined lending), crowdfunding (online securities sale), Neobanks (digital banking), and RegTech (regulatory technology). Malaysia sees growth in Islamic FinTech, especially in crowdfunding and data analytics (Hasan et al., 2020), with potential for expansion and regulatory calls.

Reliance is defined as an ongoing association and attachment founded on the consistent reliability of one party (Baier, 1986). Reliance on technology refers to the substantial trust and dependence that people, enterprises, and communities invest in technological resources, setups, and strategies to accomplish diverse functions, oversee activities, and foster interaction and data sharing. This reliance on technology, while advantageous for efficiency and comfort, introduces difficulties that might cause potential obstacles for both industries and consumers. This is due to the adjustments required to meet business targets and evolving consumer preferences. Allianz (2018) stated that technology is being used to help increase safety onboard ships, including improving navigation. However, over-reliance on technology does have its downsides, notably vulnerability to cyberattacks. Therefore, it led to the formulation of the following hypotheses:

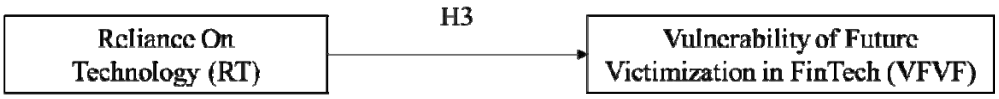

Figure 5. Hypothesis 3 (H3)

$H_0$3: The reliance on technology does not have a significant positive relation with the vulnerability of future victimization in FinTech.

H_A3: The reliance on technology has a significant positive relation with the vulnerability of future victimization in FinTech.

3. Methodology

3.1 Sampling Procedures

Among the 4,370,000 Malaysians who engage with FinTech, the study focuses on Malaysian service sector personnel aged between 18 and 65. The study's sampling frame was derived from a table by Bartlett et al. (2001). The table determines the minimum returned sample size for a Given Population Size for Continuous and Categorical Data. Consequently, the optimal sample size for the Malaysian population is 384 respondents, sufficient for data analysis.

3.2 Data Collection and Analysis Procedures

This study utilized questionnaires to acquire sufficient data from the populations. It pertained to the data on which values may be based and the dependability and validity of data quality (Burns et al., 2014). This study's primary instrument was a questionnaire with a Likert scale (5-point Likert scale). Two sections are included in the questionnaire. The first section contains respondents' demographic information, including age, gender, profession, and salary. The second section is based on the study's dependent variable (DV) and independent variables (IVs). Vulnerability of Future Victimization in FinTech is the dependent variable (DV), while the independent variables (IVs) are economic shutdown due to COVID-19, income inequality and reliance on reliable technology. Data was obtained by online questionnaires that were distributed using Google Forms via email and WhatsApp. Although hand distribution could result in a higher response rate, time and cost were the significant limitations.

The data was encoded and processed using the Statistical Package for the Social Sciences (IBM SPSS version 25). Initially, the SPSS software package was employed for descriptive analysis (Pallant, 2010), aimed at examining the basic characteristics of the data. Subsequently, a normality test was conducted to determine the adherence of the dataset to a normal distribution. This was followed by a reliability test to determine the stability and consistency of the measurement tool. Subsequently, the Pearson Correlation Test was employed to ascertain the presence of multicollinearity concerns among the variables. Finally, a regression analysis assessed the relationship between the independent variables (economic shutdown, income inequality and reliance on reliable technology) and the dependent variable (vulnerability of future victimization in FinTech).

4. Results

4.1 Examining Response Rate

Table 1 indicates a generally acceptable online survey response rate of around 30%.

Table 1. Acceptable Response Rates

No.	Type of survey	Acceptable response rates
1	Phone	80% good
2	Email	40% average, 50% good, 60% very good
3	Online	30% average
4	Face-to-face	80% - 85% good

Source: The University of Texas at Austin (2015).

Subsequently, Table 2 presented below summarises the distributed questionnaires, which were returned and usable. The data in the table reveals a response rate of 51.5% for this study, surpassing the average percentage of 30%. This response rate is considered acceptable. As Nulty (2008) highlighted, online surveys typically experience lower response rates than paper surveys. Moreover, this study received 198 responses, representing a 51.5% rate, which adheres to the criteria outlined by Bartlett et al. (2001) for determining an appropriate sample size when considering both continuous and categorical data about the population size. The minimum number of respondents required for the data in Table 2 was 384. Consequently, the current study possesses a total sample size of 198 respondents to proceed with the subsequent data analysis effectively.

Table 2. Total percentage of returned and usable

Total questionnaire distributed	Total questionnaire returned (percentage)	Total usable questionnaire (percentage)
384	198 (51.5%)	198 (51.5%)

4.2 Demographic Profile

Descriptive analysis was employed to examine participants' demographic profiles, encompassing factors such as gender, age, employment status, service sector, household monthly income, and purpose of using Fintech. The results, displayed in Table 3, elucidated the demographic composition of respondents within the study's area.

Table 3. Sample Characteristics (N=198)

Variable	Frequency	Percentage	CumulativePercentage
Gender			
Female	91	45.9	45.9
Male	107	54.1	100.0
Age			
58－65 years old	16	8.1	8.1
42－57 years old	71	35.9	44.0
26－41 years old	87	43.9	87.9
18－25 years old	24	12.1	100.0
Employment Status			
Full time	152	76.8	76.8
Part time	46	23.2	100.0
Service Sector			
Wholesale and retail trade	28	14.1	14.1
Food & beverages and accommodation	59	29.8	43.9
Transportation and communication	51	25.8	69.7
Finance, insurance, real estate & business services	54	27.3	97.0
Other services	6	3.0	100.0
Household Monthly Income			
> RM2,500	27	13.6	13.6
RM 2,501－5,000	107	54.0	67.6
RM 5,001－7,500	42	21.1	88.7
RM 7,501－10,000	13	6.6	95.3
> RM 10,001	9	4.7	100.0
Purpose of using FinTech			
Payment	119	60.1	60.1
Lending	0	0	60.1
Marketplace	15	7.6	67.7
Cryptocurrency	64	32.3	100.0

Based on the results, among the 198 respondents, 45.9 percent were identified as female, while 54.1 percent were classified as male. Regarding age distribution, the largest portion of participants fell within the 26 to 41 age range, constituting 43.9 percent (87 individuals) of the total sample. The subsequent age groups included those between 42 and 57 years old, comprising 35.9 percent (71 individuals); 18 to 25 years old, accounting for 12.1 percent (24 individuals); and finally, 58 to 65 years old, making up 8.1 percent (16 individuals).

Regarding employment status, a majority of 76.8 percent of respondents were employed full-time, with 23.2 percent (46 respondents) engaged in part-time work. Given the study's focus on service sector employees, a significant proportion of respondents were employed in

the food, beverages and accommodation sector, representing 29.8 percent (59 respondents) of the sample. This was followed by the finance, insurance, real estate and business services sector, accounting for 27.3 percent (54 respondents); the transportation and communication sector, encompassing 25.8 percent (51 respondents); wholesale and retail trade sector, involving 14.1 percent (28 respondents); and other services sector, with 3.0 percent (6 respondents).

Regarding household monthly income, 54.0 percent (107 respondents) reported an income range of approximately RM 2,501 to 5,000. The second highest income bracket was RM 5,000 to 7,500, constituting 21.2 percent (42 respondents). The third highest range was RM 2,500, representing 13.6 percent (27 respondents). Subsequently, the income categories of RM 7,501 to 10,000 and > RM 10,001 were each reported by 13.6 percent (27 respondents) and 4.5 percent (9 respondents), respectively.

Regarding the purpose of utilizing FinTech, 60.01 percent (119 respondents) indicated its use for payments, while 32.3 percent (64 respondents) reported using it for cryptocurrencies. A smaller subset of 7.6 percent (15 respondents) utilized FinTech for marketplace activities. Other FinTech platforms appeared to have limited exposure among Malaysians, particularly in the service sectors.

4.3 Descriptive Statistics

Table 4. Mean and Standard Deviation

Variables	Mean	Std. Deviation
Economic shutdown due to the COVID-19 (ES)	4.51	0.273
Income Inequality (II)	4.51	0.253
Reliance on Technology (RT)	4.68	0.269
Vulnerability of Future Victimization in FinTech (VFVF)	4.34	0.338

Table 4 presents the mean and standard deviation values for the four variables: Economic Shutdown due to COVID-19, Reliance on Technology, Income Inequality, and Vulnerability of Future Victimization in FinTech. The findings from this study show that Reliance on Technology (RT) holds the highest mean score, at 4.68. Following closely are the variables of Economic Shutdown due to COVID-19 (ES) and Income Inequality (II), both recording mean scores of 4.51. The mean Vulnerability of Future Victimization in FinTech (VFVF) score is 4.34. These results signify an agreement among the respondents with the statements presented in the questionnaire.

4.4 Normality Test

A normality test is conducted by analyzing the skewness and kurtosis values for the variables related to Vulnerability to Future Victimization, Economic Shutdown, Income Inequality, and Reliance on Technology. A perfectly normal distribution is defined by skewness, and kurtosis

values is zero, but such distributions are infrequent in the social sciences (Pallant, 2016). Table 5 provides a summary of the statistical findings.

Table 5. Tests of Normality

	Kolmogorov-Smirnov[a]	Shapiro-Wilk
Vulnerability of Future Victimization	0.254	.872
Economic Shutdown	0.153	0.919
Income Inequality	0.131	0.957
Reliance on Technology	0.337	0.823

Note. a. Lilliefors Significance Correction.

Table 5 indicates that all variables' skewness and kurtosis values are within the acceptable boundaries for a normally distributed dataset, ranging from 0.131 to 0.957. Pallant (2016) mentioned that a normal distribution is characterized by skewness and kurtosis values within the range of ±2.0. Furthermore, the mean scores for Vulnerability to Future Victimization, Economic Shutdown, Income Inequality, and Reliance on Technology are regularly distributed.

4.5 Reliability Test

As described by Sekaran and Bougie in 2013, a measure's dependability indicates its freedom from bias (error), ensuring consistent measurement over time and across different moments in the instrument. Essentially, a measure's dependability indicates the instrument's reliability and consistency in assessing the underlying concept, and it plays a vital role in evaluating the quality of the measure. Cronbach's alpha is a reliability coefficient that assesses how effectively items within a set are positively correlated. In essence, the higher the internal consistency among the items within a scale, the more favourable the measurement, as Gliem and Gliem (2003) emphasized. A higher coefficient value signifies a more robust measurement, aligning with Sekaran (2003). When interpreting Cronbach's coefficient, the following rules of thumb apply:

Table 6. Reliability Test

	Cronbach's Alpha
Vulnerability of Future Victimization	0.788
Economic Shutdown	0.888
Income Inequality	0.763
Reliance on Technology	0.812

Note. Overall Cronbach's Alpha (N = 198) = 0.891.

Table 6 presented the scores for each construct, and the overall Cronbach's alpha score met

the requirement of being at least 0.7, following Sekaran (2003). In summary, the findings were deemed reliable since random errors were avoided.

4.6 Correlation "r"

Correlation analysis was employed to examine potential associations among the variables, namely Vulnerability to Future Victimization, Economic Shutdown, Income Inequality, and Technology Reliance. Given that the variables exhibited are normally distributed, the study utilized the Pearson Coefficient Correlation tool, which is a parametric correlation tool that assesses linear relationships between two variables. Schober et al. (2018) define correlation as a measure of a monotonic relationship; whereas one variable's value increases, the other's value consistently increases as well; conversely, as one variable's value decreases, the other's value consistently decreases. Care, Subagio and Rahman (2018) have outlined the levels of relationship, which are quantified as numerical values. Larger numbers indicate a stronger relationship, as demonstrated in Table 7:

Table 7. Interpretation of Relationship Level

Value of Correlation Coefficient	Relationship Interpretation
0.000－0.199	Very Weak
0.200－0.399	Weak
0.400－0.599	Moderate
0.600－0.799	Strong
0.800－1.000	Very Strong

Table 8 summarizes the bivariate analysis conducted to assess the correlation between different variables. According to the statistical results, the correlation coefficients between these variables fell within the range of 0.692 to 0.805. This range suggests that there is no evidence of multicollinearity among the variables. Specifically, the variables "Economic Shutdown (ES)" and "Reliance on Technology (RT)" exhibit a strong positive correlation with the vulnerability of future victimization in the FinTech sector. The correlation coefficients for these relationships are 0.692 and 0.673, respectively, which are statistically significant at $p < 0.01$, indicating a highly significant and strong association. Furthermore, "Economic Shutdown (ES)" demonstrates an even stronger positive relationship with vulnerability to future victimization in the FinTech sector, with a correlation coefficient of 0.805, also significant at the $p < 0.01$ level.

Table 8. Pearson Correlations Matrix among Variables

		Economic Shutdown	Income Inequality	Reliance on Technology
Vulnerability of Future Victimization in FinTech	Pearson Correlation	.805**	.692**	.673**
	Sig. (2-tailed)	.000	.000	.000
	N	198	198	198

Note. **. Correlation is significant at the 0.01 level (2-tailed).

4.7 Examining Response Rate

Multiple regression statistical approaches were employed to examine the research hypothesis and assess the impact of the independent factors, namely economic shutdown, income inequality, and reliance on technology, on the dependent variable.

Table 9. ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1249.609	3	416.536	139.984	.000[b]
	Residual	577.265	194	2.976		
	Total	1826.874	197			

Note. a. Dependent Variable: Vulnerability; b. Predictors: (Constant), Reliance, Income, Economic.

Table 10. Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.827[a]	.684	.679	1.72499

Note. a. Predictors: (Constant), Reliance, Income, Economic; b. Dependent Variable: Vulnerability.

Table 9 presents the results of the multiple regression analysis, as denoted by (F = 139.984, P = 0.05). In this context, the model demonstrates statistical significance. Moreover, the R^2 value (R^2 = 0.684) signifies that the model is fit and acceptable and meets the criteria proposed by Hair et al. (2010), where an R^2 exceeding 0.10 is considered fit. This result indicates that, collectively, the independent variables explain 68.4% of the variation of the dependent variable, which is the Vulnerability of Future Victimization in FinTech. The remaining 31.6% of the variation of the vulnerability of future victimization in FinTech is attributed to unknown variables.

Consequently, the effect of economic shutdown, income inequality, and reliance on technology on the vulnerability of future victimization in FinTech is considered high. The F-test is employed to evaluate the overall significance of the model. The analysis of variance

(ANOVA) for the variables affirms that the multiple regression model is indeed significant [F = 139.984, P = 0.000]. This outcome suggests that at least one of the variables maintains a significant linear relationship with the vulnerability of future victimization in FinTech.

Table 11. The Result of Multiple Regression

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	-7.148	2.374		-3.011	.003
	Economic	.931	.102	.585	9.147	.000
	Income	.375	.105	.218	3.561	.000
	Reliance	.131	.091	.093	1.445	.150

Note. Significant level: p<0.01***, p<0.05**.

The data in Table 11 illustrates that an economic shutdown positively influences the vulnerability of future victimization in FinTech ($\beta = 0.931$, $p < 0.05$). The variance in vulnerability of future victimization in FinTech is explained by the variance in economic shutdown ($t = 9.147$). Consequently, $H_0 1$ is rejected, and $H_A 1$ is accepted.

Furthermore, the findings displayed in Table 11 indicate that income inequality exerts a substantial and positive influence on future victimization vulnerability in FinTech ($\beta = 0.375$, $p = 0.001$). This research suggests that income inequality ($t = 3.561$) explains 37.5 percent of the variance in future victimization vulnerability in FinTech. Consequently, this data highlights the considerable impact of income inequality on future victimization vulnerability in FinTech. As a result, $H_0 2$ is rejected, and $H_A 2$ is accepted.

Lastly, the outcomes presented in Table 11 reveal that reliance on technology has a positive and insignificant effect on the vulnerability to future victimization in the FinTech sector ($\beta = 0.131$, $p > 0.05$). This outcome implies that only 13.1 percent of the variations in vulnerability to future victimization in FinTech can be attributed to variance in reliance on technology ($t = 1.445$). Therefore, do not reject $H_0 3$. This finding underscores the importance of considering both vulnerability to future victimization in FinTech and reliance on technology to prevent employees from becoming fraud victims.

Table 12. Summary of the Hypotheses Result

Hypotheses		Results
Hypothesis 1		
$H_0$1	The economic shutdown due to COVID-19 does not have a significant positive relation with the vulnerability of future victimization in FinTech.	Reject $H_0$1;
H_A1	The economic shutdown due to COVID-19 has a significant positive relation with the vulnerability of future victimization in FinTech.	Accept H_A1
Hypothesis 2		
$H_0$2	Income inequality does not have a significant positive relation with the vulnerability of future victimization in FinTech.	Reject $H_0$2;
H_A2	Income inequality has a significant positive relation with the vulnerability of future victimization in FinTech.	Accept H_A2
Hypothesis 3		
$H_0$3	The reliance on technology does not have a significant positive relation with the vulnerability of future victimization in FinTech.	Do not reject $H_0$3
H_A3	The reliance on technology has a significant positive relation with the vulnerability of future victimization in FinTech.	Reject H_A3

5. Discussion

Cybercrime is rapidly increasing worldwide. This study aims to assess the vulnerability of future victimization of service sector employees toward their vulnerability of future victimization while using FinTech. The service sectors are wholesale and retail trade, food and beverages (F&B) and accommodation, transportation and communication, finance, insurance, real estate, and business services. The service sector was chosen because it relies on technology more than other sectors. In this study, Vulnerability Theory was applied, as described by Skogan and Maxfield (1981). They defined physical vulnerability as how susceptible someone is to being harmed or victimized, their inability to defend against such harm, and the potential for physical and emotional trauma if they are attacked. They also highlight another aspect of vulnerability: the social and economic impact of victimization, which can be significant. Therefore, this study focuses on three specific factors that may contribute to an individual's vulnerability, which are economic shutdown due to COVID-19 (ES), income inequality (II) and reliance on technology (RT).

This study's findings suggest that the economic shutdown due to COVID-19 (ES) and income inequality (II) support the anticipated relationships. According to respondents' perspective, particularly those working in the service industry, these two factors affect an individual's vulnerability to future victimization in FinTech. Cybercrime is a significant concern as it operates on a large scale. There is a staggering amount of malicious activity on the Internet. One major internet service provider (ISP) detects 80 billion malicious scans daily. These scans result from automated attempts by cybercriminals to identify vulnerable targets.

Consequently, companies have been compelled to operate digitally over the past two years

due to the pandemic. This has raised concerns about the system's vulnerability and ability to withstand attacks, especially since essential and sensitive data is now stored online. Furthermore, income distribution also influences crime and can increase users' vulnerability.

However, the study's findings indicate that reliance on technology does not significantly influence the vulnerability to future victimization in FinTech. This can be explained by companies or individuals who use technology often take strong preventive measures to protect themselves from cybercrime. They implement robust cybersecurity measures, which protect against the vulnerabilities that can lead to future victimization. This is especially relevant since many employees have been working from home and extensively using financial technology, making them more vigilant about online security. Additionally, the high level of technological literacy among these individuals makes them more aware of new threats and risks, reducing their vulnerability to future victimization in FinTech. Therefore, the two research objectives set for this study have been successfully accomplished. Moreover, this research contributes valuable knowledge and awareness to employees in the Malaysian service sector by identifying potential factors that can influence their vulnerability of future victimization in FinTech.

6. Conclusion

This research has certain limitations that should be acknowledged. Firstly, the study's scope is restricted to employees in the services sector in Malaysia, and this may not accurately represent the overall vulnerability of all Malaysians. It primarily focuses on a segment of the economy affected by the pandemic. Additionally, many parts of the service sector, such as wholesale and retail trade, food and beverage, and accommodation, rely on physical operations and cannot transition to work from home or online work. These industries require employees to interact with customers in person. Given that COVID-19 has impacted various industries beyond the services sector, future studies could be more valuable if they incorporate a more diverse range of samples for analysis rather than being limited solely to the services industry. Furthermore, comparing the outcomes of these other industries with those of the service sector would be beneficial.

Moreover, this research explicitly examines economic shutdown, income inequality, and reliance on technology in the context of vulnerability to future victimization in financial technology (FinTech). It is worth noting that various other factors could contribute to this vulnerability, which requires further investigation. Consequently, additional research is imperative to expand this study's scope by considering a range of other significant factors, including individual characteristics. Despite its limitations, hopefully, this study will offer valuable insights into the susceptibility of future victimization within the FinTech sector. It is crucial to emphasize the importance of individuals having cybercrime prevention control and raising awareness to reduce their vulnerability to future victimization in FinTech.

Furthermore, it would be valuable for future research to employ qualitative approaches, such as interviews with individuals who know about cybercriminal activities or those who have been victims of cybercrimes. These interviews could provide insights into their real-life experiences and the various factors involved, including the methods employed in

cybercriminal activities and how individuals fall prey to these crimes. This is because individuals involved as criminals or victims are more likely to understand the circumstances surrounding cybercrimes comprehensively. Subsequent studies could also investigate the nature of crime prevention, detection, and investigation and whether these functions should be distinct within an organization, using qualitative and quantitative research methods. Combining survey techniques with qualitative methods, such as conducting live direct conversations, can help support survey findings and enhance the understanding of the issues being examined.

Acknowledgement

We would like to thank the Accounting Research Institute (ARI HICoE) Universiti Teknologi MARA, Shah Alam Malaysia; Ministry of Higher Education Malaysia; and Research Management Centre (RMC), Universiti Teknologi MARA, Shah Alam, Malaysia, for the research fund (600-RMC/ARI 5/3(010/2023).

References

Allianz Global Corporate & Specialty (Allianz). (2018). *Safety and Shipping Review 2018: An annual review of trends and developments in shipping losses and safety*. Munich, Germany: Allianz Global Corporate & Specialty.

Amoah, B. (2018). Mr. Ponzi with a fraud scheme is knocking investors who may open. *Global Business Review*, *19*, 1115–1128. https://doi.org/10.1177/0972150918788625

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). 150 Years of Fintech: An Evolutionary Analysis. *JASSA*, 22–29.

Baier, A. (1986). Trust and Antitrust. *Ethics*, *96*(2), 231–260. https://doi.org/10.1086/292745

Bartlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Organizational research: Determining appropriate sample size in survey research. *Information Technology Learning and Performance Journal*, *19*(1), 43–50. https://doi.org/10.5032/jae.2002.03001

Bissell, K., & Ponemon, L. (2019). *The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study*. Accenture: Ninth Annual Cost of Cybercrime Study, 18. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Bollen, N. P. B., & Pool, V. K. (2012). Suspicious patterns in hedge fund returns and the risk of fraud. *Review of Financial Studies*, *25*, 2673–2702. https://doi.org/10.1093/rfs/hhs085

Brush, J. (2007). Does income inequality lead to more crime? A comparison of cross-sectional and time-series analyses of United States counties. *Economics Letters*, *96*(2), 264–268. https://doi.org/10.1016/j.econlet.2007.01.012

Burns, A. M., Erickson, D. H., & Brenner, C. A. Cognitive-behavioral therapy for medication-resistant psychosis: a meta-analytic review. *Psychiatr Serv.*, *65*(7), 874–880. https://doi.org/10.1176/appi.ps.201300213

Button, M., Gee, J., Lewis, C., & Tapley, J. (2010). *The Human Cost of Fraud: A Vox Populi*. London: MacIntyre Hudson/CCFS.

Care, F., Subagio, B. S., & Rahman, H. (2018). Porous concrete basic property criteria as a rigid pavement base layer in Indonesia. *MATEC Web of Conferences*, *147*, 02008. https://doi.org/10.1051/matecconf/201814702008

Checkpoint Risk Intelligence. (2020). *27th April-Threat Intelligence Bulletin*. Retrieved May 6, 2020, from https://research.checkpoint.com/2020/27th-april-threat-intelligence-bulletin/

Choe, J. (2008). Income inequality and crime in the United States. *Economic Letters*, *101*, 31–33. https://doi.org/10.1016/j.econlet.2008.03.025

Crisanto, J. C., & Prenio, J. (2020). *Financial crime in times of COVID-19 - AML and cyber resilience measures, bank for international settlements*. Retrieved October 15, 2020, from https://www.bis.org/fsi/fsibriefs7.htm

Davis, L. R., & Wilson, L. (2011). Estimating JP Morgan Chase's profits from the Madoff deposits. *Risk Management and Insurance Review*, *14*, 107–119. https://doi.org/10.1111/j.1540-6296.2011.01196.x

Ehrlich, H. J. (1973). *The social psychology of prejudice: A systematic theoretical review and propositional inventory of the American social psychological study of prejudice*. John Wiley & Sons.

Europol. (2021). *COVID-19 sparks an upward trend in cybercrime* [Press release]. Retrieved from https://www.europol.europa.eu/media-press/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

Federal Trade Commission. (2019). *Phone Scams. Washington, DC: Federal Trade Commission*. Retrieved March 20, 2022, from https://www.consumer.ftc.gov/articles/0208-phone-scams

Financial Industry Regulatory Authority. (2015). *Non-Traditional Costs of Financial Fraud: Report of Survey Findings*. Washington, DC: FINRA Investor Education Foundation.

Fineman, M. (2008). The vulnerable subject: Anchoring equality in the human condition. *Yale Journal of Law and Feminism*, *20*(1), 1–24.

Frost, J. (2020). *The Economic Forces Driving FinTech Adoption Across Countries. Monetary and Economic Department*. BIS Working Papers No. 838. https://doi.org/10.2139/ssrn.3515326

Gliem, J. A., & Gliem, R. R. (2003). *Calculating, Interpreting, And Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales*.

Goh, J. (2019, June 10). *Riding the fintech wave*. The Edge Markets. Retrieved March 18, 2022, from https://www.theedgemarkets.com/article/riding-fintech-wave

Goldstein, I., Jiang, W., & Karolyi, G. A. (2019). To FinTech and Beyond. *The Review of Financial Studies*, *32*(5), 1647–1661. https://doi.org/10.1093/rfs/hhz025

Grima, S., Boztepe, E., & Baldacchino, P. J. (2020). *Contemporary Issues in Audit Management and Forensic Accounting*. https://doi.org/10.1108/S1569-37592020102

Hasan, R., Hassan, M. K., & Aliyu, S. (2020). Fintech and Islamic Finance: Literature Review and Research Agenda. *International Journal of Islamic Economics and Finance* (IJIEF), *3*. https://doi.org/10.18196/ijief.2122

Imrohoroglu, A., Merlo, A., & Rupert, P. (2006) Understanding the determinants of crime. *Journal of Economics and Finance*, *30*(2), 270–283. https://doi.org/10.1007/BF02761491

IPSOS. (2021, January 21). *Pandemic's Impact on Malaysian Workforce | Ipsos*. Retrieved March 6, 2022, from https://www.ipsos.com/en-my/press-release-pandemics-impact-malaysian-workforce

Kadoya, Y., Saidur, M., Khan, R., Narumoto, J., & Watanabe, S. (2021). Who Is Next? A Study on Victims of Financial Fraud in Japan. *Frontiers in Psychology*, *12*, 1–13. https://doi.org/10.3389/fpsyg.2021.649565

Killias, M. (2000). Different Measures of Vulnerability in their Relation to Different Dimensions of Fear of Crime. *British Journal of Criminology*, *40*(3), 437–450. https://doi.org/10.1093/bjc/40.3.437

Lachvajderová, L., & Kadarova, J. (2021). Digitization, Digitalization, and Digital Transformation in Industry. *A Systematic Literature Review*, 298–309. https://doi.org/10.7441/dokbat.2021.25

Loewenstein, G. F., Weber, E. U., & Hsee, C. K. (2001). Risk as Feelings. *Psychological Bulletin*, *127*. https://doi.org/10.1037/0033-2909.127.2.267

Lynch, J. P., Berbaum, M. L., & Planty, M. (2002). *Investigating repeated victimization with the NCVS, executive summary* (No. 193414).

Magnus, G., & Matz, D. (2008). Inequality and crime: Separating the effects of permanent and transitory income. *Oxford Bulletin of Economics & Statistics*, *70*(2), 129–153. https://doi.org/10.1111/j.1468-0084.2007.00492.x

Malaysia Fintech Report. (2022). *Malaysia Charts a New Path for Fintech Growth*. Retrieved from https://fintechnews.my/31945/malaysia/fintech-report-malaysia-2022/

Mehanna, R. A. (2004). Poverty and economic development: Not as direct as it may seem. *Journal of Socio-Economics*, *33*, 217–228. https://doi.org/10.1016/j.socec.2003.12.013

Nicoletti, B. (2017). *The Future of FinTech, Palgrave Studies in Financial Services Technology*. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-51415-4_2

Nulty, D. D. (2008). The Adequacy of Response Rates to Online and Paper Surveys: What Can Be Done? *Assessment & Evaluation in Higher Education*, *33*, 301–314.

https://doi.org/10.1080/02602930701293231

Pallant, J. (2016). *SPSS Survival Manual: A Step-by-Step Guide to Data Analysis Using SPSS Program* (6th ed.). London, UK: McGraw-Hill Education.

Schober, P., Boer, C., & Schwarte, L. (2018). Correlation Coefficients: Appropriate Use and Interpretation. *Anesthesia & Anesthesia*, *126*, 1763–1768. https://doi.org/10.1213/ANE.0000000000002864

Sekaran, U. (2003). *Research Methods for Business*. New York, NY: John Wiley and Sons, Inc.

Skogan, W. G., & Maxfield, M. G. (1981). *Coping with Crime: Individual and Neighbourhood Reactions*. Beverly Hills, Ca: Sage.

Teles, V. K. (2004). The effects of macroeconomic policies on crime. *Economic Bulletin*, *11*(1), 1–9. https://doi.org/10.2139/ssrn.487504

The United States Department of Justice. (2020). *Financial Fraud Crimes*. Retrieved March 20, 2021, from https://www.justice.gov/usao-ak/financial-fraud-crimes

Copyrights