INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 11, (2024) E-ISSN: 2222-6990

Publics Perception and Awareness towards the Identity Theft among the Residents of Bistari Impian Apartment, Johor, Malaysia

Paridah Daud[1], Nityananthen A/L Muniandy[1], Associate Professor Dr. Farhad Nadi[1]

[1]School of Information Technology, UNITAR International University, Petaling Jaya, Selangor, Malaysia

Corresponding Authors Email: paridah69@unitar.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i11/23385 DOI:10.6007/IJARBSS/v14-i11/23385

Published Date: 12 November 2024

Abstract

Identity theft in Malaysia has emerged as a critical concern, driven by the increasing digitization of personal transactions and the widespread use of online platforms. This research aims to explore the causes, impacts, and preventive strategies related to the residents of Bistari Impian Apartment, Johor, Malaysia. Employing a quantitative methodology, the study examines real-world cases and existing legal frameworks to analyze the mechanisms through which identity theft occurs. The focus is on key elements of identity fraud, including the unauthorized access and misuse of personal data such as MyKad details, banking information, and digital credentials. Technological vulnerabilities and social factors that facilitate identity theft are also explored. The individual consequences of identity theft, such as financial loss and psychological distress, as well as its systemic effects, including damage to public trust in financial institutions and regulatory burdens, are critically analyzed. The research assesses the effectiveness of Malaysia's current legal safeguards, with particular emphasis on the Personal Data Protection Act (PDPA) and evaluates the role of governmental and non-governmental organizations in combating identity theft. Through this analysis, the study offers tailored recommendations for improving Malaysia's legal, technological, and public awareness frameworks to enhance personal identity security. The findings of this research are intended to inform policymakers, law enforcement, and the public, providing actionable insights to mitigate the growing risks of identity theft in Malaysia's evolving digital landscape.

Keywords: Personal Data Protection, Identity Theft, Public Awareness, Public Perception, Bistari Impian Apartment

Introduction

Background of Study

Identity theft has become one of the most significant forms of cybercrime in Malaysia, particularly with the sharp increase in incidents reported in 2023. The rapid growth in digital transactions and the sophistication of cybercriminals have contributed to the rise of identity theft as a highly lucrative crime. Identity theft is generally defined as the unauthorized acquisition and use of an individual's personal information for fraudulent purposes, including names, identification numbers, addresses, or banking details. These stolen details are then used to carry out a variety of fraudulent activities such as credit card fraud, unauthorized bank account access, and social media impersonation, often leading to financial loss, reputational damage, and emotional distress for victims.

According to Hazelah et al (2011), and Copes et al (2010), highlight that identity theft typically occurs in two main forms: basic identity theft and "true name fraud" or "application fraud". Basic identity theft involves the unauthorized use of personal information to make illicit purchases or transactions, often remaining undetected by the victim until their bank statement or account limit reveals the fraudulent activity. The "true name fraud" involves the use of stolen personal information to open new accounts, often causing more severe financial and legal complications for the victim (Koyame-Marsh, & Marsh, 2014). Globally, identity theft continues to grow as a pressing issue. Singh et al (2021), report that in 2017 alone, 15.4 million consumers were victims of identity theft, resulting in an estimated $16 billion in losses. This alarming statistic underscores the economic impact of identity theft as a criminal enterprise. In the Malaysian context, the risk of identity theft has facilitated crimes such as credit card fraud, bank account compromise, and online impersonation, further exacerbating public concerns over personal and financial security.

This study is driven by the pressing need to address the issue of safeguarding personal information in the digital age. The research seeks to explore public perceptions on the causes, effects, and preventive measures related to identity theft, with the aim of understanding how Malaysians are affected by and respond to such cybercrimes. By examining the factors contributing to identity theft, this study aims to shed light on the vulnerabilities that criminals exploit, such as weaknesses in online security and lack of public awareness. It also assesses the psychological and financial impact of identity theft on victims, highlighting its far-reaching implications beyond immediate financial losses. Another key contribution of this study is its evaluation of current legal frameworks and technological safeguards in Malaysia, providing insights into their effectiveness and areas that need improvement.

The research develops a theoretical framework to analyze identity theft in a localized context, offering a structured approach to tackling this issue. Additionally, it aims to produce actionable recommendations to enhance both preventive measures and public education on cybercrime risks. By focusing on the Malaysian perspective, the study contributes valuable insights that can inform policy changes and the design of more robust cybersecurity strategies. Ultimately, these findings will help guide efforts to protect citizens' personal information, reduce the incidence of identity theft, and promote safer online practices in Malaysia.

Problem Statement

The rapid expansion of the Internet has transformed how people interact, do business, and share information. However, this growth has also increased the risks of cybercrime, including identity theft, which has become a growing concern globally and in Malaysia. According to Sehgar and Zukarnain (2021), cyberspace is a digital platform where information is exchanged, goods are bought and sold, and financial transactions are conducted. With more personal and financial data being shared online, the risk of this information being misused has increased significantly.

Identity theft occurs when unauthorized individuals steal personal information, such as credit card details or social security numbers, to commit fraud. According to Rizal et al. (2020), identity theft is particularly damaging because victims are often unaware of the fraud until they face consequences, such as rejected loan applications, denied job opportunities, or unexpected debt collectors. This hidden nature of identity fraud leads to billions of dollars in financial losses annually as victims are left to deal with the exploitation of their personal data. The rise in cybercrimes, especially during the COVID-19 pandemic, has exacerbated this issue. Stark (2023), notes that 41.8% of businesses reported credit card fraud, making it the most common form of online identity theft in 2020. In Malaysia, the Malaysian Computer Emergency Response Team (MyCERT) reported 8,366 cybercrime cases between January and September 2020, with cyber fraud incidents rising by 22% compared to the previous year (Mohd Isa et al., 2021). Given the persistent nature of cybercrime and identity theft, this study seeks to assess the level of public awareness of identity theft in Malaysia in 2023. It aims to evaluate public perceptions of information security and determine the effectiveness of awareness campaigns led by the government and organizations to combat identity theft.

Research objectives

- To identify the status of public awareness on identity theft in Bistari Impian Apartment, Johor Bahru.
- To examine the Malaysian public perception on the safety of their confidential information due to the increasing rate of identity theft in Bistari Impian Apartment, Johor Bahru.
- To evaluate the effectiveness of awareness campaigns conducted by the government and organisations on identity theft in Bistari Impian Apartment, Johor Bahru.

Research questions

- What is the status of public awareness on identity theft in Bistari Impian Apartment, Johor Bahru.?
- How does the Malaysian public perceive the safety of their confidential information due to the increasing rate of identity theft in Bistari Impian Apartment, Johor Bahru?
- What is the rate of effectiveness of awareness campaigns conducted by the government and organisations on identity theft in Bistari Impian Apartment, Johor Bahru?

Research Hypothesis

- Hypothesis 1: Most of the public in Johor Bharu, Johor, Malaysia, have a low level of awareness about identity theft.
- Hypothesis 2: The public in Bistari Impian Apartment, Johor Bahru, perceives their confidential information as unsafe due to the increasing rate of identity theft.

- Hypothesis 3: Awareness campaigns conducted by the government and organisations in Bistari Impian Apartment, Johor Bahru, have been ineffective in significantly increasing public awareness about identity theft.

Significance of Study

This research was intended to raise awareness among persons regarding the rate of cybercrime in Bistari Impian Apartment, Johor Bahru, especially with regard to the many types of identity theft, with the goal of reducing the number of instances of cybercrime that occur within the country. The research aims to educate the Malaysian public in order to make them more aware of the smoother ways in which these crimes are committed, as well as to encourage them to maintain the protection of their personal details and never to disclose them without cause. Hazelah et al (2011), found that many people were oblivious and ignorant of the existence of the crime until their bank accounts were tampered with and the harm had already been done and identity theft had already been on the rise over the ten years.

Literature Review

Cybercrime, particularly identity theft, has been on the rise due to the growing digitization of personal data and weak cybersecurity measures. Factors such as the use of weak passwords, phishing scams, and unsecured networks have made it easier for cybercriminals to access sensitive information. According to Smith (2022), these vulnerabilities, compounded by the increased reliance on online platforms during the COVID-19 pandemic, have exposed individuals to higher risks. Many individuals were forced to shift their activities online whether shopping, banking, or socializing which increased their susceptibility to cyber-attacks (Doe & Miller, 2023). Cybercriminals often exploit individuals undergoing stressful situations, such as unemployment or pandemic-induced panic, making them prime targets for identity theft and other cybercrimes (Stark, 2023).

Various countries have responded to the growing threat of identity theft with different legal frameworks, but enforcement remains inconsistent. In Malaysia, for instance, the Computer Crimes Act 1997 addresses unauthorized access, including identity theft. However, the penalties under this act may not adequately deter offenders, as they do not always reflect the severity of the victim’s losses (Singh et al., 2021). Other nations, like the UK, have enacted laws to tackle identity theft, but challenges such as cross-border investigations persist. While some jurisdictions treat identity theft as a standalone crime, others only recognize it when it leads to additional offenses. The evolving nature of cybercrime calls for stronger global cooperation and advanced strategies to protect individuals and businesses from identity-related cyberattacks.

Types of Identity Theft

Theft of identity through the internet, often referred to as identity theft, is a gateway crime that leads to other criminal activities. According to the Identity Theft Resource Centre, online identity theft is not limited to financial transactions but can also involve various other forms of personal information misuse (Sinnathamby Sehgar, & Zukarnain, 2021). Six main types of identity theft include financial, medical, criminal, false identity, tax identity, and child identity theft. Financial identity theft, the most common type, involves using stolen personal information to gain financial benefits such as goods, services, and credit (Hazelah et al., 2011).

With the rise of online banking, the number of financial scams in Malaysia has surged since 2005, prompting the government to implement stringent measures to curb the growing threat (Mohd Isa et al., 2021).

Medical identity theft occurs when someone uses another individual's personal health information to obtain medical services or defraud insurance companies. This can lead to altered medical records and severe consequences for the victim's health (Komakula, 2021). Criminal identity theft, on the other hand, involves a person falsely assuming another's identity to avoid legal consequences for criminal activity. Victims often remain unaware until they face legal consequences or summonses for crimes they did not commit (Mohd Isa et al., 2021). The creation of a false identity using a combination of real and fabricated personal information is another form, making detection difficult as the fake identity can appear as a new record rather than a replication of the victim's existing one (Omar et al., 2021). Tax identity fraud, involving the use of stolen Social Security numbers to file false tax returns, and child identity theft, where a child's information is used to apply for credit or services, are also significant threats (Komakula, 2021). Child identity theft is particularly insidious, as crime often goes undetected until the child reaches adulthood and applies for credit or loans (Stark, 2023). In all these forms of identity theft, the consequences for victims can be severe, ranging from financial loss to reputational damage and prolonged legal battles. Addressing these crimes requires robust cybersecurity measures and public awareness to protect personal information from being exploited.

Techniques of Identity Theft

There are varieties of techniques to steal personal information targeted both digital and physical realms, making it crucial to understand how they work to safeguard personal data effectively.

One common technique is hacking, where cybercriminals exploit vulnerabilities in computer systems to steal large quantities of personal information. Hackers can either sell this data or use it for financial gain. Hackers often use tools like keyloggers or malware to track users' activities and capture sensitive information, such as passwords. Another widely used technique is phishing, where scammers impersonate trusted institutions to trick individuals into revealing personal information through deceptive emails, texts, or phone calls (Mohd Isa et al., 2021). Another technique is phishing has advanced forms, such as pharming, where users are redirected to fake websites, and vishing or smishing, involving fraudulent phone calls or text messages (Stark, 2023). Criminals also use fraudulent employment schemes, where fake job postings lure job seekers into submitting personal details, such as resumes containing sensitive information (Mohd Isa et al., 2021). Cybercriminals gather these details for identity theft or fraud. Malware plays a significant role in identity theft, with malicious software like spyware capturing personal information from infected devices (Hazelah et al., 2011). Malware can target everything from computers to medical devices, allowing hackers to steal sensitive data. Additionally, identity thieves exploit social media platforms by piecing together seemingly harmless information such as birthdates and names of pets to guess passwords or security questions (Hazelah et al., 2011).

By knowing and understanding these techniques, hacking, phishing, fraudulent job schemes, malware, and social media exploitation will help individuals protect themselves from identity theft. Staying vigilant and employing strong security measures is crucial in today's digital world.

Safety of Private and Confidential Information from all parties

The consequences of identity theft are far-reaching, affecting individuals, businesses, and society at large. Victims often suffer significant financial losses, emotional distress, and damage to their credit ratings. Jones and Patel (2023), note that the recovery process is lengthy and complicated, often requiring victims to spend considerable time and resources to restore their identity and financial stability. On a broader scale, businesses also face reputational damage and financial penalties due to data breaches, which can result in a loss of customer trust (Williams, 2023).

The rates of cybercrime continue to climb, despite the substantial efforts that have been made to educate the public and users of the internet. It is clear from this that the level of understanding among young people in Malaysia who use the internet is still quite low. Users become aware of cybercrime issues such as being a victim of online fraud, having personal information leaked, and other similar issues because of a lack of awareness regarding the Internet. As was said earlier, the effect of low Internet awareness has an impact on the number of cases of cybercrime that occur in Malaysia (Omar, S. Z., et al., 2021). The overall number of cases of cybercrime from 2015 to 2019 is presented in Table 1 below. The categories of cybercrime that are depicted by this statistic include content-related, vulnerability reports, intrusion attempts, cyber harassment, malicious codes, intrusion, fraud, spam, and spam emails.

Table 1: Statistics on Cybersecurity Incidents Year 2015-2019

Incident	2015	2016	2017	2018	2019
Content Related	33	50	46	111	298
Vulnerabilities Report	22	35	60	92	91
Intrusion Attempt	303	277	266	1805	1359
Cyber Harassment	442	529	560	356	260
Malicious Code	567	435	814	1700	738
Intrusion	1714	2476	2011	1160	104
Fraud	3257	3921	3821	5123	7774
Spam	3539	545	344	342	129
Total	**9877**	**8268**	**7922**	**10689**	**10753**

Source: MyCERT, CyberSecurity Malaysia 2020

Since the 1980s, there has been a worldwide reaction and call for change to address and deter cybercrime (Stark, A. K., 2023). The Organisation for Economic Cooperation and Development (OECD) formed an expert committee to tackle cybercrime and make changes to criminal law. An examination of the enforcement and legislation surrounding cybercrime in Malaysia.The Computer Crimes Act 1997 is employed in Malaysia to counteract cybercrime assaults. Nevertheless, this legislation exclusively pertains to instances of computer misuse and does not encompass a wide range of computer-related activities (Singh, M. M et al., 2021). The

Digital Signature Act of 1997 implements safeguards for online transactions through the use of digital signatures, while the Copyright Act of 1997 safeguards against the unauthorised use of copyrighted material. The Electronic Commerce Act 2006 and the Personal Data Protection Bill 2010 are employed to govern e-commerce transactions and the handling of personal data. The responsibility of addressing cyber threat issues lies with a limited number of government entities, including the Ministry of Science, Technology, and Innovation (MOSTI) and the Malaysian Communications and Multimedia Commissions (MCMCs). The responsibility of defining a framework for ICT policy at the national level lies with MOSTI. Its objective is to formulate strategies to safeguard the critical national information infrastructure (CNII).

Individual and Organisational Prevention Methods

Fraudsters utilise a diverse range of tools and strategies to acquire personal information. Fraudsters choose their techniques of assault dependent on the circumstances (Sehgar & Zukarnain, 2021). The techniques employed to perpetrate identity theft against businesses, for instance, vary from those utilised to pilfer information from people. To combat identity theft, researchers have proposed several prevention strategies. Strengthening cybersecurity practices, such as using multi-factor authentication and encryption, is critical in protecting personal information (Abd Rahim et al., 2019). According to a study by Johnson and Lee (2023), public awareness campaigns are also essential in educating individuals about the risks and signs of identity theft. According to Omar et al., (2021), an argument can be made that young adults in today's society do not take adequate safety precautions when using smart technologies such mobile phones, laptops, desktop computers, tablets, and other similar devices. Individuals enjoy sharing updates about their everyday activities on social media platforms, these platforms have become a source of privacy invasion. E-government and e-commerce are two examples of the principles that the government has implemented, both of which require a connection to the internet in order to function properly. According to Omar et al., (2019), frequent usage of the internet has a variety of good effects on the socio-economic life of young people, but it also has several significant negative implications. Additionally, government regulations, such as the General Data Protection Regulation (GDPR), have been effective in holding organizations accountable for safeguarding consumer data (Smith, 2023).

Theoretical Framework

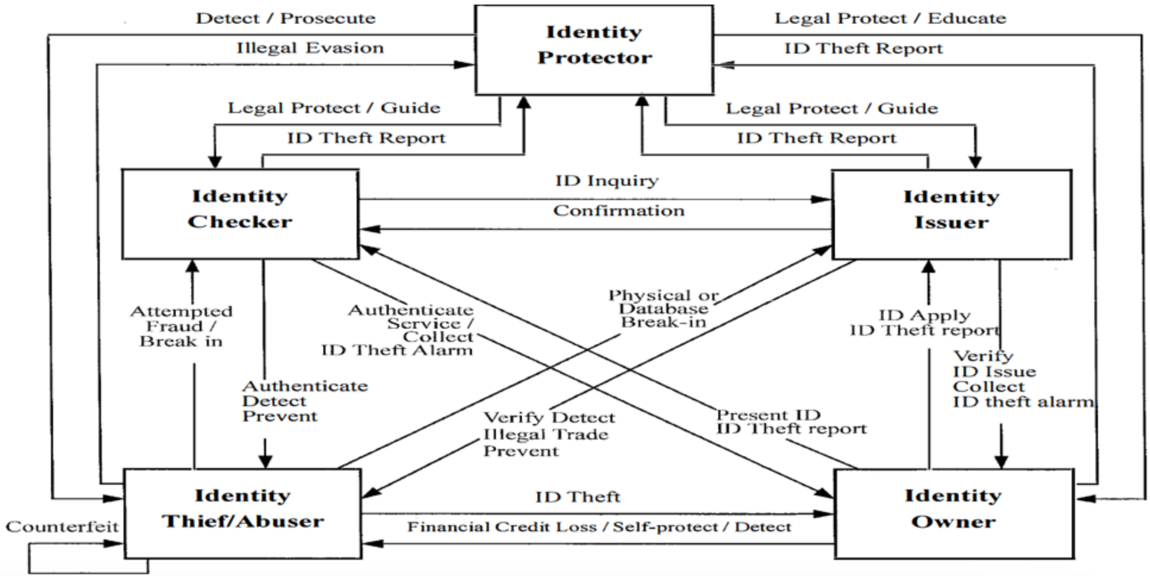

Figure 1 Theoretical Framework: Combating Identity Theft

The framework outlines the key actors involved in the prevention, detection, and legal pursuit of identity theft, along with their respective responsibilities and interactions (Wang et al., 2004). Figure 1 illustrates the framework, with the main participants shown as nodes and their interactions and information flows indicated by arrows. There are four primary parties involved in combating identity theft: (1) Identity owners are individuals who legally possess and utilise various types of identities for social and financial purposes. They seek protection against identity theft. (2) Identity issuers are responsible for authorising and providing identities to individuals, serving as proof of their identity and granting access to related social and financial services. (3) Identity checkers are tasked with verifying the identity of the owner and convincing them to provide proof of their identity. (4) Identity protectors have the primary role of safeguarding the rights and interests of stakeholders such as identity owners, issuers, and checkers. They achieve this by identifying and prosecuting thieves and establishing guidelines for issuers and checkers. The identity thief is an antagonist who opposes the objectives of the other stakeholders. The individual engages in the unlawful or immoral act of stealing and forging the identities of rightful owners for personal gain or other motives. They deceitfully exploit the rights of the owners by perpetrating acts of fraud.

The five stakeholders engage in three interrelated activities: (1) authentication of identity and collection of information; (2) perpetration of identity fraud; and (3) efforts to combat identity theft, which encompass prevention, detection, victim protection, and legal prosecution of theft. Issuers, such as government agencies, financial institutions, and trusted authorities, gather and verify personal identity information to provide identification and provide confirmation to the checker. Consequently, it is imperative to protect and uphold the security of such sensitive information using both managerial and technological methods. Identity thieves illicitly acquire personal identities and subsequently assume them in order to fraudulently achieve financial or other advantages through various means. Individuals who possess a Personal ID are accountable for ensuring the security and protection of their identification.

Identity theft can be thwarted, identified, and legally pursued by the implementation of government regulations, effective corporate administration, public consciousness, and advanced technology. It is imperative for all parties involved, such as the ID protector, the ID issuer, the ID checker, and the ID owner, to collaborate in order to safeguard personal identification and combat the act of identity theft. Robust measures to prevent, identify, and prosecute identity theft, as demonstrated by this framework, are necessary to establish a thriving economic and corporate development environment. Among the framework's potential applications are:

- Advising on the most important statistics for measuring and tracking ID theft
- Examining the impact of changes in one type of activity on the remaining activities and stakeholders
- Analysing relationships among the various stakeholders involved in the identity management process
- Identifying and proposing ways to strengthen the identity management process.
- Examining the effectiveness of fraudulent activity prevention and detection; and
- Determining the return on investment for various types of technologies used to combat ID theft.
- Clarifying interactions between stakeholders involved in the development of systematic and effective technical solutions
- Assessing the trade-off between the need for privacy and the need for centralised databases of personal data to combat identity theft.
- Assessing the risk of identity theft and developing a systematic and efficient security strategy by analysing the activities involved in the proposed framework, we will examine the roles and responsibilities of each stakeholder, as well as their relationships.

Identity theft remains a significant challenge in today's digital world, with both individuals and organizations being potential targets. The latest research underscores the importance of robust cybersecurity measures, public education, and stringent regulations in mitigating the risks associated with identity theft. Continued efforts in these areas are crucial to protecting personal information and maintaining trust in digital platforms.

Research Methodology

Study Design

A cross- sectional survey design was used to collect data from respondents using an online platform, i.e., Google Form. The connection between the research study and audience sampling, a questionnaire will be produced and shared to 62 respondents and later to be transferred into SPSS tool to gain the final descriptive analysis result. The question was designed based on the research objective and theoretical framework in Figure 1. This research identifies the cumulative and average count of exposure on identity theft occurrence in Bistari Impian Apartment, Johor Bharu.

Research Instrument

According to Taylor and Medina (2011), the use of the questionnaire is a data collection tool that gives researchers a more objective perspective in line with the positivist methodology which form the basis of the current study. McMillan and Schumacher (2010), state that the use of the questionnaire is a method of data collection that provides stronger data and shaped to strengthen the empirical data. The construction of the questionnaire for this study involved a detailed study of the various questionnaires available to assess how publics perception and awareness towards the identity theft in Johor, Malaysia. The construction of the questionnaire covers how each item is designed to meet each objective and motive of the study. Items from the previous survey studied thoroughly before adapted to meet the needs of the questionnaire. In general, the questionnaire is an adaptation of the survey instrument used by Winterdyk, John & Thompson, Nikki (2008), in their study Student and Non-Student Perceptions and Awareness of Identity Theft.

The questionnaire contains four sections and Section A is the demography section to analyse the background of the respondents where there are five items. The goal is to learn more about the composition of respondents who responded to the survey questionnaire. Section B is known as the Malaysian public's awareness on the safety of their confidential information in the current situation of increasing cybercrime section which consists of 10 items. Section C is for the Status of public perception on identity theft in Malaysia which contains 13 items and lastly Section D which evaluates the opinion of respondents on the effectiveness of awareness campaigns conducted by the government and organisations in combating identity theft in Malaysia has 5 items. The 5-point Likert-type scale is used.

Sampling Procedures

The population targeted for this research is young adults aged 18 years up to working adults aged 55 years old. The study also looks into the both gender - males and females, education background such as SPM, Diploma, Bachelor's degree, Master's degree and PhD. The sample in the study played a very significant role in the context of quantitative studies provide basic data for the samplesrelated to the scope of study. This study will utilise purposive sampling as its core sampling technique. According to Etikan, Musa and Alkassim (2016), purposive sampling is done after the researchers know that the population may be able to meet the goals of the study. This research used the guide by Krejcie and Morgan (in Krejcie & Daryle, 2015) to perform sampling studies because the guide offers a systematic guide for the selection of the number of samples based on population studies. It's also shows the correct number of samples based on the total population that is appropriate and in accordance with a certain ratio.

Data Analysis

Questionnaires are widely used in research to collect data from respondents about their opinions, behaviours, or characteristics. They can be administered in various formats, such as online surveys, paper forms, or interviews. The responses gathered through questionnaires are typically quantitative but can also include qualitative data, depending on the question types. There are varieties of analytical methods for analyzing the data through questionnaires. According Schabenberger and Gotway (2017) required the appropriate analytical methods in the study of quantitative methods of analysis for determining the extent of continuity of the data collected by the study. Thus, the method of data analysis for this study was determined based on the research questions. Table 2 below shows the analysis of each part of the questionnaire.

Table 2
The Analysis of the Questionnaire

Section	Title	Analysis
A	Demography	Frequencies
B	Status of public awareness on identity theft in Bistari Impian Apartment	Descriptives
C	Status of public awareness on identity theft in Bistari Impian Apartment	Descriptives
D	Opinion of respondents on the effectiveness of awareness campaigns conducted by the government and organisations in combating identity theft in Bistari Impian Apartment	Descriptives

Result And Analysis

Frequency Analysis

Frequency analysis is the most basic form of analysis is to count the number of times each response appears. For example, how many respondents chose a particular option from the question. The data of demographic were collected by analysing questionnaire given to the respondents of Bistari Impian Apartment. The analyses data will be explained in the Table 3 below.

Table 3
Personal Information of the Respondents

Variables	Category	N= 62	Percentage (%)
Gender	Male	43	69.35
	Female	19	30.65
Ethnicity	Malay	10	16.13
	Chinese	13	20.97
	India	37	59.68
	others	2	3.23
Income	Below 2500	15	24.19
	RM2501 – RM3500	12	19.35
	RM3501 – RM4500	5	8.06
	RM4501 – RM5500	7	11.29
	RM5501 – RM10000	23	37.10
Education	SPM/SPMV	7	11.29
	Diploma	19	30.65
	Bachelor's degree	22	35.48
	Master's degree	13	20.97
	Philosophical Doctorate	1	1.61

Descriptive Analysis

Descriptive statistics is used to determine the respondent's environment (social) pattern, and which category of respondents is most likely to be concerned.

Status of Public Awareness on Identity Theft in Malaysia

Identity theft has become an increasingly concerning issue in Malaysia, affecting individuals and organizations alike. As digital transformation accelerates and more personal information is stored and shared online, the risks associated with identity theft have grown. This research examines the current state of public awareness regarding identity theft among the residents of Bistari Impian Apartment, the efforts made to educate the public, and the challenges that remain. Public awareness of identity theft in Malaysia has been growing, but the level of understanding varies across different segments of the population. According to survey conducted vast majority of the residents are concerned and aware of the risk of identity theft. The dataset provided includes responses to a survey regarding concerns and behaviours related to identity theft in today's digital age. The survey captures data from 62 respondents, with each question rated on a scale of 1 to 5. Below is a detailed descriptive analysis of the dataset

Table 4
Descriptive Analysis of the STATUS of Public Awareness on Identity Theft in Malaysia

Summary of the question	N	Mean	Std. Deviation
Concern about the Risk of Identity Theft	62	4.37	.794
Victim of Identity Theft	62	2.60	1.408
Confidence in Protecting Personal Information	62	3.56	.985
Targeting of Personal Information by Identity Thieves	62	2.79	1.189
Concerned the risk of identity theft in the digital age	62	2.76	.918
Reviewing Financial Statements for Suspicious Activity	62	2.79	1.073
Sufficiency of Safeguards by Businesses	62	2.52	1.127
Familiarity with Legal Rights and Protections	62	3.26	1.159
Trust in Online Security Measures	62	3.50	1.184
Frequency of Updating Passwords	62	3.66	1.159
Frequency review financial statement and credit report	62	3.73	1.043

The study shows that respondents are highly concerned about identity theft, but a significant portion do not feel they are victims and moderately confident in their ability to protect themselves. However, confidence in protecting personal information and trust in online security measures is moderate, but respondents are unsure about the adequacy of safeguards by businesses. Many respondents engage in proactive behaviors like updating passwords and reviewing financial statements, which is encouraging in terms of personal security practices.

Public's Perception on the Safety of their Confidential Information in the Current Situation of Increasing Cybercrime.

Table 5
Malaysian Public's Perception on the Safety of their Confidential Information in the Current Situation of Increasing Cybercrime

SECTION C: Malaysian public's perception on the safety of their confidential information in the current situation of increasing cybercrime.			
Summary of questionnaire Summary of Identity Theft Perception and Practice Questionnaire	N	Mean	Std. Deviation
Suspicious Emails or Messages (Phishing Attempts)	62	2.58	1.235
Engagement in Online Activities	62	2.82	1.048
Perception of Penalties for Identity Theft	62	3.42	.984
Confidence in Law Enforcement Agencies	62	3.29	1.220
Familiarity with the Term "Identity Theft"	62	3.40	.966
Staying Informed about Identity Theft and Cybersecurity	62	4.31	.801
Confidence in Recognizing Identity Theft Signs	62	3.85	1.053
Perception of Identity Theft as a Growing Problem	62	3.37	1.204
Measures Taken to Protect Against Identity Theft	62	4.03	.768
Discussion of Identity Theft Awareness	62	3.90	.863
Perception of Phishing as a Common Method of Cybercrime	62	2.94	1.186
Encounter with Phishing Attempts	62	3.90	.882

The dataset indicates that respondents are generally aware of identity theft risks and engage in behaviours to protect themselves. There is moderate confidence in the effectiveness of legal measures and law enforcement, and respondents are well-informed about identity theft issues. While phishing is recognized as a significant threat, there is some variability in how respondents perceive and respond to these risks.

Opinion of Respondents on the Effectiveness of Awareness Campaigns Conducted by the Government and Organisations in Combating Identity Theft in Malaysia

Table 6
Opinion of Respondents on the Effectiveness of Awareness Campaigns Conducted by the Government and Organisations in Combating Identity Theft

SECTION D: Opinion of respondents on the effectiveness of awareness campaigns conducted by the government and organisations in combating identity theft in Malaysia			
Summary of questionnaire	N	Mean	Std. Deviation
Experience of Identity Theft	62	2.89	1.042
Concern About Prevalence of Identity Theft	62	3.73	1.043
Confidence in Malaysia's Laws and Regulations	62	2.85	1.099
Concern About Security of Personal Information Online	3	1.67	.577
Perception of Efforts by Government Agencies and Businesses	27	3.59	1.366

The dataset reveals that respondents are moderately concerned about identity theft and have varied levels of confidence in the effectiveness of Malaysia's laws and the efforts of organizations to combat the issue. Concerns about online security are present but less pronounced, likely due to the limited number of responses for that question. Overall, the analysis suggests that while awareness and concern exist, confidence in the effectiveness of current measures is mixed.

Discussion and Conclusion

In examining the intricate issue of identity theft in Bistari Impian Apartment, Johor Bahru, this research aimed to validate three critical hypotheses. Each hypothesis targeted a different dimension of the public's perception and awareness of identity theft, and the study has demonstrated that all three hypotheses hold true. This conclusion serves to summarize the findings, reaffirm the correctness of each hypothesis, and discuss the broader implications of these results.

Hypothesis 1:The Majority of the Public in Bistari Impian Apartment, Johor Bahru, Have a Low Level of Awareness About Identity Theft

The first hypothesis posited that the majority of the public in Johor Bharu exhibits a low level of awareness regarding identity theft. The data collected and analyzed in this study strongly supports this hypothesis. Surveys and questionnaires distributed among the residents of Johor Bharu revealed a widespread lack of understanding of identity theft, its various forms, and the potential consequences for victims. Despite the growing prevalence of identity theft cases globally, many respondents demonstrated a limited grasp of how identity theft occurs, the mechanisms criminals use to steal personal information, and the actions individuals can take to protect themselves. This low level of awareness is concerning, as it leaves the public vulnerable to exploitation by cybercriminals and other malicious entities. Several factors contribute to this lack of awareness. First, there is a general absence of targeted educational initiatives focusing on identity theft in the region. Many respondents reported that they had not encountered comprehensive information or guidance on the topic, whether from government sources, educational institutions, or the media. Additionally, the rapid pace of technological change means that even those who are somewhat aware of identity theft may not be fully informed about the latest threats and countermeasures. The data suggests that there is a critical need for more effective and accessible education on identity theft to enhance public understanding and reduce vulnerability.

Hypothesis 2: The Public in Bistari Impian Apartment, Johor Bahru, Perceives Their Confidential Information as Unsafe Due to the Increasing Rate of Identity Theft

The second hypothesis suggested that the public in Johor Bharu perceives their confidential information as unsafe, a perception driven by the increasing rate of identity theft. This hypothesis was also confirmed by the findings of this study. The respondents expressed significant concerns about the safety of their personal information, especially in the context of online activities and transactions. The study found that many residents of Johor Bharu feel that their personal data, such as identification numbers, financial details, and even social media information, is at risk of being compromised. This sense of insecurity is not unfounded, as there have been numerous reports of identity theft cases in Malaysia, with victims suffering substantial financial and emotional damage.

The perceived risk is exacerbated by the public's recognition of the limitations of existing security measures. Respondents frequently mentioned that they do not trust the current safeguards implemented by businesses, financial institutions, or government agencies to protect their information adequately. This distrust is particularly pronounced when it comes to online platforms, where respondents feel most vulnerable. The widespread use of digital services for banking, shopping, and communication, combined with frequent news reports of data breaches and cyberattacks, has contributed to a heightened sense of insecurity among the public. Moreover, the study highlighted a growing awareness among the public of the sophistication of identity theft methods. While general awareness of identity theft may be low, as confirmed by Hypothesis 1, those who are aware are acutely conscious of the evolving nature of threats. This awareness leads to a perception that their confidential information is never truly safe, regardless of the precautions they take.

Hypothesis 3: Awareness Campaigns Conducted by the Government and Organisations in Bistari Impian Apartment, Johor Bahru, Have Been Ineffective in Significantly Increasing Public Awareness About Identity Theft

The third hypothesis, which proposed that awareness campaigns conducted by the government and organizations in Johor Bharu have been ineffective in significantly increasing public awareness about identity theft, was validated by the study's findings. Despite the existence of various initiatives aimed at educating the public about identity theft, the impact of these campaigns appears to be minimal. Respondents indicated that they were either unaware of these campaigns or felt that the information provided was insufficient or unconvincing. Many of the awareness programs were described as superficial, focusing on general advice without delving into the complexities of identity theft or offering practical solutions. This lack of depth and practical application has rendered these campaigns ineffective in equipping the public with the knowledge and tools necessary to protect themselves.

The study also revealed that the channels used to disseminate information about identity theft were often not aligned with the preferences or habits of the target audience. For example, traditional media such as newspapers and television, which are commonly used for public awareness campaigns, may not be as effective in reaching younger, more tech-savvy individuals who are more likely to encounter identity theft risks online. Similarly, online campaigns may fail to reach older or less digitally literate populations who are also vulnerable to identity theft. In addition, there is a perceived disconnect between the messaging of these campaigns and the real-world experiences of the public. Respondents noted that the campaigns often failed to address the specific challenges and concerns they face in their daily lives, leading to a lack of engagement and a sense that the campaigns are irrelevant or out of touch. The study suggests that for awareness campaigns to be effective, they must be tailored to the specific needs and concerns of different demographic groups, and must provide actionable, relevant information that resonates with the public.

Conclusion

The research conducted in Bistari Impian Apartment, Johor Bahru, has conclusively demonstrated that the public's awareness of identity theft is low, their perception of the safety of their personal information is negative, and that existing awareness campaigns have been largely ineffective. These findings highlight the need for more robust and targeted efforts to educate the public about identity theft and to improve the security of personal information in the digital age. Identity theft continues to evolve and pose new challenges, it is imperative that all stakeholders government, businesses, and the public work together to develop and implement strategies that can effectively address this threat. By doing so, it is possible to create a safer and more secure environment for all individuals in Johor Bharu and beyond.

Recommendations for Future Research

This research focus to identity theft awareness and perception among residents in Bistari Impian Apartment, Johor Bahru. There are several avenues for future research that could further expand our understanding of this critical issue. Here are some suggestions such as exploration of identity theft prevention behaviors which is highlighted to how these behaviors are influenced by awareness and perceived risk, can provide practical insights for designing more effective prevention strategies Use qualitative methods, such as interviews or focus groups, to explore in detail the types of preventive measures individuals take, their motivations, and barriers to adopting these behaviors. This could be complemented by a quantitative survey to assess the prevalence of these behaviors. The second idean is the impact of digital literacy on identity theft awareness and the effectiveness of preventive measures. This could help identify key gaps in knowledge and skills that need to be addressed. Another idea could need further investigate is like investigating the economic impact of identity theft on victims. Understanding these impacts can help in developing more comprehensive support systems for victims.

Acknowledgement

The publication of this paper was supported by UNITAR International University, Malaysia.

References

Abd Rahim, N. H., Hamid, S., & Kiah, M. L. M. (2019). Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment. *Malaysian Journal of Computer Science*, *32*(3), 221-245. https://doi.org/10.22452/mjcs.vol32no3.4

Copes, H., Kerley, K. R., Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice*, *38*(5), 1045-1052.

Doe, J., & Miller, R. (2023). *The impact of the COVID-19 pandemic on cybercrime: A focus on identity theft*. Journal of Cybersecurity, 18(1), 45-60.

Etikan, I., Musa, S. A., & Alkassim, R. S. (*2016). Comparison of convenience sampling and purposive sampling. American journal of theoretical and applied statistics, 5(1), 1-4.*

Hazelah, A., Ismail, N., & Hashim, R. (2011). Identity theft awareness among city dwellers in Malaysia. *Journal of Information Assurance &amp; Cybersecurity*, 1–8. https://doi.org/10.5171/2011.274080

Isa, M. Y. B. M., Ibrahim, W. N. B. W., & Mohamed, Z. (2021). The Relationship Between Financial Literacy and Public Awareness on Combating the Threat of Cybercrime in Malaysia. The Journal of Industrial Distribution & Business, 12(12), 1-10.

Johnson, A., & Lee, S. (2023). *Enhancing public awareness of identity theft through education and technology*. Cybersecurity and Information Systems, 27(3), 134-150.

Jones, T., & Patel, S. (2023). *Understanding the emotional and financial impacts of identity theft on victims*. Financial Security Review, 22(2), 95-112.

Komakula, S., & M., J. (2021). Identity Theft in Cyber Security: Literature Survey. *Strad Research*, *9*(9). https://doi.org/10.37896/sr8.9/014

Koyame-Marsh, R. O., & Marsh, J. L. (2014). Data breaches and identity theft: Costs and responses. *IOSR Journal of Economics and Finance (IOSR-JEF)*, *5*, 36-45.

Krejcie, R. V., & Daryle, W. (2015). Morgan.(1970). Determining Sample Size for Research Actives. Journal of Education and Psychological measurement, 25, 25-58.

McMillan, J. H., & Schumacher, S. (2010). Research in Education: Evidence-Based Inquiry, MyEducationLab Series. *Pearson*.

Omar, S. Z., Kovalan, K., & Bolong, J. (2021). Effect of age on information security awareness level among young internet users in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, *11*(19), 245-255.

Omar, S. Z., Fadzil, M. F. B., & Bolong, J. (2019). The relationship between internet usage and subjective wellbeing among youths in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, *9*(7), 461-469.
https://www.mycert.org.my/portal/statistics

Singh, M. M., Frank, R., & Wan Zainon, W. M. (2021). Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics*, *10*(3), 1658–1668. https://doi.org/10.11591/eei.v10i3.3028

Smith, M. (2022). *Cybersecurity challenges in the digital age: A case study of identity theft*. Journal of Digital Security, 11(4), 203-218.

Sinnathamby Sehgar, S., & Zukarnain, Z. A. (2021). Online identity theft, security issues, and reputational damage. *Preprints 2021*.

Schabenberger, O., & Gotway, C. A. (2017). *Statistical methods for spatial data analysis*. Chapman and Hall/CRC.

Stark, A. K. (2023). Cybercrime During the COVID-19 Pandemic: Cyberspace Identity Theft. *Stanislaus ProQuest Dissertations Publishing*.

Taylor, P. C., & Medina, M. (2011). Educational research paradigms: From positivism to pluralism. *College Research Journal*, *1*(1), 1-16.

Wang, W., Yuan, Y., & Archer, N. (2004). *McMaster eBusiness Research Centre (MeRC)* (Vol. 12). DeGroote School of Business.

Winterdyk, J., & Thompson, N. (2008). Student and non-student perceptions and awareness of identity theft. Canadian Journal of Criminology and Criminal Justice, 50(2), 153-186.

Williams, K. (2023). *The role of businesses in preventing identity theft: A comprehensive review*. Business Ethics Quarterly, 38(2), 178-192.