INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 13, Issue 12, (2023) E-ISSN: 2222-6990

Exploring Teenage Awareness of Social Media Fraud in Malaysia

Kuwihoi New & ZianXiang Kong

Faculty of Humanities and Social Sciences, Department of Journalism & Communication Studies, Southern University College, 81300 Skudai, Johor, Malaysia

Corresponding Author Email: khnew@sc.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v13-i12/19859 DOI:10.6007/IJARBSS/v13-i12/19859

Published Date: 04 December 2023

Abstract

Social media platforms have become integral to modern communication, allowing individuals to connect with loved ones and stay abreast of trends. However, recent studies have uncovered the prevalence of fraud within today's social media landscape, highlighting it as a global issue. This research aims to explore into the perceptions of Malaysian teenagers regarding social media fraud. The primary objective of this study is to explore the experiences of Malaysian teenagers in relation to social media fraud, with a focus on identifying the psychological aspects of both teenagers and fraudsters involved. Furthermore, the research seeks to develop effective strategies to reduce and prevent social media fraud among teenagers in Malaysia, while also providing practical recommendations and raising awareness among this demographic. A comprehensive quantitative online survey questionnaire was administered to 385 teenage respondents in Malaysia. The collected data was analysed using IBM SPSS Statistical Package, and an ANOVA test was employed to verify the research hypotheses. The results revealed compelling evidence supporting the hypotheses put forth in this study. Firstly, the analysis indicated that sharing personal information on social media significantly increases the likelihood of teenagers falling victim to fraud (p-value = 0.013). Furthermore, a strong correlation was established between increased social media usage and heightened risk of fraudulent activities (p-value = 0.049), underlining the statistical significance of this relationship. Lastly, the study demonstrated that social media platforms can be exploited as tools for perpetrating fraud (p-value = 0.017), solidifying this assertion with rigorous statistical support. Additionally, the majority of respondents strongly agreed that avoiding suspicious links or websites on social media could effectively reduce the incidence of fraud.

Keywords: Social Media, Fraud, Teenager, Awareness, User Experience, Weird Link.

Introduction

In contemporary society, the prevalence of social networking among young individuals is noteworthy, with many dedicating substantial amounts of time to browsing and chatting on these platforms primarily for entertainment purposes. Originally designed to facilitate connections between professionals in the corporate world, social networking sites have now extended their reach to encompass interactions between friends and family, serving as a means for individuals to connect with one another (Madden et al, 2020). The global convenience of these platforms has contributed to their widespread usage, although their impact on society, particularly among young people, cannot be understated. As social media gained popularity, numerous researchers became interested in studying the development of these networking sites and exploring their advantages and disadvantages (Singh & Guruprasad, 2019).

Technology, as defined by Lun et al. (2020), encompasses the creation, invention, method, or system of new entities that aim to overcome human limitations and facilitate the completion of tasks beyond our capabilities. In the present era, social media represents a technologically advanced digital tool that enables users to rapidly generate and share content with the public (Supedium, 2020). Consisting of a diverse array of websites and applications, social media platforms vary in their functionality. Twitter, for instance, specializes in link sharing and concise text messages, while Instagram and TikTok prioritize photo and video sharing (Hudson, 2020). Nevertheless, it is important to acknowledge that social media has increasingly become a vehicle for fraudulent activities in contemporary society (Martins, 2019; Lutkevich & Wigmore, 2021).

Fraud refers to the deliberate dissemination of false or deceptive information with the intent of illegally depriving individuals of their finances, assets, or rights. To perpetrate fraud, individuals fabricate information or goods to entice and deceive unsuspecting victims. In the physical world, fraud can be prosecuted as both a criminal and civil offense, with legal repercussions including imprisonment, fines, and restitution for victims (Longley, 2020). The convergence of social media and fraudulent practices has given rise to the phenomenon of social media fraud, wherein fraudsters exploit social media platforms as tools to advertise their fraudulent goods or services, which can range from scams to potentially harmful offerings. Instances of fraud can occur across various social media platforms, including Facebook, Instagram, WhatsApp, and many others.

Social media, while serving as an effective means of communication and trend monitoring, has increasingly become a breeding ground for fraudulent activities (Martins, 2019). The pervasive nature of online fraud has transformed it into a global dilemma, with individuals falling victim to deceptive practices (Button et al., 2014). Fraud encompasses deliberate acts or omissions aimed at acquiring unauthorized benefits through deception, false suggestions, concealment, or other unethical methods, relying on the belief and trust of others referring to University of Southern Indiana Web Services. (2019). It entails the dissemination of false information, whether by intentionally withholding crucial details or providing misleading statements to gain access to information that would otherwise not be disclosed without the employment of fraud (Chen, 2021).

The appeal of social media for criminals stems from its various attributes, and as its usage continues to surge worldwide, the opportunities for identity theft and online fraud have magnified (Lewis, 2019). Fraudsters can exploit social media platforms to project an appearance of legitimacy, concealing their true identities while reaching a vast number of individuals at minimal cost according to the United States Securities and Exchange

Commission. (2018) the widespread adoption of social media has granted malicious actors numerous avenues to engage with people and perpetrate fraud. These individuals consistently devise novel and innovative methods to deceive individuals, extracting financial gains or obtaining personal data for their own advantage. Social media fraud poses significant risks in terms of financial loss, emotional well-being, and diminished trust. Therefore, immediate action is imperative to safeguard individuals and minimize the resultant harm (Consumer International, 2019)

Research Rationale

Social media has emerged as a prominent communication tool, facilitating connections among family members, friends, and romantic partners. However, this convenience blurs the boundaries between personal distance and privacy on social media platforms, enabling users to share personal information and update their profiles with ease. This ease of access also leads users to overlook the potential risks associated with online privacy, such as the ease with which anonymous or fraudulent individuals can obtain and misuse personal information like dates of birth, phone numbers, home addresses, school addresses, and names of family members (Trepte & Reinecke, 2011). Incidents such as photo theft, cyberbullying, phone harassment, identity theft, and cyberstalking are frequently reported on platforms like Facebook and Instagram, with teenagers being particularly vulnerable (Maryani et al., 2020). Social media exerts a profound influence on the younger generation, shaping their acceptance of modern cultural ideologies laden with relativism, individualism, emotionalism, modernism, materialism, autonomy, and victimise. These doctrines often engender attitudes that fail to critically evaluate the adverse effects of social media or even foster indifference towards them, resulting in a lack of self-control, excessive consumption, selfishness, and disregard for applicable rules. Certain social media platforms wield substantial impact over individuals' quality of life and habits, leading to detrimental consequences such as compromised health and excessive time spent on social media. For individuals who have been victims of fraud, their ability to manage their emotions and the potential lingering impact on their social connections may become significant concerns (Maryani et al., 2020).

Social media serves as a valuable tool for various purposes, including communication with friends, conducting business, building new connections, and providing entertainment, among other benefits. Its widespread adoption and daily usage by individuals stem from the enjoyment, relaxation, and stress relief it offers. This trend is particularly evident among today's teenagers who possess a natural inclination to explore novel experiences and seek entertainment. However, many users, especially teenagers, remain unaware of the potential threats creep around within social media platforms. These threats encompass various risks such as fraudulent activities, hacking attempts, and the dissemination of viruses. Additionally, the appeal of new discoveries often shields teenagers from recognizing the dangers they may encounter. These threats manifest discreetly, blending seamlessly with appealing content such as money-making schemes, social networking sites, or counterfeit accounts, making them difficult to detect by unsuspecting individuals. Consequently, only those who have fallen victim to these threats understand their menacing nature. By addressing these concerns, it becomes crucial to raise awareness about the darker aspects of social media usage and offer practical suggestions to mitigate these problems effectively (Madden et al, 2020).

In the contemporary era, teenagers are immersed in a highly advanced technological environment, characterized by the ubiquity of smartphones and the indispensability of social media in their daily lives. The influence of social media platforms on teenagers, particularly

those belonging to "Generation Z," has raised concerns due to their increased vulnerability to scams. A research study conducted by the California-based social media investigative service, SocialCatFish.com (Jordan, 2021) has revealed a higher incidence of scams targeting teenagers and young adults. The susceptibility of teenagers to scams can be attributed to their inclination towards connecting with others through social media platforms. They actively engage in sharing their personal experiences and seek to establish new friendships, often without verifying the identities of their online acquaintances. Consequently, the risks associated with online interactions become more pronounced, leading to a higher probability of falling victim to fraudulent schemes (Shannon, 2021).

Another significant issue faced by teenagers is their low self-control, as observed in their tendency to prioritize immediate gratification over delayed rewards. This characteristic trait, commonly observed during adolescence, arises due to the insufficient development of the brain structures responsible for self-control. The emotional immaturity, lack of impulse control, susceptibility to peer pressure, and the inability to accurately assess the risks associated with potentially harmful decisions further compound the challenges faced by teenagers (Siraj & Ghazal 2021; Cauffman, 2019).Thus, it is crucial to investigate the impact of technological advancements on teenagers and their susceptibility to scams, as well as the underlying causes for their low self-control. By understanding these issues, appropriate measures can be developed to protect teenagers from scams and foster the development of effective strategies to enhance their self-control during this critical stage of their lives.

Research Questions

This study seeks to investigate the perspectives and recommendations of Malaysian adolescents regarding social media fraud. The research aims to address the following questions:

1. To what extent is social media utilized as a tool for perpetrating fraud?
2. Does the act of sharing personal information on social media platforms contribute to an increased risk of fraud?
3. Does engaging with social media platforms result in a higher likelihood of falling victim to fraudulent activities?

Research Objectives

The primary aim of this research is to investigate the experiences of Malaysian teenagers regarding social media fraud. The specific objectives of this study are as follows:

1. To explore Malaysian teenagers' experiences with social media fraud.
2. To identify the psychological aspects of both teenagers and fraudsters involved.
3. To reduce and prevent social media fraud among teenagers in Malaysia.
4. To provide practical suggestions and raise awareness among Malaysian teenagers.

Hypothesis

There are three hypotheses in this research.

H1: Sharing personal information on social media increases the likelihood of teenagers being victims of fraud.

H2: Increased usage of social media is associated with a higher risk of fraudulent activities.

H3: Social media platforms can be exploited as tools for perpetrating fraud.

Literature Review

This section provides a comprehensive examination of the topic, encompassing frauds, knowledge, and theories. It offers an insightful exploration of the background, information, and situational factors that demand attention when engaging with social media and its platforms. Moreover, it highlights prevalent forms of fraud and their consequential impact on individuals utilizing social media. The review also underscores the significance of cultivating awareness, knowledge, and preventive measures in countering fraud and navigating social media, including the crucial aspect of media literacy.

Social Media Fraud

According to the Hertfordshire Constabulary (2021), fraudsters exploit social media platforms to advertise scams to a wide audience, using various means such as posts, ads, and other promotional methods. These scams can range from investment opportunities to the sale of goods or services. Furthermore, fraudsters resort to sending direct messages, including text messages and anonymous chats, in an attempt to extract money or personal information, which can then be used to commit privacy or financial theft. While research conducted by Emma (2020) reveals that fraudsters often conceal themselves on social media to perpetrate scams, leveraging ads, posts, and offers to promote fake products or services. Bridget (2020) reported that in the first half of 2020 alone, victims reported losing nearly $117 million to social media scams. These cases primarily involved instances where individuals sent money to online sellers who failed to deliver, fell victim to romance scams, or were deceived by false offers of financial assistance.

Besides, Panda Security (2020) defined social media platforms as a double-edged sword, offering avenues for users to connect with family and friends while also posing threats if precautions are not taken. The platform harbors numerous scammers, resulting in individual users and businesses collectively losing over $100 billion to internet fraud. Moreover, the Better Business Bureau recorded a surge in fraud cases from 45,811 in 2017 to 48,369 in 2018 (Panda Security, 2020). Earlier on, Samarati (2016) highlighted that despite efforts by social media platforms like Facebook and Instagram to implement account verification services, such as the display of a blue check mark next to verified accounts, cybercriminals and fraudsters have found ways to manipulate this feature. They can imitate legitimate users by copying the verification badge into their background image, deceiving other users and customers. Anonymous scams, pornography scams, fake business partnership/investment scams, and the use of malicious software to perpetrate fraud are among the most common scams observed on social media.

Cybercrime

Cybercrime, as defined by Brush et al. (2019), encompasses criminal activities that are organized through computers, network equipment, or networks. The primary motive behind most cybercrimes is financial gain, although some specifically target computers or equipment to cause direct damage or disablement, such as hacking into others' systems. Additionally, cybercriminals employ tactics like utilizing social media or websites to maliciously spread viral software, illegal information, or pornographic images. These activities not only pose a threat to individuals but also undermine their overall experience with social media platforms. According to Williams (2021), cybercrime involves illegal actions perpetrated through electronic products or networks, including computers, social media, websites, and online and offline applications. The vastness of the cyber world allows for the existence of both legal and

illegal messages and actions, making it easier for criminal acts to be concealed or disguised. Cybercrimes are typically characterized by a deliberate and intentional nature rather than being accidental or coincidental.

While, Kaspersky. (2021) asserted that cybercrimes encompass all criminal activities conducted using the Internet, computer networks, or networked devices. These activities are often orchestrated by organized groups or individuals with advanced technological skills, although there are also less experienced novices involved. Financial gain and information theft are common motives driving cybercriminals to scam and defraud unsuspecting individuals, often employing sophisticated techniques. Besides, the Federal Bureau of Investigation (2021) highlighted several common crimes and risks associated with online platforms. E-mail bombing, for instance, involves the use of unregistered, anonymous, and illegal email addresses to deceive and engage in fraudulent activities. Perpetrators continuously send false cooperation or investment information to compromised or publicly available email addresses. Identity theft is another prevalent cybercrime, where personal information, including phone numbers, addresses, and email addresses, is stolen and used for theft or fraud under someone else's identity.

Furthermore, online predators increasingly target young individuals, exploiting their relative lack of market exposure and heightened trust in others. As a result, young people are particularly susceptible to threats and scams, exposing them to various risks and potentially falling victim to enticing schemes Federal Bureau of Investigation (2021). In conclusion, cybercrime encompasses a range of criminal activities organized through computers, network equipment, or networks. The motivations behind such crimes often involve financial gain, information theft, or direct damage to individuals' systems. Cybercriminals employ advanced technology and various tactics to deceive, defraud, or threaten individuals. It is essential for individuals and organizations to remain vigilant and take proactive measures to protect themselves from the risks posed by cybercriminals.

Cyberstalking

Cyberstalking, as defined by Awati (2021), refers to a criminal activity occurring on the internet or social media platforms where individuals, known as cyber stalkers, employ electronic or digital means to track or harass others. This can be done through various methods such as social media platforms, SMS, emails, or by posting messages in discussion groups or forums, with the intention of instilling fear or threats in their targets. These cyber stalkers often utilize anonymous accounts to carry out their tracking and harassment activities specifically targeting individuals on social media and other online platforms (Awati, 2021).

Gordon (2021) coincided with Awati's definition, stating that cyberstalking involves the use of social media, the internet, and other platforms to follow or harass other users online. This behavior, also referred to as online harassment, is an extension of in-person stalking and cyberbullying. Cyber stalkers employ various methods such as emails, text messages, social media posts, and other means to engage in methodical, deliberate, and ongoing harassment. Even when victims express their discontent or request the cessation of such behavior, individuals engaged in cyberstalking often persist. Consequently, targeted individuals may experience discomfort, unease, fear, distress, anxiety, and worry.

Earlier on, Tomaszek (2012) provided a comprehensive description of stalking, emphasizing its repetitive nature, which can occur multiple times within a single day. This behavior, unwanted and undesirable to the victim, induces a profound sense of fear and danger. Stalking can manifest through direct face-to-face contact or through contact initiated via the

internet, which is commonly referred to as cyberstalking. Furthermore, Pietkiewicz and Treder (2018) asserted that cyberstalking encompasses all forms of internet activities aimed at intimidating victims through electronic communications, including email. They note the similarities between cyberstalking and traditional stalking, wherein perpetrators seek to threaten and exert control over their victims. While conventional stalking tends to disproportionately affect women, cyberstalking is considered more prevalent and indiscriminate, leaving anyone vulnerable to being targeted.

In conclusion, cyberstalking involves the use of electronic or digital means to track and harass individuals on the internet or social media platforms. It shares similarities with traditional stalking but extends the scope and methods of harassment through online channels. Victims of cyberstalking experience a range of negative emotions and may feel a sense of fear and danger. It is crucial to address and prevent cyberstalking due to its potentially harmful consequences for individuals targeted by these activities.

Social Media Attack

Social media platforms such as Facebook, Instagram, and Snapchat have become the most popular and frequently visited social media platforms today, as revealed by a survey conducted by Smith and Anderson (2018) from the Pew Research Centre. With users frequently visiting these sites throughout the day, companies of all sizes are increasingly drawn to these platforms for marketing purposes, as well as for customer service and engagement (Smith & Anderson, 2018). As these platforms continue to grow in popularity, they also become more susceptible to cyber-attacks, as noted by Help Net Security (2019). With a wide range of users, both legitimate and malicious, it becomes increasingly difficult for users to discern between genuine and harmful content, making them vulnerable to cyber-attacks (Help Net Security, 2019). Research conducted by McGuire (2013), cited in Laura (2019), indicates that social media platforms can deliver malware to users at a rate as high as 20 percent, making it imperative for users to take necessary precautions to protect their personal information and privacy (Laura, 2019).

According to McAfee (2014), a leading antivirus company, social media attacks refer to targeted attacks on platforms with a large user base, such as Facebook and Instagram. These attacks are carried out by criminal groups, hackers, or other threat actors who employ advanced techniques and traps to exploit or steal information from social media users. The stolen information, including personal details, location, and activities, can be used to launch fake campaigns, target specific individuals, or facilitate real or virtual crimes (McAfee, 2014). The significance of social media in society has significantly increased, as highlighted by Martins (2019). While social media offers a valuable means of communication and staying updated on trends, it has also become increasingly prone to fraudulent activities. Fraudsters frequently utilize various phishing techniques, such as deceptive posts and direct messages, to deceive individuals and obtain money or personal information. For instance, they might create enticing links with phrases like "Free," leading users to fake websites where they are at high risk of falling victim to scams and having their privacy and personal information compromised (Martins, 2019; Hertfordshire Constabulary, 2021).

Clickbait Scam

Zhang (2020), clickbait refers to a deceptive practice where fake web links employ enticing and confusing content to entice individuals into clicking on them. This form of deception and scam has experienced rapid growth in recent years, posing a significant problem in today's

digital landscape. The proliferation of clickbait diminishes the value of digital content and erodes people's trust, making it a pressing concern. Social media platforms, in particular, have become a breeding ground for this deceptive practice, allowing clickbait to reach a wide and unsuspecting audience. Nee (2019) provided a definition of clickbait as the use of popular or attention-grabbing headlines and text on the Internet to trap people into clicking on a link that leads to a virtual or threatening page. Criminals employ clickbait as a tactic to attract more views and exploit the opportunity to steal visitors' information. This deceptive strategy leverages users' curiosity and entices them to click on intriguing headlines, stories, and articles, despite being aware of their dubious nature.

As highlighted by The California Aggie (2018), many individuals who are familiar with using social media have likely encountered yellow or catchy news, which appears to be genuine but is, in fact, a link leading to a website with threatening messages. While some people approach such content with suspicion, the appeal of these intriguing headlines and stories often overrides their better judgment. Consequently, people continue to fall for clickbait scams, failing to learn from their experiences and effectively distinguish right from wrong. Clickbait typically manifests as sensational headlines aimed at enticing social media users to click on links leading to articles, images, or videos. GCF Global (2020) defined these headlines as appeals to users' emotions and curiosity, rather than providing objective facts. Scammers take advantage of this by posting amusing content that appeals consumers into clicking, subsequently exploiting the opportunity to collect personal information or distribute viruses. Once users click on the enticing link, a pop-up window may prompt them to "update their video player" or "scan" their computer for potential viruses.

According to the United States Attorney General (2018), many users mistakenly believe they are downloading a new version of their current software, but they end up unconsciously downloading malware instead. Other clickbait posts can redirect users to fraudulent websites, tricking them into providing personal information that can be used for identity theft or sold to spammers. Clickbait scams have a significant impact on society as a whole, with teenagers being particularly vulnerable. This susceptibility arises from their obsession and trustfulness, making it easy for them to fall victim to clickbait due to the attractive nature of the headlines. It is crucial to educate teenagers and children to avoid falling for such scams by teaching them to recognize suspicious titles such as "Click now" or "Free Download," which are often associated with clickbait (Common Sense Media, 2019). By instilling this knowledge, the risk of being deceived can be reduced.

Identity Theft

Dan (2020) explained that criminals can employ various methods to create convincing social media profiles using stolen identities, enabling them to engage in criminal activities. One common approach involves stealing someone's photo from the Internet and combining it with the stolen person's name to establish a new account. By doing so, fraudsters can deceive not only others but also the victim's close associates, including friends and family members. According to O'Loughlin (2020), social media platforms serve as a fertile ground for cybercriminals and fraudsters. Accepting invitations from unknown or anonymous individuals and clicking on suspicious links sent via email can expose individuals to viruses, allowing the sender to extract personal information, particularly banking details. In this way, the fraudster gains unauthorized access to the victim's account and can also distribute the stolen bank information, making it vulnerable to theft by others as well. Jtrout (2021) noted that despite the efforts made by social media giants like Facebook to protect user information through

technology, incidents of hacking still occur. Even if users are not entirely hacked, social media can still facilitate criminal activities by allowing the sharing of information and the theft of identities. Some scammers adopt fake accounts to propagate political messages or spread false content, avoiding the use of their own identities and photos. This practice tarnishes the reputation of the individuals whose information has been stolen.

Besides, identity fraud through social media can also occur due to the theft of usernames and passwords, as mentioned by Kaspersky. (2021). Criminals recognize that many users employ the same email, account, or password for multiple platforms. Thus, if a criminal gains access to a person's social media account and password, they are likely to possess the same credentials for financial websites, bank accounts, credit card numbers, and other platforms associated with the victim. It is advisable for individuals to use different passwords for each site or platform to mitigate such risks.

Personal Privacy

Personal privacy, as defined by Winston and Strawn (2021), refers to the safeguarding of individuals' information and privacy, particularly in relation to their connection to the Internet. Social media platforms, as highlighted by Winston and Strawn (2021), generally prioritize the protection of personal and financial data, communications, and user preferences to ensure online security. Internet users commonly adopt various measures to enhance their personal data and privacy, such as employing anti-virus software, choosing strong passwords, being cautious of tracking activities, securing browsing sites, and utilizing privacy tools or devices. Research conducted by Tulane University (2020) indicated a significant increase in concerns about privacy among social media users in recent years. The occurrence of data breaches has raised alarm among many users, prompting them to reconsider their relationship with social media and the security of their personal information. This situation underscores the fact that social media infrastructure supports a wide range of activities, including convenient financial transactions, targeted marketing, and potentially despicable practices involving data abuse. Even back to those old days, Altman (1975) characterized privacy as a means of exerting control over personal information, thereby safeguarding it from unauthorized access. Westin (1967), on the other hand, described privacy in terms of individuals' temporary protection of their information from being accessed by others.

Moreover, Oghazi et al. (2020) argued that individuals often engage in disclosing personal information, sometimes even to the point of addiction, due to the prevalence of others' personal information in the online world. Similarly, Maryani et al. (2020) asserted that sharing personal information is a common process when joining social media platforms, as account creation typically involves providing detailed information about individuals. From one perspective, any act of sharing personal information on social media can be seen as a relinquishment of privacy. Michael and King (2019) suggested that such behavior may be driven by the desire to access personal data and or influence specific target populations, particularly teenagers. Furthermore, Petters (2020) emphasized that privacy serves as the foundation of human freedom, requiring moments of reserve, reflection, intimacy, and solitude to protect people personal data and privacy. Although social media offers a convenient means of connecting with like-minded individuals and staying in touch with friends and family, Axel (2019) warned that if teenagers fail to take appropriate steps to protect themselves, their shared information can compromise their privacy, reputation, and security.

Media Literacy

Media literacy is a crucial skill for individuals, particularly teenagers who frequently engage with social media platforms (Allison & Hiwot, 2018). Despite the perception that teenagers, often referred to as "digital natives," are inherently adept at navigating the online world, they are still susceptible to various risks and misinformation on social media World Health Organization (2019). The term "literacy" traditionally relates to reading and writing skills, which bear similarities to media literacy (Common Sense Media, 2019). According to the Young Leaders of the Americas Initiative (YLAI network, 2019), media literacy involves the ability to recognize different types of media and the messages they convey. In order for teenagers to become critical consumers of media, it is essential for them to develop media literacy skills and habits. These skills encompass the capacity to access media at a basic level, critically analyze it based on key concepts, evaluate its content based on this analysis, and even create their own media (Mediasmarts, 2017).

Media literacy, as described by Mediasmarts (2017), is a component of media education, which equips individuals with the ability to critically comprehend the nature, technology, and impact of media information and products. By embracing media education, individuals can explore, evaluate, understand, and appreciate the multimedia they encounter, fostering an active and engaged approach to media consumption. It further enables youth to discern between reality and fantasy, differentiating virtual and real experiences, media heroes and real heroes, and media role models from authentic individuals (Robertson & Tisdall, 2020). Media literacy plays a vital role in empowering teenagers to navigate the complex media landscape, enhancing their ability to analyze and critically evaluate media content. By developing these skills, teenagers can cultivate a deeper understanding of media's influence and make informed decisions when engaging with social media platforms (Allison & Hiwot, 2018; Mediasmarts, 2017).

Conceptual Of Framework

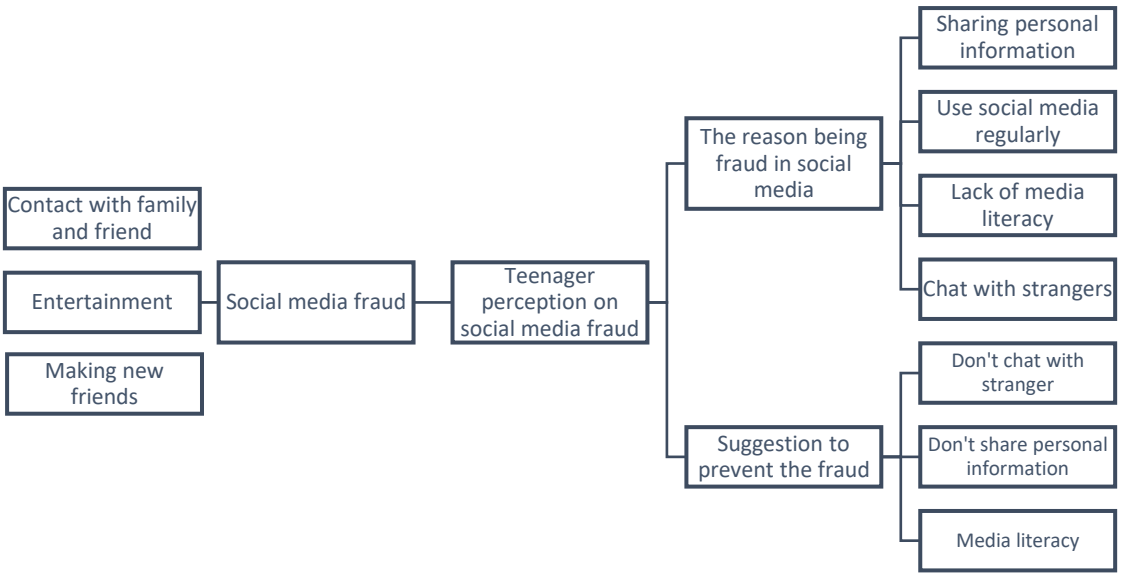

Figure 1: Conceptual Framework

Figure 1 presents the conceptual framework utilized in this research which have been adopted and modified by referring to Shikati (2018) to fit into the objectives of this study. The pervasive influence of social media has revolutionized various aspects of society, ranging from

maintaining connections with family and friends to seeking entertainment and forging new relationships. Nevertheless, it is crucial to recognize that contemporary social media platforms are increasingly plagued by fraudulent activities (Martins, 2019). According to him in a recent study that social media channels are common with fraud. Notably, Shannon (2021) asserted that individuals belonging to Generation Z, particularly teenagers and young adults, are particularly vulnerable to scams. This study aims to comprehend why Malaysian teenagers fall victim to social media fraud by investigating their perspectives on various factors such as information sharing, regular social media usage, lack of media literacy, and engaging in conversations with strangers. Furthermore, the study endeavours to gather recommendations from Malaysian teenagers regarding the prevention of social media fraud for the purpose of evaluation.

Theory Discussion

This research is based on the application of routine activity theory, which is a key theory in environmental criminology. According to the Government of New South Whales (2011), routine activity theory explains that three factors must occur simultaneously for a crime to take place. These factors include the presence of an accessible target, the absence of a competent or intervening guardian, and the existence of a motivated offender. The theory emphasizes that crime can happen at any time and in any space. Wickert (2020) provided a definition of routine activity theory, stating that if there is a motivated offender, a suitable target, and no competent guardian, the likelihood of a crime occurring increases. This can be observed in the context of social media, where a large number of anonymous users make it difficult to identify potential offenders. Consequently, crimes such as scams, hacking, and spamming tend to proliferate.

Routine activity theory is a branch of rational choice theory, initially proposed by Felson and Cohen (1947), cited in McMurtry and Curling (2008) asserted that this theory requires the presence of three elements to cause a crime: a perpetrator with criminal intent and capability, a targeted victim, and an ineffective guardian who fails to prevent the crime. The convergence of these factors in both time and space is essential for a crime to occur. Traditional activity theory offers a macro-level perspective on crime, predicting changes in overall social and economic conditions and their impact on crime rates and victimization. Cohen and Felson (1979) hypothesized that criminal activity is a significant phenomenon influenced by the daily routines and interactions of individuals. People engaged in routine activities may be perceived as suitable targets by motivated criminals. Traditional activity theory posits that crime is a normal occurrence dependent on available opportunities, but motivated offenders will commit crimes if they encounter an unprotected target with sufficient reward.

Routine activity theory is closely related to lifestyle contact theory and gained prominence in criminology during the late 1970s. According to Wikström (2009), routine activities encompass the general patterns of social activities in a society, including family, leisure, work, and time patterns. This theory highlights that changes in routine activities within a society can impact the situations people face and subsequently influence their involvement in criminal behaviour. Additionally, alterations in individuals' exposure to certain situations can lead to changes in their likelihood of engaging in crime, ultimately affecting the overall crime rate of a society. So, routine activity theory, as explained by Cohen and Felson (1979), aims to identify and understand criminal activity at a macro level by examining trends in crime rates. It focuses on the spatio-temporal distribution and grouping of elements within a criminal event, rather than solely exploring the motivations of criminals. By providing a framework for specific and

individual crime analysis, routine activity theory enables the development of effective policies and practices aimed at addressing the factors necessary for crime to exist, thereby preventing it (Tilley, 2011). Cohen and Felson (1979) noted the sociological paradox that, despite improvements in well-being and socioeconomic status during the 1960s, crime rates, particularly violent crime, showed a substantial increase, pointing to factors such as lack of education, poverty, and unemployment as potential causes.

Methods

In the process of research design, methods play a crucial role in collecting and analyzing data. The development of appropriate methods is an integral part of the research design process (Pfeiffer Library, 2021). It is important to distinguish between research methods and research methodologies, as they pertain to different aspects of data collection for a research project. Depending on the topic, the required data types, and the subjects or objects from which data will be gathered, various research methods can be employed (Pfeiffer Library, 2021). These methods can be broadly categorized into quantitative, qualitative, and mixed research techniques.

Quantitative research methodologies involve the use of objective measurements alongside statistical, mathematical, or numerical analyses of data obtained from surveys, polls, questionnaires, or pre-existing statistical data as University of Southern California. (2021). The primary focus of quantitative research is the analysis of numerical data, which allows researchers to identify patterns, determine averages, test causal relationships, and generalize results to a larger population. Quantitative research finds extensive applications in natural and social sciences, including biology, chemistry, psychology, economics, sociology, and marketing (Bhandari, 2021). In contrast, qualitative research aims to uncover the behaviors and perceptions of a target audience regarding a specific topic. Qualitative research employs diverse methods such as in-depth interviews, focus groups, ethnographic research, content analysis, and case study research (Bhat, 2021). It is primarily concerned with the collection and analysis of non-numerical data, such as text, video, or audio. Various fields, including biology, chemistry, psychology, economics, sociology, and marketing, employ qualitative research methods to gain insights into complex phenomena (Bhat, 2021). Mixed methods research combines elements of both quantitative and qualitative approaches to address specific research questions. By utilizing mixed methods, researchers can obtain a comprehensive understanding that surpasses what can be achieved through standalone quantitative or qualitative studies. This approach is particularly valuable in multidisciplinary settings and when investigating complex societal conditions in the behavioral, health, and social sciences (George, 2022).

For the present study, a quantitative research design has been adopted to collect and analyze data in accordance with the research objectives, hypotheses, and workflow. Quantitative research is defined as a systematic investigation of phenomena through the collection of quantifiable data and the application of statistical, mathematical, or computational techniques (Fleetwood, 2021). In this survey, quantitative research methods are employed to examine social media fraud among teenagers, understand the reasons behind their victimization, and provide effective suggestions for prevention. Zikmund et al. (2013), the quantitative method enables researchers to achieve research objectives through empirical evaluation involving numerical measurements and analysis. This study follows a systematic process to describe and test relationships between variables, investigate causal relationships, and collect primary data. Data are collected through sampling, typically with the aim of

describing occurrences or studying the causes of specific activities. Surveys are commonly employed to gather data from specific populations, with respondents answering a series of questions posed by the researcher.

In conclusion, research methods are essential components of the research design process, determining how data is collected and analyzed. Depending on the research topic, data requirements, and target population, researchers can choose from a range of quantitative, qualitative, or mixed methods. Quantitative research focuses on numerical data analysis, while qualitative research delves into non-numerical data to explore behaviors and perceptions. Mixed methods research combines both approaches to gain a comprehensive understanding. For the present study, a quantitative research design is employed, utilizing empirical evaluation and numerical measurements to investigate social media fraud among teenagers and propose preventive measures (Zikmund et al., 2013). Surveys are used to collect primary data from specific populations, enabling the research objectives to be met.

Data Collection Instrument

A data collection technique is a systematic approach employed to gather and analyze data from diverse sources to obtain a comprehensive understanding of a specific area of interest. Accurate data collection is vital for ensuring quality assurance, making informed business decisions, and upholding research integrity. Various sources, including interviews, questionnaires, focus groups, and online surveys, can be utilized to collect data (McLaughlin, 2022). In this research, a survey research technique based on quantitative research principles will be employed. Survey research involves distributing surveys to respondents and subsequently performing statistical analysis on the collected data to derive meaningful conclusions. Surveys have proven to be the most effective and reliable method for conducting research, as they provide valuable insights into consumer opinions and preferences, aiding in informed business decision-making (QuestionPro, n.d.).

For this particular research, questionnaires designed in the form of surveys will be used to gather and analyze opinions and suggestions from Malaysian teenagers. Questionnaires are chosen due to their efficiency, reliability, and accuracy in collecting information from multiple respondents (Preston, 2009). Google Forms will be utilized as the data collection tool, as it allows for the creation of various types of questionnaires and facilitates automated data collection. Upon data collection, the researcher will employ the Statistical Package for the Social Sciences (SPSS) for data analysis. SPSS is a powerful statistical software platform provided by IBM, offering a user-friendly interface and robust features to derive actionable insights from data. Its advanced statistical procedures ensure highly accurate and high-quality decision-making throughout the analytics lifecycle, encompassing data preparation, management, analysis, reporting, and visualization (IBM, 2014).

Questionnaires, which serve as research tools consisting of a series of questions, has been employed to gather valuable information from respondents. These instruments resemble interviews and can be administered in various formats, including online, telephone, paper-based, or in-person, without requiring the researcher's physical presence during the questioning process. Questionnaires can comprise qualitative or quantitative questions and may include a combination of open-ended and closed-ended questions. Open-ended questions allow respondents to provide detailed or concise answers, while closed-ended questions provide predetermined response options (Lucid, 2021). The questionnaire used in this research will be available in English and Chinese languages to accommodate respondents who may not understand either language fully. This language choice ensures that participants

can refer to another language to answer the questionnaire. The questionnaire is organized into sections labeled A, B, C, D, and E, each focusing on a specific subtopic. Section A collects demographic information such as age, gender, and education level. Section B explores respondents' experiences with social media fraud, while Section C investigates the reasons why teenagers fall victim to social media fraud. Section D delves into the motives behind individuals cheating teenagers, and Section E evaluates awareness levels and provides suggestions for preventing fraud by fraudsters. To collect responses, Likert scales will be employed, where respondents indicate their agreement or disagreement on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree) (Lucid, 2021).

Table 1:
Reliability Statistical Test for the Questionnaire

Reliability statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Item	N of Items
.951	.952	17

Table 2:
Summary of Reliability Test

	Number of questions	Corrected Item-Total Correlation	Cronbach's Alpha if item Deleted
Q6	I agree that social media is a new tool for fraud.	.738	.948
Q7	I agree that using social media increases the risk of being cheated.	.876	.946
Q8	I agree that chatting with strangers/fake profiles on social media increases the risk of being cheated.	.833	.946
Q9	I agree that clicking on weird links/websites in social media increases the risk of being cheated.	.769	.947
Q10	I agree that sharing personal information and privacy on social media increases the risk of being cheated, such as residential location.	.759	.947
Q11	I agree that using social media for transactions increases the risk of being cheated, such as payments or business transactions.	.885	.945
Q12	People cheat because of low moral behaviour, such as a lack of guidance.	.720	.948
Q13	People cheat for personal satisfaction or to have fun.	.588	.951
Q14	People cheat due to influence from the external world, such as other people or fraud groups.	.786	.947
Q15	I agree that humans are greedy	.613	.950
Q16	I agree that humans can resist temptation	.534	.952
Q17	I agree that teenagers can control their emotions after being scammed.	.884	.945

Q18	I agree that not sharing personal information on social media can reduce the rate of fraud.	.663	.949
Q19	I agree that setting a strong password for social media accounts can reduce the rate of fraud.	.621	.950
Q20	I agree that avoiding weird links/websites on social media can reduce the rate of fraud.	.725	.948
Q21	I agree that not talking to strangers/anonymous persons can reduce the rate of fraud.	.655	.949
Q22	I agree that improving awareness of media use can reduce the rate of fraud.	.520	.952

Mean and Standard of Questionnaires

The survey questionnaires are divided into four sections, namely sections 1, 2, 3, and 4. Section 1 focuses on demography, encompassing questions 1 to 5, which gather information about gender, age, current location, and experiences with social media. Section 2 explores the reasons behind social media fraud, consisting of questions 6 to 11. Section 3 delves into the motivations behind cheating, covering questions 7 to 12. Finally, section 4 investigates awareness and suggestions for preventing fraud, encompassing questions 13 to 17. Upon analysing the research questions, it is evident that the highest mean score in section 2 is attributed to question 9, which states, "I agree that clicking on weird links/websites in social media increases the risk of being cheated," with an average score of 4.23. Conversely, the lowest mean score in section 2 is associated with question 7, which states, "I agree that using social media increases the risk of being cheated," scoring an average of 3.94. In section 3, the question with the highest mean score is question 12, stating, "People cheat because of low moral behaviour (e.g., lack of guidance)," with an average score of 4.28. Conversely, the lowest mean score in section 3 is attributed to question 17, which states, "I agree that teenagers can control their emotions after being scammed?" scoring an average of 2.46. Moving on to section 4, question 18 attains the highest mean score, stating, "I agree that never sharing personal information on social media can reduce the rate of fraud," with an average score of 4.35. Conversely, question 19 achieves the lowest mean score in section 4, which states, "I agree that setting a strong password for social media accounts can reduce the rate of fraud," with an average score of 3.94. In conclusion, the questionnaire reveals that the statement with the highest mean score overall is question 18, which states, "I agree that never sharing personal information on social media can reduce the rate of fraud," with an average score of 4.35. Conversely, question 17, which asks, "I agree that teenagers can control their emotions after being scammed?" obtains the lowest mean score of 2.46.

Table 3:
Mean Score and Standard Deviation

	Number of Questions	Mean	Std Deviation
Q6	I agree that social media is a new tool for fraud.	4.12	.914
Q7	I agree that using social media increases the risk of being cheated.	3.94	.928
Q8	I agree that chatting with strangers/fake profiles on social media increases the risk of being cheated.	4.18	.855
Q9	I agree that clicking on weird links/websites in social media increases the risk of being cheated.	4.23	.876
Q10	I agree that sharing personal information and privacy on social media increases the risk of being cheated, such as residential location.	4.21	.826
Q11	I agree that using social media for transactions increases the risk of being cheated, such as payments or business transactions.	4.17	.861
Q12	People cheat because of low moral behaviour, such as a lack of guidance.	4.28	.837
Q13	People cheat for personal satisfaction or to have fun.	3.78	1.01
Q14	People cheat due to influence from the external world, such as other people or fraud groups.	3.89	1.04
Q15	I agree that humans are greedy	4.06	.879
Q16	I agree that humans can resist temptation	2.57	.955
Q17	I agree that teenagers can control their emotions after being scammed.	2.46	.976
Q18	I agree that not sharing personal information on social media can reduce the rate of fraud.	4.35	.773
Q19	I agree that setting a strong password for social media accounts can reduce the rate of fraud.	3.94	1
Q20	I agree that avoiding weird links/websites on social media can reduce the rate of fraud.	4.28	.904
Q21	I agree that not talking to strangers/anonymous persons can reduce the rate of fraud.	4.15	.978

Q22	I agree that improving awareness of media use can reduce the rate of fraud.	4.19	.973

Data analysis

According to LeCompte (2000), data analysis involves transforming statistical information into a narrative to derive insights. To handle large volumes of data effectively, it is crucial to break it down into manageable components. This process comprises three key aspects: organizing the data for structure and accessibility, summarizing it to reduce complexity and identify patterns, and approaching analysis from either a bottom-up or top-down perspective. The complexity and challenges inherent in data analysis are emphasized, highlighting the need to bring order, structure, and significance to collected data (LeCompte, 2000). In the present study, data analysis will involve using Google Forms for data collection, with responses automatically stored in Microsoft Excel for easy reference. The collected data will then be evaluated and analyzed using the Statistical Package for the Social Sciences (SPSS), which offers professional statistical tools, including the ANOVA test for determining p-values and exploring variable relationships.

Selection of Social Media

Social media platforms, such as Facebook, Twitter, and Instagram, have become vital for building and engaging online communities (Survey Monkey, 2021). These platforms attract like-minded individuals who share information and ideas, making them ideal for researchers and businesses seeking feedback on their work. Utilizing Facebook, for example, offers numerous advantages due to its popularity and extensive user base. Researchers can easily reach their target audience, especially Malaysian teenagers, and collect significant amounts of data by creating surveys and posting them on the platform. Additionally, the wide range of public and private groups on Facebook provides researchers with ample opportunities to join and collect data that aligns with their research objectives (Survey Monkey, 2021).

Online Survey

Online surveys were chosen as the method for data collection in this study due to their convenience and cost-effectiveness (Caroline, 2020). Respondents have the flexibility to answer questions at their own pace and on their own schedule, which is facilitated by the ease and low cost of online surveys. The use of online surveys has reduced the overall cost of data collection, as there are numerous websites and platforms available that allow for easy survey creation at reasonable prices. Additionally, the immediate feedback provided by online surveys helps identify and rectify any issues with contact data (Caroline, 2020). However, it is important to acknowledge the potential challenges associated with online surveys. Survey fraud can be a significant concern, with respondents providing fake answers or rushing through surveys without genuine engagement. Moreover, certain populations may have limited access to the internet or be less likely to respond to online questionnaires, leading to sampling and respondent availability limitations. Furthermore, online survey problems may arise from respondents deleting or ignoring surveys if they feel annoyed or inconvenienced (Mahmutovic, 2021). Therefore, researchers must carefully design their surveys, address potential limitations, and select suitable participant groups when conducting online surveys.

Sampling

In this study, convenience sampling was employed as the sampling method (Turner, 2020). Convenience sampling is a non-probability sampling technique that involves selecting individuals who are easily accessible or readily available as participants in the study (Lavrakas, 2008). This approach was chosen because social media platforms offer a powerful and reliable means of distributing the survey form online, either through posting in groups or sharing with friends (Turner, 2020). Convenience sampling allows researchers to collect data more quickly and at a lower cost compared to other sampling methods that aim to reach every member of the population (Turner, 2020). By distributing questionnaires to individuals within their proximity or to acquaintances on social media, the researcher can conveniently gather the required data (Lavrakas, 2008). Furthermore, to ensure voluntary participation and increase the likelihood of obtaining representative responses, simple random sampling will be employed in addition to convenience sampling. Simple random sampling is a technique that involves selecting individuals from the population in such a way that each member has an equal chance of being chosen. This method, also known as a "method of chances," relies solely on random selection, thereby minimizing biases and increasing the generalizability of the findings (Fleetwood, 2021). By utilizing both convenience and simple random sampling techniques, this study aims to efficiently gather data from respondents while maintaining the principles of voluntary participation and unbiased representation.

Scheme of Analysis

In the statistical analysis section of this study, a quantitative research method was employed, and two analysis methods were used: descriptive analysis and regression analysis, in order to analyze the data (Rawat, 2021). Descriptive analysis was chosen as it allows for the examination of data using statistical tools such as graphs and charts, enabling the description, presentation, and summarization of data points in a meaningful manner to identify patterns that meet specific conditions. This step is crucial in analyzing statistical data, as it facilitates the determination of data distributions, the identification of errors and anomalies, and the recognition of associations between variables, thereby enabling further statistical analysis (Rawat, 2021). Typical techniques employed in descriptive analysis include the development of tables containing quantiles and means, conducting dispersion analysis (e.g., variance or standard deviation), and constructing cross-tabulations or "crosstabs" to test multiple hypotheses. Regression analysis was utilized in this study to test and estimate the relationship between a dependent variable and independent variables (Jordan, M. 2021). It helps identify the variables that significantly impact a particular topic and reveals the importance and influence of each factor on the others. In regression analysis, the dependent variable represents the key factor for understanding or predicting the data, while the independent variables refer to factors that are hypothesized to have a significant impact on the dependent variable (Jordan, M, 2021). Before conducting regression analysis, it is crucial to have a dependent variable that has been hypothesized to be affected by one or more independent variables, and a comprehensive dataset must be established. This dataset can be created by administering surveys to the target audience, covering all relevant independent variables of interest.

Results

Demography Information

A total of 385 respondents participated in the survey, acknowledging the possibility that some responses may have been fraudulent. Notably, a majority of the respondents fall within the age range of 19-24, which corresponds to the demographic of teenagers who frequently utilize social media platforms. The research methodology employed in this study involves the application of ANOVA tests. All data obtained from the respondents will be analysed using SPSS to calculate various statistical measures such as mean, standard deviation, and hypotheses testing. By employing this rigorous approach, the research aims to draw meaningful insights and contribute to a better understanding of the subject matter. Among the participants, 55.6% (214) identify as male, while 44.4% (171) identify as female. Furthermore, the age distribution reveals that 57.9% (223) of respondents are aged 21-22, 24.4% (94) are aged 19-20, 10.1% (39) are aged 23-24, 5.5% (21) are aged 17-18, and 2.1% (8) are aged 15-16.

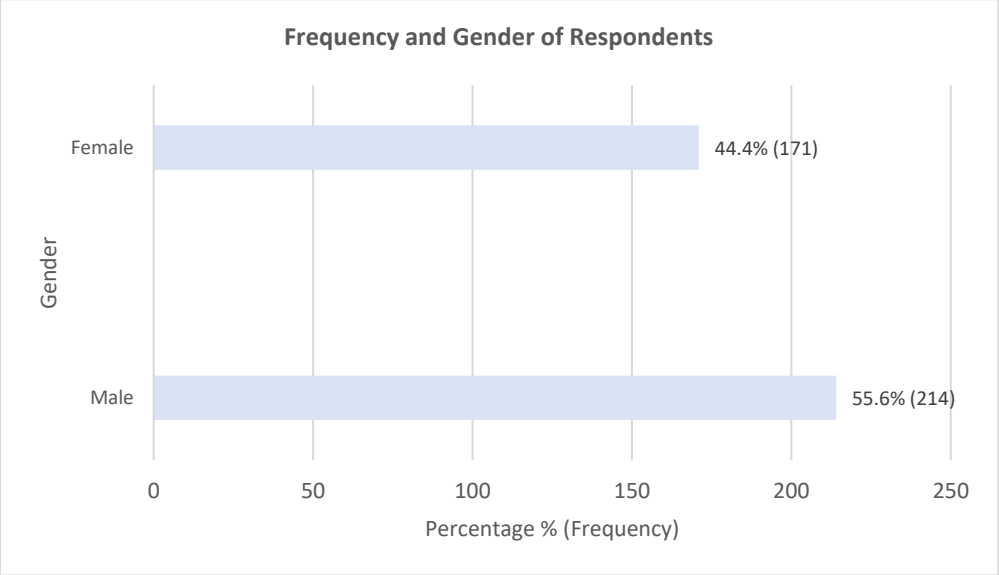

Figure 2: Summary of Respondents according to Gender

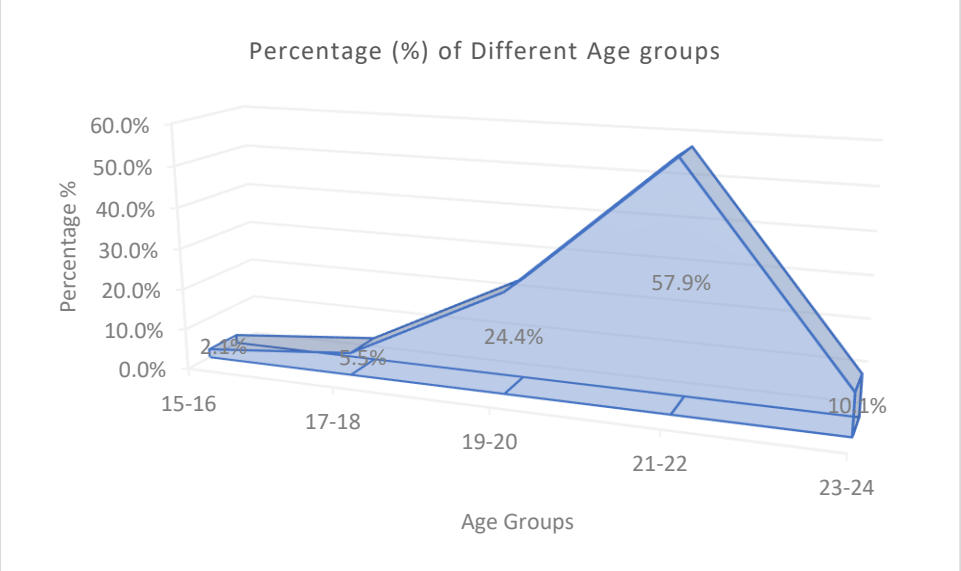

Figure 3: Summary of Respondents according to Age Groups

Table 4:
Geographical Location of Respondents

States	Frequency	Percentage (%)
Johor	248	64.4%
Kedah	16	4.2%
Kelantan	20	5.2%
Malacca	25	6.5%
Negeri Sembilan	20	5.2%
Pahang	14	3.6%
Penang	12	3.1%
Perak	2	0.5%
Perlis,	3	0.8%
Sabah	5	1.3%
Sarawak	8	2.1%
Selangor	10	2.6%
Terengganu.	2	0.5%
Total	385	100%

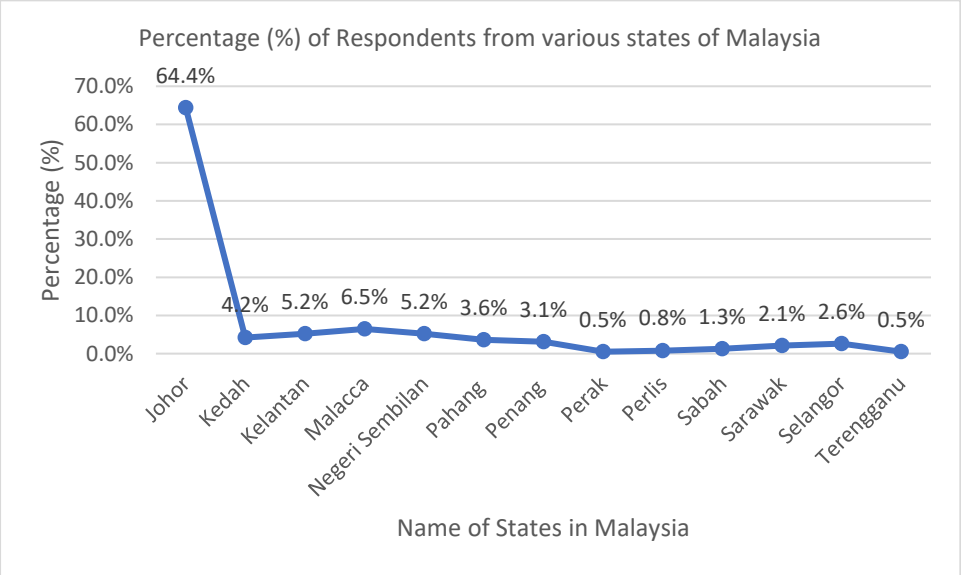

Figure 4: Summary of Geographical Location of the Respondents

Based on the findings presented in Figure 4, it is evident that the largest proportion of respondents, amounting to 64.4% of the total, originated from Johor. On the other hand, the smallest percentage of respondents, comprising a mere 0.5%, hailed from Terengganu. Consequently, it can be concluded that Johor exhibited the highest percentage, indicating that the majority of respondents in this study reside in Johor.

Regarding the geographical representation of the respondents, it is noteworthy that a significant proportion of respondents, Figure 5 below shows, 96.4% (371), demonstrate awareness of social media fraud, while a minority, 3.4% (14), indicate unfamiliarity with the concept. Moreover, in Figure 6, 55.6% (214) of respondents admit to having experienced social media fraud, while 44.4% (171) claim not to have encountered such fraudulent activities on social media platforms.

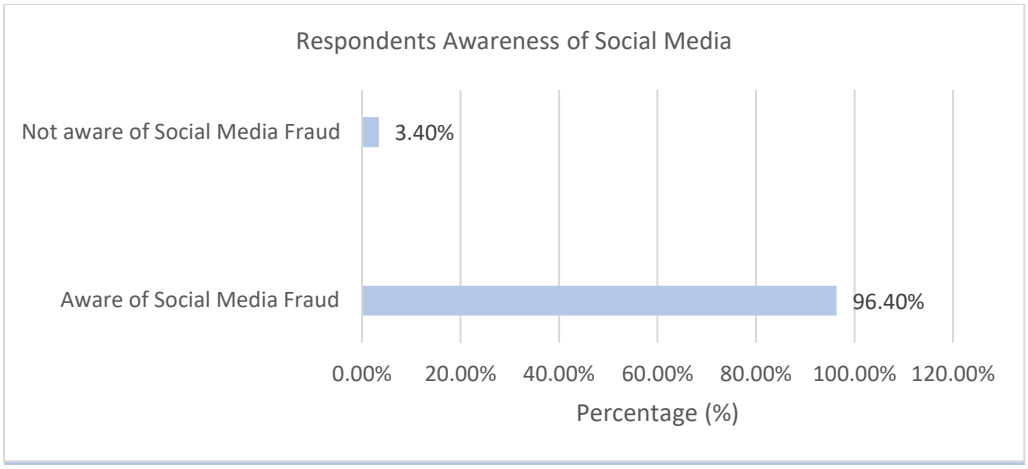

Figure 5: Percentage of Respondents Awareness of Social Media Fraud

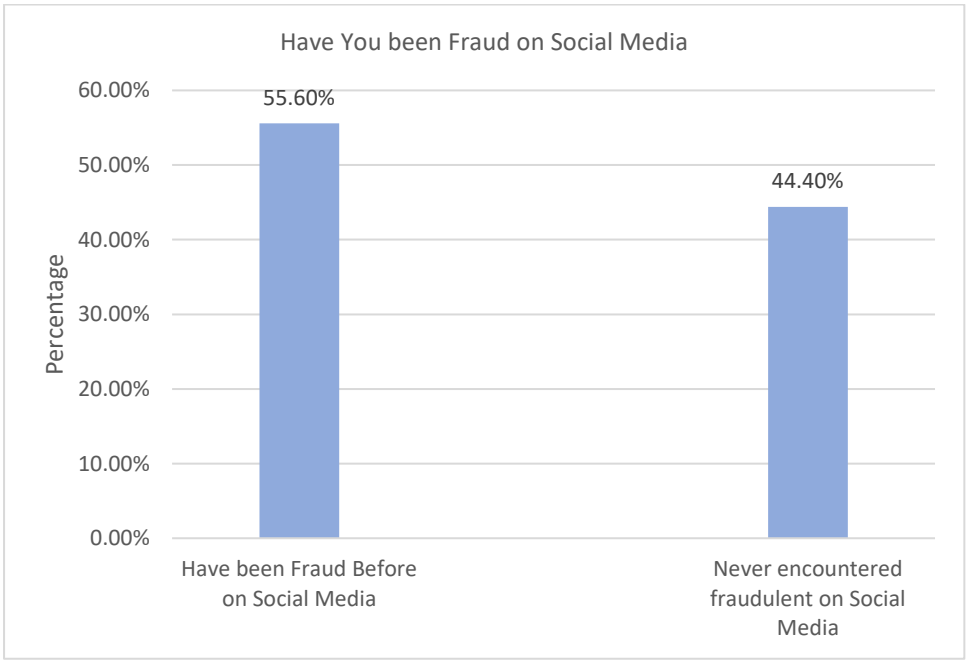

Figure 6: Summary of Respondents been Fraud on Social Media

Table 5:
Reasons for Being Fraud on Social Media

Respondents (%) / Question	S. Disagree	Disagree	N. Agree nor Disagree	Agree	S. Agree
I agree that social media is a new tool for fraud.	0.8%	6%	13.8%	39.5%	40%
I agree that using social media increases the risk of being cheated.	1%	6.2%	21%	40.8%	30.9%
I agree that chatting with strangers/fake profiles on social media increases the risk of being cheated.	0.8%	3.9%	12.7%	41.8%	40.8%
I agree that clicking on weird links/websites in social media increases the risk of being cheated.	1%	4.2%	10.6%	38.7%	45.5%
I agree that sharing personal information and privacy on social media increases the risk of being cheated, such as residential location.	0.5%	2.9%	14%	40.3%	42.3%
I agree that using social media for transactions increases the risk of being cheated, such as payments or business transactions.	1%	3.6%	12.7%	42.3%	40.3%

Table 5 presents a comprehensive analysis of the respondents' perspectives on various aspects related to the risks of fraud on social media. It reveals that 45.5% of respondents strongly agree that clicking on unusual links or visiting suspicious websites through social media increases the likelihood of being cheated. This is primarily due to the potential exposure of personal information and passwords to these websites, which can be recorded by the website owners, consequently escalating the risk of fraud (Di Girolamo, 2020). Furthermore, 41.8% of respondents agree and 42.3% strongly agree that engaging in conversations with strangers or fake profiles on social media heightens the risk of falling victim to scams. The Australian Cyber Security Centre (2020) has highlighted that personal information and privacy hold significant value in the digital realm. When such information is divulged in public spaces, it becomes susceptible to identity theft by fraudsters or hackers.
In addition, 40% of respondents strongly agree that social media has emerged as a new tool for fraud, while 40.8% agree that utilizing social media platforms increases the risk of being cheated. As mentioned previously, the majority of respondents perceive social media as a breeding ground for fraudulent activities. The anonymity offered by the internet allows fraudsters or hackers to create fake profiles and engage in deceptive conversations. Once individuals reveal their personal information and privacy, their identities become vulnerable

to theft by these malicious actors. Overall, the findings from Table 5 highlight the respondents' awareness of the risks associated with social media fraud. They emphasize the importance of cautious behaviour when interacting with unfamiliar links, strangers, and sharing personal information online in order to mitigate the risk of falling victim to scams or identity theft.

Table 6:
Reasons Why People Cheat

Respondents (%) / Question	S. Disagree	Disagree	N. Agree nor Disagree	Agree	S. Agree
People cheat because of low moral behaviour, such as a lack of guidance.	0.8%	3.6%	9.4%	39.7%	46.5%
People cheat for personal satisfaction or to have fun.	0.8%	11.9%	23.4%	36.1%	27.8%
People cheat due to influence from the external world, such as other people or fraud groups.	1.3%	10.9%	19.2%	34.5%	24%
I agree that humans are greedy	1.3%	4.9%	13%	47.8%	33%
I agree that humans can resist temptation	12.2%	34.8%	41.3%	7%	4.7%
I agree that teenagers can control their emotions after being scammed.	18.7%	30.4%	40.3%	7.8%	2.9%

The analysis presented in Table 6 sheds light on various factors contributing to why people engage in cheating behaviours. The findings indicate that 47.8% of respondents agree that human nature is inherently driven by greed. This aligns with the notion that individuals often desire more than what is necessary, falling into the mind-set of "the more, the better." For instance, when an individual already possesses sufficient funds for their daily needs but desires more, they may resort to stealing or cheating from others if legal means are unavailable (Richard, 1996). Furthermore, 46.5% of respondents strongly agree that people cheat due to low moral behaviour. Individuals with compromised moral values may not think rationally and fail to consider the consequences of their actions, leading them to engage in cheating behaviours. Additionally, a lack of guidance contributes to people cheating. When individuals lack proper guidance, such as parental support or mentorship, they may be more inclined to engage in unethical activities or fail to comprehend the gravity of their actions (Ahmad, 2017).

In terms of resisting temptation, 41.3% of respondents neither agree nor disagree, suggesting that there is uncertainty regarding human capacity to resist temptation. Moreover, 34.5% of respondents agree that people cheat due to external influences, such as peer pressure or involvement with fraudulent groups. This phenomenon can be explained by cultivation theory, which posits that individuals are influenced by the virtual world, such as television. For instance, exposure to news related to fraud or scams can trigger thoughts and ideas about engaging in similar activities, potentially leading to actual criminal behaviour

(Wang, 2018). In summary, the findings from Table 6 highlight the role of factors such as greed, low moral behaviour, lack of guidance, and external influences in explaining why people cheat. These insights contribute to a better understanding of the underlying motivations and circumstances that drive individuals to engage in dishonest behaviours.

Table 7:
Awareness and Suggestion to Prevent Fraud

Respondents (%) / Question	S. Disagree	Disagree	N. Agree nor Disagree	Agree	S. Agree
I agree that not sharing personal information on social media can reduce the rate of fraud.	0.8%	2.3%	6.8%	41.6%	48.6%
I agree that setting a strong password for social media accounts can reduce the rate of fraud.	1.6%	7.5%	21.6%	34.3%	35.1%
I agree that avoiding weird links/websites on social media can reduce the rate of fraud.	1.8%	3.4%	9.6%	35.1%	50.1%
I agree that not talking to strangers/anonymous persons can reduce the rate of fraud.	1.8%	6.5%	10.9%	36.6%	44.2%
I agree that improving awareness of media use can reduce the rate of fraud.	1.8%	6.5%	9.1%	35.8%	46.8%

The analysis presented in Table 7 explores the effectiveness of various preventive measures against fraud. The findings reveal that 46.8% of respondents strongly agree that improving awareness of media use can serve as a preventive measure. Media literacy, as discussed in the literature review, plays a crucial role in enhancing awareness while using social media or the internet. It enables individuals, especially teenagers, to critically analyse situations, evaluate the consequences, and develop a heightened sense of awareness (Mediasmarts, 2017). Similarly, 50.1% of respondents strongly agree that avoiding suspicious links or websites on social media can significantly reduce the incidence of fraud. By refraining from clicking on such links, individuals can prevent the sharing of personal information or privacy with potentially malicious websites. "Clickbait" and "Hidden URLs/Shortened Links" are common methods employed by fraudsters, utilizing attractive or fake images to deceive individuals. Clicking on these links can result in personal information being stolen by hackers or fraudsters (Drolet, 2019). Furthermore, 44.2% of respondents strongly agree that refraining from engaging in conversations with strangers or anonymous individuals can reduce the risk of being cheated. This awareness of the potential risks associated with interacting with strangers helps individuals avoid falling prey to temptations or addictive behaviour. It is particularly relevant in the context of love scams, where women, in particular, may be targeted due to their desire for affection. Responding to strangers can lead to deeper involvement and increase the risk of fraud (Erik, 2019; Manes, 2019). In summary, the findings

from Table 7 underscore the importance of improving awareness of media use, avoiding suspicious links or websites, and refraining from interactions with strangers as effective measures to prevent fraud. These insights highlight the significance of media literacy and cautious online behaviour in mitigating the risks associated with fraudulent activities on social media platforms.

Hypothesis Testing

H_1: Sharing personal information on social media increases the likelihood of teenagers being victims of fraud.

ANOVA TEST

Table 8:

Summary of ANOVA analysis results for hypothesis 1

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	8.593[a]	4	2.148	3.222	.013
Within Groups	253.366	380	.667		
Total	261.958	384			

b. R Squared = .016 (Adjusted R Squared = .014)

One-way ANOVA was employed to analyse to test the hypothesis, the results, presented in Table 8, indicate that the p-value associated with the impact of sharing personal information on social media increases the likelihood of teenagers being victims of fraud is 0.013, which is less than the commonly accepted significance level of 0.05. This finding implies that there is a statistically significant difference between sharing personal information on social media and teenagers falling victim to fraudulent activities. The calculated F-value is 3.222, and the associated p-value is 0.013, further confirming the strength of the evidence. Consequently, Hypothesis 1, which suggests that sharing personal information on social media can lead to teenagers being cheated, has been rigorously tested and found to have significant statistical support..

H2: Increased usage of social media is associated with a higher risk of fraudulent activities.

Table 9:

Summary of ANOVA analysis results for hypothesis 2

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	8.179[a]	4	2.045	2.409	.049
Within Groups	322.564	380	.849		
Total	330.743	384			

b. R Squared = .017 (Adjusted R Squared = .015)

One-way ANOVA was utilized to examine the relationship between the age level of teenagers and their social media usage. The results, presented in Table 9, reveal that the p-value associated with the connection between using social media and the occurrence of fraud

is 0.049, which is less than the conventional significance level of 0.05. This finding suggests that there is a statistically significant differences between increased usage of social media and a higher risk of engaging in fraudulent activities. The calculated F-value is 2.409, with a corresponding p-value of 0.049, providing further support for the evidence. Consequently, Hypothesis 2, which posits that an elevated use of social media is linked to an increased risk of fraudulent activities, has been rigorously tested and found to have significant statistical backing.

H3: Social media platforms can be exploited as tools for perpetrating fraud.

Table 10:
Summary of ANOVA analysis results for hypothesis 3

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	10.017[a]	4	2.504	3.065	.017
Within Groups	310.487	380	.817		
Total	320.504	384			

b. R Squared = .06 (Adjusted R Squared = .004)

One-way ANOVA was employed to analyse the hypothesis, the data presented in Table 10, investigating the potential exploitation of social media platforms as tools for perpetrating fraud. The obtained results reveal that the p-value associated with this relationship is 0.017, which falls below the conventional significance level of 0.05. Thus, it can be concluded that there is a statistically significant differences between social media platforms and their potential utilization for fraudulent activities. Consequently, Hypothesis 3, which suggests that social media platforms can be exploited as tools for perpetrating fraud, has been rigorously tested and found to have significant statistical support.

Discussions

This study employed a quantitative research method to investigate the perception of teenagers regarding social media fraud. The research focused on respondents between the ages of 15 and 24 years. By administering a questionnaire, the study aimed to gain insights into the experiences of teenagers and raise awareness about the potential threats associated with social media usage. This section discusses the findings and presents the results of the research questions along with corresponding hypotheses, as summarized in the table below.

Table 11:
Result of Research Questions

Research Questions	Hypothesis	P value	Result
To what extent is social media utilized as a tool for perpetrating fraud?	Sharing personal information on social media increases the likelihood of teenagers being victims of fraud.	0.017	Supported
Does the act of sharing personal information on social media platforms contribute to an increased risk of fraud?	Increased usage of social media is associated with a higher risk of fraudulent activities.	0.013	Supported
Does engaging with social media platforms result in a higher likelihood of falling victim to fraudulent activities?	Social media platforms can be exploited as tools for perpetrating fraud.	0.049	Supported

The results of hypothesis 1 indicated that sharing personal information on social media can make teenagers vulnerable to fraud, and the findings were statistically significant and supported and in line with Di Girolamo (2020). Similarly, hypothesis 2 demonstrated that the use of social media can increase the risk of fraud, and the statistical analysis confirmed its significance and support. Additionally, hypothesis 3 revealed that social media has become a new tool for fraudulent activities, and the results were statistically significant and supported. Based on the descriptive analysis, the majority of respondents were male, and most of them fell within the age range of 21-22 years old. Furthermore, the respondents predominantly resided in Johor. The findings also indicated that a significant number of respondents were familiar with the concept of social media fraud, and a majority of them reported having experienced fraud on social media platforms. Overall, the findings highlight the active role of social media in the lives of teenagers, who utilize these platforms for various purposes such as sharing updates, making connections, and entertainment. While social media offers convenience and the ability to connect with others, it also comes with inherent risks. As discussed in the literature review, teenagers can become targets of fraudulent activities, including deception and data theft by anonymous individuals (Di Girolamo, 2020).

Analyzing Table 5, which outlines the reasons for falling victim to social media fraud, it was observed that a substantial number of respondents strongly agreed that clicking on suspicious links or websites in social media significantly increases the risk of being deceived. As noted by Di Girolamo (2020), visiting suspicious websites can expose personal information, such as usernames and passwords, to the site owners, thereby elevating the risk of account hacking and unauthorized tracking. Similarly, Nee (2019) explains that criminals employ clickbait tactics, utilizing enticing headlines and text on the internet to lure individuals into clicking on links that redirect to malicious pages, allowing them to exploit the visitors and steal their information. In conclusion, this study's findings support the notion that sharing personal information on social media, as well as the general use of social media platforms, can increase

teenagers' vulnerability to fraud. Social media serves as a significant avenue for fraudulent activities, and clicking on suspicious links or websites poses a substantial risk of falling victim to deception and data theft. It is crucial for teenagers to be aware of these risks and exercise caution while using social media (Di Girolamo, 2020; Nee, 2019).

According to Ahmad (2017), individuals may engage in cheating due to a lack of guidance. When people lack proper guidance, particularly from parents or other influential figures, they may be more inclined to engage in unethical behavior without fully grasping the seriousness of their actions. Consequently, they resort to cheating as a means to satisfy their desires. This assertion is supported by the findings presented in Table 6, which indicate that a significant number of respondents strongly agreed that people cheat due to low moral behavior, often resulting from insufficient guidance. In a study conducted by Drolet (2019), it was suggested that avoiding suspicious links or websites on social media can help reduce the incidence of fraud. By refraining from interacting with questionable links, individuals can minimize the risk of sharing personal information or compromising their privacy with fraudulent websites. Examples of suspicious links include "Clickbait" or "Hidden URLs/Shortened Link," which exploit attractive or fake visuals to deceive people. Once these links are clicked, the fraudster or hacker may gain access to sensitive personal information. The findings presented in Table 6 support this notion, as a majority of respondents strongly agreed that avoiding strange links or websites on social media can effectively lower the occurrence of fraud.

Common Sense Media (2019) highlighted in the literature review that clickbait scams have a pervasive impact on society as a whole, with teenagers being particularly vulnerable. Teenagers and children are more susceptible due to their obsessions and gullibility. The captivating titles associated with clickbait lure them into clicking without exercising caution or self-control. However, through appropriate education and awareness, they can be trained to recognize and avoid suspicious titles such as "Click now" or "Free Download" that are commonly associated with deceptive content. By adopting such preventive measures, the risk of falling victim to fraudulent schemes can be mitigated.

The results obtained for hypothesis 1 indicated that sharing personal information on social media significantly increases the risk of fraud among teenagers ($P < .005$, $p = 0.13$), thus supporting the hypothesis. This finding aligns with the research conducted by Tulane University (2020) which highlighted the privacy concerns of social media users, particularly following recent data breaches. The researchers at Tulane University emphasized that these privacy concerns might prompt individuals to reconsider their relationship with social media platforms and prioritize their security. The act of sharing personal information on social media platforms can potentially lead to data breaches, allowing fraudsters to exploit the stolen information for criminal activities.

The findings related to hypothesis 2 revealed a statistically significant differences between social media usage and fraud ($P < .005$, $p = 0.49$), supporting the hypothesis. This finding is consistent with the literature review conducted by McAfee (2014), which emphasized that social media platforms, given their extensive user base, have become prime targets for cyber-attacks. As discussed in Help Net Security (2019), the popularity of these platforms attracts both legitimate users and malicious actors, rendering them more vulnerable to cyber threats. Users who are unable to distinguish between trustworthy and malicious content on these platforms are at a heightened risk of falling victim to cyber-attacks and fraud.

Furthermore, the analysis of hypothesis 3 demonstrated a statistically significant differences between social media and the emergence of new fraudulent techniques ($P < .005$, $p = 0.17$), confirming the hypothesis. The Federal Bureau of Investigation (2021) supported this finding,

reporting an increase in online predators targeting young individuals for threatening and scamming purposes. Young people, due to their inherent trust and limited exposure to the market, are particularly susceptible to being deceived and falling victim to scams. Emma (2020) also noted that fraudsters frequently utilize social media to promote counterfeit products or services, as evidenced by the rising number of fraud reports to the Federal Trade Commission and the agency's recent focus on combating this issue. In conclusion, social media harbors various threats and risks, many of which remain unknown to the general public. The present study's results affirm the significant association between sharing personal information, social media usage, and the emergence of fraudulent activities. It is crucial for individuals to be aware of these risks and adopt appropriate measures to protect themselves from potential fraud on social media platforms.

Implications Of Study

The findings of this study have significant implications regarding the vulnerability of teenagers to online fraud on social media platforms. The Malaysian government should prioritize the maintenance and enhancement of online security across all online and social platforms to ensure a safe cyberspace and prevent malicious attacks from external sources. Moreover, schools play a crucial role in raising students' awareness of the online world. By incorporating assignments and facilitating discussions on topics related to online platforms, such as social media, students can develop a better understanding of potential risks and threats posed by strangers and other online dangers. Additionally, parents have a pivotal role in protecting their children from social media threats. They should provide guidance on safe and responsible social media usage, educating their children on identifying and avoiding potentially harmful individuals, such as strangers or anonymous accounts. By imparting this knowledge, parents can help their children resist the temptation of engaging with individuals who may pose a threat.

Furthermore, social media users themselves must exercise a sense of responsibility and prudence while using these platforms. Given that there is no direct supervision during online activities, users should equip themselves with the necessary knowledge and awareness to make informed decisions. Engaging in pre-usage research and self-education about best practices and potential risks associated with social media can go a long way in mitigating threats and minimizing instances of fraud. In conclusion, the implications drawn from this study highlight the importance of collective efforts involving the government, schools, parents, and individual users in safeguarding against online fraud. By prioritizing online security, raising awareness among students, providing parental guidance, and promoting responsible social media usage, the incidence of fraud can be significantly reduced, creating a safer digital environment for teenagers and society as a whole. The implications of this study extend to educational institutions, families, and schools alike. It offers valuable knowledge about social media usage, the prevalent threats on social media platforms, and other pertinent information. Families can utilize this knowledge to educate their children about safe practices while using social media, thereby enhancing their media literacy and awareness. Local schools can also benefit by incorporating campaigns or dedicated curriculum chapters on social media awareness. This proactive approach ensures that students gain awareness of potential risks and learn how to responsibly navigate the world of social media.

Significance Of Study

This research endeavour aims to conduct a comprehensive investigation into teenagers' perceptions regarding the motivations behind cheating, the factors contributing to individuals becoming victims of deception, the concept of humanity, the emotional resilience of individuals when faced with deceit, and the valuable suggestions provided by teenagers themselves. The study also intends to assess agreement or disagreement among individuals with the statement "Teenagers can easily be tricked on social media," given previous research indicating the vulnerability of teenagers to deception. Numerous studies have highlighted the susceptibility of teenagers to fraudsters and their elevated risk of falling prey to scams. This research seeks to delve deeper into the underlying reasons, methods, and platforms through which teenagers are victimized, aiming to gather invaluable insights directly from teenage respondents.

Focusing on teenagers is particularly important due to their natural curiosity and eagerness to explore novel phenomena, especially within the realm of social media. Consequently, this study can gather authentic data pertaining to teenagers' perspectives, experiences, and suggestions. Furthermore, the study aims to explore the emotional and psychological impact on teenagers who have experienced deception on social media. Understanding how teenagers react to being cheated, with some taking it to heart while others remaining unaffected, is crucial. Additionally, the research aims to examine whether and how teenagers can exercise control over their mind-set when faced with fraud. By delving into teenagers' perceptions, opinions, and suggestions regarding social media fraud, this study endeavours to identify the most effective strategies for preventing teenagers from falling victim to scams, ultimately reducing the incidence of such cases in Malaysia.

Given the widespread use of social media across all age groups, this research has the potential to raise awareness within society as a whole, extending beyond just teenagers. By incorporating the perspectives and suggestions of Malaysian teenagers, this study can serve as a valuable reference for readers from Malaysia and other countries conducting future research in the field of social media. Moreover, the research aims to raise awareness among individuals about the risks associated with social media usage. It introduces the concept of fraud, categorizes different types of fraud, and provides insights on how to identify and avoid such threats. By understanding how fraudsters craft enticing content to lure victims, individuals can protect themselves and abstain from engaging with fraudulent schemes.

Limitation Of Study

This research study is subject to certain limitations that may impact future investigations. Firstly, the research was constrained by time limitations, as well as the specific focus on the Malaysian population. Moreover, the scope of the study was limited by the researcher's capacity, including the availability of manpower and resources. These factors restricted the breadth and depth of the study. Secondly, the researcher had to establish a manageable scope within the designated timeframe and with the available human resources. Consequently, certain aspects or variables related to the research topic may not have been included due to practical constraints. Thirdly, the online research conducted through Facebook as a platform may have limitations in terms of reaching all Malaysian young Facebook users. The study's findings and conclusions are therefore limited to the specific network accessible through Facebook and may not be representative of the entire population of young Facebook users in Malaysia. It is important to acknowledge these limitations as they may impact the generalizability and comprehensiveness of the research findings. Future

studies should aim to overcome these limitations by expanding the scope, considering a wider audience, and utilizing diverse research methodologies to ensure a more comprehensive understanding of the topic.

Recommendations For Future Research

To address topics related to social media, conducting an online survey is highly recommended. In future research, it would be beneficial to consider conducting a national-level study on a larger scale by collaborating with researchers from various parts of Malaysia or different universities. Additionally, allocating more time for the research would enable reaching a broader audience across different states. Furthermore, it is advisable to explore other social media platforms, such as Instagram, Snapchat, and TikTok, for conducting online surveys. By leveraging these platforms, researchers can effectively reach a wider range of target audiences.

Conclusions

The study's findings indicate that the age group most affected by social media fraud is between 21-22 years old, accounting for 55.6% of the respondents. While social media has become an essential platform for people to have fun, make friends, and communicate, it is crucial to exercise caution while using it. Users should avoid clicking on suspicious links and refrain from sharing personal information or sensitive data on social media platforms. It is the responsibility of relevant authorities, such as government, schools, and parents, to educate teenagers and children about using social media safely, thus enhancing their knowledge and awareness. Moreover, this research acknowledges certain limitations, including time constraints, limited manpower, and networking resources. However, despite these constraints, the researcher has diligently conducted the study. To overcome these limitations, future research endeavors can involve collaborations with researchers from different states or even countries, facilitating the execution of a comprehensive national-level investigation.

In the year 2023, Malaysia's remarkable economic growth and its impressive income levels are undeniable. This progress is intrinsically linked to the widespread adoption of social media and internet accessibility among Malaysians. A staggering 91.7% of the population actively engages in social media, with 96% enjoying internet access (Commission Factory, 2023). The digital landscape in Malaysia is of paramount significance, as it unravels the profound impact of online behavior on various facets of society. This research has unearthed a disquieting trend within Malaysia: the act of sharing personal information on social media platforms is demonstrably associated with an increased susceptibility to fraud, particularly among teenagers. This is a matter of great concern, given the vulnerability of young individuals who may not possess the capacity to accurately assess the risks inherent in their online actions.

Moreover, this study unveils a significant correlation between social media usage and the likelihood of falling victim to cybercrime. As asserted by Siraj and Ghazal (2019), individuals who struggle to distinguish between trustworthy and malicious content on these platforms face an elevated risk of falling prey to cyberattacks and fraud. This discovery is pivotal for comprehending the intricate interplay between online behavior and the potential for victimization. Furthermore, data reported in the New Straits Times Malaysia (Mohamed Basyir & Hana Naz Harun, 2022) underscores the growing prevalence of diverse scams within Malaysia. The surge in reported cases and associated financial losses is nothing short of alarming, with young people, particularly students, emerging as the expected prime targets. These revelations underscore the immediate necessity for in-depth research into online fraud

and cybersecurity in Malaysia, as validated by sources such as The Sun Daily (2023) and Tham (2023).

The results of this research unequivocally demonstrate that social media has evolved into a significant platform for fraudulent activities. This aligns with the observations made by Griffiths (2023), which indicate a rising trend of cybercriminals using social media to target individuals for scams. The economic implications are substantial, with considerable costs associated with cyber breaches and cybercrime. Notably, the largest demographic affected by scams in Singapore comprises young adults aged 20 to 39, representing 53.5% of all scam victims. Among the various types of scams, job scams were the most prevalent within this age group (Tham, 2023). In a global context, cybercrime trends suggest an anticipated increase in costs, and data on cybercrime in Malaysia highlights the urgency of addressing social media fraud. This research underscores the critical link between social media usage, online behavior, and the risk of fraud, particularly among teenagers in Malaysia. The findings offer valuable insights into the growing issue of cybercrime and its far-reaching economic and societal consequences. It is imperative that these insights be used as a foundation for policy development, education, and awareness campaigns aimed at mitigating the risks associated with online behavior in Malaysia. This research contributes significantly to the body of knowledge on this pressing issue and emphasizes the importance of addressing it at both the national and global levels.

References

Ahmad, R. (2017). Teacher Guidance and Counseling Efforts to Prevent Cheating Behavior. In Proceedings of the 9th International Conference for Science Educators and Teachers (ICSET 2017) (p. 118). https://doi.org/10.2991/icset-17.2017.126

Allison, G., & Hiwot, H. (2018, August 16). What we learned about media literacy by teaching high school students fact-checking. Poynter. https://www.poynter.org/tech-tools/2018/what-we-learned-about-media-literacy-by-teaching-high-school-students-fact-checking/

Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, and crowding.

Australian Cyber Security Centre. (2020, April 19). Personal information and privacy. Cyber.gov.au. https://www.cyber.gov.au/acsc/view-all-content/advice/personal-information-and-privacy

Awati, R. (2021, August 5). Cyberstalking. Search Security. https://www.techtarget.com/searchsecurity/definition/cyberstalking

Axel. (2019, September 10). How To Protect Your Personal Information On Social Media. Medium. https://medium.com/@AxelUnlimited/how-to-protect-your-personal-information-on-social-media-c3aa6242f1cf

Bhandari, P. (2021, December 8). An introduction to quantitative research. Scribbr. https://www.scribbr.com/methodology/quantitative-research/

Bhat, A. (2021, December 17). Qualitative Research: Definition, Types, Methods and Examples. QuestionPro. https://www.questionpro.com/blog/qualitative-research-methods/

Bridget, S. (2020, October 21). Scams that start on social media. Consumer Information. https://www.consumer.ftc.gov/blog/2020/10/scams-start-social-media

Brush, K., Rosencrance, L., & Cobb, M. (2019, December 23). Cybercrime. Search Security. https://www.techtarget.com/searchsecurity/definition/cybercrime

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391–408. https://doi.org/10.1177/0004865814521224

Caroline, H. (2020, October 29). Advantages and Disadvantages of Online Surveys. Cvent Blog. https://www.cvent.com/sg/blog/events/advantages-disadvantages-online-surveys

Chen, J. (2021, July 6). Fraud. Investopedia. https://www.investopedia.com/terms/f/fraud.asp

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588. https://doi.org/10.2307/2094589

Common Sense Media. (2019). What is media literacy, and why is it important? https://www.commonsensemedia.org/news-and-media-literacy/what-is-media-literacy-and-why-is-it-important

Consumers International. (2019, May). Social media scams: May 2019 Understanding the consumer experience to create a safer digital world. https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf

Commission Factory. (2023, May 8). Malaysia Social Media Statistics and Facts 2023. Commission Factory Blog. https://blog.commissionfactory.com/affiliate-marketing/malaysia-social-media-statistics#:~:text=7-,Social%20Media%20Users%20by%20Age,24%20age%20range%20at%2022%25.

Cauffman, E. (2019). Studying the connection between the maturity of judgment in adolescents and their legal accountability. University Communications. Retrieved from https://news.uci.edu/2009/10/12/studying-teens-emotional-maturity-gap/

Dan, R. (2020, October 22). Social Media Identity Theft: How to Protect Yourself. Norton Life Lock. https://www.lifelock.com/learn/internet-security/social-media-behavior-leads-identity-theft

Di Girolamo, R. (2020, February 20). Never Click and Tell: Staying Safe on Social Media. Connected. https://community.connection.com/never-click-and-tell-staying-safe-on-social-media/

Drolet, M. (2019, September 9). Top Social Media Scams And How To Avoid Them. Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/09/09/top-social-media-scams-and-how-to-avoid-them/?sh=5884d9f1873d

Emma, F. (2020, October 21). Scams starting on social media proliferate in early 2020. Federal Trade Commission. https://www.ftc.gov/news-events/blogs/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020

Erik. (2019, February 27). Women Love To Be Wanted & Desired. Skill Of Attraction. http://www.skillofattraction.com/women-love-to-be-wanted-desired/

Federal Bureau of Investigation (FBI). (2021, October 5). Cyber Crime. Federal Bureau of Investigation. https://www.fbi.gov/investigate/cyber

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. Human Ecology, 8(4), 389–406. https://doi.org/10.1007/bf01561001

Fleetwood, D. (2021, January 22). Simple Random Sampling: Definition and Examples. QuestionPro. https://www.questionpro.com/blog/simple-random-sampling/

Fleetwood, D. (2021, June 22). Quantitative Research: Definition, Methods, Types and Examples. QuestionPro. https://www.questionpro.com/blog/quantitative-research/

GCF Global. (2020). Digital Media Literacy: What is Clickbait? GCFGlobal.Org. https://edu.gcfglobal.org/en/digital-media-literacy/what-is-clickbait/1/

George, T. (2022, January 4). An introduction to mixed methods research. Scribbr. https://www.scribbr.com/methodology/mixed-methods-research/

Gordon, S. (2021, August 17). Cyberstalking: Prevention, Consequences, and Coping. Verywell Mind. https://www.verywellmind.com/what-is-cyberstalking-5181466

Government of New South Wales. (2011). Routine activity theory crime prevention. Crime Prevention NSW.
http://www.crimeprevention.nsw.gov.au/Documents/routine_activity_factsheet_nov2014.pdf

Griffiths, C. (2023, October 2). The Latest 2023 Cyber Crime Statistics (updated October 2023). Aag-it.com. https://aag-it.com/the-latest-cyber-crime-statistics/

Help Net Security (2019, February 26). Social media-enabled cybercrime is generating $3.25 billion a year. Help Net Security.
https://www.helpnetsecurity.com/2019/02/27/social-media-enabled-cybercrime/

Hertfordshire Constabulary. (2021). Social media fraud.
https://www.herts.police.uk/Information-and-services/Advice/Crime-prevention/Protect-your-money/Social-media-fraud

Hertfordshire Constabulary. (n.d.). Social media fraud.
https://www.herts.police.uk/Information-and-services/Advice/Crime-prevention/Protect-your-money/Social-media-fraud#:%7E:text=Fraudsters%20use%20social%20media%20sites,access%20bank%20accounts%20and%20cards.

Hudson, M. (2020, June 23). What Is Social Media? The Balance Small Business. https://www.thebalancesmb.com/what-is-social-media-2890301

IBM. (2014). What's new in IBM SPSS Statistics 28. IBM Corporation.
https://www.ibm.com/downloads/cas/DKA95AXM

Jordan, M. (2021, August 26). What is Regression Analysis and Why Should I Use It? | Alchemer Blog. Alchemer. https://www.alchemer.com/resources/blog/regression-analysis/

Jordan. (2021, November 16). 5 Common Scams Targeting Teens and Young Adults 2021. https://socialcatfish.com/scamfish/5-common-scams-targeting-teens-and-young-adults-2021/

Jtrout. (2021, July 9). Identity Theft and Social Media: What you Need to Know. Retirement Living. https://www.retirementliving.com/identity-theft-and-social-media

Kaspersky. (2021, April 26). What is a security breach? Www.Kaspersky.Com. https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach

Kaspersky. (2021, July 5). Tips on how to protect yourself against cybercrime. Www.Kaspersky.Com. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Laura, B. (2019, February 26). Cybercriminals raking in over $3bn a year from social media crime | University of Surrey. University of Surrey.
https://www.surrey.ac.uk/news/cybercriminals-raking-over-3bn-year-social-media-crime

Lavrakas, P. (2008). Convenience Sampling. Encyclopaedia of Survey Research Methods. https://doi.org/10.4135/9781412963947.n105

LeCompte, M. D. (2000). Analysing Qualitative Data. Theory Into Practice, 39(3), 146–154. https://doi.org/10.1207/s15430421tip3903_5

Lewis, K. (2019). How Social Media Networks Facilitate Identity Theft and Fraud. Entrepreneur Organization. https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud

Longley, R. (2020, January 17). What is Fraud? Definition and Examples. ThoughtCo. https://www.thoughtco.com/fraud-definition-and-examples-4175237

Lucid. (2021, October 21). What Is a Questionnaire | Types of Questionnaires in Research. https://luc.id/blog/what-is-a-questionnaire/

Lun, C. W., Idrus, S. Z. S., Ali, W. N. A. W., Ishak, N. A., Mustafa, W. A., Jamlos, M. A., & Wahab, M. H. A. (2020). The Development of an Interactive Animation to Prevent Social Media Fraud. Journal of Physics: Conference Series, 1529. https://doi.org/10.1088/1742-6596/1529/3/032081

Lutkevich, B., & Wigmore, I. (2021, September 1). Social media. WhatIs.Com. https://whatis.techtarget.com/definition/social-media

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2020, August 17). Teens, Social Media, and Privacy. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/#:%7E:text=good%20about%20themselves.-,Teens%20are%20sharing%20more%20information%20about%20themselves%20on%20social%20media,as%20changing%20norms%20around%20sharing.

Mahmutovic, J. (2021, September 1). 12 Advantages of Online Surveys (and 4 Disadvantages). SurveyLegend. https://www.surveylegend.com/online-survey/advantages-of-online-surveys/

Manes, Y. (2019, February 5). 16 real women reveal why they cheated on their partners. Insider. https://www.insider.com/why-do-women-cheat-2018-1

Martins, A. (2019, August 26). Cybercriminals Use Social Media for Fraud. Business News Daily. https://www.businessnewsdaily.com/15269-cybercriminals-social-media-fraud.html

Maryani, E., Rahmawan, D., Garnesia, I., & Ratmita, R. A. (2020). Management and Psychological Aspect: Teenagers' Awareness of Privacy in Social Media. Jurnal Komunikasi Ikatan Sarjana Komunikasi Indonesia, 5(2). https://doi.org/10.25008/jkiski.v5i2.429

McAfee. (2014). How Cybercriminals Target Social Media Accounts | McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/cy

McLaughlin, E.C. & Stedman, C. Industry Editor. (2022). (This was last updated in February 2022). Definition of data collection. TechTarget.
https://searchcio.techtarget.com/definition/data-collection

McMurtry, R. R. and Curling, A. (2008). Ontario, Ontario. Cabinet Office, Ontario. Ministry of Children and Youth Services, & Ontario. Review of the Roots of Youth Violence. The Review of the Roots of Youth Violence [E-book]. Service Ontario Publications.

MediaSmarts. (2017, January 19). Media Literacy Fundamentals
https://mediasmarts.ca/digital-media-literacy/general-information/digital-media-literacy-fundamentals/media-literacy-fundamentals

Michel, M. C. K., & King, M. C. (2019). Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. 2019 IEEE International Symposium on Technology and Society (ISTAS).
https://doi.org/10.1109/istas48451.2019.8938009

Mohamed Basyir, & Hana Naz Harun. (2022, September 26). Online scam cases increasing in Malaysia. The New Straits Times, Malaysia. https://www.nst.com.my/news/nation/2022/09/834531/online-scam-cases-increasing-malaysia

Nee, J. (2019, November 27). Why Social Media Companies Should Ban Clickbait. UCSD Guardian. https://ucsdguardian.org/2019/11/26/social-media-companies-ban-clickbait/

O'Loughlin, E. (2020, March 27). Identity Theft and Social Media: How Are They Related? Security Intelligence. https://securityintelligence.com/identity-theft-and-social-media-how-are-they-related/

Oghazi, P., Schultheiss, R., Chirumalla, K., Kalmer, N. P., & Rad, F. F. (2020). User self-disclosure on social network sites: A cross-cultural study on Facebook's privacy concepts. Journal of Business Research, 112, 531-540. https://doi:10.1016/j.jbusres.2019.12.006

Panda security. (2020, October 13). 10 Social Media Scams and How to Spot Them. Panda Security Media center. https://www.pandasecurity.com/en/mediacenter/panda-security/social-media-scams/

Petters, J. (2020, September 29). Data Privacy Guide: Definitions, Explanations, and Legislation | Varonis. Inside Out Security. https://www.varonis.com/blog/data-privacy/

Pietkiewicz, M., & Treder, M. (2018). Cyberstalking in social media – Polish view. Journal of Modern Science, 38(3), 29–40. https://doi.org/10.13166/jms/99217

Preston, V. (2009). Questionnaire Survey - an overview Science Direct Topics. Science Direct. https://www.sciencedirect.com/topics/earth-and-planetary-sciences/questionnaire-survey

QuestionPro. (n.d.). Survey research: Definition, Examples, and Methods. https://www.questionpro.com/article/survey-research.html

Rawat, A. S. (2021, March 21). What is Descriptive Analysis? - Types and Advantages | Analytics Steps. https://www.analyticssteps.com/blogs/overview-descriptive-analysis

Richard, F. T. (1996, May 28). Social Basis of Human Behavior: Greed. WSU. https://public.wsu.edu/%7Etaflinge/socgreed.html

Robertson, J., & Tisdall, E. K. M. (2020). The importance of consulting children and young people about data literacy. Journal of Media Literacy Education, 12(3), 58–74. https://doi.org/10.23860/jmle-2020-12-3-6

Samarati, M. (2016, September 8). 7 types of social media account fraud. IT Governance USA Blog. https://www.itgovernanceusa.com/blog/7-types-of-social-media-account-fraud

Shannon, F. (2021, August 20). Teens falling prey to online scams faster than seniors. The Star. https://www.thestar.com.my/tech/tech-news/2021/08/19/teens-falling-prey-to-online-scams-faster-than-seniors

Shikati, C. (2018, May 26). Ways social media has changed our society - What it Takes. Medium. https://medium.com/w-i-t/ways-social-media-has-changed-our-society-38fd4d3e5ce8

Singh N, D., & Guruprasad, D. N. (2019). Impact of Social Media on Youth. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3506607

Siraj, R., Najam, B., & Ghazal, S. (2021). Sensation seeking, peer influence, and risk-taking behavior among adolescents. Institute of Applied Psychology, University of Punjab, Lahore, Pakistan. Retrieved from

file:///C:/Users/lc7504/Downloads/Sensation_Seeking_Peer_Influence_and_Risk-Taking_B.pdf

Smith, A., & Anderson, M. (2018, March 1). Social Media Use in 2018. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/

Supedium. (2020, November 6). What's Social Media and How It Works? https://supedium.com/improvements-and-learning/whats-social-media-and-how-it-works/

SurveyMonkey. (2021). Using Social Media Surveys & Questionnaires. https://www.surveymonkey.com/mp/social-media-surveys/

Tham, D. (2023, February 8). In Singapore, S$661 million lost to scams in 2022, with young adults most likely to fall victim: SPF. Channel News Asia. https://www.channelnewsasia.com/singapore/police-scam-cybercrime-statistics-young-adults-2022-3262141

The California Aggie. (2018, October 31). Clickbait: Fake news on social media. https://theaggie.org/2018/10/30/clickbait-fake-news-on-social-media/

The Sun Daily. (2023, June 9). Who is to blame for online fraud? The Sun Daily. https://www.thesundaily.my/local/who-is-to-blame-for-online-fraud-FI11081545

Tilley, N. (2011). Crime Prevention. Willan Publishing (UK).

Tomaszek, K. (2012). Stalker – psychological characteristics of perpetrators of crimes "persistent harassment," Studies in Psychology at KUL, 18, 135-156. https://www.kul.pl/files/55/Stud_psych_18-2012_Tomaszek.pdf

Trepte, S., & Reinecke, L. (Eds.). (2011). Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web. Springer. https://doi.org/10.1007/978-3-642-21521-6

Tulane University. (2020). Social Media Privacy Issues for 2020: Threats & Risks. https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020

Turner, D. P. (2020). Sampling Methods in Research Design. Headache: The Journal of Head and Face Pain, 60(1), 8–12. https://doi.org/10.1111/head.13707

U.S. Securities and Exchange Commission. (2018, September 26). Internet and Social Media Fraud | Investor.gov. https://www.investor.gov/protect-your-investments/fraud/types-fraud/internet-and-social-media-fraud

United States Attorney General. (2018). Can You Tell Real Social Media Posts From "Click Bait" Scams? Stop Fraud Colorado. https://stopfraudcolorado.gov/fraud-center/digital-fraud/click-bait-scams.html

University of Southern California (2021). Research Guides: Organizing Your Social Sciences Research Paper: Quantitative Methods. USC Library. https://libguides.usc.edu/writingguide/quantitative

University of Southern Indiana Web Services. (2019). What Is Fraud? - University of Southern Indiana.https://www.usi.edu/internalaudit/what-is-fraud/#:%7E:text=Fraud%20is%20a%20deliberate%20act,and%20relied%20upon%20by%20others.

Wang, Congxi. (2018). Online News Coverage about Fraud and Self-Defensive Behavior in China. Rochester Institute of Technology. https://www.scholarworks.rit.edu/theses/9764/

Westin, A. F. (1967). Privacy And Freedom. Scholarly Commons, 25(20). https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/

World Health Organization. (2019, July 18). Adolescent health. https://www.who.int/southeastasia/health-topics/adolescent-health

Wickert, C. (2020, December 6). Routine Activity Theory (RAT). SozTheo. https://soztheo.de/theories-of-crime/rational-choice/routine-activity-theory-rat/?lang=en

Wikström, P. O. H. (2009). Routine Activity Theories. Oxford Bibliographies Online Datasets. https://doi.org/10.1093/obo/9780195396607-0010

Williams, L. (2021, October 7). What is Cybercrime? Types, Tools, Examples. Guru99. https://www.guru99.com/cybercrime-types-tools-examples.html

Winston & Strawn. (2021). What is the Definition of Online Privacy? | Winston & Strawn Legal Glossary. https://www.winston.com/en/legal-glossary/online-privacy.html

YLAI Network. (2019, July 8). The Importance of Media Literacy | YLAI Network. Young Leaders of the Americas Initiative. https://ylai.state.gov/importance-media-literacy/

Zhang, C., & Clough, P. D. (2020). Investigating clickbait in Chinese social media: A study of WeChat. Online Social Networks and Media, 19, 100095. https://doi.org/10.1016/j.osnem.2020.100095

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2013). Business Research Methods [E-book]. Van Haren Publishing.