

Emerging Trends in Money Scams Targeting Adult Telegram Users in Malaysia

Nur Syifaa' Faharudin¹, Nur Azyan Nabilah Othman², Sarah Nursabrina Badruzaman³, Alis Mohd Nazril⁴, Mohamad Hafifi Jamri⁵, Nanang Suryana⁶, Yusa Djuyandi⁷

^{1,2,3,4,5} Faculty of Communication and Media Studies, Universiti Teknologi MARA (UiTM), Melaka, Malaysia.

^{6,7} Department of Political Science, Universitas Padjadjaran, Indonesia.

Corresponding author: Mohamad Hafifi Jamri.

Email: hafifijamri@uitm.edu.my

Abstract

The rise of cyber fraud targeting Telegram users in Malaysia poses a major threat to the trust and financial security of the digital platform. Therefore, this study will focus on two main objectives, which are to identify the strategies used by scammers to target adult users of Telegram Malaysia and evaluate the effectiveness of public awareness efforts aimed at educating the public about scams among Telegram users. By using Uses and Gratification Theory, which states that individuals engage with media to fulfill social and psychological needs, this research explores why scammers exploit Telegram's large user base and secure messaging for financial gain. To ensure accurate and reliable findings, a quantitative methodology was employed, using a structured questionnaire distributed via Google Forms, gathering responses from 416 participants through the integration of purposive and convenience sampling, chosen for its efficiency in reaching a diverse respondent pool. The results show that users are aware of online scams and can identify their various patterns as well as prevalent tactics. Susceptibility can be caused by a variety of factors, including a lack of awareness, being easily deceived, and financial desperation. Hence, in order to prevent cybercrime and promote digital safety, it is crucial to put pre-emptive measures into place, collaborate with governments, and launch effective awareness programs. In conclusion, social media platforms serve as vital tools for disseminating scam-related information.

Keywords

Telegram, money scam, patterns tactics, causes effects, social media awareness

Introduction

Scam is a form of fraud aimed at illegally obtaining money from individuals. Notably, scams target people of all demographics and succeed by appearing legitimate, often catching victims off guard (Dictionary.cambridge.org, 2024). Consequently, as scammers become increasingly sophisticated, everyone is at risk of falling victim to these deceptive schemes. The spread of digital communication platforms in recent years has completely changed how people communicate. For instance, Telegram has become a favorite among adult users in Malaysia due to its numerous features and advantages. This is because the public believes that its emphasis on user privacy has made it incredibly popular, which in early 2021, a large number of users switched from Whatsapp to Telegram (Vanian, 2021). However, this rising popularity has also brought about some issues, as Telegram has long been a popular platform for scams, leading to a rise in money scams that target adult users. Due to the quick growth of our online activities, cybercriminals now have more ways to commit different types of scams.

They can now carry out conventional scams on a large scale for very little money, or even create completely new scam schemes. As a result, many people who would have

never been publicly targeted by these kinds of crimes now run the daily risk of becoming victims (Quek, 2023). Constantly modifying their strategies to trick gullible people, scammers frequently employ sophisticated techniques to control and coerce victims into paying them money. Furthermore, there has been an apparent rise in the quantity of commercial offenses documented in Malaysia, particularly fraudulent scams, where between 2019 and 2021, a total of 51,631 cybercrime cases with losses of RM1.61 billion were reported. As of July 2021, 12,092 cases with losses of RM414.8 million had been reported (Royal Police Malaysia, 2022).

Besides that, according to one of the researchers (Wilson et al., 2023) said that taking credit card numbers, login credentials, or identity information is frequently the main objective of these scams. In order to deceive their victims, scammers frequently employ a variety of false attractions, including fake multi-level marketing or pyramid schemes, business opportunities, auctions, credit card offers, loans, job openings, and more. Numerous cybercrime trends can be attributed to contemporary trends. According to Cybersecurity Malaysia Fraudulent, activities in Malaysia that result in victims losing their money include credit card scams, parcel scams, insurance scams, and

many more (Wilson et al., 2023). Besides that, ensuring public safety is crucial for maintaining a high quality of life for citizens. It is the joint responsibility of the Malaysian government and non-governmental agencies to collaborate in preventing crime and safeguarding public well-being especially in raising awareness about scams (Wilson et al., 2023).

The majority of studies have looked at online scams generally rather than concentrating on particular platforms like Telegram, which has special privacy features that could affect scam tactics (Morgia et al., 2021). Furthermore, there is a lack of research on the psychological and emotional effects of scams on victims, especially in Malaysia, despite the financial impact of these schemes being widely documented (Quek, 2023). Studies that already exist also frequently ignore the victim's demographics, which is important for creating focused preventative tactics. Addressing these gaps is crucial for several reasons. Understanding regional variations in scam tactics can lead to the development of more effective local prevention measures. Examining the specific dynamics of Telegram can help create better platform-specific security policies. Additionally, a comprehensive understanding of the impact on victims can improve public campaigns to increase awareness. This research seeks to address these

gaps by exploring the trends and patterns of money scams targeting adult Telegram users in Malaysia. By analyzing the techniques used by scammers and the demographics of victims, this study aims to provide valuable insights to inform prevention and mitigation strategies while also raising awareness about money scams among Malaysian adults.

Method

A research methodology was created to study the dynamics of money scams targeting Telegram users in Malaysia. To address the issue of cybercrime, particularly focusing on money scams through Telegram, this study employed a quantitative research approach. Quantitative methodology serves as the primary research framework in the social sciences, aiming to generate knowledge and understanding about the social world (University of Texas Arlington, 2023). Hence, a structured questionnaire was employed to gather data from 416 respondents via the Google Forms platform, serving as the primary instrument for data collection. This choice was made due to Google Form's feature of automatically generating results, providing totals and percentages for each question response. Next, we manually interpreted and documented the collected data for analysis. The questionnaire is divided

into five sections: A, B, C, D, and E, which cover topics such as respondent demographics, knowledge, attitude, practice, and effectiveness. Each section contains bilingual questions to make it easier for our respondents to answer. The sample size was determined using the Raosoft sample size calculator. To select the sample, we integrated both convenience and purposive sampling techniques, focusing on Malaysian adults. We specifically attract respondents who meet our criteria through purposive sampling. Additionally, we employ convenience sampling to include respondents who are readily accessible and convenient for our research. Convenience sampling entails utilizing respondents who are easily accessible to the researcher (Edgar & Manz, 2017). Meanwhile, purposive research sampling is a method where the researcher selects a sample based on their judgment of its relevance to the study's goals (Bisht, 2024). Amongst the entry requirements for this research involving purposive sampling are:

1. The respondent must be a Malaysian citizen,
2. The respondent must be 18 years of age and above,
3. The respondent must have common knowledge about Telegram

Discussion

Telegram has become a popular platform for communication, learning, and doing business. But, unfortunately, it has also become a place for fraudsters to spread money scams. Telegram fraud is becoming more common and many people are becoming victims. Financial losses and psychological wounds can come together. Therefore, we need to know how to protect ourselves from these fraudsters.

The loss of citizens due to various fraudulent activities via Telegram from January to May 2023 reached 45 million Malaysian Ringgit. The scammers promote a fraudulent investment scheme, luring potential investors with promises of extremely high returns. They further emphasize the exclusivity of the opportunity, claiming that the scheme is only available to new customers for a limited time.

The Malaysian government has conveyed a firm view on the importance of Telegram and any messaging or social media application to always comply with and comply with the laws in force in Malaysia.

Telegram money scams are a crime mode in which perpetrators pretend to offer fake investments, goods, or services. They use messages, groups, and bots to deceive people. Generally, fraudsters send messages that are too good to be

true, then trick victims into sending money.

Common characteristics of this scam include offers that are too tempting, urgent messages, and requests for personal data. They also often send links that lead to fake sites.

Common Types of Fraud

Fake investments and pyramid schemes: The perpetrators offer investment opportunities that promise big profits in a short time. Usually, these are pyramid schemes that eventually collapse when many victims lose their money.

1. Selling fake goods or services: Offering cheap goods but never delivering them after payment is made.
2. Phishing via private or group messages: Fraudsters send links or attachments that contain viruses or other cybercrimes. The goal is to get the victim's sensitive data and money.
3. Signs and Modus Operandi of Telegram Fraud
4. Recognize the Signs of Fraud
5. Offers that are too good to be true, such as big free gifts
6. Time pressure to make a quick decision
7. Request for account numbers, personal data, or OTP codes
8. Intimidating or threatening messages if you don't follow directions

9. Messages from strangers with unclear identities
10. Fraudster Techniques and Strategies
11. Creating fake groups, channels, or bots that claim to be trusted places
12. Using fake identities, pretending to be bank officers, or famous figures
13. Sending malicious links that lead to phishing sites

a) Demographic Profile

The demographic samples, including gender, age, ethnicity, education level, employment status, residential location, and monthly income, were discussed to identify trends in money scams targeting Telegram users in Malaysia. The demographic information of 416 respondents is shown in Table 1. According to the collected data, most respondents who completed the surveys were female, with 267 (64.2%) of respondents aged 18 to 25. Additionally, 250 (60.1%) respondents held a Bachelor's degree, 251 (60.3%) respondents were students, and 287 (69%) respondents resided in urban areas. The survey also revealed that 138 (33.2%) respondents had a monthly household income below RM2,000.

b) Telegram's Adult Users Awareness On Online Money Scam

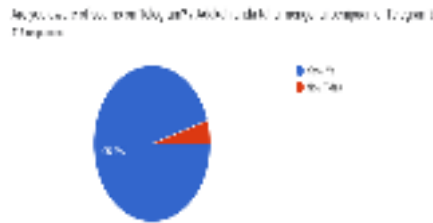


Figure 1.0

Based on Figure 1.0 that has been distributed regarding money scams among adults on Telegram in Malaysia, we discovered that 396 (95.2%) out of 416 respondents are aware of scams on Telegram. Despite the high level of awareness among the respondents in this study, there are still some of them who have fallen victim to online scams. This can be proven from the survey, which found that approximately 147 (35.3%) respondents who were between the ages of 18 to 25 had been victims.

Moreover, this study highlighted that respondents are strongly aware of the common scam types, with investment scams being reported as the most frequent, followed by job and Macau scams. These types of scams typically involve the use of fake Telegram channels as a common tactic in order to mislead victims. Morgia et al. (2021) refer to the fact that fake

Telegram channels posing as trustworthy entities or groups offering easy money are a commonly used tactic, similar to fake accounts. Fortunately, most respondents in this study could identify scams on Telegram channels that are clearly designed to deceive and exploit users through fraudulent activities. Acharya et al. (2024) note that scammers exploit the growing trend of using social media for technical support by targeting victims on these channels.

Referred to Li et al. (2024), scammers defraud users through a variety of tactics, including impersonating family members and friends, prominent channel owners, or investment advisors. However, despite the majority of respondents acknowledging their awareness of online scams on Telegram, 360 respondents also agreed that a lack of awareness is the primary factor behind the increasing prevalence of scams.

c) Public Attitude Towards Money Scam Issues Among Adults

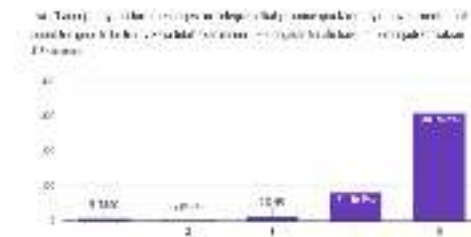


Figure 2.0

According to Figure 2.0, the data collected from 416 responses reveals that 310 (74.5%) respondents strongly agree they would not accept random Telegram messages promising quick money or too-good-to-be-true investments. Furthermore, additional data indicates that respondents who are aware of money scams on Telegram are more concerned and tend to be more proactive in protecting their family and friends from scams, utilizing their knowledge and awareness. Wilson et al. (2023) suggest individuals use their own safety measures, stay informed about scam tactics, and share news with friends and family to stay vigilant. The data also shows that 255 (61.3%) respondents strongly agree that they recognize the emotional damage caused by being scammed. This demonstrates that victims are well-informed about anti-scam campaigns and understand the appropriate actions to take if they receive suspicious calls or messages (Wilson et al., 2023). Overall, public awareness and knowledge about online fraud are interconnected and significantly influence public attitudes towards online scams (Zwilling et al., 2020).

136

d) Action And Prevention To Be Taken

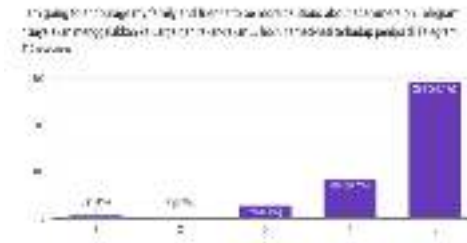


Figure 3.0

Continuing our research findings, the highest level of agreement emerged in response to a question highlighted in Figure 3.0, where 293 (70.4%) respondents strongly expressed their intention to advocate for increased vigilance among family and friends regarding Telegram scams. This proactive approach aims to safeguard loved ones from falling victim to monetary scams. Among the recommended actions is the practice of verifying the authenticity of contacts, offers, or information on Telegram before engaging, as scammers often impersonate others. A majority of 265 (63.7%) respondents demonstrated favorable attitudes towards implementing such measures, with over half of them strongly endorsing the proposed actions. Additionally, to fortify personal security against potential scams, 255 (61.3%) respondents indicated their strong inclination towards adopting enhanced security measures such as Two-Step

Verification to safeguard personal data and accounts. Moreover, they expressed their willingness to report fraudulent or suspicious activities on Telegram to platform administrators or local law enforcement agencies for appropriate intervention.

Furthermore, in order to stay informed about common scam tactics employed on Telegram, half of the total respondents frequently rely on newspapers or online sources. This practice is illustrated in a Today Online article (Ong, 2024), which reports on police warnings regarding a specific phishing scam perpetrated through the Telegram messaging app using fake Budget 2024 graphics.

e) Initiatives Effectiveness On Addressing Telegram Money Scam

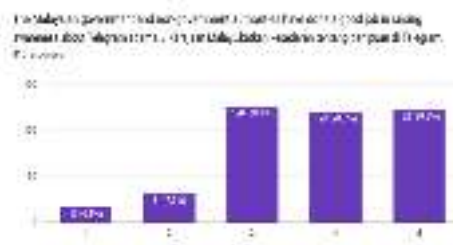


Figure 4.0

The findings of the study reveal that anti-scam campaigns by the government and non-governmental organizations in Malaysia have shown promising effectiveness. Most respondents agree that awareness campaigns

about scams on Telegram have successfully educated the Malaysian public. Notable examples include the #JanganKenaScam campaign, organized by the banking industry to combat financial scams, unify efforts, and promote anti-scam messaging (The Association of Banks in Malaysia, 2023). According to our sample, which reflects the broader target population, such efforts have a positive impact. However, the study also indicates that most respondents believe that the government and NGOs have not yet fully maximized their efforts in raising awareness about Telegram scams. This is shown in Figure 4.0, where 126 (30.3%) respondents gave neutral answers. Additionally, our respondents believe that the information provided by authorities on identifying and avoiding Telegram scams has been beneficial in protecting themselves, their loved ones, and the general public. Notably, 169 (40.6%) of respondents strongly agree that public efforts, such as past scam victims sharing their experiences, have significantly aided the government in reducing the number of people falling victim to Telegram money scams. This is because the data collected can offer a unique perspective on the cybercrimes experienced by social media users who share their stories (Górka, 2023). Consequently, this helps the community increase their

awareness, addressing the primary factor that leads to falling victim to Telegram money scams.

Conclusion

In conclusion, despite its growing popularity and numerous benefits, Telegram has become a hotspot for cybercrimes such as money fraud. These scams include investment schemes, fake job offers, phishing, and romance scams (Wilson et al., 2023). Although many respondents in this study are aware of these online scams on Telegram, a significant number still fall victim due to a lack of awareness. Consequently, the primary challenge is bridging this awareness gap, which makes Telegram users especially vulnerable. This lack of awareness leads to difficulties in recognizing the common tactics used by scammers. Furthermore, Telegram's features, such as allowing anonymity and not requiring phone numbers for sign-up, make it particularly appealing to scammers. The situation worsens when individuals are under financial stress, making them even more susceptible to these scams.

To address the growing issue of cybercrimes on Telegram, proactive measures are necessary from all parties. Firstly, individuals should report suspicious activity to the administration to help safeguard the community (Wilson et al., 2023). Additionally, Telegram must take immediate steps to improve security

monitoring and prevent misuse of the platform, such as implementing stricter user verification processes. Moreover, the public should stay informed about the latest developments on this issue by regularly reading newspapers and browsing social media. Lastly, the government and non-governmental organisations need to increase their efforts in launching more anti-scam campaigns and awareness programs throughout Malaysia to curb this problem before it escalates.

This research recommends that future efforts should expand the study of money scams on Telegram to address the current lack of focused research on this topic. The existing research on money scams and Telegram is limited and not comprehensive. Therefore, it is suggested that future researchers delve deeper into this subject by examining a different angle—specifically, the impact and consequences on individuals whose data is used without their knowledge to perpetrate scams. By expanding research efforts and considering new perspectives, we can work towards mitigating the risks posed by cybercrimes on platforms like Telegram and fostering a safer digital environment for all users. It is our hope that the research we have undertaken will prove beneficial and add to the existing body of knowledge for generations to come. Additionally, we also hope that the

research urges both government and non-government organizations to strengthen regulations and collaborate effectively to combat online scams, as well as enhance digital security for all users.

References

- Acharya, B., Cispá, Saad, M., Cinà, A., Cispá, L., Dai Nguyen, H., Oest, A., Vadrevu, P., & Cispá, T. (2024). *Conning the Crypto Conman: End-to-End Analysis of Cryptocurrency-based Technical Support Scams*. <https://arxiv.org/pdf/2401.09824>
- Akhtar, I. (2016, September). *Research Design*. ResearchGate; www.researchgate.net. https://www.researchgate.net/publication/308915548_Research_Design
- ALAVI, K., SOOED, M. S. A., & BAKAR, A.-A. (2018). Love Scam di Selangor: Satu Penerokaan terhadap Modus Operandi Jenayah Siber ke atas Wanita Profesional. *Jurnal Pembangunan Sosial*, 21. <https://doi.org/10.32890/jps.21.2018.11558>
- Australian Competition and Consumer Commission. (2023a, June 30). *Investment scams*. www.scamwatch.gov.au. <https://www.scamwatch.gov.au/types-of-scams/investment-scams>
- Australian Competition and Consumer Commission. (2023b, July 24). *Romance scams*. www.scamwatch.gov.au. <https://www.scamwatch.gov.au/types-of-scams/romance-scams>
- Bank Central Asia. (2023, October 12). *BCA*. www.bca.co.id. <https://www.bca.co.id/en/Individu>
- Bisht, R. (2024, January 30). *What is Purposive Sampling? Methods, Techniques, and Examples | Researcher.Life*. Researcher.Life. <https://researcher.life/blog/article/what-is-purposive-sampling-methods-techniques-and-examples/>
- Borges, E. (2024, March 7). *What is Information Gathering? Tools and Techniques*. www.recordedfuture.com. <https://www.recordedfuture.com/threat-intelligence-101/intelligence-sources-collection/information-gathering>
- Bressmer, A. (2022, April 21). *Cause and Effect: Definition, Meaning, and Examples*. Prowritingaid.com. <https://prowritingaid.com/ca>

use-and-effect

Cheung, K.-F. (2023, July 9). *Cracking the code: why people fall for scams*. www.businessthink.unsw.edu.au.

<https://www.businessthink.unsw.edu.au/articles/cracking-the-code-why-people-fall-scams>

Commonwealth Fraud Prevention Centre. (2020, July 20). *The total impacts of fraud*. Commonwealth Fraud Prevention Centre. <https://www.counterfraud.gov.au/total-impacts-fraud>

Cyber Security Agency Of Singapore. (2023, September 9). *CSA's 2022 Survey Shows Increase in Respondents' Perceived Likelihood of Falling Victim to Cyber Incidents and Online Scams*. Default. <https://www.csa.gov.sg/News-Events/Press-Releases/2023/csa-2022-survey-shows-increase-in-respondents-perceived-likelihood-of-falling-victim-to-cyber-incidents-and-online-scams>

DeNicola, L. (2021, April 29). *The Latest Scams You Need to Be Aware of in 2021*. www.experian.com. <https://www.experian.com/blogs/ask-experian/the-latest-scams-you-need-to-aware->

of/

Department of Statistics Malaysia. (2023). *Malaysia - Populasi Penduduk Malaysia | OpenDOSM*.

[Open.dosm.gov.my](http://open.dosm.gov.my).

<https://open.dosm.gov.my/ms-MY/dashboard/population>

Dictionary.cambridge.org. (2024). *SCAM | meaning in the Cambridge English Dictionary*.

Dictionary.cambridge.org. <https://dictionary.cambridge.org/dictionary/english/scam>

Dove, M. (2024, February 27). *Top 5 Scam Techniques: What You Need to Know | Tripwire*. www.tripwire.com. <https://www.tripwire.com/state-of-security/top-scam-techniques-what-you-need-to-know>

Edgar, T. W., & Manz, D. O. (2017). *Convenience Sampling - an Overview | ScienceDirect Topics*. Sciencedirect. <https://www.sciencedirect.com/topics/computer-science/convenience-sampling>

Federal Trade Consumer Commission Advice. (2020, December 3). *Investment Scams*. Consumer Advice. <https://consumer.ftc.gov/articles/investment-scams>

Fletcher, E. (2023, October 6). *Social media: a golden goose for scammers*. Federal Trade

- Commission.
<https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers>
- Fronozo, E. J. (2020, November 2). *Phishing Tactics and Techniques - Keeping Businesses Safe*. Slingshot.tel.
<https://slingshot.tel/business/phishing-tactics-and-techniques/>
- Górka, M. (2023). Manipulation techniques of cyber fraudsters using the example of phishing attempts for private content. *Policyjny Biuletyn Szkoleniowy/Interaktywny Biuletyn Policyjny/Przegląd Policyjny*, 150(2), 207–220.
<https://doi.org/10.5604/01.3001.0053.8540>
- Goundar, S. (2019). *Research Methodology and Research Method*. ResearchGate.
https://www.researchgate.net/publication/333015026_Chapter_3_-_Research_Methodology_and_Research_Method
- Gunnell, M. (2024, June 26). *TELEGRAM* (N. Medleva, Ed.). Techopedia.
<https://www.techopedia.com/definition/telegram>
- Hoofman, J. (2019, July 5). *Summer, Sun and Scams: Protect your Vacation from Fraud*. Buckingham Strategic Wealth.
<https://www.buckinghamstrategicwealth.com/resources/investing/summer-sun-and-scams-protect-your-vacation-from-fraud>
- Khanday, S. (2023). THE RESEARCH DESIGN. In *Research Gate*.
https://www.researchgate.net/publication/368257495_THE_RESEARCH_DESIGN
- Li, X., Rahmati, A., & Nikiforakis, N. (2024). Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms. *Proceedings 2024 Network and Distributed System Security Symposium*.
<https://doi.org/10.14722/nds.s.2024.24060>
- Lin, B. X. (2023). *A Study of Awareness of Cyber Scams and Cybersecurity Among University Students In Malaysia*.
http://eprints.utar.edu.my/5842/1/BONG_XU_LIN_FYP_Clean_version.pdf
- Marwick, A. (2018). GEORGETOWN LAW TECHNOLOGY REVIEW WHY DO PEOPLE SHARE FAKE NEWS? A

SOCIOTECHNICAL
MODEL OF MEDIA
EFFECTS. *WHY DO
PEOPLE SHARE FAKE
NEWS?* A
SOCIOTECHNICAL
MODEL of MEDIA
EFFECTS.
<https://doi.org/10.1177/1464884917730217>

- Moon, J.-W., An, Y., & Norman, W. (2022). Exploring the application of the uses and gratifications theory as a conceptual model for identifying the motivations for smartphone use by e-tourists. *Tourism Critiques: Practice and Theory*, 3(2), 102–119.
<https://doi.org/10.1108/trc-03-2022-0005>
- Morgia, M., Mei, A., Mongardini, A., & Wu, J. (2021). *Uncovering the Dark Side of Telegram: Fakes, Clones, Scams, and Conspiracy Movements*.
<https://arxiv.org/pdf/2111.13530>
- Murad, F. A. (2020). PERSONALITY AND LOW SELF-CONTROL AS CONTRIBUTING FACTORS FOR SCAM VICTIMIZATION: A CONCEPT PAPER. *International Journal of Psychosocial Rehabilitation*, 24(4), 4448–4461.
<https://doi.org/10.37200/ijpr/>

v24i4/pr201548

- National Anti-Scam Centre. (2023, September 19). *Unexpected money*.
[Www.scamwatch.gov.au](http://www.scamwatch.gov.au).
<https://www.scamwatch.gov.au/types-of-scams/unexpected-money#:~:text=Scammers%20try%20to%20convince%20you>
- Ong, S. (2023, April 23). *Police warn of phishing scam involving fake Budget 2024 infographics on Telegram*. TODAY.
<https://www.todayonline.com/singapore/police-warn-phishing-scam-involving-fake-budget-2024-infographics-telegram-2409046>
- Oregon State University. (2012, April 27). *Snowball Sampling*. Research Office.
<https://research.oregonstate.edu/irb/policies-and-guidance-investigators/guidance/snowball-sampling#:~:text=Snowball%20sampling%20is%20a%20recruitment>
- Quek, H. L. (2023). *Influential factors of online scam awareness among generation X in Malaysia*. Eprints.utar.edu.my.
<http://eprints.utar.edu.my/6302/>

- Rana, J., Gutierrez, P. L., & Oldroyd, J. C. (2021). Quantitative Methods. *Global Encyclopedia of Public Administration, Public Policy, and Governance*, 1–6. Springer.
https://doi.org/10.1007/978-3-319-31816-5_460-1
- Rashid, A. (2023, December 10). *Preventing emotional manipulation by online scammers (Poll Inside)*. The Star.
<https://www.thestar.com.my/news/focus/2023/12/10/preventing-emotional-manipulation-by-online-scammers>
- Rasmus, Gerlings, J., & Ferwerda, J. (2024). Do Awareness Campaigns Reduce Financial Fraud? *European Journal on Criminal Policy and Research*.
<https://doi.org/10.1007/s10610-024-09573-1>
- Romance Scams: *Unraveling the Web of Deceit*. (n.d.). DataVisor.
<https://www.datavisor.com/wiki/romance-scams/>
- Royal Police Malaysia. (2022, October 18). *Technology advancement drives scammers' adaptability*. The Malaysia Reserve.
<https://themalaysianreserve.com/2022/10/18/technology-advancement-drives-scammers-adaptability/>
- Sanction Scanner. (2019). *What is a Romance Scam and How to Avoid It? - Sanction Scanner*. www.sanctionsscanner.com.
<https://www.sanctionsscanner.com/knowledge-base/romance-scam-868>
- Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, 7(1).
<https://doi.org/10.1093/cybs/ec/tyab019>
- Social Media Research Institute. (2024). *Social Media Awareness*. www.smri.world.
<https://www.smri.world/research-topics/social-media-awareness#:~:text=0%3A00%20%2F%204%3A49>
- St. Clair, E. (2022). *City University of Seattle Library: Research Methods and Design: Quantitative Research Methods*. library.cityu.edu.
<https://library.cityu.edu/researchguides/researchmethods/quantitative>
- Swe, R. (2015). *Chapter 13: Patterns and Tactics* (p. 51).
- Teo, L., & Liew, P. (2019). *WHO ARE THE MONEY GAMES INVESTORS? A CASE*

STUDY IN MALAYSIA.

- The Association of Banks in Malaysia. (2023). *#JanganKenaScam – Safe Online Banking | The Association of Banks in Malaysia*. www.abm.org.my.
<https://www.abm.org.my/safe-online-banking/jangankenascam/>
- The Star. (2023a, April 23). *Toward protecting scam victims*. The Star.
<https://www.thestar.com.my/news/nation/2023/04/24/toward-protecting-scam-victims>
- The Star. (2023b, December 12). *“I ask myself why I’m so stupid”: Scam victims face serious mental health issues*. The Star.
<https://www.thestar.com.my/aseanplus/aseanplus-news/2023/12/12/i-ask-myself-why-im-so-stupid-scam-victims-face-serious-mental-health-issues>
- Ticha, V. (2023, September 20). *Cracking the code: why people fall for scams*. UNSW Sites.
<https://www.unsw.edu.au/newsroom/news/2023/09/cracking-the-code--why-people-fall-for-scams>
- Tookitaki. (2024, March 19). *Investment scams* - [Moneysmart.gov.au](https://moneysmart.gov.au).
<https://moneysmart.gov.au/financial-scams/investment-scams>
- University of Texas Arlington. (2023, December 8). *Subject and course guides: Quantitative and qualitative research: Understand what quantitative research is*. Uta.edu.
https://libguides.uta.edu/quantitative_and_qualitative_research/quant
- Vanian, J. (2021, January 16). *WhatsApp delays privacy policy update as users flock to Signal, Telegram*. Fortune.
<https://fortune.com/2021/01/15/whatsapp-delays-privacy-policy-changes-after-users-defect-to-rivals-signal-and-telegram/>
- Vinney, C. (2019). *What is uses and gratifications theory? Definition and examples*. ThoughtCo.
<https://www.thoughtco.com/uses-and-gratifications-theory-4628333>
- Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26(1), 277–292.
<https://doi.org/10.1108/jfc-10-2017-0095>
- Wilson, S., Nor Azlili Hassan, Khor, K., Santhidran Sinnappan, Abu, R., & Soon Aun Tan.

(2023). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime*. <https://doi.org/10.1108/jfc-06-2023-0151>

Zolkepli, F. (2022, September 22). *Scammers' adaptability has led to 50% increase in cybercrime over past two years, says IGP*. The Star. <https://www.thestar.com.my/news/nation/2022/09/26/scammers039-adaptability-has-led-to-50-increase-in-cybercrime-over-past-two-years-says-igp>

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 1–16. <https://doi.org/10.1080/08874417.2020.1712269>