MULTIDISCIPLINARY SCIENCE JOURNAL

RESEARCH ARTICLE
Published Online: October 17, 2025
https://doi.org/10.31893/multiscience.2026298

The role of communication technology in money mule victimisation: Platforms, content, and periods

Nurul Zaitul Itri Alias[a] ✉ | **Azlina Kamaruddin**[b] | **Nik Adzrieman Abdul Rahman**[b]

[a]Faculty of Education, Social Science and Humanities, Universiti Poly-Tech Malaysia, Malaysia.
[b]School of Multimedia Technology and Communication, Universiti Utara Malaysia, Malaysia.

Abstract The development and advancement of communication technologies, especially digital platforms and social media channels, has significantly contributed to the increase of financial crimes, with money mule scams being the most prevalent incidence with the highest consequences. Money mule scams encompass the recruitment of individuals, who are frequently unaware of such scams, to facilitate the transfer of illicit funds across borders or into personal accounts, with the individuals serving as intermediaries in fraudulent financial operations. The current study examined the communication process between scammers and money mule victims and delineated the findings derived from comprehensive interviews with nine money mule scheme victims in terms of relevant communication content, platforms, and periods between both parties. Relevant contents involved loans, Bitcoin, trading, part-time jobs, Companies Commission of Malaysia (SSM), and online games, whereas communication platforms included WhatsApp, Facebook, Instagram, short messaging service (SMS), telephone calls, and face-to-face interactions. The periods encapsulated days, weeks, and months. The study outcomes pinpointed that technological advancements led money mule victims to being manipulated into transferring money or goods on behalf of criminals by believing that personal actions could assist other individuals in need or in effortlessly earning money, which engendered substantial financial losses, legal issues, and emotional distress among the victims.

Keywords: communication technology, communication activities, money mules, scammers, cybercrime

1. Introduction

Communication means and technological advancements have constantly and simultaneously evolved throughout human history, with the availability and provision of mobile and internet services further advancing communication technologies to a more sophisticated level (Harankhedkar, 2011). While profound societal benefits of communication technological development have been observed, the advancement has also provided multiple opportunities for scam activities. The most ubiquitous approach to scamming victims in the past several years was robocalls or automated phone calls that concurrently delivered pre-recorded messages to various recipients, whereas contemporary scammers leverage online chatbots, text messages, email, and social media platforms (Weiss, 2025). Specifically, phishing is performed by sending emails labelled with a seemingly legitimate company website or sharing malicious links with software viruses via social media channels (Orman, 2013). Titus and Grover (2001) elucidated that scams might require a corresponding degree of communication and collaboration from the victim or not. For instance, identity theft and fraud can be conducted without victims being cognisant of such activities or dating scams can be performed by involving a certain engagement degree from the victim with the scammer to develop interpersonal trust through prolonged communication, which is recognised as grooming.

Scammers frequently recruit gullible individuals to serve as money mules, who are frequently incognizant of such illegal operations facilitated through personal involvement and actions. The money mules are employed to transfer illegal funds and launder illicit money for criminal organisations, which instil an additional layer of complexity for legal enforcement entities to trace the source of the stolen assets. A money mule refers to an individual who transfers money acquired illicitly on behalf of or at the instruction of another individual without being directly linked to the members of the criminal organisation, although relevant actions of money mules tend to disrupt the money trail while the criminal organisation profits from the laundered monies (Esoimeme, 2020; Vedamanikan & Devi, 2020; Raza et al., 2020; Leukfeldt & Kleemans, 2019). The first instance of money mules was revealed and reported in Australia in January 2005, wherein a total of 61 money mules were recruited ostensibly as part-time workers for World Transfer Inc. and were offered salaries up to $4,000 per month. The continuous development and advancement of communication technologies have also elevated the sophistication degree of scam activities, with money mules acting as the intermediaries within the expanding network of financial crime. A thorough comprehension of how relevant scams operate and the effective methods to protect oneself from becoming inadvertently involved in scams are highly essential in the contemporary era with uninterrupted connections between individuals and across the world. The

 Received: July 9, 2025 | Accepted: September 19, 2025

present study appraised the communication activities occurring between money mule victims and scammers in terms of the employed communication channels, relevant communication content, and the periods of different communication processes.

2. Research Questions and Research Objectives

2.1. Research questions (RQs)

Which platform is employed in the communication between the money mule and the scammer?
What is the content of the communication between the money mule and the scammer?
What is the period of communication between the money mule and the scammer?

2.2. Research objectives (RQs)

To determine the platform utilised in the communication between money mules and scammers.
To assess the content of the communication between money mules and scammers.
To pinpoint the period of communication between money mules and scammers.

3. Method

The current study evaluated the communication between money mules and scammers in Malaysia. The informant in this study is identified as a money mule victim, referring to an individual whose financial accounts were exploited to transfer or receive illicit funds on behalf of criminal actors. This categorization is significant because it situates the informant as a direct victim of financial crime, thereby providing firsthand insights into the mechanisms and impacts of money mule schemes. The selection of this informant was guided by purposive sampling, as the individual possesses specific characteristics central to the research objectives, namely the lived experience of being involved in money mule activities. At the same time, the study also employed convenience sampling, as the informant was accessible and willing to participate, which facilitated the data collection process. The combination of purposive and convenience sampling ensured that the participant not only met the research criteria but was also practically available, thereby strengthening both the relevance and feasibility of the data collection.

The researcher liaised with Persatuan Pengguna Islam Malaysia (PPIM) to acquire relevant respondent details by sending a formal self-introduction letter with the ROs to the individual responsible at the PPIM. The PPIM is a non-governmental organisation (NGO) registered with the Malaysian Societies Registration Department (JPPM) and established based on Section 2 of the Societies Act 1966. The PPIM seeks to advocate for matters concerning halal and haram while resolving the issues related to persecution, injustice, malevolence, and cruelty directed towards Muslim individuals. Accordingly, victims of the money mule scheme reported personal scam cases to the PPIM. The researcher contacted potential respondents after acquiring relevant details from the PPIM. The researcher explicated the interview objective and guaranteed the respondents that actual names and personal information would remain confidential without being divulged or published in the study findings or any other written materials. Interview sessions were arranged upon obtaining the respondents' consent.

The present study conducted semi-structured interviews with two sections. The first section comprised questions to collect respondents' demographic details while the second section consisted of questions according to the RQs. A semi-structured interview is a data collection technique, which encompasses asking specific questions related to the study topic within a stipulated thematic framework. Simultaneously, the questions are not strictly framed and defined, which allows the researcher the flexibility to ask further questions based on the responses provided by respondents. The researcher conducted semi-structured interviews both online and physically through Bahasa Melayu as the primary communication language. The online interview was performed via the internet platform Webex, whereas the physical interview was conducted at the PPIM headquarters. The interview was recorded after obtaining the respondent's consent.

A total of nine respondents participated in the interview. The number was established according to the notion of data saturation, which transpires when further interviews cease to yield novel themes, insights, or variations pertinent to the research topics. Throughout the data collection procedure, it became apparent that following the ninth interview, the replies started to converge with previously recognized patterns, signifying that the information obtained was adequate to thoroughly fulfill the study's objectives. In qualitative research, saturation is prioritized over sample size, as the depth and repetitiveness of data are more significant than numerical representation (Creswell, 2018; Guest, Bunce, & Johnson, 2006). Furthermore, previous qualitative research on sensitive subjects like financial fraud and victimization has also indicated that saturation can be attained with relatively small sample sizes, often between six and twelve participants (Guest et al., 2006; Saunders et al., 2018). Consequently, the choice to finalize data collection with nine informants was supported both methodologically and empirically.

The collected interview data were analysed through qualitative content analysis. Furthermore, the interview transcripts were promptly generated and subsequently translated into English before data analysis on the NVivo software.

4. Result

4.1. Interview respondent demographic

The current study scrutinised the communication activities between money mules and scammers among nine semi-structured interview respondents. Table 1 depicts respondent demographics, which encompass age, gender, educational background, occupation, and year of victimisation. Specifically, the highest educational level was a Diploma, with only three respondents attaining the certification while the remaining six respondents achieved only the SPM level. A majority of victimisation cases occurred between 2020 and 2023, namely during the coronavirus disease (COVID-19) pandemic, with only one case in 2017.

Table 1 Demographic Profile of Respondent.

Respondent	Age	Gender	Education	Occupation	Year of Victimisation
1	22	Male	SPM	Self-employed	2020
2	40	Male	Diploma	Maxis Centre supervisor	2021
3	27	Male	SPM	Self-employed	2020
4	36	Female	SPM	Diner assistant	2020
5	29	Female	SPM	Sales assistant	2021
6	37	Female	Diploma	Civil servant	2020
7	35	Female	SPM	Unemployed	2023
8	32	Male	Diploma	Self-employed	2021
9	45	Male	SPM	Self-employed	2017

4.2. The platform utilised in the communication between money mules and scammers

The platforms employed for the communication between scammers and money mules included Facebook, Instagram, WhatsApp, Short Messaging Service (SMS), Line, phone calls, and physical interactions, with Table 2 illustrating the themes and sub-themes.

Table 2 Themes and sub-themes regarding the communication platforms between money mules and scammers.

Theme	Sub-theme
Platform	Facebook
	WhatsApp
	Instagram
	SMS
	Phone call
	Physical interaction

4.2.1. Facebook

Scammers employed Facebook to promote loans, part-time work opportunities, and online businesses to attract the interest of respondents through relevant advertisements targeted at individuals seeking pertinent information. Respondents highlighted the discovery process of a loan advertisement on Facebook:

I first saw this advertisement on Facebook because, during the COVID period, my entire family couldn't go out.

Through WhatsApp and Facebook, I obtained his number and initiated contact on WhatsApp.

Okay. In the beginning, my husband mentioned he was thinking of getting a loan. I was like, 'What kind of loan?' and made it clear I wasn't up for it. He said he saw it on Facebook, but I didn't allow it, I said I didn't want to. Then, it was in 2020, during the COVID-19 era, when all transactions were mainly done online.

4.2.2. WhatsApp

WhatsApp is a free messaging platform that enables individuals to exchange text messages, construct audio and video chats, and other actions through the Internet connection. Essentially, WhatsApp is one of the most popular instant messaging applications worldwide. Scammers employed multiple channels, including WhatsApp, to communicate with money mule victims to ensure that the victims were deceived through fraudulent techniques. The current study respondents delineated that WhatsApp was the communication channel employed by scammers for further interactions with the victims after first corresponding with the scammers on social media or other platforms:

I checked it, found it logical, and they requested me to WhatsApp them. So, the first thing I did on WhatsApp—regarding it, I discussed everything with my wife, and we settled, agreed upon, and started making calls, mostly using WhatsApp calls and regular calls.

After working on the ship for about 6 months, I received a WhatsApp message from someone outside. They found me on Facebook and then contacted me through WhatsApp to purchase a PIN.

4.2.3. Instagram

Instagram is a famous social media platform being utilised by scammers to communicate with victims, on top of Facebook:

Initially, she chatted through IG, Instagram. She asked if I had a bank account because she intended to use it for trading BITCOIN, or something like that. I explained that I seldom use IG.

4.2.4. Short message service (SMS)

The SMS is a text messaging service part of most smartphone, Internet, and mobile device networks. According to the respondents, the scammer employed the software, namely Blaster, to send messages in bulk to numerous recipients in the specific area within the coverage of Blaster:

It all began with SMS, initiated by them. They blasted SMS using a device, and we knew it because we work in telco, using a device we call the Blaster. When it detects the numbers in that area, it sends out an SMS, one SMS, and it can be done on a PC as well. This program stays on the laptop.

4.2.5. Phone call

Another communication channel between the money mule and the fraudster was phone calls. Particularly, the respondent was called by the scammer to arrange a meeting regarding the ATM card. The scammer purportedly claimed the ATM card was swallowed by the machine or the personal identification number (PIN) was altered:

He also made one phone call. One day, he called and invited me to meet as he needed my help to change a PIN.

4.2.6. Physical interaction

The scammer requested a physical meeting with the respondent to obtain the automated teller machine (ATM) card for loan processing and bank account opening:

After that, we met; I only met their runner on Jalan Klang Lama. That's all. Their process didn't take up to 2 weeks. Their process with me didn't take up to 3 days.

4.3. Content of the communication between money mules and scammers

The content of communication was categorised into seven sub-themes, namely loans, Bitcoin, online gaming, part-time jobs, trading, Companies Commission of Malaysia (SSM), and online gambling, which were primarily leveraged by scammers to captivate the interest of respondents in initiating a conversation. Table 3 portrays the themes and sub-themes of the communication content between money mules and scammers.

Table 3 Themes and sub-themes of the communication content between money mules and scammers.

Theme	Sub-theme
Content	Loan
	Bitcoin
	Online gambling
	Part-time job
	Trading
	SSM
	Online game

4.3.1. Loan

Respondents elucidated the intention to seek and obtain a loan. Relevant loan information was accessed on Facebook, with the scammer reaching out to the respondents after indicating personal interest in the loan advertisement. Concurrently, the respondents required emergency funds due to financial hardships. The emergency engendered respondents to be more susceptible and willing to relinquish personal ATM cards and disclose personal online banking credentials when the loan advertised by the scammer appeared to be highly accessible:

I first saw this advertisement on Facebook because, during the COVID period, my entire family couldn't go out. At that time, I was looking for an alternative loan option, and I noticed many could be applied online, meaning the process is managed online. I also had experience with personal loans.

What happened to me was that I was facing financial problems at that time. So, I made an application, sorry, not making an application. I explored on Facebook, Instagram, and other platforms. I came across an advertisement offering personal loans initially. I left my phone number in the comments section on Facebook, and then the scammer contacted me.

4.3.2. Bitcoin

Bitcoin is a digital payment system operating through virtual cash instead of traditional fiat or physical currencies. The system employs a blockchain to safeguard transaction data from centralised intermediaries, who manage and oversee transactions in conventional financial institutions. The respondent elucidated that a friend requested the respondent's account as the friend sought to utilise the account for Bitcoin:

Initially, she chatted through IG, Instagram. She asked if I had a bank account because she intended to use it for trading BITCOIN, or something like that.

4.3.3. Online gambling

The third sub-theme is online gambling. The respondent indicated a personal interest in online gambling to earn additional money. The respondent was only required to submit the personal ATM card and online banking information:

They mentioned using it for a casino. From my perspective, I wasn't aware that engaging in gambling activities was considered wrong. Typically, I understand that those who gamble do so voluntarily, contributing money willingly. Therefore, I didn't comprehend that this could lead to fraudulent activities.

4.3.4. Part-time job

The respondent highlighted a personal interest in a part-time job by searching for relevant opportunities on Facebook. The respondent discovered one potential part-time job opportunity and the respondent was required to transfer money overseas before being commissioned with the job. The commission was higher compared to the current baking business:

I was indeed looking for a part-time job, initially, I made traditional pastries at home. The profit wasn't much. I saw the advertisement for a part-time job, where you transfer money and get a 10% commission. I was intrigued because it seemed so easy to earn money.

4.3.5. Trading

Trading is the process of selling and purchasing stocks, bonds, commodities, currencies, or other financial products within a brief period to generate profits. The primary distinction between trading and traditional investing is that the former emphasises short-term strategies while the latter focuses on long-term returns. The respondent was interested in learning trading to acquire additional income:

He mentioned that to learn trading, I needed an account, and he wanted to register that account. I had no knowledge about trading. So, he convincingly explained that for this purpose, he needed to register this account.

4.3.6. SSM

The respondent explicated that the respondent and the respondent's cousin were being urged to register with the SSM, which was the principal regulatory authority overseeing corporate and business matters in the local area to guarantee that corporations and businesses adhere to Malaysian laws and regulations. The scammer proclaimed of providing assistance to foreigners in establishing companies and would receive a commission for offered services. The respondent, the respondent's cousin, and the scammer went to the bank to open a bank account before providing the ATM card, account number, and Internet banking details:

In Sabah, we are not familiar with the concept of mule accounts and such. The security staff asked my cousin and me if we wanted to register with the SSM, saying there was assistance available.

4.3.7. Online game

The respondent operated an Internet gaming business by selling PINs for online games. Several scammers exploited the online gaming business to deceive gamers by utilising the respondent's account number:

They found me on Facebook and then contacted me through WhatsApp to purchase a PIN. The PIN was for Razer PIN, a platform for buying online games. They would buy a PIN from me, input it into Razer PIN, and from there, they could use it for mobile legends or PUBG games.

4.4. The period of communication between money mules and scammers

The communication periods between the money mule and the scammer were defined in days, weeks, and months (see Table 4).

4.4.1. Days

The scammer required only several days to deceive the respondents. A respondent underscored that the personal account was blocked owing to certain suspicious transactions after the respondent allowed the friend to utilise the respondent's account for Bitcoin transactions. Another respondent delineated that the respondent physically met with the

scammer to open a bank account for the SSM within a day. The period was incorrect as the period was a lie from the scammer to ensure the respondent agreed with the idea:

However, not even within a week, my account got blocked and banned.

Their process with me didn't take up to 3 days. After that, I handed over the card, and within a week, there were numerous transactions.

Table 4 Themes and sub-themes of the communication period between money mules and scammers.

Theme	Sub-theme
Period	Days
	Weeks
	Months

4.4.2. Weeks

The second sub-theme is weeks. The respondents only realised being scammed after several weeks. Specifically, the scammer called the respondent for a physical meeting to resolve the issue related to the respondent's ATM card after three weeks of communication and the respondent decided not to agree. Hence, the scammer might require more time to leverage the respondent's account for scamming other victims.

That encapsulates the extent of our interaction, which spanned approximately 3 weeks.

I engaged in this for less than a month. The scammer mentioned that after a month, they would distribute the promised 10% commission, but I have not received it yet.

4.4.3. Months

Respondent No. 6 elucidated that four to six months were required for the respondent to trust the scammer as the respondent was initially uncertain about trading before the scammer convinced the respondent to agree to share personal bank details:

I wouldn't say it was long, maybe around 4, 5, 6 months, more or less. I was hesitant to give at first, but the way he spoke was convincing.

After approximately three months, I experienced significant profits due to their frequent purchases. On some days, I would receive up to 20 receipts from their transactions. Then, I received a call from the police, informing me that it was a scammer case, and my bank accounts were also blocked.

5. Discussion

The present study identified that scammers employed loan applications, Bitcoin, online gambling, part-time employment opportunities, trading, SSM registration, and online gaming, as the means to develop communication with money mule victims. Particularly, the scammers coaxed the victims to relinquish personal account information and ATM cards, with money mules generally as a diversion for the legal enforcement bodies. The fraudster typically contacts potential money mule victims after perusing potential victims' social media profiles before involving the victims in the illicit scheme. The scammer would utilise the data from the money mule victim's account and ATM card to execute a fraud scheme aimed at further victims, as delineated by the study respondents. A respondent explicated during the interview that the respondent was interested in acquiring a loan and expressed personal interest in a Facebook loan advertisement. The respondent was subsequently approached by the scammer to offer a loan. The scammer's description of the loan, with the clarification of relevant processes and required documents, captivated the respondent. Other respondents also experienced similar circumstances. Specifically, a respondent searched for trading information on Facebook before being approached by a fraudster who elucidated the trading process. The experience corresponded to the investigation by the Home Team Behavioural Team Centre (2020), which demonstrated that scammers might engage potential victims by presenting as a prospective romantic partner or confidant or a representative from a reputable organisation, such as a loan provider from a well-established financial institution. The respondent also delineated that the respondent's friend intended to employ the respondent's personal bank account for Bitcoin transactions. The respondent was convinced that the friend required financial assistance and the respondent was resolved to aid the friend by sharing personal account information. This pattern resonates with findings from the Netherlands, where Leukfeldt and Jansen (2015) demonstrated that cybercriminal networks often rely on social ties and online forums to build credibility with potential mules. Likewise, Australian research has indicated that scammers frequently employ personal narratives to gain victim trust, with romance or friendship themes evolving into financial exploitation (Cross, 2018). These similarities reinforce the idea that social engineering remains a core strategy in mule recruitment, regardless of national boundaries. Moreover, scammers would leverage part-time employment opportunities, online gaming, social media, and Internet gambling to initiate conversations with victims. Particularly, a respondent highlighted that a co-worker invited the respondent to engage with the SSM and explicated that a significant number of individuals recruited to aid a firm, with the assurance of obtaining a reward. The respondent was only required to open a bank account and provide the account

information together with the ATM card to a designated party. Another respondent managed an online gambling business and provided PINs to consumers without being aware of the PIN exploitation to execute fraud schemes.

Multiple channels were leveraged by the scammer to contact money mule victims. The current study revealed that scammers predominantly utilised technology-mediated communication platforms to target money mule victims. While the Internet and related technologies provided substantial advantages to society, extensive opportunities for large-scale fraud and other criminal activities were also facilitated (Button et al., 2014). WhatsApp and Facebook were the primary platforms utilised by scammers to contact victims. The findings were consistent with prior studies discovering that a majority of money mule victims, who were interested in earning additional income, were recruited via Facebook and WhatsApp (Leukfeldt, 2014; Mauritz, 2014; Stalenberg, 2011). This trend is consistent with studies in Europe and North America, which show that social media platforms and encrypted messaging applications provide fertile ground for mule recruitment (Europol, 2020; Button et al., 2014). For instance, UK Finance (2021) reported that over 70% of mule cases in the United Kingdom involved initial contact via social media or instant messaging. While Malaysia-focused studies (Abd Rahman, 2020; Vedamanikam & Chetiyar, 2020) emphasis WhatsApp and Facebook, these platforms are similarly central to recruitment globally, suggesting that platform choice is influenced more by global user penetration than local culture. In addition, SMS was employed as a communication channel between scammers and money mule victims. The respondent reported receiving SMS messages from a scammer offering a personal loan. The description was aligned with Foozy, Ahmad, and Abdollah (2013) who uncovered four distinctive phishing strategies, namely Bluetooth, SMS, vishing, and mobile website applications. Phishing is performed by disseminating deceptive messages seemingly trustworthy from a credible and trustworthy source via email and text messaging. The SMS dispatched through the BLASTER software also contained a loan proposal from the scammer, as indicated by the respondent. Additionally, phone calls were another channel employed by the scammer. The European Commission (2020) reported that scammers also leveraged traditional communication methods, including telephones. A respondent elucidated that the fraudster contacted for a physical meeting to accelerate the loan application process. Physical interactions were occasionally employed by fraudsters to persuade victims. Therefore, fraud can be performed through various communication methods, including physical interactions, postal correspondence, telephone conversations, text messages, and Internet platforms (Cross, 2018). The respondent underscored that the scammer convinced the respondent of the loan offer, which led to the belief in the scammer and subsequent submission of the loan application.

The duration of communication between victims and scammers also varied in this study, with some interactions lasting only days, while others extended for months. This aligns with international evidence that scam typologies differ in their temporal strategies. For instance, romance scams in the United States and Australia often span months to establish emotional dependence before financial exploitation (Dove, 2018; Cross, 2018). Conversely, Europol (2020) has reported that “fast-burn” scams, such as loan or quick investment offers, typically conclude within days or weeks. The present study therefore adds Malaysian evidence to a broader global pattern where the communication timeline reflects the scammer’s chosen persuasion strategy.

6. Conclusions

While communication technology has offered numerous benefits, significantly adverse impacts have also been observed on individuals who have been victimised by money mule schemes. The ease of access to digital platforms and social media channels has enabled scammers to exploit victims with higher efficiency and anonymity. The victims have also frequently been misled by fraudsters via persuasive online communication methods, including emails, fake job offers, and social media messages, into participating in illegal activities without adequately comprehending relevant consequences. Technological advancements have also led to financial losses, legal issues, and emotional distress among money mule victims, with numerous victims manipulated into transferring money or goods on behalf of criminals by believing in personal actions that could assist other individuals in need or in effortlessly earning additional income. The victims eventually encounter profound legal consequences and tarnished reputations. Moreover, communication technology has increased the challenge for authorities to trace and prevent relevant fraud crimes as perpetrators can effortlessly conceal personal identities behind fake versions and through encrypted channels. While communication technology can connect individuals through virtual platforms, the technology also fosters more criminal activities and enables scammers to target vulnerable individuals with long-lasting jeopardies. Drawing from the experiences of money mule victims, authorities may produce a brief film and chronological scenes to elucidate how scammers communicate and manipulate their victims. Other than that, we as the people that may be the target of scam can be more cautious and skeptical to any attempt of scam activity.

Acknowledgement

The author would like to express sincere gratitude to Universiti Utara Malaysia and Universiti Poly-Tech Malaysia for providing the necessary resources and support to conduct the current investigation. The author also extends appreciation to Associate Professor Dr Nik Adzrieman Abdul Rahman and Associate Professor Dr Azlina Kamaruddin for valuable guidance, encouragement, and insightful feedback throughout this study.

Ethical considerations

The present study involved semi-structured interviews with money mule victims, necessitating strict adherence to ethical protocols to protect participants' rights and confidentiality. All informants were assigned alphanumeric codes (e.g., I1, I2) in place of personal identifiers. Names, contact details, and other identifiable information were omitted from transcripts, reports, and publications.

Conflict of Interest

The authors declare no conflicts of interest.

Funding

The current study was fully funded by the University Research Grant (URG) from Universiti Poly-Tech Malaysia.

References

Abdul Rahman, M. R. (2020). Online scammers and their money mule in Malaysia. *Journal of Law and Society, 26*(8). https://doi.org/10.17576/juum-2020-26-08

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*, 1–18. https://doi.org/10.1177/0004865814521224

Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.

Cross, C. (2018). (Mis)Understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders*. https://doi.org/10.1080/15564886.2018.1474154

Dove, A. (2018). Romance fraud: Examining the impact on victims and the wider community. *Journal of Financial Crime, 25*(2), 370–383. https://doi.org/10.1108/JFC-07-2017-0058

Esoimeme, E. E. (2020). Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-05-2020-0053

Europol. (2020). *Money muling: Don't be a mule – Be smarter than a criminal*. https://www.europol.europa.eu

Federal Trade Commission. (2022). *Protecting consumers from money mule scams*. https://www.ftc.gov

Foozy, C. F. M., Ahmad, R., & Abdollah, M. F. (2013). Phishing detection taxonomy for mobile device. *International Journal of Computer Science Issues, 10*(1), 338–344.

Harankhedkar, H. (2011). Impact of technology on communication. http://www.buzzle.com/articles/impact-of-technology-on-communication.html

Home Team Behavioural Team Centre. (2020). *Scammer, beware: Building societal resilience to scams*. Crime, Investigation, and Forensic Psychology Branch.

Lea, S., Fischer, P., & Evans, K. (2009). The psychology of scams: Provoking and committing errors of judgement. Report for the Office of Fair Trading. https://ore.exeter.ac.uk/repository/bitstream/handle/10871/20958/OfficeOfFairTrading2009.pdf

Leukfeldt, E. R., & Kleemens, E. R. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives, and involvement mechanism. https://www.researchgate.net/publication/334090389

Leukfeldt, R., & Jansen, J. (2015). Cybercriminal networks, social ties and online forums: Social mechanisms in a digital environment. *Crime, Law and Social Change, 64*(2–3), 111–130. https://doi.org/10.1007/s10611-015-9599-4

Malaysian Communications and Multimedia Commission. (2023). *Internet users survey 2023*. https://www.mcmc.gov.my

Mauritz, H. J. (2014). The nature and extent of money muling: Internet banking fraud and money laundering. Dutch Police Report.

Orman, H. (2013). The complete story of phish. *IEEE Internet Computing, 17*(1), 87–91.

Raza, M. S., Zhan, Q., & Rubab, S. (2020). Role of money mules in money laundering and financial crimes: A discussion through case studies. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-02-2020-0028

Royal Malaysia Police. (2024). *Annual report: Commercial Crime Investigation Department*. https://www.rmp.gov.my

Shawyer, A., & Walsh, D. (2007). Fraud and peace: Investigative interviewing and fraud investigation. *Crime Prevention and Community Safety, 9*(2), 102–117. https://doi.org/10.1057/palgrave.cpcs.8150035

Titus, R. M., & Gover, A. R. (2001). Personal fraud: The victims and the scams. *Crime Prevention Studies, 12*, 133–152.

UK Finance. (2021). *Fraud: The facts 2021*. UK Finance. https://www.ukfinance.org.uk

Vedamanikam, M., & Chetiyar, S. D. M. (2020). Money mule recruitment among university students in Malaysia: Awareness perspectives. *International Journal of Teaching, Education and Learning, 34*(1), 19–37. https://doi.org/10.20319/pijtel.2020.41.1937

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications.

Source details

Multidisciplinary Science Journal

Years currently covered by Scopus: from 2019 to 2026

Publisher: Malque Publishing

E-ISSN: 2675-1240

Subject area: Multidisciplinary

Source type: Journal

View all documents > | Set document alert | Save to source list

CiteScore 2024
0.5

SJR 2024
0.125

SNIP 2024
0.226

CiteScore | CiteScore rank & trend | Scopus content coverage

CiteScore 2024

$$0.5 = \frac{367 \text{ Citations } 2021 - 2024}{698 \text{ Documents } 2021 - 2024}$$

Calculated on 05 May, 2025

CiteScoreTracker 2025

$$0.8 = \frac{1{,}030 \text{ Citations to date}}{1{,}221 \text{ Documents to date}}$$

Last updated on 05 October, 2025 • Updated monthly

CiteScore rank 2024

Category	Rank	Percentile
Multidisciplinary Multidisciplinary	#158/200	21st

View CiteScore methodology > | CiteScore FAQ > | Add CiteScore to your site

About Scopus

What is Scopus

Content coverage

Scopus blog

Scopus API

Privacy matters

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us