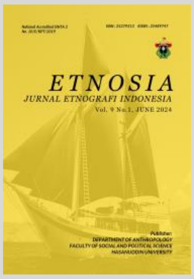
ETNOSIA:
JURNAL ETNOGRAFI INDONESIA
Volume 10 Issue 2, Dec 2025
P-ISSN: 2527-9319, E-ISSN: 2548-9747



Social Media Scams: A Netnography Investigation in Malaysia and Indonesia

Anak Agung Gde Satia Utama[1]*, Erna Andajani[2], Aaiman Siddiqui[3], Khaslinda Akasyah Binti Mujin[4], Siti Rochmah Ika[5], Siow Xiu Yun[4], Parwita Setya Wardhani[6]

[1] *Universitas Airlangga, Indonesia.*
[2] *Surabaya University, Indonesia.*
[3] *Khwaja Moinuddin Chishti Language University, Lucknow.*
[4] *University Malaysia Sabah, Malaysia.*
[5] *Janabadra University, Indonesia.*
[6] *Sekolah Tinggi Ilmu Ekonomi Mahardhika, Indonesia.*

* *Correspondence author:* gde.agung@feb.unair.ac.id

ARTICLE INFO

Keywords:
Online scams; netnography; fraud prevention; digital literacy; cybercrime; Indonesia; Malaysia.

How to cite:
Utama, A. A. G. S., Siddiqui, A., Mujin, K. A. B., Ika, S. R., Yun, S. X., Wardhani, P. S., & Andajani, E. (2025). Social Media Scams: A Netnography Investigation in Malaysia and Indonesia. ETNOSIA: Jurnal Etnografi Indonesia, 10(2), 245–260.

DOI:
https://doi.org/10.31947/etnosia.v10i2.44227

Article history:
Received: Mei 20, 2025
Revised: Dec 19, 2025
Approved: Dec 23, 2025

ABSTRACT

Online scams have become increasingly sophisticated across Southeast Asia, yet current studies primarily focus on single-platform fraud, specific scam types, or victim psychology in isolated contexts. Existing literature has examined romance scams, online investment fraud, digital labor scams, and general scam perceptions. However, few studies adopt a comparative Netnography approach across multiple social media platforms or explore the interconnectedness of scams with emerging issues such as human trafficking, particularly in Indonesia and Malaysia where scam incidents are rapidly escalating. This study fills this gap by providing a cross-country, multi-platform netnography investigation of scam techniques and victim responses. Using a non-participatory netnography approach, this research analyzed public interactions tagged with #scam and #scammeralert on Facebook, Instagram, and YouTube over a five-day period in 2024. The study examined scammer strategies and victim narratives drawn from scam-reporting communities and fraud-victim support groups. The findings identify four dominant scam types: (1) selling products at cheaper prices, (2) impersonation, (3) offering job with high salary, and (4) offering online part-time job. The study also reveals three major victim responses: (1) shooting and uploading the fraud on social media, (2) creating fraud's victim association, and (3) freezing of their bank account on priority basis. This research contributes new insights by demonstrating how digital platforms function as interconnected ecosystems of fraud, where multiple scam types operate simultaneously and victims mobilize collective counteractions. The study highlights the urgent need for enhanced digital literacy, cross-border enforcement, and integrated anti-scam policies in Indonesia and Malaysia.

1. Introduction

Online scams have become a global concern, exploiting technological advancements and the increasing reliance on digital platforms (Tambe et al., 2024). In Southeast Asia, particularly in Malaysia and Indonesia, the rapid expansion of internet accessibility and digital transactions has created an environment where scams proliferate (Wilson et al., 2024). Scammers exploit social media, e-commerce platforms, and digital banking systems to target individuals with enticing offers that often lead to financial fraud or, in severe cases, human trafficking (Dupuis et al., 2023; AllahRakha, 2024).

In Indonesia, the prevalence of online scams has reached alarming levels. Between 2020 and November 2024, the Indonesian Ministry of Foreign Affairs recorded 5,111 cases involving Indonesian citizens in online scams, with 1,290 identified as victims of human trafficking.[1] Additionally, the Ministry of Communication and Information Technology reported 572,000 online scam incidents from 2017 to 2024, predominantly involving fraudulent online transactions and investments.[2]

In Malaysia, a national scam awareness survey conducted by CelcomDigi in 2024 revealed that 73% of respondents had encountered scams, indicating widespread vulnerabilities. (BERNAMA, 2024). Many fraudulent activities involve the Trafficking in Persons (TIP) industry, where victims are misled by fake job offers and then subjected to passport confiscation, forced labor, and exploitation (IOM UN Migration, 2023). The Malaysian and Indonesian governments have implemented legal frameworks to combat online fraud, but the fast-evolving nature of scams makes enforcement challenging (Sarkar & Shukla, 2024).

Previous research has highlighted the psychological and social factors contributing to victimization in online scams. Whitty and Buchanan (2016) found that individuals with lower digital literacy and higher trust in online interactions are more susceptible to fraud. Similarly, Norris et al. (2019) emphasized that scammers strategically manipulate victims using social engineering tactics, such as urgency and authority, to bypass rational decision-making processes. Anderson et al. (2024) further argued that trust and technology play crucial roles in online investment fraud, where victims are deceived by seemingly legitimate financial schemes.

Fraudsters leverage various deceptive techniques, including phishing, impersonation, fake job offers, and fraudulent e-commerce transactions, to manipulate victims into financial losses or personal exploitation (Ridho, 2024;

[1] https://nasional.kompas.com/read/2024/12/18/15022471/kemenlu-catat-5111-wni-terlibat-online-scam-sepanjang-2020-2024, accessed on November 25, 2025.

[2] https://inp.polri.go.id/artikel/ministry-of-communication-and-information-records-572000-bank-account-online-scams, accessed on November 25, 2025.

Anderson et al., 2024). Scams not only target individuals, but also impact families and communities (Taodang & Gundur, 2023). Hence, it contributes to an environment where trust and online safety are increasingly compromised (Wilson et al., 2024). Alongside scamming, human trafficking remains a critical issue in the region, with online platforms often exploited to lure victims through promises of employment or financial gain, leading to exploitation and abuse (Owen et al., 2017; Yu, 2015; Norris & Dowell, 2019; Iqbal et al., 2018; Antonopoulos, 2020).

Given these concerns, this study adopts a netnography approach, which involves systematically observing and analyzing naturally occurring online interactions in public digital spaces. This study contributes to the growing body of research on cybercrime and online fraud, reinforcing the need for a comprehensive strategy to ongoing efforts in enhancing public awareness, digital literacy, and policy development to mitigate the growing threat of online scams in Indonesia, Malaysia, and beyond.

2. Method

This study employs a Netnography research approach to examine online scam activities and victim responses within digital environments. Netnography, introduced by Kozinets (2015), is well-suited for exploring cultural interactions in online communities because it allows researchers to observe naturally occurring behaviors, discussions, and social patterns without interfering with the digital setting. The study was conducted in virtual research locations, namely Facebook, Instagram, and YouTube, which are widely used in Indonesia and Malaysia and frequently serve as platforms for scam-related interactions.

Data collection took place over a five-day fieldwork period from 10 to 15 November 2024, during which scam-related posts, comment threads, and victim discussions were systematically monitored.

In netnography, research informants are naturally occurring online participants rather than individuals recruited through interviews. Therefore, the informants in this study consist of social media users who publicly posted or commented on scam-related content, members of scam-victim communities such as the Sambhara Kawal Siber pages on Facebook and Instagram, and victims who shared their narratives and experiences in public comment sections.

Data were collected through non-participatory observation, also referred to as the “lurking” technique, which involves observing digital interactions without engaging with users. This method enables us to record scam techniques, public reactions, and victim testimonies in their natural form. The method includes: (1) observing posts tagged with #scam and #scammeralert alongside testimonials from scam-victim associations and individuals affected by fraudulent schemes, (2) recording publicly available narratives from scam-victim communities, (3) identifying scam techniques and victim responses.

The data were analyzed using thematic analysis following Braun and Clarke (2006), which allowed us to identify and interpret patterns across the dataset.

Analytical steps included coding scam tactics, categorizing types of fraud such as fake product sales, high-salary job scams, impersonation schemes, and fraudulent part-time job offers, and identifying victim responses including filing police reports, blocking scammer accounts, freezing bank accounts, joining victim associations, and raising awareness through social media. Data validity was strengthened through triangulation across multiple platforms and cross-checking scam narratives from different victim groups, ensuring that findings were credible and consistent with Nowell et al.'s (2017) recommendations for qualitative trustworthiness.

Ethical principles of netnography research were strictly followed throughout the study. Only publicly available data were used, and no direct interaction with online users occurred to avoid influencing their behavior. Personal identifiers, usernames, and sensitive information were anonymized to protect participant privacy. The study did not enter private groups nor access restricted content, ensuring compliance with ethical guidelines for unobtrusive online research (Mkono, 2016).

3. Result and Discussion

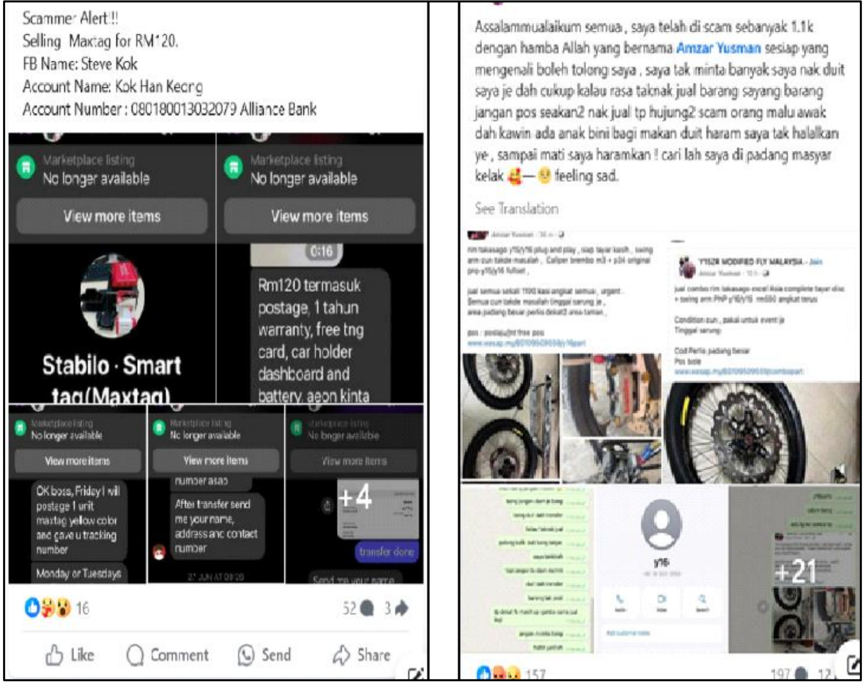
- **Types of Scams**

Social media has become an integral part of daily life, offering convenience and connectivity to millions of users. However, its wide reach, anonymity, and open-access nature also create vulnerabilities that enable fraudulent activities to flourish. Across platforms such as Facebook, Instagram, YouTube, and in some cases WhatsApp, scammers actively exploit digital spaces to deceive users. Using the hashtags (#scam and #scammeralert) on Facebook and Instagram, supported by additional observations on YouTube, this study identified four dominant scam types circulating in Indonesia and Malaysia. These include: (1) selling products at cheaper prices, (2) impersonation, (3) offering job with high salary, and (4) offering online part-time job. Each of these scam types is discussed in detail in the following sections, with consistent reference to the platforms observed in the data collection stage.

Selling Products at Cheaper Prices

One of the most frequently observed scam techniques on social media involves the sale of products at unusually low prices. Scammers exploit users' desire for affordability by advertising items that appear legitimate but are priced far below market value. This tactic creates a false sense of urgency and triggers impulsive purchases, especially among users who may be unfamiliar with standard pricing or who are motivated by financial constraints. Across Facebook, Instagram, and YouTube, such posts typically use persuasive visuals, fabricated testimonials, and limited-time offers to gain credibility (see Figure 1 & 2 below).

Figure 1 & 2. Scamming Through Selling Products at Cheaper Prices.



Scammer Alert!!
Selling Maxtag for RM120.
FB Name: Steve Kok
Account Name: Kok Han Keong
Account Number : 080180013032079 Alliance Bank

Rm120 termasuk postage, 1 tahun warranty, free tng card, car holder dashboard and battery aeon kinta

OK boss, Friday I will postage 1 unit maxtag yellow color and gave u tracking number

Monday or Tuesdays

After transfer send me your name, address and contact number

transfer done

Assalammualaikum semua , saya telah di scam sebanyak 1.1k dengan hamba Allah yang bernama Amzar Yusman sesiap yang mengenali boleh tolong saya , saya tak minta banyak saya nak duit saya je dah cukup kalau rasa taknak jual barang sayang barang jangan pos seakan2 nak jual tp hujung2 scam orang malu awak dah kawin ada anak bini bagi makan duit haram saya tak halalkan ye , sampai mati saya haramkan ! cari lah saya di padang masyar kelak 🥰—😔 feeling sad.

Source: Facebook, 14 November 2024.

Scammers frequently use deceptive pricing tactics to lure victims into fraudulent transactions. By offering goods at unrealistically low prices, they exploit consumer psychology, triggering impulsive purchases driven by the fear of missing out (Tambe et al., 2024). Victims often receive counterfeit products or nothing at all. Similar fraudulent schemes have been documented in e-commerce research, where scammers manipulate digital storefronts to deceive buyers (Beg et al., 2024).

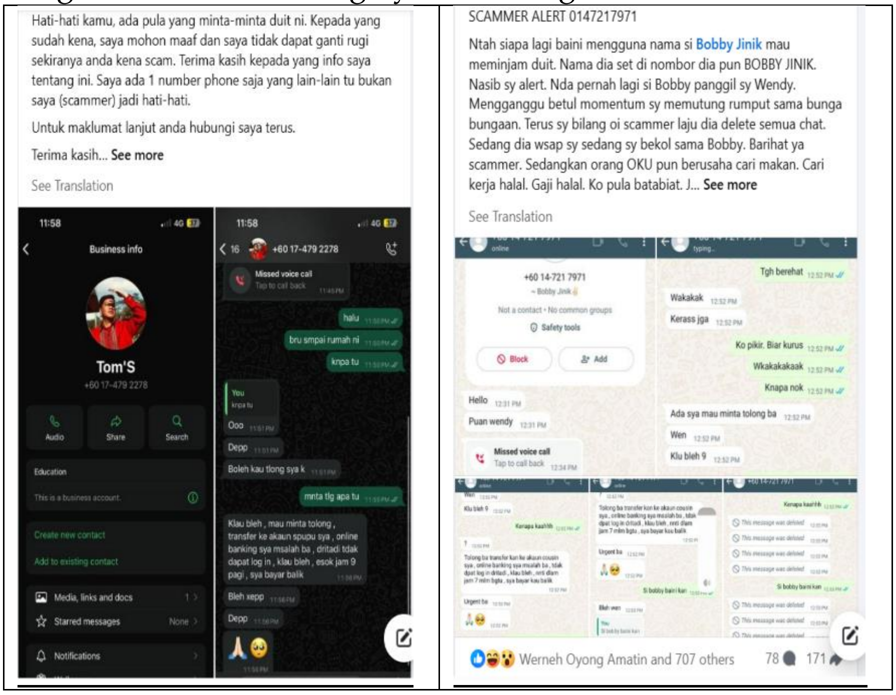
All the posts indicate that one of the most commonly used techniques by scammers is selling products or services at a lower price compared to other companies or businesses. This tactic is highly effective in attracting victims, as it plays on the universal desire to secure a good deal or save money. Scammers often advertise products that appear to be high-quality or in high demand, offering them at prices far below what would normally be expected in legitimate markets. This creates an illusion of a rare opportunity, enticing individuals who are looking for a bargain. These fraudulent posts often include convincing descriptions, fake testimonials, or images of the products that make them seem legitimate and trustworthy.

However, once the victim proceeds with the transaction, the scammer's true intent becomes apparent. In many cases, the individual either receives a product that is substandard, counterfeit, or of significantly lower quality than what was promised, or no product is delivered at all. In some instances, the scammer may continue to manipulate the victim by requesting additional payments for 'shipping fees' or 'processing costs,' further exploiting the individual's trust. This deceptive practice leads to financial losses. The effectiveness of this scam lies in its ability to exploit human psychology—specifically, the desire for instant gratification and the allure of deals that seem too good to miss. It often targets those who may not be familiar with the typical pricing of certain products or services, or those who are desperate for a particular item. Additionally, the anonymity provided by online platforms and the ease of creating fake listings make it increasingly difficult to detect such scams before it's too late.

Impersonation

Impersonation scams constitute another major technique used by fraudsters, where scammers deliberately disguise themselves as trusted individuals or reputable entities to deceive victims. On platforms such as Facebook, Instagram, and YouTube, these impersonations often appear in the form of hacked accounts, cloned profiles, or fraudulent messages that rely on pre-existing trust between the victim and the supposed sender. By exploiting social relationships and familiarity, scammers manipulate victims into transferring money, sharing personal information, or engaging in actions that expose them to financial or emotional harm (see Figure 3 & 4 below).

Figure 3 & 4. Scamming by Pretending to Be Someone Else.



Hati-hati kamu, ada pula yang minta-minta duit ni. Kepada yang sudah kena, saya mohon maaf dan saya tidak dapat ganti rugi sekiranya anda kena scam. Terima kasih kepada yang info saya tentang ini. Saya ada 1 number phone saja yang lain-lain tu bukan saya (scammer) jadi hati-hati.

Untuk maklumat lanjut anda hubungi saya terus.

Terima kasih... **See more**

See Translation

11:58

Business info

Tom'S

+60 17-479 2278

Education

This is a business account.

Create new contact

Add to existing contact

Media, links and docs 1

Starred messages None

Notifications

11:58

+60 17-479 2278

Missed voice call
Tap to call back 11:46 PM

halu

bru smpai rumah ni

knpa tu

You
knpa tu

Ooo 11:51 PM

Depp 11:51 PM

Boleh kau tlong sya k 11:51 PM

mnta tlg apa tu

Klau bleh , mau minta tolong , transfer ke akaun spupu sya , online banking sya msalah ba , dritadi tdak dapat log in , klau bleh , esok jam 9 pagi , sya bayar balik

Bleh xepp

Depp

🙏🥺

SCAMMER ALERT 0147217971

Ntah siapa lagi baini mengguna nama si Bobby Jinik mau meminjam duit. Nama dia set di nombor dia pun BOBBY JINIK. Nasib sy alert. Nda pernah lagi si Bobby panggil sy Wendy. Mengganggu betul momentum sy memutung rumput sama bunga bungaan. Terus sy bilang oi scammer laju dia delete semua chat. Sedang dia wsap sy sedang sy bekol sama Bobby. Barihat ya scammer. Sedangkan orang OKU pun berusaha cari makan. Cari kerja halal. Gaji halal. Ko pula batabiat. J... **See more**

See Translation

online

+60 14-721 7971
~ Bobby Jinik

Not a contact • No common groups

Safety tools

Block

Add

Hello 12:31 PM

Puan wendy 12:31 PM

Missed voice call
Tap to call back 12:34 PM

typing...

Tgh berehat 12:52 PM

Wakakak 12:52 PM

Kerass jga 12:52 PM

Ko pikir. Biar kurus 12:52 PM

Wkakakakaak 12:52 PM

Knapa nok 12:52 PM

Ada sya mau minta tolong ba 12:52 PM

Wen 12:52 PM

Klu bleh 9 12:52 PM

Kenapa kaahhh

Tolong ba transfer kan ke akaun cousin sya , online banking sya msalah ba , tdak dpat log in dritadi , klau bleh , nnti diam jam 7 mlm bgtu , sya bayar kau balik

Urgent ba

🙏🥺

Si bobby bairi kan

Bleh wen

This message was deleted

This message was deleted

This message was deleted

This message was deleted

Si bobby bairi kan

This message was deleted

This message was deleted

Werneh Oyong Amatin and 707 others 78 171

Source: Facebook, 14 November 2024.

Some scammers also resort to pretending to be someone else, often using fake identities to gain the trust of their victims. This tactic is particularly insidious because it exploits the victim's trust in people they believe they know or can rely on. Scammers might impersonate a friend, family member, or even a well-known figure, such as a celebrity or a business professional, in order to manipulate individuals into sharing sensitive information, sending money, or engaging in other fraudulent activities. In some cases, scammers will hijack social media accounts, using the victim's friend list to reach out to their contacts and convince them that the message is genuine. These impersonators often create highly convincing narratives, such as claiming that a family member is in urgent need of financial help or that a long-lost friend is offering a business opportunity or investment that promises high returns.

Scammers usually pretend to be a famous face from the business or industrial world, celebrities or someone who might be very close to the potential victim. The scammer tries to win the trust of the victim and then they begin to extort money. This form of scamming is not only dangerous in terms of financial loss, but also loss of mental state, human trafficking, and murder involvement. This tactic is particularly effective due to the psychological principle of authority and trust (Norris et al., 2019). Research on online deception confirms that impersonation scams are among the most challenging fraud types to detect, as they exploit pre-existing relationships and social trust dynamics (Whitty, 2013).

The psychological manipulation involved in these scams is particularly effective, as the victim is more likely to trust someone they think they know, or someone they respect, such as a perceived professional or authority figure. The emotional connection established through these impersonations makes it more difficult for victims to recognize that they are being deceived. In some cases, victims may only realise they have been scammed once it is too late, having already sent money or shared personal details that lead to further exploitation.

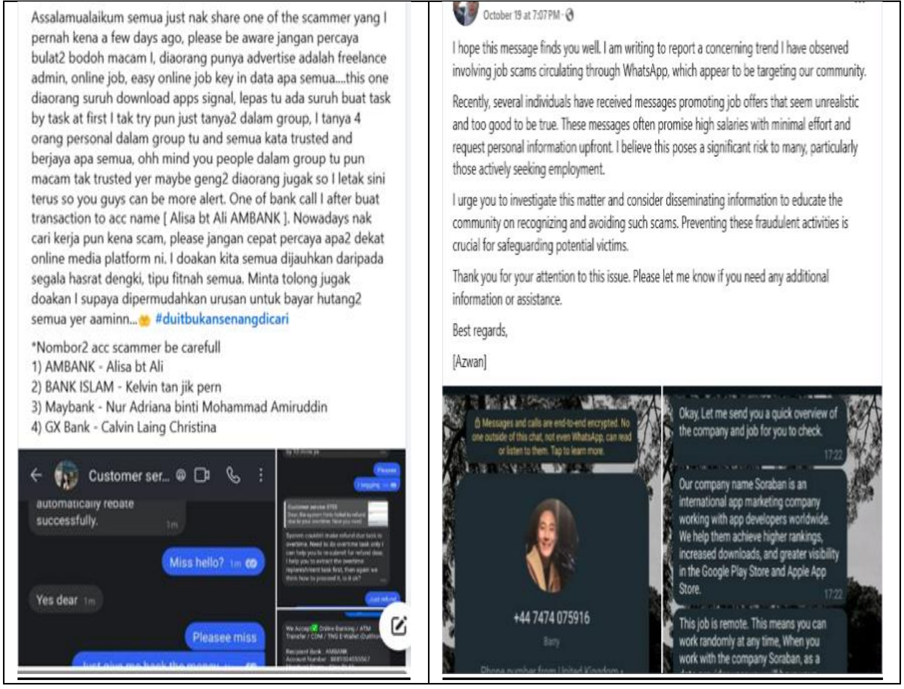
This form of scamming is dangerous not only because of its emotional manipulation but also due to the broader implications it has on online security and personal privacy. It highlights the ease with which scammers can fabricate identities and exploit social connections for financial or personal gain. As social media and digital platforms continue to grow, this type of scam is becoming increasingly common and harder to detect.

Offering Job with High Salary

As a part of deceptive tactics, scammers also use tools of offering jobs with less or no work accompanied with high salary. The scammers often make fake notes of job opportunities. They especially target people with less or no working opportunities. The study found that scammers often promise high-paying, low-effort job opportunities to lure victims, particularly individuals facing financial hardship. These fraudulent job offers sometimes lead to more severe consequences, including human trafficking (Sarkar & Shukla, 2024). Victims are deceived into traveling abroad, only to have their passports confiscated and forced into exploitative labor conditions. Prior research highlights how online job scams disproportionately target vulnerable populations, exploiting their economic insecurities and trust in digital recruitment platforms (Antonopoulos et al., 2020). They circulate such advertised posts widely on Facebook, Instagram, and YouTube, taking the form of recruitment ads that appear credible at first glance.

Scammers typically promise high-paying roles in various industries, such as hospitality, sales, or customer service, with the allure of better life opportunities abroad. Victims, often seeking financial relief or a career upgrade, are enticed by the exaggerated salary packages and the prospect of a brighter future (see Figure 5 & 6 below). For many people struggling economically, these offers promise a "quick escape" or a chance at a better life, making them especially persuasive. However, behind these attractive offers lie deceptive schemes that may involve upfront payments, identity theft, or even human trafficking.

Figure 5 & 6. Scamming Through High-Salary Job Offers.



Assalamualaikum semua just nak share one of the scammer yang I pernah kena a few days ago, please be aware jangan percaya bulat2 bodoh macam I, diaorang punya advertise adalah freelance admin, online job, easy online job key in data apa semua....this one diaorang suruh download apps signal, lepas tu ada suruh buat task by task at first I tak try pun just tanya2 dalam group, I tanya 4 orang personal dalam group tu and semua kata trusted and berjaya apa semua, ohh mind you people dalam group tu pun macam tak trusted yer maybe geng2 diaorang jugak so I letak sini terus so you guys can be more alert. One of bank call I after buat transaction to acc name [Alisa bt Ali AMBANK]. Nowadays nak cari kerja pun kena scam, please jangan cepat percaya apa2 dekat online media platform ni. I doakan kita semua dijauhkan daripada segala hasrat dengki, tipu fitnah semua. Minta tolong jugak doakan I supaya dipermudahkan urusan untuk bayar hutang2 semua yer aaminn... #duitbukansenangdicari

*Nombor2 acc scammer be carefull
1) AMBANK - Alisa bt Ali
2) BANK ISLAM - Kelvin tan jik pern
3) Maybank - Nur Adriana binti Mohammad Amiruddin
4) GX Bank - Calvin Laing Christina

automatically rebate successfully. 1m

Miss hello? 1m

Yes dear 1m

Pleasee miss

October 19 at 7:07 PM

I hope this message finds you well. I am writing to report a concerning trend I have observed involving job scams circulating through WhatsApp, which appear to be targeting our community.

Recently, several individuals have received messages promoting job offers that seem unrealistic and too good to be true. These messages often promise high salaries with minimal effort and request personal information upfront. I believe this poses a significant risk to many, particularly those actively seeking employment.

I urge you to investigate this matter and consider disseminating information to educate the community on recognizing and avoiding such scams. Preventing these fraudulent activities is crucial for safeguarding potential victims.

Thank you for your attention to this issue. Please let me know if you need any additional information or assistance.

Best regards,

[Azwan]

Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

+44 7474 075916

Barry

Okay, Let me send you a quick overview of the company and job for you to check. 17:22

Our company name Soraban is an international app marketing company working with app developers worldwide. We help them achieve higher rankings, increased downloads, and greater visibility in the Google Play Store and Apple App Store. 17:22

This job is remote. This means you can work randomly at any time, When you work with the company Soraban, as a

Source: Facebook, 19 October 2024.

However, upon accepting the offer, victims are sometimes transported to other countries, where they are forced into labor under harsh conditions, or are sold to trafficking rings. The scammers often go to great lengths to create a sense of legitimacy, providing fake documentation, conducting fake interviews, and even offering fake visas to convince their targets that the job offer is genuine. In some cases, victims may not realise they are being scammed until it is too late, when they are already in a foreign country with little means of escape or support.

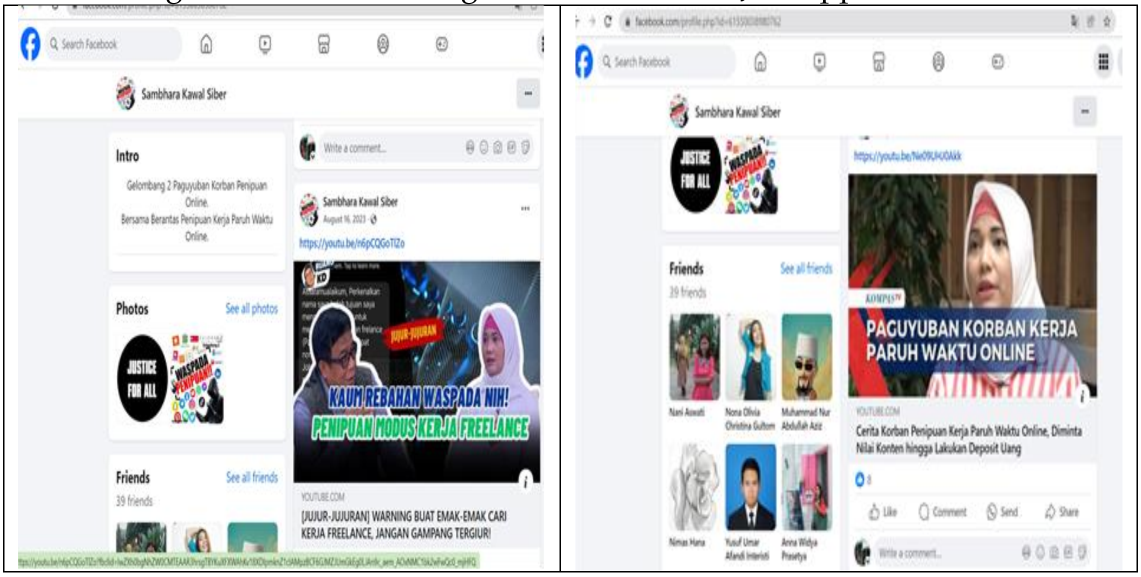
This scam is especially dangerous because it preys on vulnerable individuals, such as those in financial distress or those seeking better employment opportunities often using promises of a better life to mask their true intentions. This form of scam is highly concerning as it involves not only financial exploitation, but also severe human rights violations. It is a stark reminder of the dangers of blindly trusting online job offers and the importance of verifying the legitimacy of employment opportunities, especially those that involve moving to a foreign country.

Offering Online Part-time Job

Another prevalent scam involved fraudulent part-time job offers, where victims were initially paid small sums for simple tasks but later pressured into making financial deposits under false pretenses. This scheme aligns with pyramid fraud models observed in digital labor scams, where scammers use small initial payouts to establish credibility before escalating financial demands (Ridho, 2024). Previous studies indicate that individuals seeking flexible online income opportunities, such as students and stay-at-home parents, are particularly vulnerable to these deceptive practices (Wilson et al., 2024).

Scammers also entice victims through online part-time job offers that appear attractive and effortless (see Figure 7 & 8 below). These posts, commonly found on Facebook, Instagram, and YouTube, advertise simple tasks such as liking posts or following accounts, often accompanied by testimonials to appear genuine. Victims usually receive small early payments, giving the impression of legitimacy, before being pressured to make repeated deposits to "unlock" higher-level tasks or withdraw commissions. Over time, these demands escalate, leading victims to substantial financial losses.

Figure 7 & 8. Promoting Online Part-Time Job Opportunities.



Gelombang 2 Paguyuban Korban Penipuan Online.
Bersama Berantas Penipuan Kerja Paruh Waktu Online.

Sambhara Kawal Siber
August 16, 2023

https://youtu.be/n6pCQGoTIZo

YOUTUBE.COM
[JUJUR-JUJURAN] WARNING BUAT EMAK-EMAK CARI KERJA FREELANCE, JANGAN GAMPANG TERGIUR!

https://youtu.be/Nw09UHJOAkk

YOUTUBE.COM
Cerita Korban Penipuan Kerja Paruh Waktu Online, Diminta Nilai Konten hingga Lakukan Deposit Uang

Source: Facebook, 16 August 2023.

Part-time jobs are highly sought after by the public, including housewives, students, and freelancers, who are eager to earn extra income. This demand has created opportunities for fraudulent parties to exploit individuals, a situation that is currently widespread in Indonesia. According to several comments on the Sambhara Kawal Siber Facebook page, the victims are not only from Indonesia but also from abroad. The losses suffered by these victims vary widely, ranging from thousands to millions, tens of millions, and even hundreds of millions of local currency. One of the victims shared their experience, explaining that they initially received an invitation via WhatsApp offering a part-time job. The tasks involved simple actions such as liking, sharing, and following social media accounts, with the requirement to send a screenshot as proof of completion. After completing these tasks and submitting several links, the victim received payment, which was part of the scammer's strategy to gain their trust.

Once the victim was convinced of the legitimacy of the offer, they were assigned a series of increasingly difficult tasks that required them to make deposits of escalating amounts. The scammer set the condition that these deposits could not be withdrawn until all tasks were completed, which created a false sense of urgency and fear of losing out. If the victim hesitated or refused to make further deposits, the scammer threatened that all previous payments would be forfeited. Over time, as the victim continued to comply, the deposits grew larger, and the victim eventually realized they had fallen prey to the scam. By the time the scam was uncovered, significant financial losses had already been incurred, leaving the victim unable to recover the money sent to the scammer. This type of scam highlights the vulnerabilities of individuals who are desperate for extra income and the deceptive tactics employed by fraudsters to exploit their trust.

- **The Circle of Ethical Cosmopolitanism and *Tongkonan* Symbolism Victim Responses to Online Scams**

The second objective of this research examines the actions individuals take upon discovering they have been scammed. The findings indicate that victims often respond with a mix of traditional and modern approaches to address the situation, seek justice, and prevent further harm. These actions not only reflect their immediate efforts to mitigate the impact but also highlight the growing role of collective action and technology in combating scams. The following discussions outline four key responses commonly happen among scam victims, namely: shooting and uploading the fraud on social media, creating fraud's victim association, and freezing of their bank account on priority basis.

Shooting and Uploading the Faud on Social Media

One common response identified among scam victims is the practice of recording their experiences and uploading the content to social media platforms. Victims often use Facebook, Instagram, and YouTube to document fraudulent activities, expose scammers, and warn other users. This approach reflects a growing reliance on digital platforms not only for communication but also for community-driven fraud awareness. By publicly sharing their stories, victims contribute to collective knowledge and create digital evidence that may assist others in avoiding similar scams.

This action reflects how victims are leveraging digital platforms to raise awareness and warn others about fraudulent activities. Social media (YouTube, Instagram, and Facebook) and video-sharing platforms like YouTube allow victims to share their experiences widely, providing potential targets with firsthand accounts of scams. While this method can be effective in spreading awareness, it may raise privacy and legal concerns, particularly if the videos identify individuals or include sensitive information. The growing reliance on digital media as a tool for advocacy highlights the increasing role of technology in combating scams.

Lodge a police report: Filing a police report is a traditional and formal response to scams, signifying an individual's pursuit of justice and accountability. This approach underscores the importance of involving law enforcement in tracking and addressing fraudulent activities. However, challenges such as underreporting, delayed investigations, or a lack of evidence may hinder the effectiveness of this measure. It is crucial to enhance collaboration between the public and law enforcement agencies to improve the efficacy of reporting systems.

Creating Fraud's Victim Association

In the face of widespread online scams, many victims turn to one another by creating or joining fraud-victim associations. These groups—often visible on Facebook and Instagram—become safe spaces where victims share their stories, express frustration, and seek guidance from others who faced similar losses. Beyond emotional support, these associations play an important role in raising awareness, documenting scam patterns, and demanding stronger enforcement from authorities.

The formation of fraud victims' associations demonstrates the power of collective action in addressing the aftermath of scams. Such associations provide victims with emotional support, resources, and a platform to advocate for stronger anti-fraud measures. These groups can also engage in awareness campaigns and lobby for policy changes to protect individuals from scams. However, sustaining such associations may require dedicated resources and leadership, as well as efforts to reach a broader audience.

Freezing of Their Bank Account on Priority Basis

A further response identified among scam victims is the immediate attempt to freeze or block scam-related bank accounts. Victims often contact their financial institutions as soon as they realize they have been deceived, hoping to prevent further unauthorized transactions and limit financial losses. This action reflects a growing public awareness of the role banks play in fraud prevention and the need for rapid intervention. By reporting suspicious accounts and requesting account freezes, victims contribute to the broader effort to disrupt scam networks and strengthen financial security measures.

Promptly freezing a scammer's bank account is a critical action to prevent further financial losses and disrupt fraudulent operations. This response highlights the importance of swift action by financial institutions in collaboration with victims and law enforcement. It underscores the need for advanced fraud detection systems and streamlined reporting mechanisms to enable timely intervention. However, procedural delays or lack of awareness about this option may limit its effectiveness, emphasizing the importance of public education on financial fraud prevention.

The findings indicate that victims of online scams in Indonesia and Malaysia commonly respond by reporting incidents to the police, freezing scammer bank accounts, and raising public awareness through social media. While these actions demonstrate a proactive approach to combating fraud, prior research suggests that underreporting remains a major issue due to perceived inefficacy of law enforcement and lack of immediate legal recourse (Button et al., 2009). Additionally, the study confirms previous findings that financial institutions play a critical role in scam prevention, yet delays in blocking fraudulent transactions often limit the effectiveness of this measure (Iqbal et al., 2018). Public awareness campaigns were found to be highly effective in educating potential victims and deterring scams, aligning with Wilson et al. (2024), who emphasize the role of community-driven efforts in digital fraud prevention. Overall, the results reinforce existing literature on victim responses while highlighting the need for stronger collaboration between authorities, financial institutions, and social media platforms to enhance scam prevention strategies.

In Indonesia, victims tend to be more active in disclosing fraud cases through social media and forming communities or victim groups on platforms like Facebook and Instagram. Publicity efforts and community support are used as a means of sharing experiences, seeking emotional support, and warning the wider public. Fraud victims in Malaysia prefer to take formal channels by reporting cases to the police and immediately contacting their banks to freeze their accounts. This response reflects a level of trust in formal institutions and financial mechanisms for handling fraud. Malaysians also utilize social media for public education.

4. Conclusion

The study identified four prominent scam types, namely: selling products at cheaper prices, impersonation, offering job with high salary, and offering online part-time job. These findings provide a clearer understanding of how different scam models operate across digital platforms in Indonesia and Malaysia.

In addition to classifying scam types, the study also highlights how victims respond to these fraudulent activities. Victims commonly adopt several strategies, which include: shooting and uploading the fraud on social media, creating fraud's victim association, and freezing of their bank account on priority basis. These responses indicate a combination of individual, community-driven, and institutional actions aimed at limiting financial losses and preventing further victimization. However, some online discussions reveal the sharing of sensitive information, raising concerns about the need for clearer enforcement of social media guidelines and more consistent law-enforcement protocols.

In Indonesia, the most common types of scams are online transaction scams involving very low prices and part-time jobs. Victims tend to respond by reporting cases on social media and forming communities to share experiences, gain support, and warn the public. Scams in Malaysia are dominated by high-paying job scams and impersonation scams impersonating authorities. These scams are more organized and exert intense psychological pressure. Victims in Malaysia prefer formal channels to resolve their cases.

Overall, the findings underscore the increasing sophistication and diversity of online scams in Indonesia and Malaysia. This situation reinforces the urgent need for stronger digital literacy programs, more responsive regulatory frameworks, and enhanced cross-platform fraud-prevention strategies. Strengthening cooperation between the public, financial institutions, social media platforms, and law-enforcement agencies is essential to reduce vulnerabilities and improve scam-mitigation efforts.

Future research should extend the observation period to capture long-term scam patterns, analyze activities on additional platforms such as WhatsApp, TikTok, and Telegram, and assess the psychological and economic consequences experienced by victims. Addressing these aspects will deepen understanding of scam dynamics and support the development of more effective, evidence-based intervention strategies. By integrating digital forensics, policy intervention, and community education, stakeholders can work collaboratively to build a safer and more resilient online environment.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

We would like to express our sincere gratitude to all individuals and institutions who supported this research. Special thanks to the participants and social media users whose interactions and insights provided valuable data for the Netnography analysis. We also acknowledge the contributions of the academic and cybersecurity communities in Indonesia and Malaysia for their ongoing efforts to combat online scams. Additionally, we extend our gratitude to the institutions and organizations that provided access to relevant literature and data sources, which greatly facilitated the study. Lastly, we appreciate the support from the respective universities and research funding agencies that made this investigation possible.

References

AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. International Journal of Law and Policy, 2(5), 28-36, https://irshadjournals.com/index.php/ijlp/article/view/191, accessed on November 25, 2025.

Anderson, M., March, E., Land, L., & Boshuijzen-van Burken, C. (2024). Exploring the Roles Played by Trust and Technology in the Online Investment Fraud Victimisation Process. Journal of Criminology, 57(1), 1–15. https://doi.org/10.1177/26338076241248176, accessed on November 25, 2025.

Antonopoulos, G. A., Baratto, G., Di Nicola, A., Diba, P., Martini, E., Papanicolaou, G., ... & Terenghi, F. (2020). The Role of the Internet and Digital Technologies in Human Smuggling and Trafficking in the UK. Technology, Human Smuggling and Trafficking: Case Studies from Italy and the United Kingdom, 37-68, https://link.springer.com/book/10.1007/978-3-030-42768-9, accessed on November 25, 2025.

Bartl, M., Kannan, V. R., & Stockinger, H. (2016). A Review and Analysis of Literature on Netnography Research. International Journal of Market Research, 58(4), 537-561, https://www.inderscience.com/info/inarticle.php?artid=75687, accessed on November 25, 2025.

Beg, R., Bhardwaj, V., Kumar, M., Muzumdar, P., Rajput, A., & Borana, K. (2024). Unmasking Social Media Crimes: Types, Trends, and Impact. Social Networks in Business Frameworks, 1-26, https://doi.org/10.1002/9781394231126.ch1, accessed on November 25, 2025.

Braun, V. & Clarke, V. (2006). Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3(2), 77-101, https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa, accessed on November 25, 2025.

Button, M., Johnston, L., & Frimpong, K. (2009) New Directions in Policing Fraud: the Emergence of the Counter Fraud Specialist in the United Kingdom. International Journal of the Sociology of Law. 35(4),192-208 https://www.sciencedirect.com/science/article/abs/pii/S0194659507000445?via%3Dihub, accessed on November 25, 2025.

Costello, L., McDermott, M. L., & Wallace, R. (2017). Netnography: Range of Practices, Misperceptions, and Missed Opportunities. International Journal of Qualitative Methods, 16(1),1-12, https://journals.sagepub.com/doi/10.1177/1609406917700647, accessed on November 25, 2025.

Dupuis, D., Smith, D. & Gleason, K. (2023). Old frauds with a new sauce: digital assets and space transition, Journal of Financial Crime, 30(1), 205-220, https://www.sciencedirect.com/org/science/article/abs/pii/S1359079022000616, accessed on November 25, 2025.

High Cases of Scam Victims, Low Resilience in Malaysia - National Scam Awareness Survey (2024). https://www.bernama.com/en/news.php?id=2318397, accessed on November 25, 2025.

Information On Forced Labor and Trafficking in Persons (Tip)-Indicated Cases (2023), Online Scamming Industry Overseas. Kementrian Luar Negeri, Republik Indones: IOM UN Migration, https://indonesia.iom.int/sites/g/files/tmzbdl1491/files/documents/2023-08/infosheet-online-scams-english.pdf, accessed on November 25, 2025

Iqbal, M. S., Zulkernine, M., Jaafar, F., & Gu, Y. (2018). Protecting Internet Users from Becoming Victimized Attackers of Click-fraud. Journal of Software: Evolution and Process, 30(3), https://onlinelibrary.wiley.com/doi/abs/10.1002/smr.1871, accessed on November 25, 2025.

Kozinets, R. V. (2015). Netnography: Redefined. California. Sage Publications.

Mkono, M. (2016). The Application of Netnography in Tourism Studies. Annals of Tourism Research, 59, 186-190, https://www.sciencedirect.com/science/article/pii/S0160738314000930?via%3Dihub , accessed on November 25, 2025.

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. Journal of Police and Criminal Psychology, 34, 231-245, https://link.springer.com/article/10.1007/s11896-019-09334-5, accessed on November 25, 2025.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. International Journal of Qualitative Methods, 16(1), 1-13, https://journals.sagepub.com/doi/full/10.1177/1609406917733847, accessed on November 25, 2025.

Owen, T., Noble, W., Speed, F. C., Owen, T., Noble, W., & Speed, F. C. (2017). The Challenges Posed by Scammers to Online Support Groups: the "Deserving" and the "Undeserving" Victims of Scams: New Perspectives on Cybercrime, https://link.springer.com/book/10.1007/978-3-319-53856-3, accessed on November 25, 2025.

Ridho, W.F. (2024), "Unmasking Online Fake Job Group Financial Scams: a Thematic Examination of Victim Exploitation from Perspective of Financial Behavior," Journal of Financial Crime, 31(3), 748-758. https://doi.org/10.1108/JFC-05-2023-0124, accessed on November 25, 2025.

Sarkar, G., & Shukla, S. K. (2024). Bi-Directional Exploitation of Human Trafficking Victims: Both Targets and Perpetrators in Cybercrime. Journal of Human Trafficking, 1–22. https://doi.org/10.1080/23322705.2024.2353015, accessed on November 25, 2025

Tambe Ebot, A. C., Siponen, M., & Topalli, V. (2024). Towards a Cybercontextual Transmission Model for Online Scamming. European Journal of Information Systems, 33(4), 571-596, https://doi.org/10.1080/0960085X.2023.2210772, accessed on November 25, 2025.

Taodang, D., & Gundur, R. V. (2023). How Frauds in Times of Crisis Target People. Victims & Offenders, 18(5), 889-914, https://www.tandfonline.com/doi/full/10.1080/15564886.2022.2043968, accessed on November 25, 2025.

Whitty, M. T. (2013). The Scammers Persuasive Techniques Model: Development of a Model for Romance Scams. British Journal of Criminology, 53(4), 665-684, https://www.jstor.org/stable/23640056, accessed on November 25, 2025.

Whitty, M., & Buchanan, T. (2016). The Online Dating Romance Scam: The Psychological Impact on Victims–Both Financial and Emotional. Journal of Cybercrime Studies, 2(1), 1-15, https://doi.org/10.1177/1748895815603773, accessed on November 25, 2025.

Wilson, S., Hassan, N.A., Khor, K.K., Sinnappan, S., Abu Bakar, A.R. and Tan, S.A. (2024). A Holistic Qualitative Exploration on the Perception of Scams, Scam Techniques and Effectiveness of Anti-Scam Campaigns in Malaysia.

Journal of Financial Crime, 31(5), 1140-1155, https://doi.org/10.1108/JFC-06-2023-0151, accessed on November 25, 2025.

Yu, S. (2015). Human Trafficking and the Internet, in Palmiotto, M.J., Combating Human Trafficking: A Multidisciplinary Approach, in Combating Human Trafficking (1st Edition). London: Routledge, 61-74, https://doi.org/10.1201/b17709, accessed on November 25, 2025.