Proceedings of The International Conference on Natural Sciences, Mathematics, Applications, Research, and Technology (ICON-SMART)
e-ISSN: 2963-3915

Vol. 3, December 2023,
pp. 9-13

Prevention and Strategies for Avoiding Social Media Fraud: A Case of Fraud Prevention in Indonesia

Kenedi Binowo[1,a)] and Rondo V. S. A. Morihito[2,b)]

[1]*University of Indonesia, Faculty of Computer Science, Depok, Indonesia.*
[2] *Indonesian Christian University, Jakarta, Indonesia*

[a)] *Corresponding author: kenedi.binowo@ui.ac.id*
[b)]*2003190081@ms.uki.ac.id*

Abstract. Overcoming fraud is not solely reliant on technological tools and security measures, but it is necessary to share insights and deeper understanding from experts and experienced people for effective fraud prevention mechanisms. Until now, fraud attacks through social engineering targeting certain people have not been overcome and are still rampant. Therefore, this study aims to identify crucial factors that support online fraud prevention. This study used a qualitative approach with thematic analysis as a data analysis tool. Research data were collected from video transcripts of 14 speakers from YouTube channels in Indonesia. Findings revealed 145 codes as keywords for fraud prevention. From these codes, 7 themes (important factors) effective for use as prevention strategies against fraud were selected. These 7 factors include: Turning off the Internet Connection; uninstalling apps Outside the Apple Store and Play Store; Beware of Unknown Numbers; not Click on APK files and Suspicious Links; Backup and resetting the Smartphone Immediately; Ensure Application Permissions Only When Used; Ensure the Smartphone is Installed Antivirus and the Operating System is Updated. In conclusion, to avoid falling victim to social media-based scams, one must prevent fraud by employing wisdom and understanding. Therefore, do not easily succumb to links or ads promising substantial returns with minimal risk. With vigilance, a good understanding of social media, and the use of prudent privacy strategies, we can contribute to preventing scams that harm many people.

Keyword*s:* social-media; fraud; YouTube channel

INTRODUCTION

Online fraud has become a serious threat in today's digital-based ecosystem. Various efforts have been made to address this issue, especially in terms of fraud prevention and detection. However, it should be noted that most of the research that has been conducted tends to be quantitative in nature, focusing on statistical analyses and numerical patterns. Qualitative research, which has great potential in uncovering the nuances and deeper context of fraud modes, has yet to be applied in previous research in the context of identifying aspects of online fraud prevention.

While quantitative research has provided valuable insights into the general trends of online fraud and detection methods, it tends to lack the ability to explore the motivational factors, psychological factors, and social dynamics behind fraudulent behaviour. The inability to explore these factors, we can use qualitative approaches, where qualitative approaches are the ones that can fill this gap with a more in-depth and contextualised approach. However, there are still limitations in using quantitative approaches to identify issues related to online fraud prevention. Qualitative research often requires greater time and resources for data collection and analysis, as well as strong interpretative skills to parse complex and diverse data. Qualitative methods in this case emphasize interpretation and analysis of the data rather than numbers or statistics. With a qualitative approach, this research can explore deeper information in a contextualized manner and understand emotional and social aspects that may not be captured through quantitative methods.

One important aspect of tackling fraud from social media is prevention. Fraud prevention refers to tasks or barriers designed to prevent individuals from committing fraud. This is done to create societal habits to prevent people from engaging in fraudulent activities. For example, throwing messages that threaten imprisonment to fraudsters, or creating messages that can influence their psychology into fear [1]. But tackling fraud is not enough to rely on technology alone, according to research from [2] that common technical scams can be thwarted by technological tools and security software, but social engineering attacks that target specific people have yet to be overcome.

Therefore, qualitative research that focuses on identifying factors that support online fraud prevention is still relatively rare. However, it is important to recognize that this approach can provide valuable insights and a deeper understanding of effective prevention mechanisms. Therefore, by analyzing the experiences of individuals who have been victims of fraud as well as those who have successfully avoided it, and leveraging the expertise of cybersecurity professionals, research of this nature holds the potential to identify practical strategies, challenges, and solutions that can be applied to reduce incidences of online fraud.

RELATED WORK

In research conducted by [1] the fraud prevention strategy they describe is using Social Network Analysis. This strategy can be divided into two categories, namely relationship-based approaches that use density criteria and the strength of the relationship between actors to detect fraud, and graph-based approaches that use methods such as degree centrality, closeness centrality, and betweenness centrality to identify fraudsters. Whereas by Singh and Jain [3] which uses communal detection strategies, spike detection, genetic algorithms, and threshold values.

The strategy described by [4] for fraud prevention is to coordinate high-level training, techniques, cycles, and preparation into security exercises in order to involve the application of security policies, procedures, and techniques with the aim of reducing the risk of fraud and protecting both individuals and organizations from potential financial losses and other negative impacts that can result from fraudulent practices.

There are several strategies, namely Situational strategies, which involve the use of surveillance techniques, alarms, and video surveillance to identify and prevent suspicious activity before a crime occurs, and also Community strategies, which involve community experience and monitoring the activities of strangers to prevent fraud and other crimes [2]. Likewise, as described by [5] and [6] that the strategy is to focus on early fraud detection and prevention before fraud occurs.

The strategies described in the study [7] are: Education and Awareness, increasing public education and awareness about the different types of scams that exist and ways to avoid them. This can be done through public campaigns, seminars, and counselling; Collaboration with Related Parties: Establish co-operation with financial institutions, telecommunication service providers, and authorities to share information about frauds and take effective preventive measures; Employee Training: Conduct employee training on the signs of fraud and how to deal with it. Trained employees will be better able to recognize and avoid fraud.

There are 6 steps of social media fraud prevention strategies of the donation type presented by [8] that are Watch out for Scam Emails that appear; Search for Donation Organizations/Sites/Applications; Also Search for the Name of the Donation Recipient; Research the Donation Destination Account; Make sure the Donation Site is safe; Immediately Report if you find irregularities.

METHODOLOGY

This research uses a qualitative approach. The procedure initially involved collecting data and selecting data from social media channels, in this case YouTube. The use of qualitative methods in capturing data from YouTube through scripts can be done by focusing on a deep understanding of the context and meaning behind the data captured. The data captured certainly uses the approach of Knowledge management where initially filtering raw data from YouTube into information in the form of transcripts and then used as knowledge for this research. Thematic analysis is the approach we used to analyse the collected research data by conducting open coding, axial coding and selective coding.

Data Collection

The research data we use is sourced from social media, in this case video records posted on YouTube channels. We selected videos that discuss how to overcome and prevent fraud that is rampant in online media. The videos we selected, of course, contain discussions sourced from cyber security experts who are competent in discussing fraud prevention using online media, and from people who are almost exposed to fraud. Through the selection results, there are 14 YouTube video sources that we selected as data for this research. The 14 videos are transcribed in Indonesian.

Data Analysis

Once the video data was obtained from YouTube, the next step was to transcribe all the discussion from the video into transcripts. In the transcripts, we applied thematic analysis procedures by identifying patterns of keyword usage that discussed fraud prevention strategies from social media. In this study, the thematic analysis procedure was conducted by adopting the process framework from the research conducted by [9], and by [10]which is shown as in Figure 1.

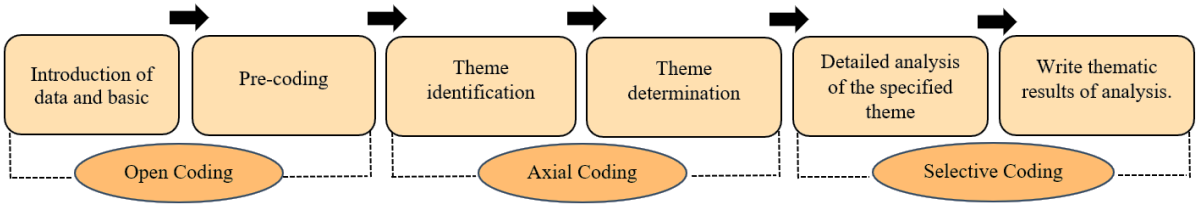

FIGURE 1. Procedure Thematic Analysis [9], [10]

In Figure 1, in open coding, the author conducted preliminary identification of keywords regarding preventive factors to overcome fraud from video transcript data, the keywords were labeled bold as pre-coding. In axial coding, determining topics or identifying initial themes is done, initial themes that have the same meaning are connected and grouped in 1 category. In selective coding, a more abstract statement that best represents the keywords in open coding and axial coding is formulated. The formulations that have been formed are explained one by one as selected themes.

RESULTS AND DISCUSSIONS

There are 14 YouTube accounts that are used as data sources for this research, these accounts contain exposure from experts and people who are almost exposed to fraud. The 14 channel accounts can be described as in Table 1. Based on the findings of this study, there are important factors that can be used as best practices and lesson learnt to prevent and overcome fraud that is rampant using social media. The results of thematic analysis obtained a total of 145 codes as keywords, and the total themes found were 7 themes. Each theme can be shown as follows and explained after Table 1.

1. Turn off the Internet Connection
2. Uninstall Apps Outside the Apple Store and Play Store
3. Beware of Unknown Numbers
4. Don't Click on APK files and Suspicious Links
5. Backup and Reset Smartphone Immediately
6. Ensure Application Permissions Only When Used.
7. Ensure the Smartphone is Installed Antivirus, and the Operating System is Updated.

TABLE 1. Profile of YouTube Channel Accounts that Discuss Fraud Prevention

No	Channel Name	Number of Views	Title
1	Ngomongin Uang	62,789	Dissecting Online Fraud Modes
2	Pace Komputer	109,922	ACCOUNT BALANCE DRAIN INVITATION APK
3	CNN Indonesia	19,359	Beware, Hacker Apps in the Guise of Wedding Invitations are Circulating
4	Uya Kuya TV	427,369	Latest Scam 2023 Cuma Like, Share, Subscribe Promised Big Profits
5	Pengeran Napitupulu	6,249	Fraud modus operandi under the guise of a wedding invitation, savings can be lost?
6	Iswa Hoorand	30,755	Love Scam Fraud Modes
7	Badan Siber dan Sandi Negara	31,098	Wedding Invitation Malware.apk
8	Mr Bert	1,072,443	Characteristics of Evil APK or Hack in 2023 Most Complete
9	Mr Bert	149,782	"WhatsApp Wedding Invitation Scams"!!! With The solution.
10	WJS Channel	3,563	Here's How to Avoid Mobile Phone Scams
11	Daftar Populer	143,586	There are many victims already!!! This is the latest online scam mode and how toavoid it
12	KompasTV	6,613,423	Check it out! Cyber Security Expert Explains the Characteristics of HP Affectedby 'Malware' that Records M-Banking PINs
13	tvOneNews	167,350	'Like' and 'Follow' Fraud is Rampant in Cyberspace, Here's the Process
14	Johan Candradinata	63,016	New fashion scam as american soldier - US Army

Theme 1: Turn off Internet Connection

As an initial step to prevent fraud is to switch off the internet connection, this strategy and method is intended when accidentally installing applications that contain malware. Disabling the internet network because it is caused by malware can be an effective action and event in overcoming potential fraudsters who will break into our financial applications. Therefore, immediately switch off the internet connection on the infected mobile device. This will stop the malware from connecting and communicating with its servers. After that, uninstall the malicious application.

"Your first solution is to switch off your mobile data and switch off your wifi." (Mr Bert)

"So I want to give tips at the beginning so that the attack cannot work, immediately turn off your data package or internet or to be safer, immediately activate airplane mode." (Pangeran Napitupulu)

"Okay the first thing is if you accidentally install the APK but you immediately realise this is a fraudulent APK immediately enter flight mode or aircraft mode, meaning turn off the internet connection, then search for the APK and uninstall it, remember this method is effective if you have just installed it." (Mr Bert)

Theme 2: Uninstall Apps Outside the Apple Store and Play Store

The next strategy and way to prevent fraud is to remove malicious apps that you think contain malware (suspicious apps can be uninstalled). Therefore, please make sure and check the list of apps installed on your mobile phone and remove any suspicious apps immediately. Make sure the apps installed on your mobile phone are listed in the app store and play store, do not install apps outside the app & play store.

"To be on the safe side, you can disable the installation of applications from unknown sources." (Pace Komputer)

"Do not install third-party apps other than on the Apple Store or Google Play." (Pratama Persada-Kompas TV)

Theme 3: Beware of Unknown Numbers

An important way to prevent prevalent scams is to always be wary of calls or messages from unknown numbers. Scammers often use unknown numbers to try to scam or collect personal information from potential victims. If you receive a phone call from an unknown number, do not provide any personal information or financial data directly. Be suspicious of any unknown numbers and block them if necessary. Avoid clicking on links or downloading attachments

from messages sourced from unknown numbers, as they can inevitably contain malware or other fraudulent schemes. Therefore, stay alert to unknown numbers, so that we can avoid the risk of fraud.

"Be alert first when a new number comes in and offers something. If a new number suddenly chats with unusual content, beware of being sent by scammers." (Pace Komputer)

"The only way is not to open files sent by unfamiliar numbers." (Pace Komputer)

"Be careful of online part-time work scams from unknown people, this is a scam that is now rampant and very massive." (Uya Kuya TV)

"So be careful if you get a short message on WhatsApp offering part-time work with the mode of like and also follow YouTube accounts because it turns out to be the latest form of fraud that can drain your money." (tvOneNews)

"know that if you win the lottery, you must be conveyed through more than one communication channel. [...] So if you only get an SMS saying you won a lottery, it is almost certain that it is not true. Just ignore the texts that say you won the lottery and don't fall for it." (WSJ Channel)

"Don't transfer outside the app, always transact on the official app and don't just transfer to unknown numbers." (Ngomongin Uang)

"Carefully ask for help to pay with our money first." (Johan Candradinata)

Theme 4: Don't Click on APKs and Suspicious Links

This theme needs to be practised by anyone who has an android mobile phone to overcome fraud. Please note this scam is targeting android users. The application in the form of APK (in this case is a wedding invitation application) if it has been installed on the victim's handphone it will be able to take its own photos and videos, can read SMS and send SMS, can open the camera gallery, and can read fingerprints so this application is really dangerous. Besides, the Popular List source confirmed that "don't rush to click on incoming links from unclear numbers or suspicious links, it could be that your data is all sucked up and sent to their telegram."

In the following, quotes from several sources can be presented that are useful for overcoming and preventing fraud regarding the fourth theme.

"APKs that contain Malware aka viruses if you install them can allow the perpetrators to access your mobile banking and drain the contents of your account." (Pace Komputer)

"[...] receiving unclear chats such as this fake digital invitation, the third characteristic is that it inserts an APK file. [...] you need to pay attention to the format of the file sent, which is APK." (Pace Komputer)

"Then also don't click on random links, it's actually forbidden, if I may say so, don't click on random links if there is a link, just type it in the browser." (Pratama Persada-Kompas TV)

"APK files or any writing with APK writing do not click [...] Android APK where this application will read all your data and the crazy thing is recording your keyboard typing so he can know you type anything." (Mr Bert)

"fraudulent wedding invitations shared on social media such as WhatsApp are an example of cyber crime that often occurs in the digital era [...] scams like this are usually carried out by sending fake wedding invitations through Android application files in the form of dot APK wedding invitations." (Badan Siber dan Sandi Negara)

"Yes, a new mode of digital banking crime was discovered again, this time fraudsters used digital wedding invitations in the form of APKs via WhatsApp to break into mobile banking." (CNN Indonesia)

Theme 5: Backup and Reset Smartphone Immediately

Backing up and resetting your smartphone are preventive measures against scams that can be quickly executed directly. Ensure to consistently backup important data as this is a smart way to mitigate potential fraud risks. In emergency situations, such as suspicious scams, resetting the smartphone to its factory settings can eliminate cybercriminals' access to sensitive personal financial data. By regularly backing up data, we won't lose valuable information when resetting our phones. This approach can reduce the risk of scams and better safeguard personal data security.

Sources confirm the importance of backing up data on our smartphones as a preventive measure against fraud when resetting phones containing financial data or mobile banking applications:

"The best and fastest method is to back up all our data on another device like a computer, then perform a factory reset, and finally restore the data and install antivirus software." (Pratama Persada-Kompas TV)

"My suggestion for added security is to try installing Malwarebytes or Clean Master on your phone to ensure there are no suspicious files, and if you want even more security, you may consider performing a factory reset." (Iswan Hoorand)

Theme 6: Ensuring Application Permissions Only When Used

Another important fraud prevention strategy and method in the research findings is to ensure that app permissions are only granted when the app is actually being used. When updating an app on your smartphone, be sure to review the permissions requested by the app. Don't blindly give permission to apps that request access to personal data that is irrelevant to the app's primary function. These findings provide a way to help prevent fraudulent apps from accessing personal information and data without permission. So keep checking your app permission settings regularly to ensure that only legitimate apps have access to your data.

"In the future, make certain that you do not simply grant access to applications about whose security you are unaware." (Pace Komputer)

Theme 7: Ensure the Smartphone is Installed Antivirus and Operating System is Updated

This theme emphasizes that our smart phones must have a credible antivirus installed and keep the operating system updated, which is a crucial proactive step. In this digital age, the strategy of installing a trusted antivirus on your smart phone can help detect and prevent hacking attempts from malicious malware that can steal personal and financial data. Therefore, make sure to keep your mobile phone's operating system up to date, as this is an effective way to maintain security. Keeping your phone's operating system updated can help you avoid cybercriminals trying to exploit its vulnerabilities. By focusing on these prevention strategies and methods, we can protect ourselves from fraud and keep our personal data safe in this increasingly complex digital world.

Here are some resources that provide guidance on preventing fraud through installing antivirus and operating system updates on mobile phones that have mobile banking or financial applications.

"Therefore, before we get scammed, we must have an anticipation to always update the operating system on our mobile phones." (Pratama Persada-Kompas TV)

"do a factor reset after that install an antivirus" (Pratama Persada-Kompas TV).

DISCUSSION

Tackling fraud is not enough to rely on security tools and technology. The use of prevention strategies and detection techniques is essential to assist in identifying suspicious activity before a crime occurs. [4] emphasize that it is important for individuals to coordinate high-level training, and preparation for security exercises as a first step to detecting fraud. This is in line with these findings, which highlight the key role of human factors in fraud prevention strategies. It is important to highlight that to tackle fraud it is not enough to rely on fraud detection system technology, as described by [7] which only relies on fraud detection systems. The same thing is also presented by [3] which emphasizes fraud prevention in terms of computational methods, namely applying communal detection strategies, spike detection, and genetic algorithms.

Whilst the previous presentation suggests that technology and computational methods may be only one aspect of a fraud prevention strategy, the investigative findings of this study highlight that the human role in prevention, detection and intervention is a very important factor. As such, the results of this study provide a clear insight into how the role of humans is critical to the implementation of social media fraud prevention and strategy. While technology plays a significant role, it is the role of the individual that is the main factor that should not be overlooked to tackle fraud. Thus, the combination of human factors and technology is key in protecting individuals and organizations from the increasingly complex threat of fraud in this modern era.

CONCLUSION

This research can provide practical and theoretical implications. From the practical aspect, it can provide knowledge, lesson learnt, and practical best for everyone to overcome and prevent fraud that is rampant in social media. Theoretically, this research can contribute and enrich the theory of fraud prevention through the aspect of human knowledge and insight approach. Overcoming fraud is not enough to rely on technological tools and security devices alone, but effectively preventing fraud from social media requires wise understanding and strategies from everyone, through a vigilant attitude, a good understanding of social media, and the use of appropriate prevention strategies, thus we can contribute to preventing fraud that harms many people.

REFERENCES

1. Z.K. Zandian and M. Keyvanpour, Int. J. Knowledge-Based Intell. Eng. Syst. **21**, 123 (2017).
2. D. Gupta, S.K. Jha, and S. Mann Maharaja Surajmal, 2021 9th Int. Conf. Reliab. Infocom Technol. Optim. (Trends Futur. Dir. ICRITO 2021 (2021).
3. A. Singh and A. Jain, Lect. Notes Electr. Eng. **605**, 935 (2020).
4. D.R. Triwahono, A. Fauzi, A. Adzansyah, B. Yulivio, M.Y. Fito, R. Ghifari, P. Yuntama, and S.W. Azhar, **2**, 68 (2023).
5. V.F. Rodrigues, L.M. Policarpo, D.E. da Silveira, R. da Rosa Righi, C.A. da Costa, J.L.V. Barbosa, R.S. Antunes, R. Scorsatto, and T. Arcot, Electron. Commer. Res. Appl. **56**, 101207 (2022).
6. J.E.F. Teitcher, W.O. Bockting, J.A. Bauermeister, C.J. Hoefer, M.H. Miner, and R.L. Klitzman, J. Law. Med. Ethics **43**, 116 (2015).
7. A. Abdallah, M.A. Maarof, and A. Zainal, J. Netw. Comput. Appl. **68**, 90 (2016).
8. G. Lumakto and N. Kumala Dewi, J. Bimas Islam **14**, 393 (2021).
9. K. Binowo and A.N. Hidayanto, Organizacija **56**, 3 (2023).
10. V. Clarke and V. Braun, Couns. Psychother. Res. **18**, 107 (2018).