International Journal of Latest Research in Humanities and Social Science (IJLRHSS)
Volume 07 - Issue 07, 2024
www.ijlrhss.com || PP. 147-151

The Persuasive Strategies of Scammers in Facebook Bitcoin Investment Posts: An Examination through the Elaboration Likelihood Model (ELM) Perspective

Lilisuriani Abdul Latif @ Bapoo[1], Masyitah Ismah Hani Binti Azman[2],
[1]*International Islamic University Malaysia,*
Kulliyyah of Sustainable Tourism and Contemporary Languages,
Johor Darul Takzim, Malaysia
[2]*International Islamic University Malaysia,*
Kulliyyah of Sustainable Tourism and Contemporary Languages,
Johor Darul Takzim, Malaysia

Abstract: The rapid growth of social media platforms has facilitated a global connection among billions of users, allowing easy content sharing and engagement. Unfortunately, this progress in technology has also provided a fertile ground for online scams, particularly Bitcoin investment scams. This study applies the Elaboration Likelihood Model (ELM) to analyze the persuasive strategies used in Bitcoin investment scam posts on Facebook, aiming to uncover the processing routes and their elements employed by scammers. A thematic analysis was conducted on 63 posts from two Facebook accounts, revealing a predominant use of peripheral route elements of ELM, such as emotional appeals and peripheral cues, over central route elements of the ELM model. Even though collecting extensive data was challenging due to the need for confirmed reports of fraudulent activity and the rapid deletion or blocking of scam accounts, the findings of this study can help to increase public awareness of scammers' persuasive language and psychological approaches, improve social media scam detection, and inform policymakers on scammers' persuasive strategies through the analyses of ELM route elements in Bitcoin investment scams posted on a social media platform.

Keywords: Persuasive strategies, Online scams, Bitcoin investments, Elaboration Likelihood Model.

1. Introduction

Advancements in technology simplify many aspects of daily life but irresponsible beings are also taking advantage of technology advancements to perform various online scams. Today, we hear about online scams like phishing scams, charity scams, job offer scams, romance scams, and investment scams that were unheard of before. These online scams and financial frauds continue to escalate despite efforts by private and governmental entities to raise awareness and implement preventive measures. In Malaysia, for instance, a staggering RM330 million was lost to online scams through Meta-owned platforms (Facebook, Instagram, and WhatsApp) in the first five months of 2023 alone [10]. This surge is primarily due to fraudsters' ability to target vulnerable individuals through persuasive language and psychological manipulations, making individuals tend to act impulsively without engaging in rational thought processes [6] [15].

Bitcoin scams, also known as cryptocurrency frauds, pose significant harm to multiple victims. While an average person might be skeptical of bitcoin investment schemes, many still fall victim due to poor decision-making tendencies and lack of self-control [2]."Rug pulls," tactics where online scammers attract investors with false hope or promises, and then disappear, are commonly employed [7]. [3] and [11] highlight the fact that social media platforms like Facebook, Twitter, WhatsApp, and Telegram provide scammers with access to a vast, global audience, enabling them to disseminate fraudulent investment opportunities to millions of potential victims.

The success of online scams can largely be attributed to the sophisticated persuasive strategies employed by scammers. According to [1] and [12], scammers commonly attract potential targets by highlighting aspects of the victims' lifestyle, such as wealth, financial incentives or benefits, job opportunities, and religious beliefs. By addressing these personal elements, scammers can create an initial connection that draws the victims in. They then use language as well as social cues to build trust and rapport, often impersonating trusted figures or aligning themselves with reputable organizations. Persuasive language plays a critical role here, as it helps establish a sense of solidarity, familiarity, and trustworthiness.

In the cognitive dimension, [13] explains that scammers may employ complex language and technical jargon to confuse victims, making it difficult for them to critically evaluate the information presented. This complexity can create a sense of authority and legitimacy, further ensnaring the victim. Additionally, scammers manipulate emotions by using both positive and negative language. Scammers might offer praise and promises

of wealth, or conversely, induce fear and urgency to compel immediate action because fear-inducing messages can cause individuals to pay closer attention and think more deeply about the content [8].The strategic use of emotional language in these contexts ensures that victims remain engaged and are less likely to question the authenticity of the scam. The credibility of their schemes is enhanced through the manipulation of carefully selected words, phrases, and evidence. This might include the use of testimonials, fabricated endorsements, and seemingly legitimate statistics. These strategies serve as the foundation of persuasion in orchestrating a scam [5].

With the growing prevalence of Bitcoin investment scams on social media platforms, comprehensive studies that focus on the persuasive strategies employed by Bitcoin scammers on the platforms are essentially needed. Examinations of scammers' approaches to psychologically manipulate their victims are also relatively unexplored because contemporary research predominantly centers on victims' perspectives [4] [14] [15]. Hence, this study looks at the constructions of online Bitcoin scam posts on Facebook, with a focus on how Bitcoin scam posts are commonly designed to be psychologically processed by potential victims, attracting them to invest.

2. Method

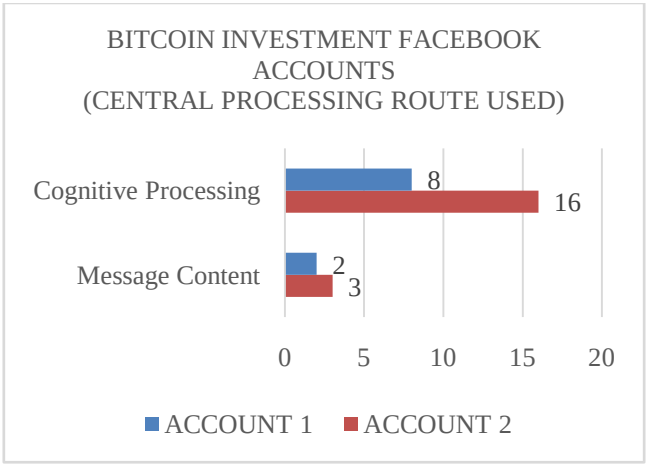
This study uses the Elaboration Likelihood Model (ELM) proposed by [9] to investigate how two Facebook Bitcoin scammer accounts commonly present their posts to be processed by readers. These accounts were selected due to their consistent postings and abilities to reactivate despite being reported and blocked multiple times. The identification of these accounts was facilitated through the “ScAm Alert” Facebook page, where members report potential scam accounts for verification. Using thematic textual analysis, the scam posts were coded accordingly to see if the messages were to be processed or evaluated via the central or peripheral route and the route elements of the Elaboration Likelihood Model (ELM).

According to ELM, the depth of thought that a person applies when evaluating a persuasive message determines their response. The central processing route involves careful thinking and detailed analysis of information before deciding. This pathway is marked by a thorough evaluation of arguments, resulting in individuals carefully scrutinizing the arguments, comparing them with their existing knowledge, and coming up with well-reasoned conclusions. The peripheral processing route, on the other hand, involves quick and shallow evaluation of information without deep analysis. It relies on mental shortcuts and superficial cues, such as emotional appeals or the attractiveness of the source, encouraging fast decisions [9]. Through thematic textual analysis, the common elements of the central route and the peripheral route were also identified and categorized to identify recurring themes and patterns within the posts. These elements are message content, argument quality, cognitive processing, and attitude change for central processing, while cues and heuristics, source characteristics, emotional appeals, and peripheral cues are for peripheral processing [9].

3. Results

The summary of findings can be seen in Figure 1.0 below. Analyses show that messages that encourage the use of the central processing route were used less than those of the peripheral processing route. The central processing elements appeared in 10 instances, with cognitive processing applied 8 times and message content, twice. Elements of argument quality and attitude change where compelling, strong, and well-structured arguments with well-supported and coherent facts, relevant to the audience’s beliefs and values to allow deep thought processing, were missing.

In comparison, the use of the peripheral processing route was much higher. From both accounts, there were 141 occurrences of peripheral route elements compared to 29 central route elements. Elements of emotional appeals and peripheral cues were the most common elements used in the Facebook Bitcoin Investment scam posts. In one account, there were 33 instances of peripheral cues and 32 instances of emotional appeals. In the other, 24 instances of peripheral cues and 26 instances of emotional appeals were featured. Peripheral cue elements included engaging graphics (mainly emojis), statements of legitimacy, statements of opportunity, and statements of guarantee. For emotional appeals, there were statements of emotions, religious sentiments, inspiring stories, and motivational speeches.



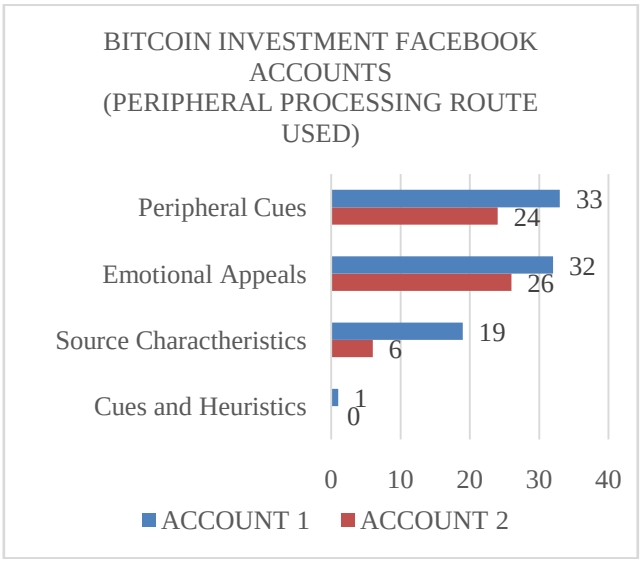


Figure 1: Common Processing Routes and Elements in Facebook Bitcoin Scam Accounts

Figure 1.0 shows that the elements of ELM found in the data are message content and cognitive processing from the central processing route, along with cues and heuristics, source characteristics, emotional appeals, and peripheral cues from the peripheral processing route.

3.1 Examples of Language that Encourages the Use of Central Processing Routes

Some use of the cognitive processing and message content elements of the central processing route was seen in both Bitcoin Investment Facebook accounts.

Cognitive processing is elements that prompt the target audience to critically evaluate the message, consider the presented arguments, and thoughtfully analyze the information before forming or changing their attitudes. Phrases such as “Maybe you think it’s too late to start, but let me tell you, it’s not! Start today, start with us!” and “With our amazing system you can become successful in just a short period of time,” the target audience were told to minimally ‘evaluate’ the situation presented and take the ‘right’ action.

Message content means strong arguments, detailed information, data, evidence, and logical reasoning are presented to persuade the audience. Examples of the ‘logical statements’ and ‘evidence’ used to strengthen the arguments to invest in Bitcoin are “Did you know that the average age of a millionaire is 57 years old?! This is according to a study that was done earlier THIS YEAR!”, “here’s my payout proof” or “here is my proof of (cash) withdrawal”.

3.2 Examples of Language that Encourages the Use of Peripheral Processing Route

All elements of the peripheral processing route were found in both FacebookBitcoin Investment accounts.

Firstly, analyses of the posts by both Facebook accounts show that peripheral cues appear in three distinct forms: engaging graphics (mainly emojis □□❤□ ···), statements of legitimacy, and statements of opportunity. Among these, emojis are the most prevalent, with at least three used in each post. Emojis are used to enhance the message through expressions of emotions, such as heart emojis for gratitude and loyalty, or confetti and champagne glasses for celebration. For statements of legitimacy, straightforward statements that require minimal cognitive effort or elaborations, such as "legitimate company", "legit and true", "legit account manager", "100% Safe and Secured, we are active 24/7, Risks are down at 0.001%" and "Your Benefit is Guaranteed" are visible. Examples of statements of opportunity are "If you have 1000 pesos dm me I'll teach you how to use your 1000 pesos to earn 30,000 pesos in just 8 Hours" and "invest 500 pesos and receive 15,000 pesos in just 2 hour time....".

Then, instances of emotional appeals include expressions of positive emotions by testimonials endorsers, religious sentiments, motivational statements, and inspiring success stories. By tapping into emotions, the posts aim to create a stronger connection with the audience, potentially making them more likely to act on the investment opportunities being promoted. Phrases like "Don't give up" and "Keep believing in yourselves" are used to encourage continued investment. There are also religious expressions like "God bless you", "God bless you all.", "May God bless you" or "All thanks to God Almighty for bringing you to my life" to create solidarity with the target audience.

Next, source characteristics refer to the focus on superficial aspects of the message, such as the credibility or attractiveness of the source. Statements such as "he is the best account manager", "the right account manager like me"and "his works deserve a lot of praise" are commonly seen.

Lastly, cues and heuristics used refer to individuals relying on superficial cues and simple heuristics rather than engaging in deep cognitive processing. These cues can include the attractiveness of the source, celebrity endorsements, simple emotional appeals and easily processed signals such as slogans, catchphrases, or logos. In the accounts studied, the use of hashtags is frequent, functioning as slogans or catchphrases that can be easily processed, without deep thinking. Hashtags such as #howtomakemoneyonline (how to make money online), #bitcoininvestment (bitcoin investment), #investmentopportunity (investment opportunity), and #bilionnaire are efforts observed to quickly influence the audience to think that they can easily gain profits by investing in bitcoin from the comfort of their home to become a billionaire.

4. Discussions

After evaluating the posts in the two Bitcoin investment accounts on Facebook, it can be said that the frequent use of peripheral processing route and its elements over the central processing route in the posts is a strategy that relies on the audience's processing of simple, exciting, and non-elaborative information rather than detailed, logical and extensive arguments. This supports [6] [15] who have reported about fraudsters' ability to target vulnerable individuals through psychological manipulations, where they are not required to engage in deep, rational thinking processes. Such an approach can be particularly effective in environments where the audiences are hasty, not interested in spending too much time engaging in deep processing thinking, or excited about getting huge incomes, making them more susceptible to simple, positive, and negative persuasive messages. Moreover, the use of peripheral cues effectively manipulates the audiences' perception, fostering a false sense of security and trust in the investment scheme especially when religious sentiments are exploited, similar to what have been mentioned by[1] and [12]. The use of cues and heuristics can initiate many individuals to impulsively make decisions, as highlighted by [2]. Even though [13] said that scammers may employ complex language and technical jargon to confuse victims, complex language and technical jargon are not at all seen in the two Bitcoin investment accounts. Instead, simplicity seems to be the approach utilized in these two accounts to create a sense of connectedness, trust, and legitimacy. Elements of cognitive processing and message content of the central processing route are also presented in a plain and direct manner to create a false sense of good logic and reason.

5. Conclusion

The study on two Bitcoin investment accounts on Facebook using the Elaboration Likelihood Model (ELM) reveals that the audience's peripheral processing route and all its elements are commonly exploited, as opposed to the central processing route. These elements of the peripheral processing route allow the posts to appear emotionally positive, attractive, reliable, and credible. Minimal applications of elements of central processing routes can be seen at times but they are non-elaborative and do not encourage deep analysis of information. Even though the findings cannot be generalized to all Bitcoin investment scams, policymakers are now more informed on scammers' persuasive strategies, and social media users should be made aware of the danger of believing attractive posts that do not provide sufficient opportunity for detailed data to be evaluated.

References

[1] Ab Aziz, A. A., Mohd Sharif, N. A., Wan Fakhruddin, W. F., Mohd Juned, A., Md Shah, N. K., Anuar Yatim, A. I., &Saidalvi, A. (2023). Linguistic cues of deception in Malaysian Online Investment Scams' promotional materials. GEMA Online® Journal of Language Studies, 23(4), 152–168. https://doi.org/10.17576/gema-2023-2304-09

[2] Caldas, L. S., Iglesias, F.,Pet Melo, I. R., & Lyra, R. L. (2019). Persuasion at Different Levels of Elaboration: Experimental Effects of Strength, Valence and Ego Depletion. Temas Em Psicologia, 27(2), 585–599. https://doi.org/10.9788/tp2019.2-20

[3] Chergarova, V., Arcanjo, V., Tomeo, M., Bezerra, J., Vera, L. M., & Uloa, A. (2022). Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest into cryptocurrency. Issues In Information Systems, 23(3), 242–252. https://doi.org/10.48009/3_iis_2022_120

[4] DeLiema, M., Li, Y., & Mottola, G. (2022). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. International Journal of Consumer Studies, 47(3), 1042–1059. https://doi.org/10.1111/ijcs.12886

[5] Garrett, B., Mallia, E., & Anthony, J. (2019). Public perceptions of internet-based health scams, and factors that promote engagement with them. Health & Social Care in the Community. https://doi.org/10.1111/hsc.12772

[6] Kadoya, Y., Khan, M.S.R. and Yamane, T. (2020). The rising phenomenon of financial scams: evidence from Japan. Journal of Financial Crime, 27(2), 387-396. https://doi.org/10.1108/JFC-05-2019-0057

[7] Kerr, D. S., Loveland, K. A., Smith, K. T., & Smith, L. M. (2023). Cryptocurrency risks, fraud cases, and financial performance. Risks, 11(3), 51. https://doi.org/10.3390/risks11030051 Ab

[8] Norris, G., & Brookes, A. (2020). Personality, emotion and individual differences in response to online fraud. Personality and Individual Differences, 169. https://doi.org/10.1016/j.paid.2020.109847

[9] Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. Advances in Experimental Social Psychology, 123–205. https://doi.org/10.1016/s0065-2601(08)60214-2

[10] Rashid, A. (2023, December 10). Preventing emotional manipulation by online scammers (Poll Inside). The Star. https://www.thestar.com.my/news/focus/2023/12/10/preventing-emotional-manipulation-by-online-scammers

[11] Siu, G., A., & Hutchings, A. (2023). "Get a higher return on your savings!": Comparing adverts for cryptocurrency investment scams across platforms. 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS'PW). https://doi.org/10.1109/eurospw59978.2023.00023

[12] Siu, G. A., Hutchings, A., Vasek, M., & Moore, T. (2022). "invest in crypto!": An analysis of investment scam advertisements found in Bitcointalk. 2022 APWG Symposium on Electronic Crime Research (eCrime). https://doi.org/10.1109/ecrime57793.2022.10142100

[13] Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., Tao, F., & Qian, X. (2022). Mental states: A key point in scam compliance and warning compliance in real life. International Journal of Environmental Research and Public Health, 19(14), 8294. https://doi.org/10.3390/ijerph19148294

[14] Williams, E. J., &Polage, D. (2018). How persuasive is phishing email? the role of authentic design, influence and current events in email judgements. Behaviour & Information Technology, 38(2), 184–197. https://doi.org/10.1080/0144929x.2018.1519599

[15] Wilson, S., Hassanrashid, N. A., Khor, K. K., Sinnappan, S., Abu Bakar, A. R., & Tan, S. A. (2023). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. Journal of Financial Crime. https://doi.org/10.1108/jfc-06-2023-0151