Preparedness against Investment Scams

Erico Tjoa[*]
Stanford University
ericotjo@stanford.edu

Abstract

Artificial intelligence (AI) has reached a level sophistication that is capable of resonating with human beings at emotional level. This can be extremely dangerous. Loan and investment scams have been known to exploit emotional cracks and get-rich-quick mentality. Uninformed people have fallen victims to carrots dangled before them through simple direct text messages. Imagine the catastrophic impact it would have when sophisticated chain of AI tools is used to convince potential victims down the rabbit hole.

1 Introduction

Loan and investment scams may be difficult to document in its entirety in part due to the profile of its potential victims. Yes, we can find several resources documenting official cases of scams, but it is the invisible force propagating through less regulated media that poses the greatest risk. To the scammers, even one percent of successful scams is a win and, as scammers become bolder and bolder, the society descends one step further into catastrophe. Imagine what happens when the entire chain of AI tools is available at a scammer's disposal.

Here, we shortly discuss (1) the psychology of scams (2) the modus operandi of AI-powered investment scams. Note: rather than going all theoretical about scam operations, we will instead write this with respect to a few particular snapshots of actual observations of scammers' fieldwork that seems to be ever evolving. We will therefore not rely much on academic publications and official documentations.

2 Discussion

Psychology of scams have been studied formally [1, 2, 3], and they shed lights into some methods of operations, e.g. using potent "baits words" that lure gullible victims into action. The basic ideas remain the same: (1) **The Lure**: attract potential victims with good offers. (2) **The Proof**: show potential victims fraudulent "proof" that they will succeed if they follow a given set of instructions. (3) **Urgent Choices**: once the victims show some interest, scammers will raise up the stakes and input an element of urgency into the pipeline. (4) **Commitment**: victims are committed to fraudulent transactions. With powerful AI tools, the potency of all four aforementioned steps can be multiplied. Many more people might fall victims into such scams. We will shortly discuss how AI can be exploited in each step.

(1) The Lure. There are certainly many ways to lure potential victims, but a potent first impression of legitimacy is key. It is arguable what the best entry point is, and this might differ from one person to the other. Having a real person converse with potential victims may well be the most convincing of all, and this is perhaps how modern generative AI is projected to augment the operation of scams. Have a GPT model send a text message with seemingly neutral intent, and, make sure that somewhere in between the conversation, let GPT subtly present a fraudulent opportunity. With personalized information, the style of conversation can be optimized to improve the probability of successful lure.

(2) The Proof. How do grifters on YouTube etc convince people that their courses will make the audience rich? Show them expensive cars, expensive watches, expensive houses etc. This might

[*] This paper consists of independent opinions. My personal email is ericotjoa@gmail.com

no longer fool some people, but, as we know it, many people might still fundamentally react at emotional levels to similar “proof of success” if their desires align. This is what generative models can potentially exploit. Create a video of a fake wealthy individual flaunting wealth? This might be too old school. Generative AI is now so powerful it might be possible to create *an entire fraudulent community of wealthy hardworkers* in action, with which even less gullible potential victims may fall victim to the appearance of legitimacy.

Let us illustrate this with a naive example. Have the victim join a zoom call featuring a fictitious panel of people from, say, JP Morgan, generated using AI. Make sure all of these individuals can be found online, i.e., they have some official profiles. Real scammers can blend into the chat to maintain some level of reality and convince potential victims to invest in some shady schemes. Potential victims may not even be aware of the fact that they are not talking to real people.

(3) Urgent Choices. Traditional scamming methods that makes use of artificial sense of urgency can be very naive, yet it seems to work. It definitely surprises many people how vulnerable potential victims can be under pressure. Some fraudulent “video conference” uses *eternal* countdown to push people towards paying for entry ticket into one of these “exclusive” opportunities. With generative AI models, things can get serious dangerously fast. Instead of silent eternal countdown, have fictitious entity talk you into purchasing the ticket. Make sure to add a few more fake people in the audience who pretended to purchase the tickets and the success rate of scams might have just skyrocketed.

(4) Commitment. One last layer of scam is the commitment phase, and generative AI models could be used as the final straw. At this point, the strategy again depends on the individual. GPT models with fake human entity can be chosen carefully to improve the chance of victims’ commitment to fraudulent deals, depending on the victims’ profiles. A/B testing and other experiments can be conducted to serve the most effective last push towards successful scams; some people might eventually fall under high pressure while others make the commitment under pseudo semi-rational apparent self-driven selection, the latter probably better handled by AI models that can fake wise and cool persona.

3 Conclusion

Augmenting investment scams and similar frauds with AI is very much a real possibility. Some resources may be needed to tune the models into effective scammers. However, scamming operations are becoming more sophisticated every day. Intervention at every stage of possible scams might be necessary to prevent catastrophic failure of the society.

References

[1] Stephen EG Lea, Peter Fischer, and Kath M Evans. The psychology of scams: Provoking and committing errors of judgement. 2009.

[2] David Modic and Stephen EG Lea. Scam compliance and the psychology of persuasion. *Available at SSRN 2364464*, 2013.

[3] Gareth Norris, Alexandra Brookes, and David Dowell. The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, 34:231–245, 2019.