Who goes to Cambodia? Characteristics and the Recognition of Fraudulent Job Supply

陳家威*

December 30, 2022

Abstract

I proposed a field experiment on job banks in Taiwan to identify the characteristics of people applying for potentially fake job opportunities online. The level of vulnerability can be measured by tracking ones' time interval of staying in our fake website. Characteristics of the targets are provided anonymously by the job banks.

1 Introduction

During summer of 2022, news about Taiwanese young people being transported to Cambodia, hostaged and disemboweled for organs shock the Taiwanese society. A report from *The Reporter* [1] shows that for most of the cases the victims were applying to high salary works abroad, such as gaming service, villa receptionist, or document typing jobs.

These fraudulent job supplies usually mimics a typical procedure of signing a contract, from well-designed DM to a seemingly formal contract paper. The organizers often kindly prepare all the procedures for going abroad, such as applying for a visa and providing fee for Covid-19 test. According to the victims, they were unable to see those through until they were maltreated in Cambodia.

Comments under posts regarding the news on social medias or BBS forums argued that the victims are simply not clever enough to identify the

*R10323045

[1] https://www.twreporter.org/a/cambodia-taiwanese-human-trafficking-survivors

fake information, knowing that the average payment for similar working opportunities are usually lower. Whether providing enough information about a specific job supply reduces the propensity of young unemployed people becomes a crucial policy for the government to consider, besides cracking down organizations of human trafficking. The effect, nevertheless, remains unclear.

To test for the difference of fraudulent job supply detection under a minimum asymmetric information circumstance, I proposed to cooperate with job banks [2] and conduct a large scale field experiment. Similar to the "Phishing Email Suspicion Test (PEST) " [3], fake job opportunities that mimics some characteristics of the existing fraudulent job advertisement are randomly assigned in their recommendation, disguising among the real ones.

2 A Very Brief Literatures Review

Experiments examined by Kumaraguru et al. (2009); Caputo et al. (2014) and all others emphasizes the importance of unawareness of the phishing test. Chen et al. (2018) examined some of the main behavior characteristics of phishing identification, including intolerance of risk, curiosity and trust, controlling age and sex.

While a variety of literatures, spanning from IEEE journals aiming at the design of anti-cyber attack, to behavioral journals focussing on the psychological aspect of the vulnerability, there seems to not have a field experiment particularly examining the social factors of an agent, such as education, debt, duration of unemployment, etc..

3 Experiment Setup

The experiment comes with three part — 1. Random selection of participants that receive warning 2. Creation of fraudulent jobs 3. Tracking the treatment group . I choose to conduct the experiment in cooperation with

[2] For example, 1111 and 106, two largest job banks in Taiwan with high reputations.

[3] PEST is a test that tests whether participants can identify fake emails. In a PEST test, participants are given either true or false emails, and when one clicks on the fake email, one is then marked as vulnerable to phishing.

large job banks due to several reasons. First is the completeness of information about participants that they can provide, such as education level, age, past job-seeking duration, category or previous jobs, and so on. As usual, the data is de-labelled for the sake of privacy, and is not open to the public. Second is the ability to track the behavior of participants. This will be clear in subsection 3.3. Briefly speaking, big companies have a higher budget to implement the technology that allows us the examine agent-specific behaviors after receiving the treatment, which broadens the dimension for further predictions and detection. Third, and the main reason, is that for all institutions posting job opportunities their information are provided with detail, which is a main difference with fraudulent jobs posted on social medias. Participants should be able to research on the institution before applying to any of the jobs.

Undoubtedly, one can argue that users willing to find jobs on social medias are probably fundamentally different from the population that seek for job on large job banks. However, it is rational to assume that all people seeking for jobs start first from job banks, and as long as there exist jobs paying higher than the average salary on the list, the populations that are seeking jobs on social medias will also want to apply to it. Statistics supporting the above assumption are needed, eventually.

3.1 Random selection of participants that receive warning

The participants will not, and must not be informed about the experiment beforehand, as previously mentioned in the literature review.

3.2 Creation of fraudulent jobs

3.3 Tracking the treatment group

References

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., and Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy*, 12(1):28–38.

Chen, Y., YeckehZaare, I., and Zhang, A. F. (2018). Real or bogus: Predicting susceptibility to phishing with economic experiments. *PLOS ONE*, 13(6):e0198213.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., and Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, New York, NY, USA. Association for Computing Machinery.