VICTIM AND ONLINE FINANCIAL SCAM: UNDERSTANDING HETEROGENEITY IN SUSCEPTIBILITY TO ONLINE FINANCIAL SCAM

NATTANICHA CHAIRASSAMEE, KANOKWAN CHANCHAROENCHAI, & PATTRAPA VEJPATTARASIRI

Introduction

During 2023-2024, Thailand reported approximately 330,000 cases of online financial fraud, resulting in damages exceeding 37 billion baht. Most of these damages stemmed from scams related to online shopping and various forms of investment fraud. This growing issue has negatively impacted the psychological well-being of the general public, particularly those who have fallen victim to such scams. Furthermore, it poses a threat to public confidence in the Thai financial system and the economy as a whole.

This study is divided into two phases. The first phase involves collecting data on actual online scam cases that have occurred in Thailand. The second phase uses the information from the first phase to design a set of online financial scam scenarios to be presented to participants. This phase aims to examine the factors that influence decision-making and victimization in various types of online financial fraud in Thailand.

Phase 1

Research method: collecting data on actual online scam cases that occurred in Thailand. The data included scam formats—such as message content, images, and the platforms where the scams were encountered—as well as scam types, such as fake product sales or side-income job offers.

Main findings:

The most common type of scam experienced was **fraudulent buying and selling.**

Word frequency analysis of terms related to online financial scams shows that respondents have encountered and/or fallen victim to the most frequently appearing words can be categorized into four groups:

1. **Money/Price-related words**
   – baht, cost, and cheap
2. **Income-related terms**
   – get money, work, investment, and high income
3. **Time-related expressions**
   – minute
4. **Emotionally triggering words**
   – special

Word frequency analysis

In addition, the word frequency also reflects the channels and formats through which respondents encountered scams, as indicated by words like Line, Facebook, TikTok, message, and image.

Phase 2

Research method: focusing on designing scam-like invitation messages. These messages are modeled after the data collected in Phase 1 and are intended to **stimulate greed and excitement among participants.**

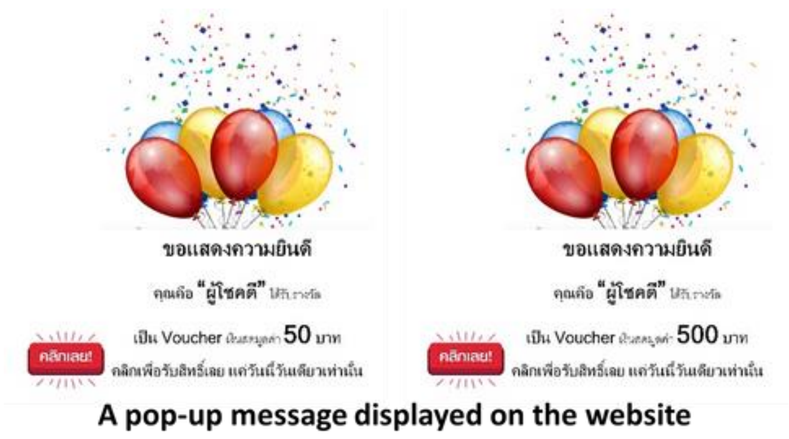
This phase tests three main hypotheses:
1. **Greedy** emotions increase the likelihood of becoming a scam victim.
2. **Different personality traits** lead to different levels of scam vulnerability.
3. **Higher monetary rewards** increase the likelihood of falling for a scam.

The experiment simulates **a pop-up message** appearing on the website while participants are answering the survey. The pop-up message is designed to closely mimic real-life scam pop-ups commonly encountered online, using text and design elements informed by

Phase 2 (cont.)

Phase 1 findings. These include:
- The cash reward amount clearly shown
- Emotionally charged language (e.g., “Congratulations!”, “You are a lucky winner!”)
- Time pressure to claim the prize within a limited period

Participants are randomly assigned to two groups based on the reward value shown in the pop-up image: 50 baht or 500 baht.



A pop-up message displayed on the website

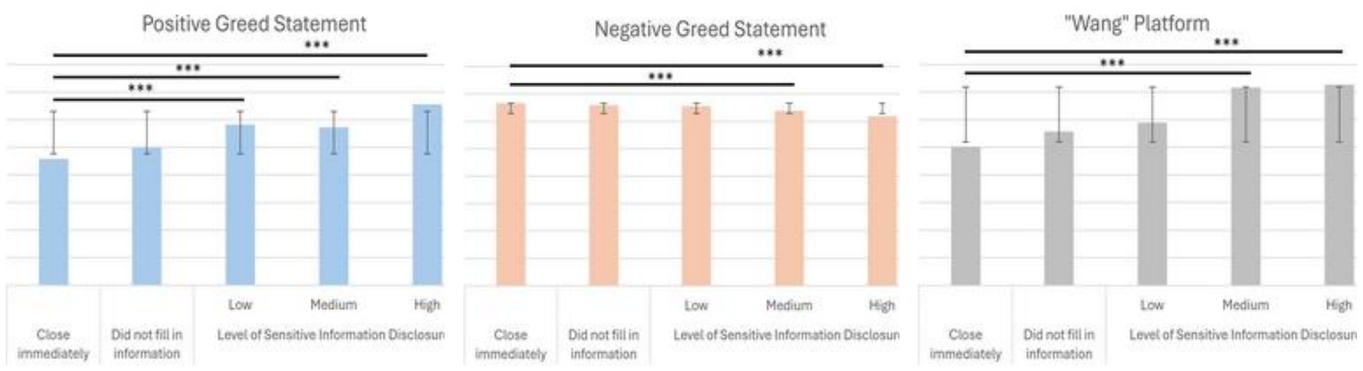
Participants who click to claim the prize will be asked to provide personal information with varying levels of sensitivity:
- **Low-sensitivity information:** Full name
- **Medium-sensitivity information:** Phone number and email address
- **High-sensitivity information:** Home address and national ID number

Participants will be prompted to enter this information gradually, in order of increasing sensitivity. They will have the option to decline the prize or stop providing personal information at any point during the questionnaire.

Empirical model:

$$sensitive_i = \alpha + \beta X' + \gamma greedy_i + \delta personal_i + \sigma value_i + \varepsilon_i$$

Main findings:
- Participants who **did not enter any personal information** had **higher scores on negative greed items** → indicating **lower greed.**
- Those who **entered personal information** showed **higher positive greed scores** → reflecting stronger feelings of greed or desire.
- **No significant difference** in skepticism across groups.
- Those who disclosed information were **more likely to believe** the pop-up came from a legitimate source (e.g., the “Wang” platform).



Results from the empirical model show five significant factors influencing decision-making.
- Higher reward values were associated with a **lower likelihood** of disclosing sensitive information.
- Participants with **higher emotional stability** were **more likely** to disclose highly sensitive personal data — a counterintuitive result.
- **Negative emotions** → decreased likelihood of disclosure
- **Positive emotions** → increased likelihood of disclosure
- A strong **belief that the pop-up came from the “Wang” platform** significantly increased the likelihood of disclosing sensitive information.

Policy implications

- Use **behavioral design** to adapt user experience (UX)/user interface (UI) for real-time scam warnings

  Example: when a message says *“You’ve won a prize”*, the system immediately displays:

  “ Warning: Be cautious of fake cash reward scams.”

- Implement **automatic warnings** in banking apps for at-risk transactions
  - Use AI to analyze user behavior in combination with known scam message patterns.
  - If a risk is detected—such as transferring money after opening a message saying “Receive 500 Baht”—the system should trigger an alert.