PUEY UNGPHAKORN INSTITUTE
FOR ECONOMIC RESEARCH

Victim and Online Financial Scams: Understanding Heterogeneity in Susceptibility to Online Financial Scams

by

Nattanicha Chairassamee, Kanokwan Chancharoenchai,
and Pattrapa Tangtatswas

January 2026
Discussion Paper
No. 245

The opinions expressed in this discussion paper are those of the author(s) and should not be attributed to the Puey Ungphakorn Institute for Economic Research.

Victim and Online Financial Scams:
Understanding Heterogeneity in Susceptibility to Online Financial Scams

Nattanicha Chairassamee
Department of Economics, Kasetsart University
Kanokwan Chancharoenchai
Department of Economics, Kasetsart University
Pattrapa Tangtatswas
Enterprise Risk Management Department, Bank of Thailand

Abstract

The growing financial fraud issue has negatively impacted the psychological well-being of the general public, particularly those who have fallen victim to such scams. This study aims to collect data to examine and understand the factors influencing decision-making and victimization in various types of online financial fraud in Thailand. By using the framing effect through greedy emotions and time pressure, our results indicate that the emotions experienced during scam encounters play a significant role in determining online financial fraud victimization. Since emotions directly influence System 1 decision-making, our study suggests that merely educating and building public awareness may not be effective in preventing long-term online scam victimization.

Keywords: emotion; financial decision; online financial scam; personality traits
JEL codes: D91, G41

Funding: Puey Ungphakorn Institute for Economic Research (PIER)

1. Introduction

The advancement of communication technologies adopted in financial systems has helped reduce procedural steps, time, and the number of personnel required for financial services. At the same time, it has enhanced convenience and efficiency, thereby contributing to economic expansion. However, these advancements have also led to the rise of cybercrime—an emerging and continuously growing threat. Such issues affect both businesses and consumers and may ultimately hinder national economic growth and lead to broader social problems.

Online fraud has been increasing across many countries. In 2021, there were as many as 293 million reported cases of online financial scams worldwide, resulting in damages of approximately USD 55.3 billion—a 10.2% increase from the previous year—making it the most significant form of payment fraud (The Global State of Scam Report, 2022). Although each incident of online fraud may involve relatively small financial losses, the sheer number of victims contributes to a massive cumulative impact (Moore & Anderson, 2011).

In 2024, Thailand experienced a surge in scam calls and SMS messages, reaching 168 million, marking a five-year high (Leesa-nguansuk, 2025). Online financial crime in Thailand appears to be growing in parallel with the progress of communication technologies used in financial systems. This growth has been further accelerated during and after the COVID-19 pandemic, as online financial transactions became more widespread in an effort to reduce viral transmission. As such, online financial crime has become part of a new type of threat to national security.

Currently, there is limited precise data on the characteristics of individuals who are most likely to fall victim to such scams in Thailand. However, among those who have reported being victims, 41.51% are aged between 30–44 years, followed by 25.33% aged between 22–29 years. In contrast, the elderly (aged 60 and above) and youth (under 18) represent the smallest proportions, at only 6.42% and 1.12% respectively. When classified by gender, 64% of the victims are women and 36% are men (Nation Thailand, 2024).

The problem of online scams in Thai society has evolved continuously in terms of tactics and strategies, adapting to changes in technology and online behavior. The persistence and evolution of online scams are largely driven by emotional manipulation strategies, which exploit psychological biases and heuristics in decision-making. According to the dual-process theory of decision-making (Kahneman & Tversky, 1974; Kahneman, 2011), decisions under uncertainty are often governed by System 1 processes—rapid, intuitive, and emotion-driven—rather than System 2, which is slower and deliberative. Scammers systematically exploit these System 1 processes by inducing strong emotional reactions such as fear, greed, and urgency, leading individuals to bypass rational evaluation.

Emotionally manipulative scams are a common type of financial cybercrime worldwide, including in Thailand. They have become a significant economic and social threat. Although Thailand has made efforts to raise public awareness and promote digital literacy—including the establishment of the "Cyber Vaccinated" initiative, which organizes activities like online scam quizzes to educate the public—such efforts may only provide short-term immunity (Scheibe et al., 2014; Burke et al., 2022; Chung & Yeung, 2023).

This limited effectiveness is due to individual differences in cognitive and emotional responses, as people do not always react based on reason, but rather on impulsive decision-making. Therefore, effective education, attitude adjustment, and behavior-based preventive strategies require a deeper understanding of personal factors, behaviors, personality traits, attitudes, and scam tactics that influence victimization. These insights are critical for government agencies and related organizations to design appropriate interventions or behavioral nudges that build long-term immunity against online financial scams.

Given the current lack of in-depth data on decision-making factors behind victimization in online financial scams, this study aims to gather comprehensive data on types of online scams, as well as the behaviors, attitudes, personalities, and emotional states of individuals who may fall victim to such scams. This study aims to fill this gap by examining both the emotional states experienced during scam encounters and individual personality traits that may predispose people to victimization. Specifically, it seeks to analyze how emotions such as greed, fear, or loneliness interact with personality dimensions to influence decision-making in online financial scams. Understanding these psychological determinants is essential for designing behaviorally informed interventions that can effectively reduce victimization risk and enhance public resilience against online financial scams.

The remainder of the paper is structured as follows. Section 2 discusses the related literature. Section 3 highlights overall research methodologies. Sections 4 and 5 show the methodology and results of research phase one and two, respectively. Section 6 provides a conclusion and discussion, and Section 7 suggests recommendations from the study.

2. Literature

The Economic and Social Impacts of Online Scams

The lack of detailed data on online scams limits the ability to evaluate their full economic and social impacts. However, from an economic perspective, online scams are comparable to conventional crimes (Moore et al., 2009). While online scams often involve small financial losses per case, their widespread reach across numerous victims leads to significant aggregate damages. The perpetrators of such crimes differ from traditional criminals in that they often possess higher education and are located in areas with weak labor markets (e.g., high unemployment) or jurisdictions with weak or loophole-ridden legal systems.

Banks and businesses are among the key entities affected. In 2009, UK banks reportedly lost £59.7 million due to online fraud, which accounted for 13.56% of all fraudulent transactions valued at £440 million (Moore & Anderson, 2011). In the U.S., a data breach involving T.J. Maxx credit card information harmed investor confidence and affected the company's stock price (Moore et al., 2009). Additionally, Americans experienced identity theft damages totaling USD 156 million in 2005, rising to USD 180 million in 2018.

Beyond direct financial losses, victims also face opportunity costs such as damaged credit scores and time lost reporting crimes (Koyame-Marsh & Marsh, 2014), as well as psychological distress.

Psychological and Behavioral Economic Concepts Related to Financial Fraud Victimization

Victimization in online scams is closely tied to emotional states. For example, when people perceive a threat (e.g., intimidation or blackmail), the brain's amygdala activates, which affects short-term decision-making. Similarly, during moments of happiness, serotonin is released, increasing risk tolerance and impulsive behavior—factors that may make individuals more susceptible to fraud (O'Neill, 2019).

Emotional decision-making can reduce rational responses. Hadnagy (2018) used fMRI scans to show that when people experience intense emotions such as fear or anxiety, emotional brain areas are activated while logical areas shut down. Scammers exploit this by crafting messages that appear trustworthy—such as imitating government agencies.

Two types of emotions influence fraud victimization:

(1) Negative Emotions (e.g., fear, greed)

A synthesis of previous research by Norris and Brookes (2021) revealed that online offenders exploit victims' fear for personal gain in approximately 60% of cases, which is considerably higher than in other types of online crimes (Kim & Kim, 2013). Typical scam messages are often designed to evoke fear of loss, employing words and phrases such as "warning," "deadline," or notifications that threaten to suspend financial accounts (Harrison et al., 2015).

Most studies have also found that victims of online crimes tend to be deceived by unrealistically high promised returns. For instance, Fischer et al. (2013) surveyed online fraud victims and found that most victims responded emotionally to prize-winning messages, believing they had a genuine chance of winning. Similarly, Hu and McInish (2013) observed in their study on investment fraud victimization that fraudulent investment solicitations typically offered excessively high short-term returns and provided specific figures, thereby appealing to investors seeking to reduce ambiguity in uncertain returns. Furthermore, investments made under the influence of fear or greed were found to yield lower returns than those made when investors were in a neutral emotional state.

Supporting this, an experimental study by Williams and Polage (2019) compared scam messages offering rewards (testing greed) with messages threatening account suspension (testing fear). The results showed that most participants perceived fear-based messages, such as account suspension threats, to be more credible and less likely to be fraudulent than reward-based messages.

(2) Positive Emotions (e.g., happiness)

Perpetrators of online fraud often employ strategies to gain victims' trust and convince them of the authenticity of the interaction before initiating financial deception. A common example is the romance scam, in which offenders build an emotional relationship (often through expressions of affection or romantic interest) to make victims believe the relationship is genuine, after which financial fraud typically occurs. Such deception is predominantly carried out through online messaging platforms (Cross & Lee, 2022).

Furthermore, victimization driven by positive emotions can involve not only financial fraud but also the theft of personal information, such as photographs, which are later exploited or misused (Cross & Layt, 2021).

Demographic and Personality Traits of Victims

Elderly individuals are often more vulnerable due to anxiety about the future and lower digital literacy (Kadoya et al., 2021; Button et al., 2014). Cognitive decline may reduce their critical thinking (Han et al., 2015; Shao et al., 2019). However, Zhang & Yi (2022) found that younger, less-educated people are also at risk due to their digital lifestyles. Whitty (2020) found no correlation with age.

Financial literacy—knowledge, attitudes, and behaviors—can reduce vulnerability (Shao et al., 2019; Engels et al., 2020). Risk-takers are more prone to fraud, although the type of scam matters (Schoepfer & Piquero, 2009).

Some traits, such as loneliness, single status, and emotional vulnerability, also increase susceptibility (Kadoya et al., 2021; Shadel & Pak, 2017; Whitty, 2020; Parti, 2022). Studies are inconclusive on whether gender or educational level consistently influences risk.

The aforementioned studies also provide empirical evidence regarding individuals who are psychologically vulnerable, socially isolated, unmarried, living with family, and experiencing loneliness—factors that make them more susceptible to financial fraud than other groups. For instance, Kadoya et al. (2021) found that unmarried men were more likely to fall victim to scams involving false debt collection. Shadel & Pak (2017) reported that men were more likely to be targeted by investment fraud, while women were more prone to believe in luck-based scams such as lotteries. Similarly, Whitty (2020) found that women were more likely to be deceived in consumer-related scams, whereas men were more often victims of investment scams. These findings align with Parti (2022), who suggested that differences in gendered social roles and needs could explain variations in vulnerability to certain types of online scams. However, Zhang & Yi (2022) found no significant association between gender and scam susceptibility, indicating that the gender-scam relationship remains inconclusive.

Educational level is another demographic characteristic expected to reduce scam vulnerability. This assumption was supported by Fan & Yu (2021), but contradicted by Whitty (2020), Zhang & Yi (2022), and Parti (2022), who found no statistically significant relationship between educational level and scam victimization. Thus, there is no clear consensus regarding the direction of the relationship between education and fraud susceptibility. While education may enhance internet literacy and awareness of scams, it could also lead to overconfidence, thereby increasing risk.

Although many studies suggest that certain demographic and personality traits may be common among scam victims, the detailed findings highlight considerable variability. For example, Lev et al. (2022) found that victims in developing countries often share similar traits: they tend to be naive and driven by a desire to escape poverty, which leads to greed, a lack of empathy, and impulsive decision-making. However, these traits and susceptibilities vary by scam type. Kadoya et al. (2021) also emphasized that financial fraud victims are diverse and influenced by the type of scam. Those experiencing loneliness and social isolation are particularly vulnerable to a wide range of scams, such as fake billing, fraudulent loans, or deceptive refund offers.

In Thailand**,** Daengsi et al. (2022) found that nearly 70% of online shopping scam victims in Thailand were aged 20–39. Supasiri Janthawarin (2022) found that women were more likely to fall for romance scams, while the elderly were more vulnerable to data theft. Highly educated and high-income individuals were more susceptible to investment scams. Pirunrat Srijam (2019) found no clear demographic patterns but highlighted usage patterns of social media and financial platforms as key risk factors.

These findings reflect the diversity of victim profiles and the influence of scam types. However, Thai research remains limited and needs expansion to keep up with evolving fraud tactics.

Research Gaps

Most previous studies rely on self-reported susceptibility rather than behavioral outcomes, and few have examined the interaction between emotions and personality in scam victimization. Furthermore, evidence from Southeast Asia, where digital financial scams are rapidly increasing (Cross & Layt, 2021), remains scarce. This study contributes to filling these gaps by providing experimental evidence on how momentary emotions at the time of scam exposure influence sensitive information disclosure behavior, compared to stable personality traits.

3. Research Methodology

This study is divided into two phases.[1] The first phase involves collecting data on actual online scam cases that have occurred in Thailand. This includes scam formats—such as message

[1] This study was approved by the Kasetsart University Research Ethics Committee for studies involving human participants under the approval codes KUREC-SSR67/064 and KUREC-SSR67/130 for Phase 1 and Phase 2 of the

content, images, and platforms where the scams were found—as well as scam types, such as fake product sales or side-income job offers.

The second phase uses the information from the first phase to design a set of online financial scam scenarios to be presented to participants. The target participants for this experiment are individuals with access to digital technology who are at risk of being deceived by online financial scams.

The sample population in this study consists of residents living in Bangkok and the surrounding metropolitan area, as this region has been reported to have a comparatively higher proportion of individuals who have experienced online fraud than other parts of Thailand (Hahpipat, 2024). A primary data collection implemented as an online questionnaire distributed via the "Wang" crowdsourcing platform, which enables Thai users to participate in surveys. Because the majority of Wang users are general Thai citizens, the recruitment of respondents for this study was conducted through random selection from the pool of platform registrants.[2]

As the present study recruited participants solely from the Bangkok metropolitan area, the findings may not entirely represent the behavior or victimization patterns of the broader Thai population. Moreover, given that the platform allows participation by any user, there is a possibility of overlap between respondents across the two rounds of data collection. Nevertheless, the data collection procedure did not disclose the identity of the research team, nor were respondents informed in advance of the study's purpose. Therefore, responses are assumed to be independent across participants. The details of each research phase are as follows:

4. Phase 1

4.1 Research Methodology

Phase 1 involved 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, including fake product sales, investment, job

research, respectively. In addition, prior to the second-phase data collection and analysis, the researchers preregistered the study hypotheses on the OSF Open Science platform. Details are available at: https://doi.org/10.17605/OSF.IO/AJBXR

[2] Among the 816,002 registered users nationwide on the Wang platform, the majority were female (78.60%), had an average age of approximately 26 years, and were not formally employed.

offers, loan, application installation, and romance. We use an online questionnaire that consists of three sections:

Section 1: Demographic information, including gender, age, and educational level

Section 2: Big Five Personality traits-related questions following Costa & McCrae (1997) with 60 questions, divided into five dimensions and 12 questions in each dimension

Section 3: Experience with or victimization by various types of online financial scams

4.2 Findings from Phase 1

The data are collected from 200 respondents residing in Bangkok and the metropolitan area, all of whom had previous experience with online financial scams (see Appendix A for respondent demographic details).

Figure 1 shows that the most common type of scam experienced was fraudulent buying and selling, which also accounted for the highest proportion of victims—approximately 50% of those who had encountered this scam type ended up as victims.

Other common scam experiences included investment scams and job offer scams. However, for these types, most respondents did not fall victim despite their exposure.

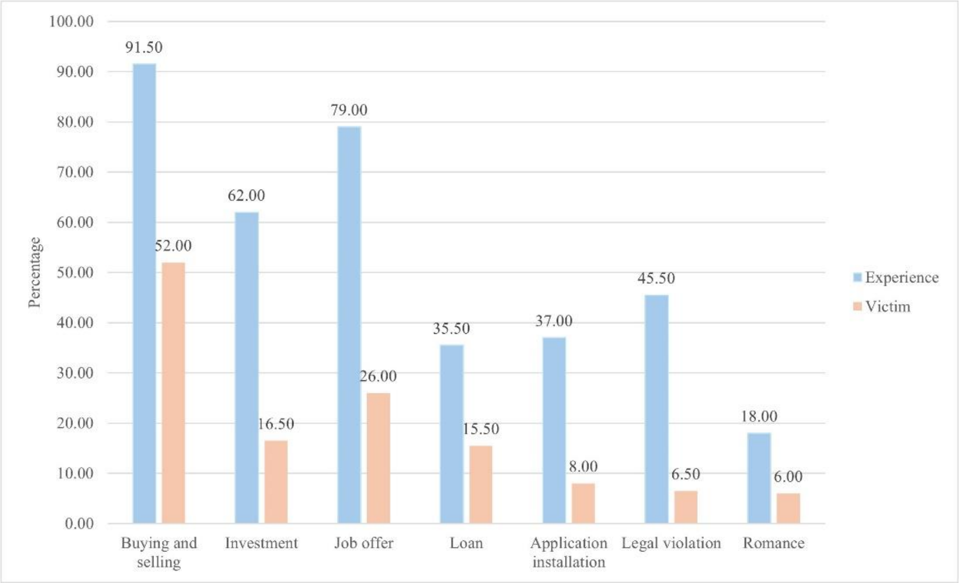

Figure 1: Proportions of respondents who experienced online scams and became victims

When examining scam channels, the findings showed variation across scam types. Most scams (e.g., product/service scams, investment scams, job offer scams, and loan scams) were encountered via websites or social media platforms such as Facebook or TikTok. These are platforms where users actively engaged with scam content, meaning the victims approached the scam rather than being directly targeted.

Scam formats typically included:

- Persuasive messages
- Images of products, offers, or opportunities that aligned with the respondent's desires or interests
- Numerical indicators such as prices or promised returns
- Time-sensitive terms implying urgency to act to obtain benefits

Regarding emotions, respondents reported experiencing negative emotional states while encountering scammers, including fear, pressure, sadness, and hopelessness. For scams involving pricing and return-on-investment promises, respondents also felt interest, greed, and excitement.

Details of the findings from Phase 1 are presented in Table 1. Overall, respondents who fell into being victims of each scam are female, aged 27 to 28, employed full-time, and have an income ranging between THB 15,000 and 25,000 per month.

Table 1: Details of scams by scam type

Type of Scam		Related Issues
Sales of goods or services	Average frequency of Victimization	2 times/person
	Average total financial loss	THB 20,147 per person
	Scam Channels	Typical websites and social media used
	Scam Patterns	• Persuasive accompanying message • Manipulative conversation conducted by fraudsters
	Emotions	Pressure and excited
Investment	Average frequency of Victimization	1 time/person
	Average total financial loss	THB 21,497 per person
	Scam Channels	Typical websites and social media used
	Scam Patterns	• Persuasive accompanying message Images of desired items or opportunities
	Emotions	Fear, pressure, interested, and greedy

Table 1: (continued)

Type of Scam		Related Issues
Job/ Side job offers	Average frequency of Victimization	1 time/person
	Average total financial loss	THB 35,338 per person
	Scam Channels	Typical websites and social media used
	Scam Patterns	• Persuasive accompanying message • Manipulative conversation conducted by fraudsters
	Emotions	Fear, discouraged, interested, tired, and sad
Loan	Average frequency of Victimization	2 times/person
	Average total financial loss	THB 73,654 per person
	Scam Channels	Typical websites and social media used
	Scam Patterns	• Manipulative conversation conducted by fraudsters • Images of desired items or opportunities
	Emotions	Fear, despair, and pressure
Application installation	Average frequency of Victimization	2 times/person
	Average total financial loss	THB 10,440 per person
	Scam Channels	Directly contacted by scammers via Email/text/application (such as Line, Tinder)
	Scam Patterns	• Persuasive accompanying message • Images of desired items or opportunities
	Emotions	Pressure, excited, and fear
Legal violation	Frequency of Victimization	1 time/person
	Total Financial Loss	THB 45,250 per person
	Scam Channels	Directly contacted by scammers via phone call
	Scam Patterns	Manipulative conversation conducted by fraudsters
	Emotions	Fear and pressure
Romance	Frequency of Victimization	4 time/person
	Total Financial Loss	THB 111,509 per person
	Scam Channels	Directly contacted by scammers via Email/text/application (such as Line, Tinder)
	Scam Patterns	Manipulative conversation conducted by fraudsters
	Emotions	Lonely, discouraged, and sad

We asked respondents to describe the details of the fraud they experienced. From the word frequency analysis of terms related to online financial scams that respondents have encountered and/or fallen victim to—visualized in Figures 2.1 and 2.2—the most frequently appearing words can be categorized into four groups:

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

4. Emotionally triggering words – such as *special*

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

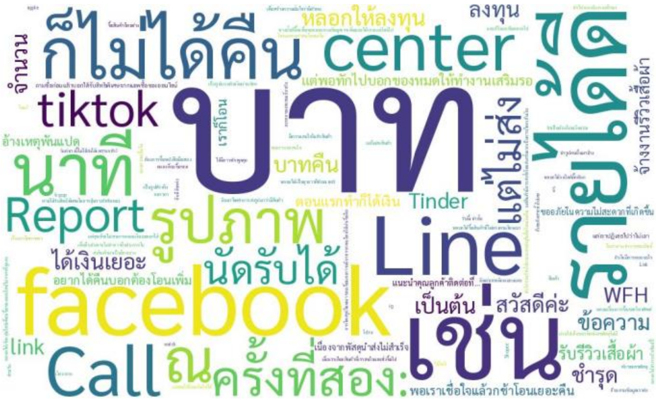

Figure 2.1: Word cloud without word segmentation

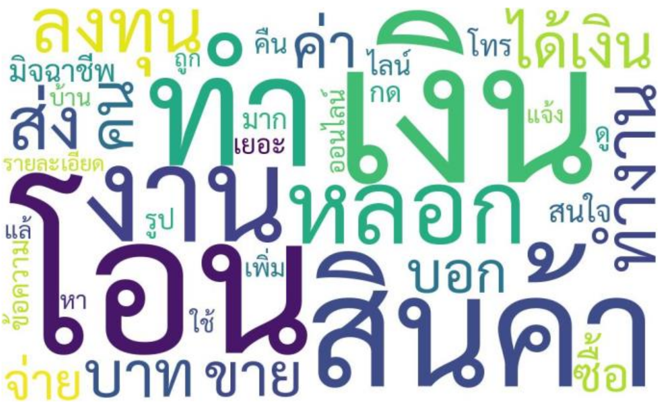

Figure 2.2: Word cloud with word segmentation

Figure 2: Word cloud of key terms extracted from open-ended responses regarding online financial fraud (in Thai)

5. Phase 2

5.1 Research Methodology for Phase 2

In line with the study’s objective to investigate the factors influencing victimization in online financial scams—particularly emotional and personality-related factors—Phase 2 focuses 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. Findings from Phase 1 revealed that scam messages or images often emphasize pricing, promised earnings, and time pressure. This phase tests three main hypotheses:

Hypothesis 1: Greedy emotions increase the likelihood of becoming a scam victim.

Hypothesis 2: Different personality traits lead to different levels of scam vulnerability.

Hypothesis 3: Higher monetary rewards increase the likelihood of falling for a scam.

Since the experiment uses an online questionnaire platform via the "Wang" platform (details mentioned earlier), the scam simulation is designed to be appropriate for an online environment.

Based on the study hypotheses, the experiment simulates a pop-up message appearing on the website while participants are answering the survey. This pop-up message informs the respondent that they are a "lucky winner" of a cash prize. Participants are randomly assigned to two groups based on the reward value shown in the pop-up image: 50 baht or 500 baht. The message also states that the prize must be claimed within a limited time.

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 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

Details of the pop-up message design are shown in Figure 3.

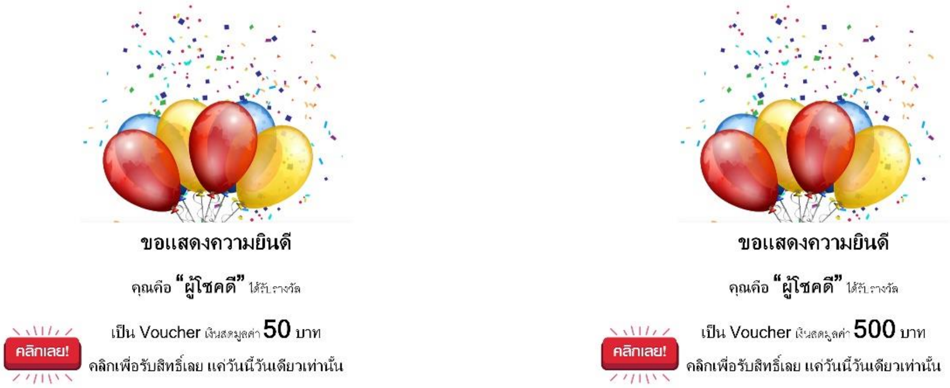
ขอแสดงความยินดี
คุณคือ "ผู้โชคดี" ได้รับรางวัล
เป็น Voucher เงินสดมูลค่า 50 บาท
คลิกเลย!
คลิกเพื่อรับสิทธิ์เลย แค่วันนี้วันเดียวเท่านั้น
ขอแสดงความยินดี
คุณคือ "ผู้โชคดี" ได้รับรางวัล
เป็น Voucher เงินสดมูลค่า 500 บาท
คลิกเลย!
คลิกเพื่อรับสิทธิ์เลย แค่วันนี้วันเดียวเท่านั้น

Figure 3: A pop-up message displayed on the website while participants were answering the questionnaire (in Thai)

Participants who click to claim the prize will be asked to provide personal information with varying levels of sensitivity:

- Low-sensitivity information: Full name and email address
- Medium-sensitivity information: Phone number and home address
- High-sensitivity information: 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.

Sensitive information disclosure is associated with the risk of online fraud (Mesch & Dodel, 2018). In this study, therefore, the act of entering personal information is used as a behavioral indicator to reflect the likelihood of falling victim to an online financial scam.

Participants in this study were recruited through the "Wang" website, which requires users to register as members prior to accessing surveys. As a result, it is possible that participants may have believed that the pop-up message was genuinely issued by the Wang website. To reduce this potential bias, the pop-up text was designed to appear different from Wang's default formatting. Additionally, respondents were asked whether they believed the pop-up came from the Wang platform. The questionnaire title was also deliberately crafted to prevent participants from anticipating the nature of the experimental scenario in advance.

Aside from the pop-up stimulus, participants were required to complete a questionnaire consisting of four sections:

Section 1: Demographic information including gender, age, educational level, employment status, and income

Section 2: Greed emotion assessment after exposure to the pop-up message, using 11 items adapted from Fischer et al. (2013)

Section 3: Personality traits measured using a short version of the Big Five Personality Traits scale following Donnellan et al. (2006), covering Openness to Experience, Conscientiousness, Extraversion, Agreeableness, and Emotional Stability[3]

Section 4: Experience with online financial scams, using the same questions as in Phase 1 of the study

[3] We reduced the number of Big Five personality traits questions to shorten the overall time in the experiment.

Generally, the pop-up appears on the screen when respondents begin answering the first section—demographic information. The structure of the information submission process is illustrated in Figure 4. After making their decision regarding information disclosure, respondents are returned to the questionnaire to complete Section 1 if they have not already done so, followed by Sections 2 through 4.

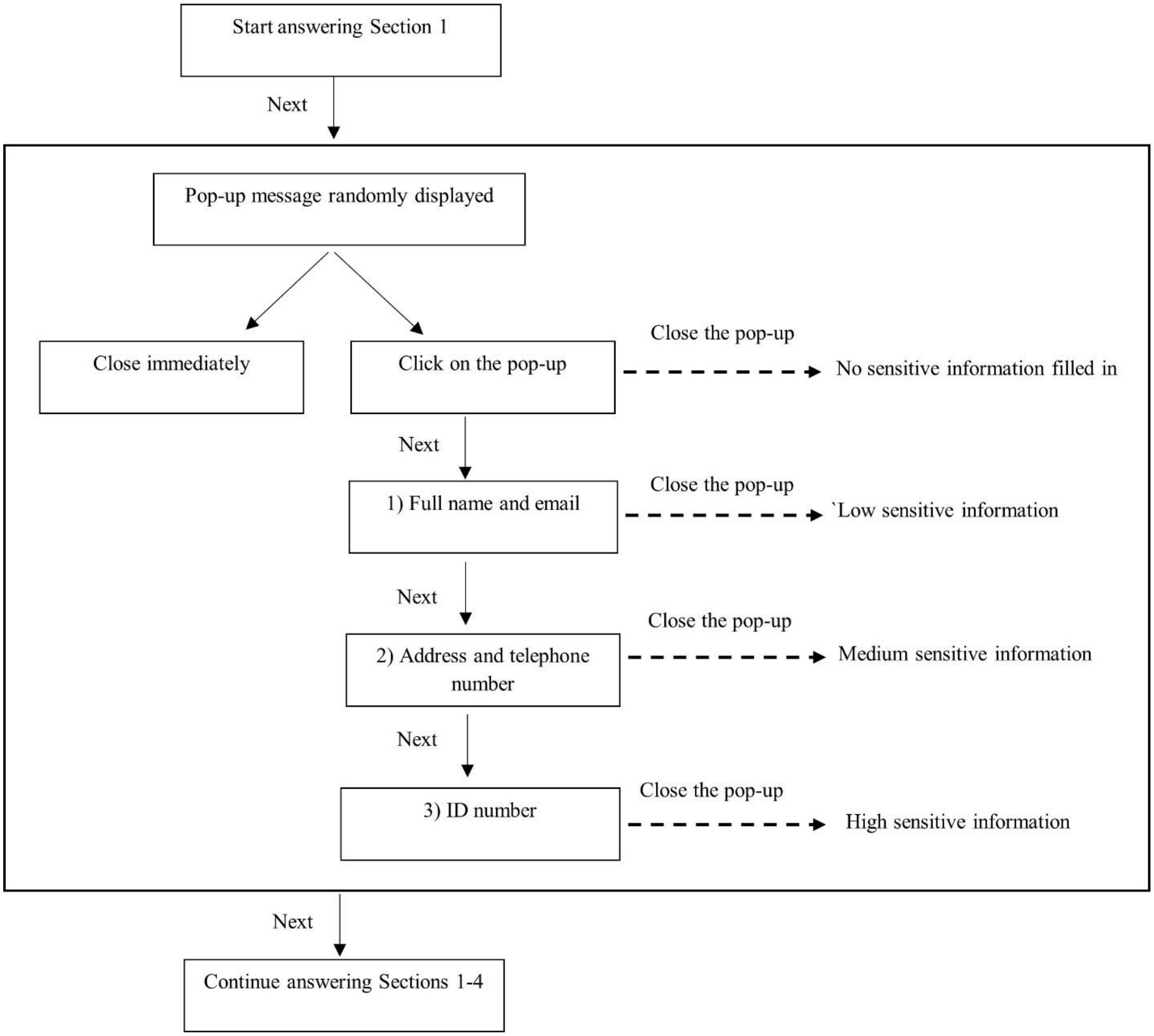
Start answering Section 1
Next
Pop-up message randomly displayed
Close immediately
Click on the pop-up
Close the pop-up
No sensitive information filled in
Next
1) Full name and email
Close the pop-up
`Low sensitive information
Next
2) Address and telephone number
Close the pop-up
Medium sensitive information
Next
3) ID number
Close the pop-up
High sensitive information
Next
Continue answering Sections 1-4

Figure 4: Experiment steps and options for sensitive information disclosure

5.2 Findings from Phase 2

A total of 1,294 participants took part in the experiment.[4] The majority were female (75%), with an average age of 25 years, predominantly single, and either currently enrolled in or graduates of undergraduate programs (Table 2).

As a result, 46.03% of the sample were neither employed nor actively seeking employment. Among those who were employed, most worked as government officials or state enterprise employees (Table 2).

Given that most participants were students or unemployed, over half of the sample reported monthly personal incomes of 15,000 baht or less and household incomes of 30,000 baht or less. These figures fall below the average household income for Bangkok and its metropolitan area in 2023, which was 39,000 baht (Table 2).

As data were collected online, this high proportion of female respondents may partly reflect gender-based differences in survey participation, as women are generally more likely to cooperate in online surveys (Smith, 2008) and are more likely to complete questionnaires than men (Stieger et al., 2007).

Nevertheless, our findings are consistent with those of Hapipat (2024), who examined experiences of online fraud among individuals aged 15–79 years across all regions of Thailand. His study similarly reported that individuals belonging to Generation Z (aged 15–27) and Generation Y (aged 28–45) were more likely to have experienced online fraud than other age groups, due to greater access to smartphones and the internet, which in turn increases their exposure to risky online behaviors and enhances opportunities for fraudulent schemes to take place. In addition, women were at a higher risk of victimization than men.

Due to the inherent limitations of online data collection in the present study, the sample may not fully align with the demographic structure of the general population and may be biased toward particular population segments. However, the characteristics of our respondents are consistent with those of individuals who have actually experienced online fraud, thus reflecting a group highly relevant to the research question.

[4] In our actual sample, 657 respondents were randomly assigned to the THB 50 condition and 637 to the THB 500 condition. The observed mean disclosure scores are 2.25 and 1.94, respectively, with a pooled standard deviation of 1.50. A post-hoc power calculation was conducted using Stata based on these observed parameters. The resulting statistical power is 0.9592 at the 5% significance level.

Table 2 Characteristics of respondents

Characteristics	Frequency	Percentage	Mean	Std. Dev.$^{\#}$
Gender				
Female	991	76.58		
Male	214	16.54		
Other	89	6.88		
Age			25.80	6.99
Educational level				
Less than bachelor’s degree	75	5.80		
Bachelor’s degree	835	64.53		
Higher than bachelor’s degree	384	29.68		
Marital status				
Single	1,149	88.79		
Married	131	10.12		
Other	14	1.08		
Employment status				
Full-time	426	32.92		
Part-time	49	3.79		
Unemployed but looking for a job	220	17.00		
Unemployed and not looking for a job	599	46.29		
Individual income (per month)				
Less than or equal THB 15,000	660	51.00		
THB 15,001-20,000	281	21.72		
THB 20,001-25,000	139	10.74		
THB 25,001-30,000	79	6.11		
THB 30,001-35,000	50	3.86		
THB 35,001-40,000	33	2.55		
THB 40,001-45,000	12	0.93		
THB 45,001-50,000	12	0.93		
More than THB 50,000	28	2.16		
Household income (per month)				
Less than or equal THB 30,000	490	37.87		
THB 30,001-35,000	215	16.62		
THB 35,001-40,000	114	8.81		
THB 40,001-45,000	82	6.34		
THB 45,001-50,000	86	6.65		
THB 50,001-55,000	59	4.56		
THB 55,001-60,000	39	3.01		
THB 60,001-65,000	54	4.17		
More than THB 65,000	155	11.98		

Note: Std. Dev. stands for standard deviation.

Hapipat (2024) results, moreover, indicate that individuals who are most vulnerable to financial losses resulting from online fraud include housewives or househusbands—those without formal employment or stable income sources. The unemployed respondents in our dataset can therefore be considered representative of this segment of the population. In addition, a large proportion of Bangkok residents have educational attainment below a bachelor’s degree, resulting in relatively low monthly income levels for both individuals and households. In 2023, 30.6% of individuals had monthly incomes of no more than THB 15,000, and 36.8% earned between THB 15,001–30,000. The income distribution observed in our sample is therefore broadly consistent with the demographic characteristics of the Bangkok population.

In Table 3, an analysis of participants' personality traits revealed that the highest average scores were observed in Agreeableness, Extraversion, and Emotional Stability. Among the five personality dimensions, nearly 80% of participants were found to have Agreeableness as their most dominant trait.

In contrast, Openness to Experience and Conscientiousness had relatively lower average scores. As a result, none of the participants exhibited these two traits as their most prominent personality characteristic.

Table 3: Big Five personality traits

Personality traits	Average score	Std. Dev.$^{\#}$	Frequency	Percentage
Openness to experience	7.97	1.75		
Conscientiousness	8.32	1.68		
Extraversion	18.98	3.92	258	19.94
Agreeableness	20.40	4.01	1,034	79.91
Emotional stability	11.08	2.77	2	0.15

Note: Std. Dev. stands for standard deviation.

Using the question items modified from Fischer et al. (2013) to measure participants' sense of greed, it was found that the average negative emotional responses toward the pop-up message were relatively high compared to positive ones. Specifically, participants reported feeling that the message was untrustworthy, suspicious upon viewing it, and annoyed by the appearance of the pop-up. These three items received the highest average scores among all questions in this section.

Furthermore, the average score related to feeling pressured to submit personal information in order to claim the reward was above the midpoint. This indicates that the design of the pop-up message in this study effectively elicited a sense of pressure, reflecting a situation closely resembling real-world online financial fraud.

Table 4: Greed-related questions after pop-up displayed

Greed-related questions	Types of emotion	Average score (out of 5 total score)
1. I felt very positive when seeing the invitation message	Positive	2.54
2. You felt positive about future earnings upon seeing the invitation message	Positive	2.55
3. I felt bored when seeing the invitation message	Negative	3.18
4. The invitation made me want the reward and fill in the form to claim it	Positive	2.53
5. Seeing the message that I am a winner made me feel excited	Positive	2.55
6. I thought the reward amount was attractive	Positive	2.67
7. I felt negative when seeing the invitation message	Negative	3.20
8. I thought it was a great opportunity to win money without doing anything	Positive	2.54
9. I felt doubtful when seeing the invitation message	Doubtful	3.59
10. I started thinking about what you would do with the prize money	Positive	2.49
11. I felt the message was not credible at all	Negative	3.68
12. I felt pressured to fill in the form immediately	Pressure	2.73
13. I thought the message came from a "Wang" platform	Believe in the institution	2.82
Average score of positive greed		2.59
Average score of negative greed		3.26

More than 55% of participants chose to immediately close the pop-up message during the experiment. However, 16.31% of participants clicked on the pop-up to claim the reward but did not enter any personal information and eventually closed the message. It is likely that this group of participants chose not to proceed upon realizing they would be required to provide personal data. Therefore, this group is considered to be at low risk of falling victim to online financial scams.

In contrast, nearly 30% of participants opted to claim the reward offered in the pop-up. Among them, the responses were concentrated at two extremes:

- Some provided only low-sensitivity personal information (e.g., full name and email) and then closed the pop-up.
- Others proceeded to provide all requested information, including full name, email, phone number, home address, and national ID number—classified as high-sensitivity data.

It is noteworthy that a smaller proportion of participants stopped at the medium-sensitivity level (e.g., phone number and address). This may suggest that those who provided only low-sensitivity information began to feel unsafe when prompted to provide more sensitive details, prompting them to close the pop-up and opt out of claiming the reward after that point.

The study partially addressed its hypotheses by examining personality traits, greed-related emotions, and the level of personal data disclosure through a comparison of mean scores between groups. In this analysis, participants who either closed the pop-up immediately or clicked on the message but did not enter any personal information were classified as a group that did not disclose sensitive personal information.

Table 5: Levels of sensitive information disclosure

Levels of sensitive information	Frequency	Percentage
Close pop-up immediately	718	55.49
Open pop-up without information disclosure	211	16.31
Open pop-up with information disclosure	365	28.20
Full name and email (low sensitivity)	100	7.73
Phone number and address (medium sensitivity)	55	4.25
National ID number (high sensitivity)	210	16.23

The comparison of average greed scores across groups—categorized by the level of personal information shared (as shown in Table 6)—revealed that participants who did not enter any personal information scored higher on negative greed items (indicating lower levels of greed), particularly on items 3, 7, 9, and 11. Conversely, participants who did disclose personal information exhibited lower negative greed scores, and their positive greed scores (reflecting feelings of greed or desire) were generally higher.

Table 6: Greed-related questions by level of sensitive information disclosure

Greed-related questions	Close immediately	Without information disclosure	Level of sensitive information disclosure		
			Low	Medium	High
1. I felt very positive when seeing the invitation message	2.297	2.554	2.780	2.873	3.186
2. You felt positive about future earnings upon seeing the invitation message	2.267	2.564	2.990	2.800	3.219
3. I felt bored when seeing the invitation message	3.365	3.109	2.980	2.836	2.771

Table 6: (continued)

Greed-related questions	Close immediately	Without information disclosure	Level of sensitive information disclosure		
			Low	Medium	High
4. The invitation made me want the reward and fill in the form to claim it	2.221	2.479	2.960	2.927	3.343
5. Seeing the message that I am a winner made me feel excited	2.258	2.455	2.850	2.945	3.414
6. I thought the reward amount was attractive	2.411	2.673	3.020	2.945	3.338
7. I felt negative when seeing the invitation message	3.384	3.166	2.930	2.855	2.814
8. I thought it was a great opportunity to win money without doing anything	2.242	2.403	2.960	2.891	3.376
9. I felt doubtful when seeing the invitation message	3.561	3.640	3.750	3.600	3.548
10. I started thinking about what you would do with the prize money	2.320	2.318	2.810	2.636	3.057
11. I felt the message was not credible at all	3.859	3.758	3.580	3.473	3.095
12. I felt pressured to fill in the form immediately	2.475	2.810	3.120	3.200	3.214
13. I thought the message came from a “Wang” platform	2.510	2.782	2.950	3.582	3.633

Moreover, participants who disclosed personal information were more likely to believe that the pop-up message originated from the “Wang” platform.

A comparison of mean greed scores across each item found statistically significant differences between those who provided no personal information and those who did. However, no significant differences were observed among participants who disclosed personal data at different sensitivity levels. This suggests that, regardless of whether participants disclosed low-, medium-, or high-sensitivity information, their levels of greed (both positive and negative) did not differ significantly. Thus, it can be inferred that both groups demonstrated similar greed-related emotional patterns that influenced their decision to disclose sensitive information, despite being exposed to different prize values (see Appendix C for details).

When considering the overall mean scores and differences between groups, participants who immediately closed the pop-up message had significantly lower mean scores on positive greed (indicating lower levels of strong greed) compared to those who disclosed personal information (Figures 5.1 and 5.2). Meanwhile, no significant differences in positive greed scores were found among the groups that disclosed personal information at different sensitivity levels. This suggests that individuals who chose to close the pop-up immediately were less greedy than others, whereas participants who opted to disclose personal information, regardless of sensitivity level, exhibited similar levels of greed.

Conversely, participants who disclosed highly sensitive and moderately sensitive personal information had significantly lower negative greed scores (indicating higher greed levels) than those who immediately closed the pop-up, consistent with previous findings—individuals with higher levels of greed were more likely to disclose critical personal information.

As for other emotions, including skepticism toward the message (Figure 5.3), perceived pressure (Figure 5.4), and trust that the pop-up originated from a legitimate platform (Figure 5.5), the results showed that skepticism did not significantly differ between participants who disclosed information and those who did not. However, perceived pressure scores were significantly higher among participants who disclosed personal information at all sensitivity levels compared to those who immediately closed the pop-up. Additionally, those who chose to disclose information demonstrated higher trust in the legitimacy of the pop-up message than participants who opted to close it immediately.

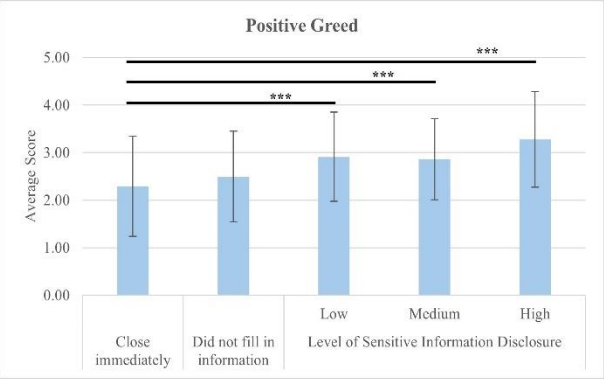

Figure 5.1 Positive greed

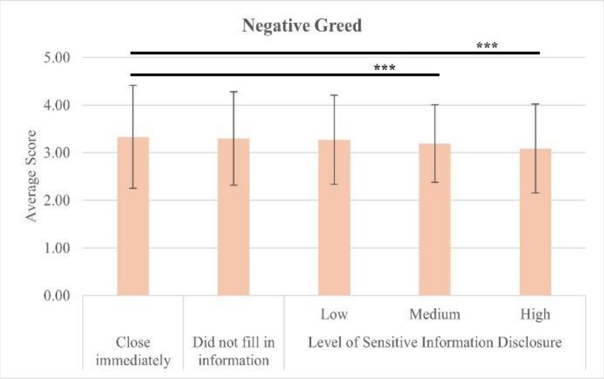

Figure 5.2 Negative greed

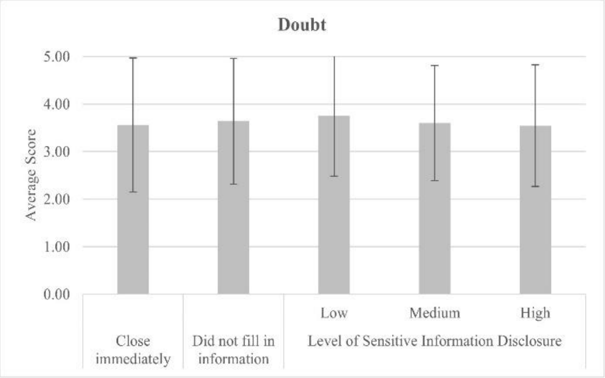

Figure 5.3 Doubt

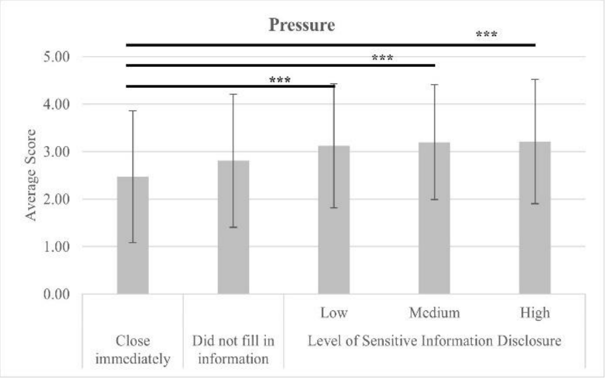

Figure 5.4 Pressure

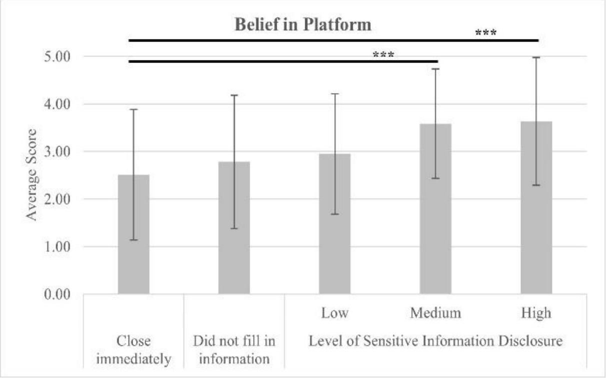

Figure 5.5 Belief in the platform

Figure 5: Mean differences of greed-related questions by level of sensitive information disclosure

Note: *p < 0.10; **p < 0.05; ***p < 0.01.

Regarding personality traits, Table 7 shows that differences in participants' personality profiles did not correspond to any clear trend in the disclosure of personal information at varying sensitivity levels. No statistically significant differences were observed between groups, even when participants were exposed to different prize values. These findings suggest that personality traits did not significantly influence the likelihood of disclosing sensitive information in this context (see Appendix C for details).

Table 7: Big Five personality score by level of sensitive information disclosure

Personality traits	Close immediately	Without information disclosure	Level of sensitive information disclosure		
			Low	Medium	High
Openness to experience	18.801	19.308	19.430	18.436	19.210
Conscientiousness	20.403	20.436	20.630	19.345	20.514
Extraversion	8.329	8.289	8.420	8.164	8.333
Agreeableness	10.967	11.180	11.420	10.945	11.262
Emotional stability	7.936	8.033	8.090	7.855	7.976

Additionally, to examine the factors influencing decision-making and victimization in online financial scams, the empirical model can be specified as follows:

$$sensitive_i = \alpha + \beta_1 pos\_greedy_i + \beta_2 neg\_greedy_i + \beta_3 oth\_emo_i + \beta_4 personal_i + \beta_5 value_i + \beta_6(pos\_greedy_i * personal_i) + \beta_7(neg\_greedy_i * personal_i) + \beta_8(oth\_emo_i * personal_i) + \beta_9(pos\_greedy_i * value_i) + \beta_{10}(neg\_greedy_i * value_i) + \beta_{11}(oth\_emo_i * value_i) + \beta_9(personal_i * value_i) + \gamma X' + \varepsilon_i.$$

Let $sensitive_i$ denotes the level of sensitivity of personal information disclosed by participant i. It is coded as zero if the participant immediately closed the pop-up message, 1 if the participant opened the message but provided no information, and 2–4 if the participant provided information categorized as low-, medium-, and high-sensitive, respectively. This ordinal coding reflects the increasing risk level associated with the disclosure of personal information.

As previously mentioned, this study examines the impact of emotions and personality traits on the likelihood of becoming a victim of online financial fraud. Thus, pos_greedy_i and neg_greedy_i represent the average scores of positive and negative greed, respectively, while $personal_i$ denotes the dominant personality trait of participant i, including agreeableness and extraversion.[5] Consequently, $personal_i$ was treated as a dummy variable, coded as 1 for participants whose dominant personality trait was agreeableness and zero for those whose dominant trait was extraversion.

[5] As only two participants were identified with emotional stability as their dominant trait, they were excluded from the analysis.

Additionally, based on the hypothesis that the prize value positively influences the likelihood of victimization, the variable $value_i$ was included, representing the prize value displayed in the pop-up message. This variable was also coded as a dummy: 1 if the prize value was 500 THB and zero if the prize value was 50 THB.

Interaction terms between greed, personality, and prize value were tested to investigate whether these factors jointly influenced participants' decisions to disclose sensitive information. Demographic variables, denoted as X', were also included as control variables.

Table 8: Variable descriptions and codes

Variables	Descriptions	Codes
Dependent variable		
$sensitive$	Level of sensitive information disclosure	This variable is coded as an ordinal scale, defined as follows: **0** if the participant immediately closed the pop-up window; **1** if the participant opened the pop-up window but did not provide any information; **2** if the participant opened the pop-up window and provided low-sensitivity information; **3** if the participant opened the pop-up window and provided medium-sensitivity information; **4** if the participant opened the pop-up window and provided high-sensitivity information.
Independent Variables		
pos_greedy	Average score of positive greed	Ranges from zero to 5; calculated as the mean score of items 1, 2, 4, 5, 6, 8, and 10 (as detailed in Table 4)
neg_greedy	Average score of negative greed	Ranges from zero to 5; calculated as the mean score of items 3, 7, and 11 (as detailed in Table 4).
oth_emo	Score of doubt, pressure, and belief in the platform	Ranges from zero to 5; the score for doubt is derived from item 9; the score for pressure is derived from item 12; and the score for belief in the platform is derived from item 13 (as detailed in Table 4)
$personal$	Personality	Dummy variable: equal to zero if a respondent has an agreeableness personality; equal to 1 if a respondent is extraversion.
$value$	Prize value displayed in the pop-up message	Dummy variable: equal to zero if the prize value displayed is 50 Baht; equal to 1 if the prize value displayed is 500 Baht.
Controls		
X'	Demographic-related controls	Including respondents' gender, education level, income, marital status, and employment status (as detailed in Table 2)

Because the dependent variable—sensitive information disclosure—can be clearly ordered, the Ordered Logistic Regression (OLR) method is appropriate for estimation. However, according to Ferrer-i-Carbonell and Frijters (2004), who compared the OLR and Ordinary Least Square (OLS) Method, the results are generally consistent between the two methods. Therefore, this study employed the OLS for ease of interpretation, particularly for interaction terms, while the OLR was additionally used to verify the robustness of the results.

Among the psychological variables reported in Table 9 (see Appendix D for full results), only the emotion experienced during the pop-up interaction significantly influenced sensitive information disclosure. Specifically, higher positive greed scores increased the likelihood of disclosing more sensitive information, whereas higher negative greed scores decreased this likelihood, consistent with the study's hypothesis. Other emotional factors—such as skepticism about the pop-up, perceived pressure, or trust in the platform—showed no statistically significant effects. Furthermore, all interaction terms were statistically insignificant, indicating that the likelihood of disclosing sensitive information did not differ significantly according to personality traits or prize value conditions.

The findings indicate that emotions experienced at the moment of encountering online scams play a crucial role in determining victimization in online financial fraud and are more influential than personality traits. This result aligns with the conclusion of Montag, Elhai, and Panksepp (2021), who argued that emotional differences form a fundamental basis for the evolution of human personality. Consequently, when individuals are engaged in System 1 decision-making—rapid, intuitive decisions based on immediate cues—emotions exert a stronger influence than personality traits.

Additional analysis was conducted by combining participants who immediately closed the pop-up message with those who opened it but provided no sensitive information into a single group, as both categories represent individuals who did not disclose sensitive information (results reported in Columns 2 and 4). The results remained consistent with the baseline findings. Furthermore, when estimating the model using the Ordered Logistic Regression (OLR) method (results reported in Columns 3 and 4), the estimated coefficients did not differ substantially from those obtained via the Ordinary Least Square (OLS) Model, demonstrating the robustness of the model's findings.

Additional robustness checks (not shown) indicate no heterogeneity by demographic characteristics. This finding strengthens the interpretation that emotional mechanisms—particularly positive and negative greed—are the primary determinants of scam vulnerability.

Table 9: Results from the model estimation

	Ordinary Least Square Regression		**Ordered Logistic Regression**	
Variables	**Sensitive Levels (5 Levels)**	**Sensitive Levels (4 Levels)**	**Sensitive Levels (5 Levels)**	**Sensitive Levels (4 Levels)**
	(1)	**(2)**	**(3)**	**(4)**
Emotions				
Positive greed	0.230*	0.191**	0.268*	0.423**
	(0.119)	(0.095)	(0.150)	(0.190)
Negative greed	-0.324***	-0.198**	-0.480***	-0.430**
	(0.119)	(0.090)	(0.170)	(0.204)
Doubt	0.075	0.037	0.140	0.072
	(0.089)	(0.068)	(0.128)	(0.157)
Pressure	0.057	0.055	0.061	0.079
	(0.084)	(0.065)	(0.113)	(0.141)
Belief in the platform	0.102	0.095	0.098	0.155
	(0.077)	(0.062)	(0.093)	(0.124)
Personality				
(Base group=Extraversion)				
Agreeableness	-0.604	-0.277	-1.051	-0.633
	(0.490)	(0.374)	(0.658)	(0.814)
Reward value	-0.414	-0.105	-0.869	-0.506
(Base group=THB 50)	(0.439)	(0.335)	(0.625)	(0.752)
Interaction terms				
(Emotion#Personality)				
Positive greed#Agreeableness	0.0003	-0.010	0.034	-0.060
	(0.119)	(0.093)	(0.158)	(0.201)
Negative greed#Agreeableness	0.063	0.039	-0.010	-0.065
	(0.118)	(0.090)	(0.176)	(0.217)
Doubt#Agreeableness	-0.068	-0.053	-0.042	-0.018
	(0.088)	(0.067)	(0.132)	(0.163)
Pressure#Agreeableness	0.028	0.009	0.074	0.086
	(0.079)	(0.061)	(0.114)	(0.143)
Belief in the platform#Agreeableness	0.128*	0.080	0.213**	0.197
	(0.077)	(0.061)	(0.099)	(0.133)
Interaction terms				
(Emotion#Reward value)				
Positive greed#THB 500	0.013	0.007	0.055	0.170
	(0.100)	(0.077)	(0.142)	(0.172)
Negative greed#THB 500	-0.026	-0.060	-0.019	-0.277
	(0.089)	(0.067)	(0.149)	(0.183)
Doubt#THB 500	0.042	0.048	0.019	0.081
	(0.062)	(0.047)	(0.106)	(0.130)
Pressure#THB 500	-0.044	-0.067	0.024	-0.097
	(0.064)	(0.049)	(0.099)	(0.123)
Belief in the platform#THB 500	-0.020	-0.025	0.013	0.038
	(0.058)	(0.045)	(0.086)	(0.108)

Table 9: (continued)

Variables	Ordinary Least Square Regression		Ordered Logistic Regression	
	Sensitive Levels (5 Levels) **(1)**	**Sensitive Levels (4 Levels)** **(2)**	**Sensitive Levels (5 Levels)** **(3)**	**Sensitive Levels (4 Levels)** **(4)**
Interaction terms				
(Personality#Reward value)				
Agreeableness#THB 500	0.298	0.253*	0.231	0.402
	(0.197)	(0.150)	(0.272)	(0.331)
Controls	YES	YES	YES	YES
Observations	1,292	1,292	1,292	1,292
R2	0.1939	0.1807	0.0853	0.124
Threshold 1			0.372	2.026
Threshold 2			1.209	2.537
Threshold 3			1.708	2.878
Threshold 4			2.041	

Notes: # indicates an interaction term. Standard errors are in parentheses. *p < 0.10; **p < 0.05; ***p < 0.01.

6. Conclusion and Discussion

This study examined the behavioral and psychological mechanisms underlying individuals' decision-making and victimization in online financial scams in Thailand. The empirical results help clarify the economic relevance of these behaviors and provide practical insights for policy interventions aimed at reducing financial losses, discouraging fraudulent activities, and protecting consumer welfare.

The findings indicate that most victims voluntarily approached scammers through online platforms they routinely used, motivated by messages that emphasized monetary rewards, investment returns, or time-sensitive opportunities. These persuasive signals induced emotional arousal and time pressure, creating a form of behavioral bias similar to present bias and scarcity bias, which distort judgment and make individuals more likely to take immediate risks for perceived gains. This aligns with findings from Lyu et al. (2025), recent experimental research, showing that perceived time pressure significantly increases vulnerability to online fraud.

Moreover, many phishing or scam designs explicitly exploit urgency and trust cues to induce compliance. In our context, the familiarity with and trust in routinely used digital platforms further reduced perceived risk and lowered the threshold for impulsive, System 1-style decision-making.

Our results highlight that emotional reactions during scam encounters are more influential determinants of victimization than personality traits or standard demographic variables. This aligns with the economic perspective that risk perception is not solely based on objective probabilities, but is dynamically shaped by context, emotions, and cognitive shortcuts. Most decisions in scam contexts occur under uncertainty and urgency, triggering the use of System 1 processing (Kahneman, 2011)—rapid, intuitive, and emotion-driven—rather than System 2's slower and more deliberate evaluation of risks and expected payoffs.

From an economic standpoint, these behavioral outcomes translate into tangible welfare costs. Individuals not only suffer direct financial losses but also incur indirect welfare losses such as anxiety, stress, reduced future willingness to participate in digital financial services, and potential declines in trust toward legitimate platforms. These outcomes collectively undermine digital economic participation and impose broader social costs.

The study also contributes to the growing literature showing that simply increasing financial literacy or disseminating factual warnings is insufficient for long-term prevention (e.g., Burke et al., 2022; Chung & Yeung, 2023). Economic theory helps explain why educating individuals increases average knowledge, but does not eliminate behavioral biases that operate under emotional pressure, nor does it correct mistaken risk perceptions that arise in fast-paced online interactions. Effective policy solutions must therefore acknowledge these psychological factors.

As with most behavioral experiments, the present study has limitations that relate to external validity and the extent to which the findings can be generalized beyond the experimental setting. These limitations concern both the characteristics of the sample recruited and the extent to which the experimental task reflects real-world online scam environments. Nevertheless, the core behavioral patterns and psychological mechanisms identified remain informative and policy-relevant.

The Wang platform user base primarily consists of individuals actively engaged with digital content and online communication networks. Since these groups are disproportionately targeted by financial scams, this enhances the ecological validity of our findings. However, respondents who rarely use mobile applications or online social media may behave differently, and future studies could aim to capture such populations.

The experimental interface was intentionally designed to mimic the psychological features of real online fraud attempts, including time pressure, reward framing, and emotionally stimulating cues. While simplified relative to real-world scenarios, the task captures the core decision processes underlying scam susceptibility, particularly System 1 decision-making. Nevertheless, the experimental nature cannot fully reproduce the dynamic and evolving strategies used by scammers, which may affect generalizability.

7. Policy Recommendations

Given that merely increasing knowledge about cognitive biases may not effectively override System 1-driven decision-making (Kahneman & Tversky, 1974), strategies to address online financial fraud should focus on preventive system designs and behavioral interventions that disrupt impulsive decision-making. The recommendations are as follows:

1. Behavioral Design to Improve User Experience and Timely Warnings

One effective strategy involves integrating behavioral design into website and application interfaces to help users detect and respond to potentially fraudulent activities. Pop-up message control systems can be implemented on popular websites and social media platforms to screen, filter, or block suspicious or fraudulent content. Given the empirical findings suggesting that victims who disclosed sensitive personal information often trusted the legitimacy of such pop-ups, an intervention at this point of contact may reduce exposure to scam attempts.

A practical implementation would be to set “block pop-up” as the default system setting, while allowing users the option to override it. Additionally, real-time alerts should be designed to notify users when they encounter high-risk messages or interactions, particularly those involving financial information. However, designers must also be cautious of potential unintended consequences, such as inadvertently blocking legitimate financial communications from trusted institutions.

In Thailand, the DE-fence application developed by the National Digital Economy and Society Commission (NDESC) currently screens phone numbers and SMS messages for potential scams. While this initiative is a significant step forward, the current system is limited to telecommunication data. Future development should extend such protective mechanisms to include digital platforms and websites, where scam activities are increasingly prevalent.

2. Design Nudges to Slow Down System 1 Decision-Making

The second intervention focuses on slowing down automatic, emotion-driven decision-making—often referred to as System 1 thinking—through behavioral nudges. High-risk financial transactions, especially those involving new or unverified accounts, should incorporate multi-step confirmation protocols or delay mechanisms. For instance, imposing a mandatory 24-hour waiting period before enabling transfers to newly added accounts can provide users with a reflective pause, potentially preventing hasty decisions influenced by fraudulent manipulation.

Additionally, limiting transaction amounts to accounts with no prior transaction history can serve as a safeguard against large-scale fraud. Repeated visual warning cues—such as emotionally salient pop-up alerts, red color schemes, and universally recognized warning symbols—should accompany each user interaction involving suspicious links or financial investments. These cues are intended to interrupt intuitive processing, prompting users to switch to slower, more deliberative System 2 thinking, thereby reducing impulsivity and increasing risk awareness.

In conclusion, integrating behavioral insights into digital infrastructure—both in the form of user-interface design and cognitive nudges—holds significant promise in reducing susceptibility to online financial fraud. Effective implementation requires a careful balance between user autonomy, technological feasibility, and the prevention of unintended negative consequences.

Future research should examine how different warning message designs—such as variations in visual salience, emotional framing, message frequency, and interactivity—can effectively reduce greed-driven behavior and mitigate engagement in risky financial transactions, particularly in online environments where users are often exposed to high-pressure decision-making situations. Such investigations could provide valuable insights into the psychological mechanisms underlying user compliance and contribute to the development of evidence-based digital interventions aimed at enhancing consumer protection and financial decision quality.

Moreover, strengthening public resistance to online scams should be pursued as a complementary policy alongside broader digital literacy initiatives and regulatory enforcement, as it remains within the practical scope of relevant authorities to implement and sustain through coordinated, multi-sectoral efforts.

Other related implications

Beyond preventive measures aimed at activating System 2 to improve individual decision-making, the implementation of broader institutional and regulatory interventions targeting relevant stakeholders can also effectively reduce the overall damage caused by scams.

For example, OECD member countries have emphasized that online platforms should implement preventive mechanisms such as identity verification for sellers, verification of bank accounts, reporting systems for suspicious activities, and cooperation agreements for information sharing with banks and law enforcement agencies when fraudulent behaviors are detected. These practices align with the findings of this study, which show that platform credibility and user trust can influence the likelihood of engaging with pop-up rewards (and, by extension, increase the risk of becoming a scam victim). Therefore, preventive measures implemented directly by online platforms are both necessary and economically justified.

Responsibility for preventing and responding to scams should not rest solely on consumers, but also on digital platforms, banks, and telecom operators. Many countries, such as Singapore, the United Kingdom,[6] and the European Union, have also introduced a "shared-liability framework," under which telecommunications companies and banks share responsibility when phishing or scam incidents occur through mobile or online channels.

Several institutions in Singapore[7]—including the police, banks, and telecommunications companies—implement coordinated anti-scam measures. These include the "SMS Sender ID Registry," which requires message senders to register their identities to prevent spoofing; "ScamShield," a system that alerts consumers to potential scam risks; and the deployment of bank representatives at the police Anti-Scam Command office to expedite the suspension of fraudulent accounts and financial transactions.

The United Kingdom implements a similar logic through the Contingent Reimbursement Model (CRM) Code, which requires banks to reimburse consumers for authorized push payment scams and introduces friction, warning messages, and delayed transfers ("slow payment") to allow time for System 2 deliberation. Likewise, the European Union's PSD2 framework assigns shared responsibility to payment service providers by requiring strong customer authentication and permitting transaction delays when risk indicators are detected. Across these jurisdictions, the regulatory approach moves beyond consumer education and focuses on structurally altering the payment environment in ways that limit behavioral vulnerabilities—such as impulsive actions under time pressure, trust in familiar platforms, and susceptibility to persuasive reward framing—which our findings identify as primary drivers of scam victimization. This suggests that policies premised on shared institutional responsibility are likely to be more effective than those targeting individual-level awareness alone.

[6] See https://www.psr.org.uk/our-work/app-scams/

[7] See https://www.tcc.or.th/cybercrime-policy-comparative/

Reference

Bar Lev, E., Maha, L. G., & Topliceanu, S. C. (2022). Financial frauds' victim profiles in developing countries. *Frontiers in Psychology*, *13*, 999053.

Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud?. *Journal of Economic Behavior & Organization*, *198*, 250-266.

Button, M., Lewis, C., & Tapley, J. (2014). *Not a victimless crime: The impact of fraud on individual victims and their families*. Security Journal, 27(1), 36–54. https://doi.org/10.1057/sj.2012.11

Chung, E. K. H., & Yeung, D. Y. L. (2023). Reducing older people's risk of fraud victimization through an anti-scam board game. *Journal of Elder Abuse & Neglect*, *35*(2-3), 121-138.

Costa, P. T., Jr., & McCrae, R. R. (1997). *Stability and change in personality assessment: The Revised NEO Personality Inventory in the year 2000*. *Journal of Personality Assessment, 68*(1), 86–94. https://doi.org/10.1207/s15327752jpa6801_7

Cross, C. & Layt, R. (2021). "I suspect that the pictures are stolen": Romance fraud, identity crime and responding to suspicions of inauthentic identities. Social Science Computer Review. Online first: https://doi.org/10.1177/0894439321999311.

Cross, C., & Lee, M. (2022). Exploring fear of crime for those targeted by romance fraud. *Victims & Offenders*, *17*(5), 735-755.

Daengsi, T., Chomchuen, P., Klamklomchit, P., Pornpongtechavanich, P., Saribua, K., Thimthong, W., & Sukniyom, N. (2022, May). Chaladohn: Website for Avoiding of Online Shopping Scams in Thailand. In *2022 IEEE 12th Symposium on Computer Applications & Industrial Electronics (ISCAIE)* (pp. 149-152). IEEE.

Deliema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: mindsets and risky behaviors. J. Consum. Res. 46, 904–914. doi: 10.1093/jcr/ucz020

Donnellan, M. B., Oswald, F. L., Baird, B. M., & Lucas, R. E. (2006). The mini-IPIP scales: Tiny-yet-effective measures of the Big Five factors of personality. *Psychological Assessment, 18*(2), 192–203. https://doi.org/10.1037/1040-3590.18.2.192

Engels, C., Kumar, K., & Philip, D. (2020). Financial Literacy and fraud detection, *European Journal* of *Finance*, 26(4-5), 420-442.

Fan, J. X., & Yu, Z. (2021). Prevalence and risk factors of consumer financial fraud in

China. Journal of Family and Economic Issues, 43, 384–396. doi: 10.1007/s10834-021-09793-1

Ferrer-i-Carbonell, A., & Frijters, P. (2004). How important is methodology for the estimates of the determinants of happiness? *The Economic Journal*, *114*(497), 641–659. https://doi.org/10.1111/j.1468-0297.2004.00235.x

Fischer, P., Lea, S. E., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology*, *43*(10), 2060-2072.

Hadnagy, C. (2018). Transcript of "How phishing scammers manipulate your amygdala and oxytocin: Christopher Hadnagy: TEDxFultonStreet". TED.

Han, S.D., Boyle, P.A., Yu, L., & Bennett, D.A. (2016). Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease*, 49.3: 845-851.

Hapipat, T. (2024). *The situation of online fraud in Thailand: A case study of people aged 15–79 years across all regions of the country* (in Thai). Bangkok: Faculty of Economics, Chulalongkorn University. Retrieved from https://www.econ.chula.ac.th/งานวิจัยจากแหล่งทุนภาย/

Harrison, B., Vishwanath, A., Ng, Y. J., & Rao, R. (2015, January). Examining the impact of presence on individual phishing victimization. In 2015 48th Hawaii International Conference on System Sciences (pp. 3483-3489). IEEE.

Hu, B., & McInish, T. (2013). Greed and fear in financial markets: The case of stock spam e-mails. *Journal of Behavioral Finance*, *14*(2), 83-93.

Kadoya, Y., Khan, M. S. R., & Yamane, T. (2020). The rising phenomenon of financial scams: evidence from Japan. J. Financ. Crime 27, 387–396. doi: 10.1108/JFC-05-2019-0057

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kahneman, D., & Tversky, A. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124–1131.

Kim, D., & Kim, J. (2013). Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis. Online Information Review, 37(6), 835-850.

Koyame-Marsh, R. O., & Marsh, J. L. (2014). Data breaches and identity theft: Costs and responses. *IOSR Journal of Economics and Finance (IOSR-JEF)*, *5*, 36-45.

Leesa-nguansuk, S. (2025). *Thai scams rise 112% in 2024*. Bangkok Post. Retrieved from https://www.bangkokpost.com/business/general/2967346/thai-scams-rise-112-in-2024

Lyu, C., Gao, S., & Zhang, Q. (2025). The impact of time pressure and type of fraud on susceptibility to online fraud. *Frontiers in Psychology*, *16*, 1508363.

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist, 62*(14), 1957–1974. https://doi.org/10.1177/0002764218787854

Montag, C., Elhai, J. D., & Panksepp, J. (2021). A meta-analysis on individual differences in primary emotional systems and Big Five personality traits. *Scientific Reports, 11*(1), 22412. https://doi.org/10.1038/s41598-021-84366-8

Moore, T., & Anderson, R. (2011). Economics and internet security: a survey of recent analytical, empirical, and behavioral research.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives*, *23*(3), 3-20.

Nation Thailand. (2024). *More women fall victim to cybercrime than men*. Nation Thailand. Retrieved July 29, 2025, from https://www.nationthailand.com/news/general/40040102

Norris, G., & Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences*, *169*, 109847.

O'Neill, P. H. (2019). How phishing attacks trick our brains. MIT Technology Review. https://www.technologyreview.com/2019/08/08/238739/how-phishing-attacks-trick-ourbrains/

Parti, K. (2022). “Elder scam” risk profiles: Individual and situational factors of younger and older age groups’ fraud victimization. nternational Journal of Cybersecurity Intelligence and Cybercrime, 5, 20–40.

Prenzler, T. (2020). What works in fraud prevention: A review of real-world intervention projects. *Journal of Criminological Research, Policy and Practice*, *6*(1), 83-96.

Schoepfer, A., & Piquero, N.L. (2009). Studying the correlates of fraud victimization and reporting, Journal of Criminal Justice, 37(2), 209-215. DOI: 10.1016/j.jcrimjus.2009.02.003

Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults’ vulnerability to fraud. J. Elder Abuse Negl. 31, 225–243. doi: 10.1080/08946566.2019.16 25842

Smith, W. G. (2008). Does gender influence online survey participation? A record-linkage analysis of university faculty online survey response behavior. *Online submission*.

Stieger, S., Reips, U. D., & Voracek, M. (2007). Forced-response in online surveys: Bias from reactance and an increase in sex-specific dropout. *Journal of the American society for information science and technology*, *58*(11), 1653-1660.

Wang, J., Shi, J., Wen, X., Xu, L., Zhao, K., Tao, F., ... & Qian, X. (2022). The effect of signal icon and persuasion strategy on warning design in online fraud. *Computers & Security*, *121*, 102839.

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. European Journal on Criminal Policy and Research, 26, 399–409. doi: 10.1007/s10610-020-09458-z

Williams, E. J., & Polage, D. (2019). How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. Behaviour & Information Technology, 38(2), 184-197.

Zhang, Z., & Ye, Z. (2022). The role of social-psychological factors of victimity on victimization of online fraud in China, Frontiers in Psychology, 13. DOI: 10.3389/fpsyg.2022.1030670

Appendix A

Respondents' Characteristics in Phase 1

Table A.1: Respondents' Characteristics in Phase 1

Characteristics	Frequency	Percentage	Mean	Std. Dev.#
Gender				
Female	124	62.00		
Male	76	38.00		
Age			26.53	7.56
Marital status				
Single	174	87.00		
Other	26	13.00		
Employment status				
Full-time	95	47.50		
Part-time	35	17.50		
Unemployed but looking for a job	60	30.00		
Unemployed and not looking for a job	10	5.00		
Individual income (per month)				
Less than or equal THB 15,000	101	50.50		
THB 15,001-20,000	50	25.00		
THB 20,001-25,000	21	10.50		
THB 25,001-30,000	8	4.00		
THB 30,001-35,000	7	3.50		
THB 35,001-40,000	6	3.00		
THB 40,001-45,000	3	1.50		
THB 45,001-50,000	1	0.50		
More than THB 50,000	3	1.50		
Debt status				
With debt	113	56.50		
No debt	87	43.50		
Debt repayment				
Less than or equal to THB 5,000	43	38.05		
THB 5,001-10,000	23	20.35		
THB 10,001-15,000	9	7.96		
THB 15,001-20,000	6	5.31		
THB 20,001-25,000	1	0.88		
THB 25,001-30,000	3	2.65		
THB 30,001-35,000	26	23.01		
More than THB 35,000	2	1.77		

Note: Std. Dev. stands for standard deviation.

Appendix B

Additional Tests between Respondents' Characteristics and Levels of Information Disclosure

Table B.1: Chi-square test between gender and levels of information disclosure

Pearson chi2 = 3.8915

Gender	Close immediately	Without information disclosure	Level of sensitive information disclosure			Total
			Low	Medium	High	
Female						
Frequency	552	160	76	44	159	991
Row percentage	55.70	16.15	7.67	4.44	16.00	100.00
Column percentage	76.88	75.83	76.0	80.0	75.71	76.58
Male		36	20	6	37	
Frequency	115	16.82	9.35	2.80	17.29	214
Row percentage	53.74	17.06	20.0	10.91	17.62	100.00
Column percentage	16.02					15.54
Other						
Frequency	51	15	4	5	14	89
Row percentage	57.30	16.85	4.49	5.62	15.73	100.00
Column percentage	7.10	7.11	4.00	9.09	6.67	6.88
Total						
Frequency	718	211	100	55	210	1,294
Row percentage	55.49	16.31	7.73	4.25	16.23	100.00
Column percentage	100.00	100.00	100.00	100.00	100.00	100.00

Table B.2: Mean differences of age across levels of information disclosure

F-stat=1.67

Information disclosure		Average age	Standard Error
Close immediately		25.57	0.25
Without information disclosure		25.59	0.50
Level of sensitive information disclosure	Low	25.66	0.56
	Medium	27.25	1.22
	High	26.22	0.52

Table B.3: Chi-square test between education and levels of information disclosure

Pearson chi2 = 14.5359***

Educational levels	Close immediately	Without information disclosure	Level of sensitive information disclosure			Total
			Low	Medium	High	
Lower than bachelor						
Frequency	41	15	3	5	11	75
Row percentage	54.67	20.00	4.00	6.67	14.67	100.00
Column percentage	5.71	7.11	3.00	9.09	2.24	5.80
Bachelor						
Frequency	470	134	77	29	125	835
Row percentage	56.29	16.05	9.22	3.47	14.97	100.00
Column percentage	65.46	63.51	77.00	52.73	59.52	64.53
Greater than bachelor						
Frequency	207	62	20	21	74	384
Row percentage	53.91	16.15	5.21	5.47	19.27	100.00
Column percentage	28.83	29.38	20.00	38.18	35.24	29.65
Total						
Frequency	718	211	100	55	210	1,294
Row percentage	55.49	16.31	7.73	4.25	16.23	100.00
Column percentage	100.0	100.00	100.00	100.00	100.00	100.00

Note: *p < 0.10; **p < 0.05; ***p < 0.01.

Table B.4: Chi-square test between individual income and levels of information disclosure

Pearson chi2 = 42.6404*

Individual Income	Close immediately	Without information disclosure	Level of sensitive information disclosure			Total
			Low	Medium	High	
Less than or equal 15,000						
Frequency	382	98	47	29	104	660
Row percentage	57.88	14.85	7.12	4.39	15.76	100.00
Column percentage	53.20	46.45	47.00	52.73	49.52	51.00
15,001-20,000						
Frequency	154	43	27	9	48	281
Row percentage	54.80	15.30	9.61	3.20	17.08	100.00
Column percentage	21.45	20.38	27.00	16.36	22.86	21.72
20,001-25,000						
Frequency	69	31	11	7	21	139
Row percentage	49.64	22.30	7.91	5.04	15.11	100.00
Column percentage	9.61	14.69	11.00	12.73	10.00	10.74
25,001-30,000						
Frequency	39	21	7	2	10	79
Row percentage	49.37	26.58	8.86	2.53	12.66	100.00
Column percentage	5.43	9.95	7.00	3.64	4.76	6.11
30,001-35,000						
Frequency	23	10	0	4	13	50
Row percentage	46.00	20.00	0.00	8.00	26.00	100.00
Column percentage	3.20	4.74	0.00	7.27	6.19	3.86
35,001-40,000						
Frequency	22	1	5	0	5	33
Row percentage	66.67	3.03	15.15	0.00	15.15	100.00
Column percentage	3.06	0.47	5.00	0.00	2.38	2.55
40,001-45,000						
Frequency	7	1	1	1	2	12
Row percentage	58.33	8.33	8.33	8.33	16.67	100.00
Column percentage	0.97	0.47	1.00	1.82	0.95	0.93
45,001-50,000						
Frequency	7	0	0	2	3	12
Row percentage	58.33	0.00	0.00	16.67	25.00	100.00
Column percentage	0.97	0.00	0.00	3.64	1.43	0.93

Table B.4: (continued)

Individual Income	Close immediately	Without information disclosure	Level of sensitive information disclosure			Total
			Low	Medium	High	
More than 50,000						
Frequency	15	6	2	1	4	28
Row percentage	53.57	21.43	7.14	3.57	14.29	100.00
Column percentage	2.09	2.84	2.00	1.82	1.90	2.16
Total						
Frequency	718	211	100	55	210	1,294
Row percentage	55.49	16.31	7.73	4.25	16.23	100.00
Column percentage	100.00	100.00	100.00	100.00	100.00	100.00

Note: *p < 0.10; **p < 0.05; ***p < 0.01.

Appendix C

Additional Tests between Emotions, Personalities, and Levels of Information Disclosure by Reward Value

Table C.1 Mean differences of emotions by information disclosure and reward value

Emotion	Sensitive Level	Average Emotion Score		t-stat
		THB 50	THB 500	
Positive greed	Close immediately	2.34	2.34	0.00
	Without information disclosure	2.49	2.60	-1.05
	Low sensitive	2.76	2.91	-1.16
	Medium sensitive	2.91	2.84	0.47
	High sensitive	3.16	3.24	-0.81
	F-stat	33.45***	29.96***	
Negative greed	Close immediately	3.43	3.42	0.16
	Without information disclosure	3.15	3.37	-2.18**
	Low sensitive	3.16	3.25	-0.67
	Medium sensitive	3.19	2.93	1.76*
	High sensitive	2.87	2.92	-0.46
	F-stat	14.12***	10.39***	
Doubt	Close immediately	3.46	3.49	-0.47
	Without information disclosure	3.51	3.47	0.27
	Low sensitive	3.56	3.64	-0.44
	Medium sensitive	3.64	3.53	0.50
	High sensitive	3.32	3.44	-0.93
	F-stat	1.14	0.34	
Pressure	Close immediately	2.55	2.45	1.35
	Without information disclosure	2.61	2.95	-2.42**
	Low sensitive	2.98	3.23	-1.35
	Medium sensitive	3.34	2.97	1.67*
	High sensitive	3.22	3.13	0.71
	F-stat	15.83***	16.05***	
Belief in Platform	Close immediately	2.55	2.53	0.29
	Without information disclosure	2.72	2.83	-0.80
	Low sensitive	2.73	3.03	-1.70*
	Medium sensitive	3.50	3.20	1.32
	High sensitive	3.35	3.60	-1.91*
	F-stat	21.16***	25.31***	

Note: *p < 0.10; **p < 0.05; ***p < 0.01.

Table C.2 Mean differences of personalities by information disclosure and reward value

Personality	Sensitive Level	Average Emotion Score		t-stat
		THB 50	THB 500	
Extraversion	Close immediately	19.00	18.90	0.45
	Without information disclosure	19.26	19.40	-0.38
	Low sensitive	19.44	19.34	0.19
	Medium sensitive	18.50	18.73	-0.35
	High sensitive	19.24	19.05	0.44
	F-stat	0.94	0.74	
Agreeableness	Close immediately	20.70	20.46	1.15
	Without information disclosure	20.62	20.61	0.03
	Low sensitive	20.72	20.51	0.40
	Medium sensitive	18.91	20.02	-1.59
	High sensitive	20.18	20.38	-0.43
	F-stat	3.61***	0.26	
Conscientiousness	Close immediately	8.42	8.31	1.20
	Without information disclosure	8.20	8.34	-0.84
	Low sensitive	8.33	8.30	0.12
	Medium sensitive	7.80	8.27	-1.70*
	High sensitive	8.15	8.26	-0.58
	F-stat	2.96**	0.06	
Stability	Close immediately	11.19	11.16	0.22
	Without information disclosure	11.38	11.44	-0.25
	Low sensitive	11.33	11.45	-0.32
	Medium sensitive	10.80	11.17	-0.80
	High sensitive	11.39	11.43	-0.13
	F-stat	0.86	0.71	
Openness to experience	Close immediately	8.03	7.94	0.88
	Without information disclosure	8.07	8.10	-0.20
	Low sensitive	8.05	8.03	0.08
	Medium sensitive	7.81	8.07	-0.83
	High sensitive	7.88	7.90	-0.07
	F-stat	0.62	0.43	

Note: *p < 0.10; **p < 0.05; ***p < 0.01.

Appendix D

Full Regression Results

Table D.1: Full Regression Results

Variables	Ordinary Least Square Regression		Ordered Logistic Regression	
	Sensitive Levels (5 Levels) (1)	Sensitive Levels (4 Levels) (2)	Sensitive Levels (5 Levels) (3)	Sensitive Levels (4 Levels) (4)
Gender				
(Base group=Female)				
Male	-0.218**	-0.164**	-0.276*	-0.274
	(0.109)	(0.084)	(0.158)	(0.186)
Other	0.006	0.012	0.014	-0.049
	(0.151)	(0.114)	(0.236)	(0.288)
Age	0.010	0.007	0.014	0.016
	(0.007)	(0.006)	(0.011)	(0.012)
Education				
(Base group=Less than bachelor)				
Bachelor	0.126	0.100	0.161	0.315
	(0.168)	(0.129)	(0.250)	(0.327)
Higher than bachelor	0.309	0.256*	0.380	0.580
	(0.191)	(0.146)	(0.284)	(0.359)
Emotions				
Positive greed	0.230*	0.191**	0.268*	0.423**
	(0.119)	(0.095)	(0.150)	(0.190)
Negative greed	-0.324***	-0.198**	-0.480***	-0.430**
	(0.119)	(0.090)	(0.170)	(0.204)
Doubt	0.075	0.037	0.140	0.072
	(0.089)	(0.068)	(0.128)	(0.157)
Pressure	0.057	0.055	0.061	0.079
	(0.084)	(0.065)	(0.113)	(0.141)
Belief in the platform	0.102	0.095	0.098	0.155
	(0.077)	(0.062)	(0.093)	(0.124)
Personality				
(Base group=Extraversion)				
Agreeableness	-0.604	-0.277	-1.051	-0.633
	(0.490)	(0.374)	(0.658)	(0.814)
Reward value	-0.414	-0.105	-0.869	-0.506
(Base group=THB 50)	(0.439)	(0.335)	(0.625)	(0.752)
Interaction terms				
(Emotion#Personality)				
Positive greed#Agreeableness	0.0003	-0.010	0.034	-0.060
	(0.119)	(0.093)	(0.158)	(0.201)
Negative greed#Agreeableness	0.063	0.039	-0.010	-0.065
	(0.118)	(0.090)	(0.176)	(0.217)
Doubt#Agreeableness	-0.068	-0.053	-0.042	-0.018
	(0.088)	(0.067)	(0.132)	(0.163)
Pressure#Agreeableness	0.028	0.009	0.074	0.086
	(0.079)	(0.061)	(0.114)	(0.143)
Belief in the platform#Agreeableness	0.128*	0.080	0.213**	0.197
	(0.077)	(0.061)	(0.099)	(0.133)

Table D.1: (continued)

Variables	Ordinary Least Square Regression		Ordered Logistic Regression	
	Sensitive Levels (5 Levels)	Sensitive Levels (4 Levels)	Sensitive Levels (5 Levels)	Sensitive Levels (4 Levels)
	(1)	(2)	(3)	(4)
Interaction terms (Emotion#Reward value)				
Positive greed#THB 500	0.013	0.007	0.055	0.170
	(0.100)	(0.077)	(0.142)	(0.172)
Negative greed#THB 500	-0.026	-0.060	-0.019	-0.277
	(0.089)	(0.067)	(0.149)	(0.183)
Doubt#THB 500	0.042	0.048	0.019	0.081
	(0.062)	(0.047)	(0.106)	(0.130)
Pressure#THB 500	-0.044	-0.067	0.024	-0.097
	(0.064)	(0.049)	(0.099)	(0.123)
Belief in the platform#THB 500	-0.020	-0.025	0.013	0.038
	(0.058)	(0.045)	(0.086)	(0.108)
Interaction terms (Personality#Reward value)				
Agreeableness#THB 500	0.298	0.253*	0.231	0.402
	(0.197)	(0.150)	(0.272)	(0.331)
Controls	YES	YES	YES	YES
Observations	1,292	1,292	1,292	1,292
R2	0.1939	0.1807	0.0853	0.124
Threshold 1			0.372	2.026
Threshold 2			1.209	2.537
Threshold 3			1.708	2.878
Threshold 4			2.041	

Notes: # indicates an interaction term. Standard errors are in parentheses. *p < 0.10; **p < 0.05; ***p < 0.01.