University Students' Awareness and Judgment Ability Toward Different Types of Fraud

By

Hung Yi-Hsuan
洪苡瑄
Liang Yu-Chieh
梁郁婕
Wang Yu-Yun
王昱云
Ling Feng-Yu
凌鳳妤

Submitted to the Faculty of
Department of International Affairs in partial fulfillment of
the requirements for the degree of
Bachelor of Arts in International Affairs

Wenzao Ursuline University of Languages
2026

WENZAO URSULINE UNIVERSITY OF LANGUAGES
DEPARTMENT OF INTERNATIONAL AFFAIRS

This senior paper was presented

By

Hung Yi-Hsuan
洪苡瑄

Liang Yu-Chieh
梁郁婕

Wang Yu-Yun
王昱云

Ling Feng-Yu
凌鳳妤

It was defended on
November 15, 2025
and approved by

Reviewer 1: Wen-Yi Lai, Associate Professor, Department of International Affairs
Signature: _____ Date: _____
Reviewer 2: Yuan-Ming Chiao, Assistant Professor, Department of International Affairs
Signature: _____ Date: _____
Advisor: Jiang-Hong Lin, Associate Professor, Department of International Affairs
Signature: _____ Date: _____

University Students' Awareness and Judgment Ability Toward Different Types of Fraud

Hung Yi-Hsuan, B.A.
Liang Yu-Chieh, B.A.
Wang Yu-Yun, B.A.
Ling Feng-Yu, B.A.

Wenzao Ursuline University of Language, 2026

Abstract

In recent years, online fraud has become increasingly diverse and sophisticated, making university students a high-risk group. This study examined university students' awareness and judgment ability regarding job, phishing, romance, and investment scams, while investigating the influence of prior scam experiences and fraud prevention education. A total of 544 valid questionnaires were analyzed using descriptive statistics, t-tests, and ANOVA. The results showed that students' overall awareness was at a moderate level, with the highest recognition of phishing scams and the lowest of job scams. While students with prior scam experience reported slightly higher awareness, the difference was not statistically significant, suggesting that personal encounters alone may not automatically enhance vigilance. Similarly, participation in fraud prevention education did not significantly improve recognition of scams, which may reflect a gap between theoretical curricula and practical application. Based on existing literature, the findings imply that students may remain vulnerable due to factors such as emotional susceptibility, trust bias, or insufficient digital literacy, although these psychological constructs were not directly measured in this study. Future research should consider integrating psychological resilience, digital literacy, and financial intelligence into educational frameworks to more effectively address real-world fraudulent threats.

Keywords: University students, fraud awareness, fraud prevention education.

摘要

近年來，網路詐騙手段日益多樣化且複雜化，使大學生成為高風險族群。本研究旨在探討大學生對求職詐騙、釣魚詐騙、情感詐騙及投資詐騙的意識與判斷能力，並進一步分析過往受騙經驗與防詐教育對其意識水平的影響。本研究共回收 544 份有效問卷，並運用描述性統計、t 檢定及變異數分析進行資料分析。研究結果顯示，大學生的整體防詐意識處於中等水準；其中，對釣魚詐騙的辨識度最高，而對求職詐騙的意識則最低。雖然曾有受騙經驗的學生在意識得分上略高，但其差異並未達到統計上的顯著水準，這暗示僅憑個人受騙經驗未必能自動提升警覺性。同樣地，參與防詐教育亦未能顯著提升學生對求職詐騙的辨識力，這可能反映出目前理論導向課程與實務應用之間存在落差。根據現有文獻推論，研究結果隱含大學生可能因情緒易感性、信任偏誤或數位素養不足等因素而仍具脆弱性，儘管本研究並未直接測量這些心理構面。未來研究應考慮將心理韌性、數位素養及財務知能整合至教育架構中，以更有效地因應現實世界中的詐騙威脅。

關鍵字：大學生、詐騙認知、防詐教育

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

Background

In the digital era, online scams have evolved into a pressing social issue, characterized by increasing diversity and complexity. Rapid developments in communication technologies and digital platforms provide scammers with tools to design highly persuasive fraudulent schemes. According to media reports from outlets such as *Liberty Times Net*, *ETtoday News*, and *Chinatimes*, as well as local police warnings, scammers leverage technological advances to create deceptive phishing websites, romance scams, and high-return investment scams. While phishing tactics often mimic official platforms like Chunghwa Telecom, romance and investment scams exploit online social interactions to deceive victims. Given their frequent reliance on digital platforms and potentially limited life experience, university students are often regarded as a vulnerable group prone to significant financial and psychological distress.

To address this, Taiwan's Ministry of Education mandates that schools enhance cybersecurity and anti-fraud education. For instance, Wenzao Ursuline University of Languages incorporates anti-fraud topics into its military education curriculum. While such measures aim to advance protective knowledge, the ever-evolving nature of fraud tactics presents a persistent challenge. The observation that some students still fall victim after receiving formal training may suggest a potential gap between theoretical instruction and practical application—a phenomenon that underscores the need for further investigation into the effectiveness of current curricula.

Motivation

The primary motivation of this study is to explore the underlying reasons why

university students remain susceptible to fraud despite receiving institutional education. By identifying specific areas where students lack understanding, this research seeks to provide insights into how risk awareness can be more effectively cultivated, ultimately reducing the likelihood of victimization.

Research Purpose

The purpose of this study is to examine university students' awareness and judgment regarding different types of scams, specifically focusing on how prior experiences and anti-fraud education influence their ability to identify and prevent fraud.

Research Questions

Question 1: What are university students' awareness of different types of fraud?

Question 2: Did prior experience with scams significantly influenced college students' awareness of scams?

Question 3: Did participation in fraud prevention education significantly improve university students' awareness and ability to recognize different types of fraud?

Contribution

This study contributes to the growing body of research on cyber fraud by specifically examining university students' awareness, understanding, and preparedness against online scams. It highlights the current effectiveness of anti-fraud education and provides insights into its practical limitations from the students' perspectives. The findings can inform educators, policymakers, and institutions on how to tailor preventive strategies and educational programs that are more relevant

and impactful. Moreover, by identifying specific areas for improvement, the research supports the development of targeted interventions that enhance students' critical thinking and digital literacy, ultimately reducing their vulnerability to online fraud.

Limits

Despite its contributions, this study has certain limitations. First, this research relies on self-reported survey data, which may be subject to recall bias or social desirability bias. Second, the sample may not fully represent the entire diversity of the student population across different socio-economic backgrounds or academic disciplines. Third, the rapid evolution of cyber scams means the findings reflect a specific snapshot in time. Finally, while the study acknowledges the role of psychological factors, it does not directly measure constructs such as emotional susceptibility or personality traits.

Delimits

This study is delimited to university students, with a specific focus on their awareness and experiences related to online scams. It did not include other demographics such as high school students, working adults, or elderly populations. Furthermore, the scope is restricted to educational and preventive aspects of cyber fraud, rather than law enforcement responses or technological countermeasures. The study also concentrates on job scams, phishing scams, romance scams, and investment scams. These boundaries maintain a focused and manageable scope aligned with the study's objectives and resource allocation.

LITERATURE REVIEW

Introduction

In the digital era, online fraud has evolved into a complex social issue characterized by the diversification of scam techniques. Modern fraudsters often blend technological deception with psychological manipulation to exploit vulnerable populations. This study examines university students' awareness of four major fraud types: job scams, phishing scams, romance scams, and investment scams. These categories were selected because they are frequently reported among young adults and consistently highlighted in crime statistics. Given their heavy reliance on digital platforms and relatively nascent financial experience, university students face a heightened risk of falling victim to these evolving threats.

The Complexity of Cyber Fraud and Young Adults' Vulnerability

Current internet scams combine technological tools, such as counterfeit websites, with emotional manipulation tactics like fear and time pressure. These strategies aim to cause victims to make erroneous judgments under emotional turmoil, suggesting that fraud is as much a psychological challenge as a technical one.[1]

Research indicates that social media is a primary channel for fraud targeting individuals aged 18–29.[2] While young people use these platforms daily, they often lack sufficient life experience to identify sophisticated deceptive tactics, such as anonymous fake accounts. This vulnerability may be related to a tendency to trust seemingly authentic information without critical verification. According to the

[1] Ntogwa Ng'habi Bundala, "Cybercrime: Psychological Tricks and Computer Securities Challenges," *Asian Journal of Research in Computer Science* 17, no. 12 (2024).
[2] E Fletcher, "Social Media: A Golden Goose for Scammers," (Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers, 2023).

UNODC, anonymity allows criminals to conceal their identities, posing significant obstacles to investigations.[3] Furthermore, a report by PYMNTS highlights that 82.9% of young people have been deceived by suspicious links, indicating substantial difficulty in identifying fraudulent messages in real-time.[4]

The Limitations of Current Campus Anti-Fraud Education

Despite active promotion of online safety, many students continue to fall victim to scams, suggesting that existing educational models may face challenges in practical application. For example, while programs like those at Wenzao Ursuline University cover extensive information, the persistence of fraud cases indicates a possible gap between theoretical knowledge and situational judgment.

As Bartlett and Miller pointed out, many young adults may "trust the first thing they see," making them vulnerable to cons and scams.[5] Currently, most university anti-fraud initiatives focus on theoretical explanations. While students may understand the basic concepts of fraud, they may struggle to apply this knowledge when confronted with complex, real-life scenarios.

The Role of Financial Literacy in Fraud Prevention

Financial literacy serves as a critical protective factor. In 2024, 44% of fraud cases in the United States involved individuals aged 20–29, highlighting an urgent need for strengthened financial education.[6] Research in the *Journal of Financial*

[3] United Nations Office on Drugs and Crime., "Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations.," https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html.
[4] PYMNTS., "Report: 82.9% of Young Adults Have Been Tricked by Suspicious Links.," (2025).
[5] Jamie Bartlett and Carl Miller, "Truth, Lies and the Internet: Exploring Digital Fluency," *School Librarian* 60, no. 1 (2012).
[6] Yoke Mui Choy, and Noor Hayati Che Man, "Analysis of Fraudulent Transactions Using Data Mining Technique," *Journal of Financial Crime* 29, no. 2 (2021).

Crime indicates that students proficient in budgeting and financial planning are significantly more vigilant in identifying investment fraud.[7] However, simply having financial goals without a solid understanding of scam operations offers limited protection, emphasizing that awareness must be paired with critical evaluation skills.

Integrating Psychological and Practical Perspectives

To better prepare students, educational institutions must move toward integrated preventive measures. Organizations like Netsafe emphasize that effective education should integrate psychological, social, and economic factors. Research suggests that utilizing social network dynamics and psychological analysis can provide a more comprehensive defense.[8]

Since fraud often targets emotional weaknesses such as greed, fear, or a desire for belonging educational models should include simulations that cultivate emotional recognition and risk assessment. For students managing finances independently for the first time, instilling disciplined budgeting habits and skepticism toward "high-return" promises is essential.[9] Strengthening fraud prevention education is not only about information dissemination but also about fostering a smart digital user community through critical thinking.[10]

---

[7] Hazlina Mohd Padil et al., "Financial Literacy and Awareness of Investment Scams among University Students," ibid.29, no. 1 (2022).
[8] Arshad Hussain Bhat and Durgeshwary Kolhe, "Crime and Fraud at the Community Level: Social Networking Understanding into Economic Crimes and Psychology Motivations," *Journal of Social Sciences and Economics* 3, no. 2 (2024).
[9] Mohd Padil et al., "Financial Literacy and Awareness of Investment Scams among University Students."
[10] ESU ENIC-NARIC and European Students' Union, "Knowledge and Awareness of Fraud in Education: A Student Perspective," (2025).

Theoretical Models of Fraud Vulnerability

This study adopts a multifaceted theoretical framework to analyze fraud vulnerability. As Button, Lewis, and Tapley noted, fraudulent behavior often exploits a combination of psychological vulnerability, social context, and economic conditions.[11] The following four theories provide the foundation for this research:

Psychological manipulation theory

This theory explores how fraudsters use emotional appeals to influence decisions. Robert Cialdini's principles such as social proof, authority, and scarcity explain how psychological pressure can lead to irrational decision-making.[12]

A study by K. Kircanski, N. Notthoff, M. DeLiema, G.R. Samanez-Larkin, D. Shadel, and G. Mottola found that Strong emotional arousal can significantly increase susceptibility to fraud, particularly during the transitional life stage of university students.[13] Therefore, studying emotional arousal may help identify situations where individuals are particularly vulnerable to fraud. This is especially true for university students, who are undergoing significant emotional and social changes, making them particularly susceptible to emotional manipulation. Their emotional responses during this transitional phase make them attractive targets for fraudulent schemes.

Social engineering theory

Social engineering involves the manipulation of trust or social norms to deceive individuals into disclosing sensitive information.[14] This fraud tactic involves impersonating trusted entities (such as friends, family, or financial institutions) to

[11] Mark Button, Chris Lewis, and Jacki Tapley, "Fraud Typologies and the Victims of Fraud: Literature Review," (2009).
[12] Robert B Cialdini, *Influenced: Science and Practice*, vol. 4 (Pearson education Boston, 2009).
[13] Katharina Kircanski et al., "Emotional Arousal May Increase Susceptibility to Fraud in Older and Younger Adults," *Psychology and aging* 33, no. 2 (2018).
[14] Fatima Salahdine and Naima Kaabouch, "Social Engineering Attacks: A Survey," *Future internet* 11, no. 4 (2019).

deceive victims into sharing personal details or transferring funds.

University students are often susceptible to these attacks because of their high level of trust in social networks and informal online communication. This theory explains why social engineering fraud is especially common among university students, as they often lack the judgment to recognize these fraud schemes. Therefore, understanding the patterns of social engineering attacks is crucial for students. Learning to verify the identity of others and question unusual requests can significantly reduce the success rate of such scams.

Phishing website scam theory

Phishing fraud theory studies how fraudulent websites imitate legitimate platforms to steal sensitive information. These tactics include fake URLs, misleading emails, and deceptive web interfaces that appear to be authentic. Rick Wash mentioned in his research that Phishing involves using fraudulent websites or emails to steal personal credentials. Experts note that these scams often trick recipients into taking actions they normally would not.[15]

Because college students use digital services extensively, they are particularly vulnerable to phishing attacks due to their lack of digital knowledge and tendency to trust online sources. Their lack of experience in detecting subtle signs of fraud increases the risk of them providing their personal credentials to malicious actors.

Enhancing digital literacy and skepticism toward unsolicited communications is crucial for students to recognize these deceptive interfaces.[16]

[15] Rick Wash, "How Experts Detect Phishing Scam Emails," *Proceedings of the ACM on Human-Computer Interaction* 4, no. CSCW2 (2020).
[16] Chusnu Syarifa Diah Kusuma and Riana Isti Muslikhah, "Strengthening of Digital Literacy to Support Student Community Service to Prevent Hoax and Cybercrime" (paper presented at the 9th International Conference on Education Research, and Innovation (ICERI 2021), 2022).

Financial investment risk theory

This theory focuses on cognitive biases and the lack of financial knowledge. In their research, Steven James Lee, Benjamin F. Cummings, and Jason Martin identified that scammers often use persuasive language to construct authenticity or claim authority, promising high returns with minimal risk.[17]

As Lusardi and Mitchell stated, financial literacy is closely linked to the ability to avoid fraudulent schemes, underscoring the protective role of specialized financial education.[18] Therefore, developing students' financial literacy is the best way to prevent fraud. Comprehensive education should include risk assessment, analysis of investment returns, and skepticism toward unrealistic profit promises.

Summary of Theoretical Insights into College Students' Vulnerability to Internet Fraud

By combining these four theories, this study comprehensively analyzes how emotional manipulation, social trust, digital habits, and financial literacy gaps contribute to student vulnerability. This multifaceted framework provides a solid theoretical foundation for examining the factors that influence students' awareness and decision-making in fraudulent situations.

Cognitive Bias and Fraud Vulnerability in University Students

When encountering fraudulent information, university students may lack sufficient social experience, making them susceptible to cognitive biases that hinder

[17] Steven James Lee, Benjamin F Cummings, and Jason Martin, "Victim Characteristics of Investment Fraud" (paper presented at the 2019 Academic Research Colloquium for Financial Planning and Related Disciplines, 2019).
[18] Annamaria Lusardi and Olivia S Mitchell, "Financial Literacy and Retirement Planning: New Evidence from the Rand American Life Panel," (CFS working paper, 2007).

their ability to recognize scams. A study on SMS fraud in the United States observed that younger individuals and college students emerged as highly vulnerable, often struggling to identify legitimate messages even when they possessed an account with the impersonated entity.[19] Despite the promotion of anti-fraud education, a persistent "knowledge-behavior gap" exists, suggesting that awareness does not always translate into protective action.

A Multidimensional Exploration of College Students' Susceptibility to Fraud

Previous studies suggest that university students may experience emotional and cognitive vulnerabilities. In this study, four theoretical perspectives are used to contextualize and interpret the findings: emotional and cognitive vulnerability, trust bias in social engineering, digital literacy related to phishing, and financial literacy related to investment scams. These perspectives serve as interpretive frameworks from existing literature rather than variables directly measured by the survey.

College Students' Emotional and Cognitive Vulnerabilities

Theoretical frameworks suggest that students' decision-making can be compromised by emotional arousal. According to Psychological Manipulation Theory, scammers use stress and urgency to trigger irrational responses. As Cialdini notes, individuals often deceive themselves to maintain consistency with prior decisions, which can reduce critical judgment during an emotional encounter.[20] For university students, this transitional life stage may heighten susceptibility to such emotional manipulation.

[19] Cori Faklaris, Heather Richter Lipford, and Sarah Tabassum, "Preliminary Results from a Us Demographic Analysis of Smish Susceptibility," *arXiv preprint arXiv:2309.06322* (2023).
[20] Cialdini, *Influenced: Science and Practice*, 4.

Trust Bias and Social Engineering Scams

Social engineering exploits the human tendency to trust familiar or authoritative sources. Scammers often impersonate friends, family, or institutions to obtain sensitive information.[21] Because university students generally report higher levels of social trust and rely heavily on peer networks, they may lower their guard when confronted with trust-based deceptions.

Lack of Information Literacy and Digital Scam Risks

While students are "digital natives," high usage frequency does not necessarily equate to high security literacy. Fraudsters utilize counterfeit URLs and deceptive interfaces to exploit those with lower cybersecurity awareness.[22] The tendency to browse information rapidly without verifying sources increases the risk of falling for sophisticated digital scams.

Insufficient Financial Literacy and Vulnerability to Investment Scams

As students begin to manage their finances independently, they become targets for scams promising "high returns with low risk." Scammers use persuasive language to lower victims' defenses, such as creating an atmosphere of success, showing authority, or appealing to noble goals Lee, Cummings, and Martin pointed out that scammers use five techniques: perceived success, familiarity, authority claimed, noble pursuits, and constructed authenticity to reduce victims' vigilance.[23] Literature

[21]Fatima Salahdine and Naima Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet* 11, no. 4 (2019).
[22]Niklas Särökaari, "Phishing Attacks and Mitigation Tactics," [Cost Calculation of a Concert.] (2020).
[23] Benjamin F. Cummings Steven James Lee, and Jason Martin, "Victim Characteristics of Investment Fraud," (2019).

suggests that while financial goals are common among students, a lack of deep financial knowledge makes them particularly vulnerable to these persuasive tactics.

Conceptual Framework and Research Significance

The susceptibility of adolescents and young adults to online fraud is a critical area of study due to their high digital engagement and emerging financial independence. Research underscores that financial knowledge is a significant predictor of fraud detection; for instance, increased knowledge has been linked to a higher probability of identifying fraudulent schemes.[24] This finding underscores the importance of addressing financial education among young people, who often demonstrate gaps in these critical skills.

Finkelhor et al. further emphasize the importance of aligning youth safety education with actual internet usage behaviors. They state that "messages of youth internet safety education programs must reflect both the dynamics of internet dangers and the efficacy of youth prevention education." This suggested that targeting adolescents with tailored education and policy interventions is essential for mitigating their fraud risk.[25]

Methods Found in Related Studies on Cyber Fraud

Prior research on susceptibility to cyber fraud has predominantly utilized qualitative approaches and structured surveys to examine individual behavioral patterns and lived experiences. In particular, qualitative interviews have proven effective for uncovering victims' emotional and cognitive reactions to fraudulent

[24] Christian Engels, Kamlesh Kumar, and Dennis Philip, "Financial Literacy and Fraud Detection," in *Financial Literacy and Responsible Finance in the Fintech Era* (Routledge, 2021).
[25] David Finkelhor et al., "Youth Internet Safety Education: Aligning Programs with the Evidence Base," *Trauma, violence, & abuse* 22, no. 5 (2021).

encounters, offering access to complex internal processes.[26] Although surveys are valuable for identifying general trends, they often fall short in reflecting intricate relationships involving digital literacy, peer dynamics, and fraud awareness. This methodological tendency underscores the rationale for adopting a mixed-method approach in the present study. Furthermore, comprehensive literature reviews have reaffirmed that digital literacy plays a crucial protective role in scam prevention, pointing to the importance of integrating psychological attributes with digital engagement in future research.[27] This highlights a growing recognition of the interplay between technical skills and emotional resilience, emphasizing the need to explore not only what people know, but also how they react in high-pressure digital scenarios.

Scholarly exploration of fraud awareness has frequently stemmed from psychology, sociology, and digital communication, with these fields collectively endorsing a qualitative lens for interpreting how individuals make decisions in deceptive digital contexts. Rather than treating behavior as purely rational, these approaches emphasize the emotional and situational factors influencing responses to fraud. For example, the article demonstrated how emotional arousal and social engineering strategies influenced victims' responses, uncovering underlying psychological patterns in the context of online deception.[28] These findings support the argument that understanding user behavior in online scams requires insights beyond statistical analysis alone.

A recent PLOS ONE study further confirms that psychological and social factors,

---

[26] Marcia J. Bates, "Fundamental Forms of Information," *Journal of the American Society for Information Science and Technology* (Vol. 57, No. 8 (2007)).
[27] Gözde Topal Arslan Murat Yıldırım, "Examining the Role of Resilience and Hope in Predicting Psychological Distress and Life Satisfaction among University Students During the Covid-19 Pandemic," *PLOS ONE* Volume 19, Issue 4 (2024).
[28] Bates, "Fundamental Forms of Information."

such as overconfidence and peer influenced, significantly affect susceptibility to cyber fraud. It utilized a structural equation modeling approach, combining quantitative self-report data with psychological constructs, supporting a hybrid methodological framework.[29] The integration of such quantitative techniques with psychological insights showeds how complex variables can be measured systematically while still accounting for subjective experiences.

The increasing sophistication of digital fraud has prompted researchers to focus more on the role of digital literacy in prevention. According to a recent review, there is a growing emphasis on interdisciplinary frameworks that merge areas such as behavioral economics and user-interface studies to better understand user susceptibility.[30] In light of these findings, there is a strong push for future studies to adopt mixed-method and longitudinal approaches, allowing for deeper insights across varied digital environments. This shift confirms that capturing the complexity of online fraud requires more than one methodological tool, encouraging the integration of qualitative, behavioral, and technical analyses into unified research models.

Quantitative research method as the Methodological Approach

This study adopted a quantitative research method to identify overall patterns of fraud awareness among university students. The approach was selected to allow for statistical comparison across different scam types and between groups with varying experiences and educational exposure.

[29] Murat Yıldırım, "Examining the Role of Resilience and Hope in Predicting Psychological Distress and Life Satisfaction among University Students During the Covid-19 Pandemic."
[30] Muhammad Adnan Pitchan、Ali Salman、Nadhirah Muhamad Arib, "A Systematic Literature Review on Online Scams: Insights into Digital Literacy, Technological Innovations, and Victimology," *Jurnal Komunikasi: Malaysian Journal of Communication* Volume 41, Issue 1 (March 2025).

While prior research has emphasized the importance of psychological, emotional, and social factors in fraud vulnerability, the present study did not directly measure these constructs. Instead, the quantitative design focused on observable awareness indicators derived from questionnaire responses. Psychological and social factors discussed in this study therefore serve as interpretive contexts informed by existing literature, rather than as empirically tested variables.

Michael Rich and Kenneth R. Ginsburg have noted that while research methods have different strengths and limitations, quantitative data remains essential in identifying statistically significant trends and generalizing findings. This study seeks to explore how college students identify, interpret, and respond to online fraud messages, while analyzing the psychological and social factors that influenced their behavioral decisions.[31] This study seeks to explore how college students identify, interpret, and respond to online fraud messages, while analyzing the psychological and social factors that influenced their behavioral decisions.

Conclusion

In summary, university students face vulnerabilities across four primary domains: psychological (emotional pressure), social (trust bias), digital (information verification skills), and financial (investment knowledge). Current campus initiatives often emphasize theoretical explanations, which may account for the observed discrepancy between students' conceptual knowledge and their practical responses in real-life situations.

[31] Michael Rich and Kenneth R Ginsburg, "The Reason and Rhyme of Qualitative Research: Why, When, and How to Use Qualitative Methods in the Study of Adolescent Health," *Journal of Adolescent health* 25, no. 6 (1999).

Drawing from previous research and the observed gaps in student awareness, future educational initiatives should consider developing integrated, practical mechanisms that combine training in psychological resilience, digital literacy, and financial intelligence. Although this study did not directly measure these specific psychological dimensions, literature suggests they are essential for a holistic strategy that addresses both the cognitive and emotional aspects of fraud prevention. Consequently, this research provides a quantitative foundation for designing more comprehensive anti-fraud programs in higher education.

METHODOLOGICAL APPROACH

Introduction

The purpose of this chapter is to describe the methodology used in this study to examine the vulnerability of university students to Internet fraud. Based on the insights gained from the literature review, this chapter describes the research design, data sources, research instruments, analytical techniques, and ethical considerations. In recent years, there has been an increase in the number of Internet fraud cases targeting the college student population, a phenomenon that has raised concerns among educational institutions and policy makers. But even though many college students have been exposed to anti-fraud education in their schools, they are still victimized by cognitive biases, emotional vulnerability, and a lack of critical digital literacy.

Therefore, our study analyzes university students' correct knowledge of Internet fraud and their ability to counteract fraud through questionnaire surveys and data analysis.

Research Design

This study employed a quantitative research design to examine university students' awareness of different types of online fraud. The focus was placed on measuring students' recognition and understanding of common scam characteristics rather than directly assessing psychological traits or emotional responses. Given the research objective focused on quantifying students' cognitive levels rather than exploring individual experiences, a qualitative research design was not adopted.

Convenience sampling was employed due to time constraints and accessibility considerations. To minimize potential bias, respondents were drawn from diverse

major, income, location and age, enhancing the reliability and generalizability of the findings. Three key variables were examined through a structured questionnaire, including anti fraud awareness, past victimization experience, and participation in anti fraud education. The awareness items were developed based on existing theoretical and empirical studies and focused on students' ability to identify common scam features embedded in job, phishing, romance, and investment fraud scenarios. Although prior literature has discussed emotional and cognitive factors related to fraud vulnerability, these psychological constructs were not operationalized as measurable variables in the present study.

Sources of Data

This study collected data from Taiwanese university students between the ages of 18 and 25. All participants were university students in Taiwan, including both native and foreign students. To ensure relevance to the topic, participants were required to have basic digital literacy and familiarity with online environments. The sampling method adopted was convenience sampling, which allowed us to efficiently recruit participants through university forums, student networks, and social media platforms. A total of around 650 students were invited, and 544 completed the full questionnaire. The sample included students from a variety of academic disciplines and year levels, ensuring diversity in background and perspectives. This approach helped improve the representativeness and applicability of the findings within the context of Taiwanese university students.

Research Instrument and Data Collection

The primary tool for data collection was a structured questionnaire designed to

explore participants' experiences with and awareness of online scams. The questionnaire included three main sections: (1) demographic information such as age, gender, field of study; (2) personal experiences with online fraud, including types of scams encountered and responses; and (3) understanding and awareness of different online scam tactics. A five-point Likert scale (1 = strongly disagree, 5 = strongly agree) was used to measure levels of agreement with specific statements.

The survey focused on four common scam categories: investment fraud, job scams, romance scams, and phishing. To ensure content validity and appropriateness, the questionnaire was reviewed by academic experts and pilot tested with a small group of students. Data collection was conducted online via Google Forms, allowing for convenient and anonymous participation.

Questionnaire items were developed based on prior research on online fraud awareness and incorporated validated digital literacy and anti-fraud awareness scales, along with scenarios reflecting college students' common vulnerabilities. The finalized questionnaire comprised four sections: (1) basic information; (2) past scam experiences; (3) participation in anti-fraud education; and (4) awareness of the four scam types. The awareness section contained 20 items rated on the five-point Likert scale.

Data Analysis Technique

This study employed the statistical software SPSS (Statistical Package for the Social Sciences) as the primary tool for data analysis. SPSS was chosen for its ability to efficiently manage and analyze large-scale questionnaire data in a systematic and reliable manner. The software was used to generate statistical outputs and summary tables that supported accurate interpretation of the results.

All questionnaire items were measured using a 5-point Likert scale ranging from

1 (strongly disagree) to 5 (strongly agree). Items were grouped according to four types of scam awareness: phishing scams, job scams, romance scams, and investment scams. Composite scores were calculated by summing item responses within each category, with higher scores indicating higher levels of scam awareness. All items were positively worded, and therefore no reverse coding was required.

The data analysis process involved several key stages. First, descriptive statistics were used to summarize respondents' basic characteristics and overall awareness levels, including frequency, percentage, mean, and standard deviation. Second, reliability analysis was conducted using Cronbach's alpha to examine the internal consistency of each scam awareness scale. Finally, inferential statistical tests, including independent sample t-tests and one-way analysis of variance (ANOVA), were applied to examine whether scam awareness differed significantly based on prior scam experience and participation in fraud prevention education.

Ethical Considerations

The research followed strict ethical guidelines to protect all participants. Participation in the study was voluntary, and informed consent was obtained from every respondent. The purpose of the study and how the data would be used were clearly explained to all participants before they joined. All collected data were treated as confidential and stored in the files that only the research team could access. No ethical risks were found. This careful process ensured that participants' rights and privacy were respected throughout the research.

Limitations of the Methodology

The main limitation of this study is the use of a self-administered questionnaire,

which may affect the authenticity of the data due to memory bias or social desirability. In addition, the convenience sampling was mainly based on college students, which limits the inference of the results to the overall young population. The study also did not explore the psychological and emotional aspects of vulnerability to fraud, and the lack of qualitative data makes it difficult to understand individual behavior.

Tools for Data Analysis

Based on the research objectives, this study adopted a quantitative approach to analyze the data collected through questionnaires. To effectively process and interpret the survey results, SPSS (Statistical Package for the Social Sciences) was used as the primary tool for data analysis.

The analysis was conducted at two levels. The first level involved descriptive statistical analysis, including measures such as mean, standard deviation, percentage, and frequency distribution. These statistics were used to present a clear profile of the participants' demographic characteristics (such as age, gender, field of study, and internet usage habits), as well as their experiences and awareness related to online fraud. This helped to identify general patterns and provide an overview of participants' responses.

The second level of analysis applied inferential statistical methods. Specifically, Pearson correlation analysis was used to examine relationships between key variables, such as the frequency of social media use and susceptibility to online scams. In addition, regression analysis was conducted to explore whether certain factors (e.g., digital behavior, fraud awareness level) could significantly predict an individual's vulnerability to online fraud.

In summary, SPSS allowed for a systematic and objective analysis of the

quantitative data. By using both descriptive and inferential statistics, the study was able to identify key trends and draw evidence-based conclusions about the factors influencing Taiwanese university students' risk of encountering cyber fraud.

Summary

This chapter systematically outlines the research methodology employed to explore the vulnerability of young adults to cyber fraud. It begins by presenting the rationale for adopting a quantitative descriptive research design, which enables the identification of key patterns and relationships among variables within the target population.

Data were collected from 544 university students in Taiwan using convenience sampling. A structured questionnaire was developed to assess participants' demographics, exposure to online scams, and perceived susceptibility to fraud. To ensure the instrument's reliability and validity, the questionnaire underwent expert review and pilot testing.

We want to look at their feelings, their trust in others, and also how much they know about internet and money. using descriptive statistics to summarize general trends, and inferential statistical methods, including T-tests and ANOVA, to examine significant relationships among key variables.

All ethical considerations were carefully observed. Informed consent was obtained from all participants, and data confidentiality was strictly maintained throughout the research process. The study also acknowledges potential limitations, such as response bias and the constraints of non-probability sampling, which may affect the generalizability of the findings. A clear and structured timeline was followed to ensure the efficient execution of the study.

Overall, the methodology provided a rigorous and ethical foundation for addressing the research objectives and contributed valuable quantitative insights into the online fraud experiences and susceptibility of young adults.

DATA ANALYSIS

Introduction

The study nvestigatesd university students' awareness and judgment ability regarding different types of fraud, including job scams, phishing scams, romance scams, and investment scams. By examining their knowledge and experiences, the research seeks to identify the factors that shape students' ability to recognize fraudulent schemes and the role of preventive education. The study aimed to answer three key questions: (1) What are university students' awareness of different types of fraud, (2) Did prior experience with scams significantly influenced college students' awareness of scams, and (3) Did participation in fraud prevention education significantly improve university students' awareness and ability to recognize different types of fraud?.

Data Collection Profile

The survey was disseminated through a range of online platforms, including Instagram, Dcard, LINE, and Email, to broaden outreach and capture participation from diverse social groups. By employing widely used communication channels, the study aimed to enhance representativeness and mitigate sampling bias associated with reliance on a single medium. All responses were collected via Google Forms and securely stored in digital format, with confidentiality and data protection measures strictly enforced. Administered in May 2025, the close-ended survey generated 544 valid responses, slightly below the initial target of 650, yet still providing a sufficiently large and diverse sample for analysis.

To assess internal consistency, reliability analysis was conducted using Cronbach's Alpha. The results yielded values of .537 for phishing scams, .459 for job

scams, .507 for romance scams, and .513 for investment scams. While these figures fall below the conventional .70 threshold, the lower reliability likely stems from the limited number of items per scale and the inherent heterogeneity of scam scenarios. Consequently, these findings should be interpreted with caution as preliminary trends in awareness rather than robust psychological measurements.

The "Basic Information" section collected demographic variables such as gender, age, monthly income, current school location, major, experiences with fraud, and participation in fraud prevention education programs. Among the respondents, 40.8% were aged 21–23, 32.9% were aged 18–20, and 26.3% were aged 24 or above, suggesting that the largest proportion of the sample fell within early adulthood. Females constituted a slight majority (52.4%), while males accounted for 47.6%, ensuring a relatively balanced gender distribution. Most respondents reported relatively lower monthly earnings, reflecting the socioeconomic background of the participants. Regarding prior experiences, 251 respondents (46.1%) had encountered fraud, while 293 (53.9%) had not. In terms of fraud prevention education, 31.8% had received such training on campus, 24.4% off campus, 23.2% in both settings, and 19.7% had never participated in any related programs. Taken together, these findings highlight that the sample consisted primarily of young and relatively low-income individuals, many of whom had prior exposure to fraud and varying levels of experience with fraud prevention programs.

Mean Score of University Students' Fraud Awareness

After data screening, a total of 544 valid responses were collected from university students. The questionnaire evaluated students' awareness of four major types of online scams, including job scams, phishing scams, romance scams, and investment

scams. Each dimension consisted of five items rated on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree).

To provide a general overview of students' overall awareness before addressing the research questions, the average scores of the four scam dimensions were summarized using descriptive statistics in SPSS. This approach offers a concise and intuitive understanding of participants' overall awareness levels toward different scam types.

Table 1 presents the overall mean and standard deviation for each dimension. The results indicated that participants demonstrated a moderate to high level of awareness across all four scam categories, with phishing scam awareness showing the highest mean score among them.

Table 1. Mean Scores of University Students' Scam Awareness

Factor	Mean	Std. Deviation
Job scam awareness	3.607	0.818
Phishing scam awareness	3.655	0.752
Romance scam awareness	3.640	0.790
Investment scam awareness	3.646	0.801

University Students' Awareness of Different Types of Fraud

RQ1: What are university students' awareness of different types of fraud?

To further examine Taiwanese college students' awareness and judgment regarding different types of fraud, descriptive statistical analyses were conducted on the four fraud-related dimensions using mean scores. The dimensions included Job Scam Awareness, Phishing Scam Awareness, Romance Scam Awareness, and Investment Scam Awareness, each calculated as the mean of five items. Descriptive statistics that included the number of valid responses, minimum, maximum, mean, and standard

deviation were computed to provide a quantitative overview of students' overall awareness and vigilance toward each type of fraud. The mean score range from 1 to 5 on the Likert scale. Higher mean scores indicated stronger recognition of fraudulent behaviors and greater caution in evaluating potential risk situations. The results are presented in Table 2.

As shown in Table 2, the highest mean score was observed for Phishing Scam Awareness (M = 3.6551, SD = 0.75219), suggesting that students were relatively more alert to phishing scams. The next highest means were for Investment Scam Awareness (M = 3.6456, SD = 0.80146) and Romance Scam Awareness (M = 3.6397, SD = 0.78955), while Job Scam Awareness (M = 3.6070, SD = 0.81831) was the lowest. Overall, students' awareness of different types of fraud was generally moderate to slightly above average. Standard deviations ranged from 0.75219 to 0.81831, reflecting a moderate degree of variation in participants' perceptions and vigilance across the four types of fraud.

Table 2. Descriptive Statistics of University Students' Scam Awareness

Factor	Mean	Std. Deviation	Min	Max
Job scam awareness	3.6070	0.8183	1.00	5.00
Phishing scam awareness	3.6551	0.7521	1.00	5.00
Romance scam awareness	3.6397	0.7895	1.00	5.00
Investment scam awareness	3.6456	0.8014	1.00	5.00

Prior Experience with Scams Influenced Students' Awareness of Fraud.

RQ2: Did prior experience with scams significantly influenced college students' awareness of scams?

An independent samples t-test was conducted to examine whether prior experience with scams influenced college students' awareness across four scam awareness factors. As shown in Table 3 and Table 4, Levene's test indicated that the assumption of equal variances was met for all factors ($p > .05$).

These results indicated that prior experience with scams did not significantly influenced students' awareness of scams on any of the four measured factors. Although students with scam experience generally had slightly higher mean scores, these differences were not statistically significant. This suggested that having prior scam experience alone may not be sufficient to enhance students' scam awareness, highlighting the potential importance of formal education or training for improving anti-fraud knowledge.

Table 3. Independent Samples t-Test Results for Scam Awareness by Scam Experience

	Student With Scam Experience		Student Without Scam Experience				
Type	M	SD	M	SD	t(542)	p	Significance
Job scam awareness	3.658	0.797	3.577	0.839	1.155	.249	Not significant
Phishing Scam Awareness	3.675	0.742	3.639	0.764	0.565	.572	Not significant
Romance Scam Awareness	3.694	0.765	3.593	0.812	1.479	.140	Not significant
Investment Scam Awareness	3.647	0.800	3.646	0.806	0.016	.987	Not significant

Table 4. Levene's Test and Independent Samples t-Test Results for Scam Awareness by Scam Experience

		Levene's Test for Equality of Variances		T-test for equality of means		
		f	Sig.	t	df	Sig.
Job scam awareness	Equal variances assumed	0.746	0.388	1.155	542	0.249
Phishing scam awareness	Equal variances assumed	0.048	0.828	0.565	542	0.572
Romance scam awareness	Equal variances assumed	0.330	0.566	1.479	542	0.140
Investment scam awareness	Equal variances assumed	0.204	0.662	0.016	542	0.987

Participation in Fraud Prevention Education Improved Students' Awareness and Ability to Recognize Different Types of Fraud.

RQ3: Did participation in fraud prevention education significantly improve university students' awareness and ability to recognize different types of fraud?

Based on the descriptive statistics conducted for Research Question 1, university students demonstrated relatively lower awareness of job scams compared to other types of fraud (see Table 2). Therefore, Job Scam Awareness was selected as the primary focus to examine whether participation in fraud prevention education could effectively enhance students' ability to recognize this type of fraud. Participants were categorized into five groups according to their responses regarding fraud prevention education: (1) Yes, on campus; (2) Yes, off campus; (3) Yes, both; (4) Not accepted; and (5) Don't remember. A one-way ANOVA was then conducted, with Job Scam as the dependent variable, to assess whether the mean scores significantly differed across the five groups. The results of this analysis are summarized in Table 5.

Table 5. One-Way ANOVA Results for Fraud Prevention Education and Job Scam Awareness

Have you received any education or lectures on fraud prevention?	N	Subgroup when alpha = .05	
		1	2
Yes, both	126	3.4902334	
Yes, Participated off Campus	133	3.5276392	
Not accepted	107	3.5354557	
Yes, Participated on Campus	173	3.8033740	3.8033740
Do not remember	5		4.2110255
Sig.		.708	.462

As shown in Table 5, A one-way ANOVA was conducted to examine whether different types of fraud prevention education influenced college students' awareness of job-related scams (fac1). The participants were grouped based on their responses: Yes, participated on campus (n = 173), Yes, participated off campus (n = 133), Yes, both (n = 126), Not accepted (n = 107), and Do not remember (n = 5).

The descriptive statistics showed that the mean Job Scam scores ranged from 3.4902 (Yes, both) to 4.2110 (Do not remember). The Tukey HSD post-hoc analysis indicated that there were no statistically significant differences among the groups (p-values ranged from .462 to .708), suggesting that the type or level of fraud prevention education did not significantly affect students' awareness of job-related scams.

Although the mean score for "Do not remember" was the highest (4.2110), this result should be interpreted with caution due to the very small sample size (n = 5). Among the larger groups, "Yes, on campus" (3.8034) had a slightly higher mean than the other categories, but the differences were not statistically significant.

Combined with previous descriptive findings that students generally have lower recognition of employment-related fraud, these results highlight a potential gap in the

content or delivery of existing educational programs. Future efforts could focus on more targeted, interactive, or scenario-based training to better equip students to identify and respond to job-related scams.

Summary of Major Findings

This section summarizes the main findings derived from the descriptive and inferential analyses of university students' awareness of four types of scams.

Overall, students demonstrated moderate levels of scam awareness, with higher recognition of phishing scams and lower recognition of job-related scams. Previous studies have noted that phishing scams receive greater emphasis in campus-based cybersecurity awareness campaigns and media reports, which may contribute to higher levels of familiarity with this type of scam. In contrast, job scams may appear less salient in students' daily experiences, potentially leading to lower vigilance. This interpretation is offered as a contextual explanation rather than a causal conclusion derived from the present analysis.

The results also indicated that prior experience with scams did not lead to statistically significant differences in awareness levels. Although students with prior experience showed slightly higher mean scores, this finding suggests that personal exposure alone may not systematically enhance fraud recognition. Previous studies have proposed that behavioral change often requires structured reflection and guided learning; however, such processes were not examined in the present study.

In addition, participation in fraud prevention education did not produce significant differences in awareness, particularly with regard to job scams. This pattern may suggest a gap between theoretical instruction and practical application, as discussed in prior research. Given the relatively low reliability of the measurement

scales, these findings should be interpreted with caution and viewed as indicative trends rather than definitive conclusions.

Drawing on prior literature rather than the empirical results of this study, existing research has suggested that current anti-fraud education may be constrained by relatively static content and lecture-based instructional formats. Such programs often emphasize information delivery over practice-oriented training aligned with students' everyday digital activities and job-seeking experiences. As noted in previous studies, this instructional approach may limit the extent to which knowledge is translated into strengthened cognitive judgment.

The major findings are summarized in Table 6 for clarity

Table 6. Summary of Major Findings

Dimensions	Indicators	Key Findings
Scam Awareness	Overall Recognition	1. Students' overall scam recognition is moderate, showing partial understanding of online and offline fraud. 2. Phishing scams are most easily identified; job scams are least recognized. 3. Students' scam awareness varies by exposure and familiarity with scam types.
	Scam Type Comparison	1. Awareness ranking: Phishing > Investment > Romance > Job scams. 2. Awareness differences suggest influenced from media exposure and relevance to daily life.
Past Victimization Experiences	Experience Effect	1. No significant difference in awareness between students with or without scam experiences. 2. Past experiences alone do not enhance judgment or prevention capability. 3. Indicateds the need for structured reflection and guided education after victimization.
Effectiveness of Anti-Fraud Education	Educational Impact	1. Participation in on-campus, off-campus, or dual-track programs did not significantly improve scam awareness. 2. Limited improvement particularly noted in job-seeking scam awareness. 3. Suggested that current anti-fraud education lacks practicality and engagement.
	Educational Recommendations	1. Incorporate interactive, experiential, and scenario-based learning in curricula. 2. Strengthen real-world coping and critical-

		thinking skills through simulations. 3. Redesign courses to enhance applicability and long-term effectiveness.

CONCLUSION

This study confirms that university students' awareness of fraud remains at a moderate level across the four examined scam types. The quantitative findings demonstrate no statistically significant differences based on prior experience or participation in fraud prevention education. While previous literature highlights the potential role of emotional and psychological factors in fraud vulnerability, such factors were not empirically measured in this study; therefore, reflections on these constructs are framed as literature-informed possibilities rather than empirical conclusions. The findings clearly address three research questions:

- Research Question 1: What are university students' awareness of different types of fraud?

This study aimed to understand college students' overall awareness of different types of fraud. Descriptive analysis revealed that students exhibited the highest awareness toward phishing scams (M = 3.6555), followed by investment scams (M = 3.6460) and romance scams (M = 3.6398). In contrast, job scams (M = 3.6145) received the lowest recognition. This result may suggest that students are marginally less vigilant toward employment-related fraud, indicating a potential area for targeted educational focus.

- Research Question 2: Did prior experience with scams significantly influenced college students' awareness of scams?

An independent samples t-test revealed no statistically significant differences in awareness scores between students with prior fraud experience and those without. Although respondents with past experience scored slightly higher on average, the non-significant result may suggest that personal encounters alone are not necessarily

sufficient to enhance an individual's systematic fraud recognition or judgment capabilities.

- Research Question 3: Did participation in fraud prevention education significantly improve university students' awareness and ability to recognize different types of fraud?

ANOVA results showed no statistically significant differences in awareness levels among students who received on-campus, off-campus, both, or not accepted. This finding could point to a potential gap between theoretical knowledge and practical application in current curricula. These results should be interpreted with caution given the recorded reliability limitations of the measurement scales.

Suggestion

Based on the findings, future programs should transition from theoretical knowledge transmission toward competence-based training. Educational institutions should prioritize scenario-based simulations that allow students to apply analytical reasoning in realistic environments, effectively bridging the observed gap between abstract knowledge and practical application.

Furthermore, future anti-fraud initiatives would benefit from a holistic and interdisciplinary curriculum design that integrates digital literacy, financial intelligence, and psychological resilience. While these specific dimensions were not empirically tested in the current study, existing literature suggests that they are essential components of a comprehensive defense strategy. It is recommended that IT specialists, financial experts, and psychologists collaborate to design curricula that address the multifaceted nature of modern fraud rather than relying on isolated interventions.

In addition, fraud awareness should be systematically embedded within broader institutional frameworks through longitudinal integration. This approach ensures that students' coping abilities evolve alongside the rapidly changing tactics used by fraud syndicates. Providing continuous exposure to real-world fraud patterns through updated digital infrastructures will better support sustained learning and adaptability than short-term, one-off programs.

Finally, regarding directions for future research, the reliability constraints and non-significant findings of the current study suggest that future work should employ more robust and multi-item scales to measure scam awareness. Future studies should also empirically operationalize and test psychological variables, such as trust bias and emotional susceptibility, to determine their specific impact on student vulnerability. This would allow researchers to move beyond the literature-informed reflections presented in this study and provide a more data-driven understanding of the psychological mechanisms underlying fraud victimization.

APPENDIX

大學生對不同類型詐騙的認知與判斷能力

University Students' Awareness and Judgment Ability Toward Different Types of Fraud

Dear Respondents,

This is an academic research questionnaire aimed at exploring university students' awareness and judgment regarding different types of fraud. As fraudulent tactics become increasingly diverse, university students, who heavily rely on the internet and digital technology, deserve in-depth study regarding their ability to recognize and respond to fraud. Through your valuable input, this study seeks to understand students' awareness of various types of fraud and further analyze the factors that influenced their judgment. The questionnaire is conducted anonymously, and all data will be used solely for academic research purposes. It will take approximately 10 minutes to complete, and I would greatly appreciate your time and participation.

I sincerely appreciate your time and assistance, which will greatly contribute to the value of this research. Thank you very much.

Department of International Affairs,
Wenzao Ursuline University of Languages
Student: Hung Yi-Hsuan, Liang Yu-Chieh
Wang Yu-Yun, Ling Feng-Yu

Part 1: Basic Information

Gender: □ Male □ Female

Age: □ 18-20 □ 21-23 □ 24 and above

Income: □ Below 10,000 □ 10,001-15,000 □ Over 15,001 (NTD/monthly)

Current school location:

□ Northern Taiwan (such as Taipei, New Taipei, Keelung, Taoyuan)

□ Central Taiwan (such as Taichung, Changhua, and Nantou)

□ Southern Taiwan (such as Kaohsiung, Tainan, Pingtung)

□ Eastern Taiwan (such as Hualien and Taitung)

□ Outlying Islands (such as Kinmen, Matsu, Penghu)

Major:

□ Humanities and Social Sciences (e.g., Foreign Languages, Sociology, History)

□ Business and Management (e.g., Finance, International Trade, Accounting)

□ Health and Medicine (e.g., Medicine, Nursing, Pharmacy, Public Health)

□ Arts and Design (e.g., Fine Arts, Music, Drama, Industrial Design)

□ Law and Education (e.g., Law, Education, Early Childhood Education)

□ Communications and Media (e.g., Journalism, Advertising and Public Relations)

□ Other (please specify)_____

Have you ever encountered different types of fraud?

□ Yes

□ No

Have you received any education or lectures on fraud prevention? (Fraud prevention training)

□ Yes, on campus

□ Yes, off campus

□ Yes, both

□ Not accepted

□ Do not remember

(1 = Strongly Disagree and 5 = Strongly Agree.)

Part 2: Awareness of Job Scams	1	2	3	4	5
1. I know that scammers may impersonate well-known companies or HR departments to contact me.					
2. I know that being asked to provide my bank account or ATM card may be a job scam trap.					
3. I know how to identify suspicious job locations (e.g., requiring work abroad or places with safety concerns).					
4. I know how to verify whether an online employer is a legitimate company.					
5. I know that scam job advertisements often include unreasonable conditions (e.g., guaranteed hiring with a high salary).					

Part 3: Awareness of Phishing Website Scams	1	2	3	4	5
1. I know that phishing websites may mimic legitimate sites to steal my personal information.					
2. I know how to verify whether a website is secure by checking if the URL has "https" or other security indicators.					
3. I know how to identify common social engineering tactics used by phishing websites, such as impersonating well-known brands or financial institutions.					
4. I know that messages such as "Your account have encountered an issue. Please log in immediately to fix it" may be phishing scams.					
5. I know how to recognize incorrect website addresses or spelling errors, which may be signs of a phishing website.					

Part 4: Awareness of Romance Scams	1	2	3	4	5
1. I know that if someone I met online keeps pressuring me to enter a romantic relationship but constantly avoids voice or video calls, this could be a scam.					
2. I know that if I meet someone on a dating platform whose social media has only a few photos and was recently created, this could be suspicious.					
3. I know that if someone I just met online claimed to be in an emergency (such as financial trouble) and asks for money, this could be a scam.					
4. I know that if someone on social media showedcases luxury items in their stories to attract attention, this could be a scam.					
5. I know that if someone I just met online constantly compliments me, making me feel highly valued and cared for, but avoids revealing much about themselves, this could be a scam.					

Part 5: Awareness of Investment Scams	1	2	3	4	5
1. I know that "guaranteed no risk, high return" investments could be a scam.					
2. I know that I can check with official agencies to verify if an investment is safe.					
3. I know that if an investment ad promises "super high returns" without clearly explaining the risks, it could be a scam.					
4. I know that if an investment company asks for "fees" upfront and is not officially registered, it could be a scam.					
5. I know that if someone sells an investment as a "guaranteed profit" program, it's probably a scam.					

Thank you for your response! Stay alert and protect yourself from scams.

REFERENCES

Adams, Richard. "Pupils in England to Be Taught About Online Spending and Scams." *The Guardian*, 2025.

Althibyani, Hosam A, and Abdulrahman M Al-Zahrani. "Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime." *Sustainability* 15, no. 15 (2023): 11512.

Amankwa, Eric. "Relevance of Cybersecurity Education at Pedagogy Levels in Schools." *Journal of Information Security* 12, no. 4 (2021): 233-49.

Arib, Muhammad Adnan Pitchan、Ali Salman、Nadhirah Muhamad. "A Systematic Literature Review on Online Scams: Insights into Digital Literacy, Technological Innovations, and Victimology." *Jurnal Komunikasi: Malaysian Journal of Communication* Volume 41, Issue 1 (March 2025): 107–24.

Bansal, Varsha. "In the Fight against Scams, 'Cyber Ambassadors' Enter the Chat." WIRED, https://www.wired.com/story/cyber-ambassadors-india/.

Bartlett, Jamie, and Carl Miller. "Truth, Lies and the Internet: Exploring Digital Fluency." *School Librarian* 60, no. 1 (2012): 6-9.

Bates, Marcia J. "Fundamental Forms of Information." *Journal of the American Society for Information Science and Technology* (Vol. 57, No. 8 (2007)): 1033–45.

Bhat, Arshad Hussain, and Durgeshwary Kolhe. "Crime and Fraud at the Community Level: Social Networking Understanding into Economic Crimes and Psychology Motivations." *Journal of Social Sciences and Economics* 3, no. 2 (2024): 127-46.

Bundala, Ntogwa Ng'habi. "Cybercrime: Psychological Tricks and Computer Securities Challenges." *Asian Journal of Research in Computer Science* 17, no. 12 (2024): 1-17.

Button, Mark, Chris Lewis, and Jacki Tapley. "Fraud Typologies and the Victims of Fraud: Literature Review." (2009).

Choy, Yoke Mui, and Noor Hayati Che Man. "Analysis of Fraudulent Transactions Using Data Mining Technique." *Journal of Financial Crime* 29, no. 2 (April 17 2021): 525–33.

Cialdini, Robert B. *Influenced: Science and Practice.* Vol. 4: Pearson education Boston, 2009.

Crime., United Nations Office on Drugs and. "Cybercrime Module 5 Key Issues:

Obstacles to Cybercrime Investigations." https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html.

Engels, Christian, Kamlesh Kumar, and Dennis Philip. "Financial Literacy and Fraud Detection." In *Financial Literacy and Responsible Finance in the Fintech Era*, 124-46: Routledge, 2021.

ENIC-NARIC and European Students' Union, ESU. "Knowledge and Awareness of Fraud in Education: A Student Perspective." (2025).

Faklaris, Cori, Heather Richter Lipford, and Sarah Tabassum. "Preliminary Results from a Us Demographic Analysis of Smish Susceptibility." *arXiv preprint arXiv:2309.06322* (2023).

Finkelhor, David, Kerryann Walsh, Lisa Jones, Kimberly Mitchell, and Anne Collier. "Youth Internet Safety Education: Aligning Programs with the Evidence Base." *Trauma, violence, & abuse* 22, no. 5 (2021): 1233-47.

Fletcher, E. "Social Media: A Golden Goose for Scammers." Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers, 2023.

Goel, Sanjay, Kevin Williams, and Ersin Dincelli. "Got Phished? Internet Security and Human Vulnerability." *Journal of the Association for Information Systems* 18, no. 1 (2017): 2.

Kaabouch, Fatima Salahdine and Naima. "Social Engineering Attacks: A Survey." *Future Internet* 11, no. 4 (2019): 89.

Kircanski, Katharina, Nanna Notthoff, Marguerite DeLiema, Gregory R Samanez-Larkin, Doug Shadel, Gary Mottola, Laura L Carstensen, and Ian H Gotlib. "Emotional Arousal May Increase Susceptibility to Fraud in Older and Younger Adults." *Psychology and aging* 33, no. 2 (2018): 325.

Kusuma, Chusnu Syarifa Diah, and Riana Isti Muslikhah. "Strengthening of Digital Literacy to Support Student Community Service to Prevent Hoax and Cybercrime." Paper presented at the 9th International Conference on Education Research, and Innovation (ICERI 2021), 2022.

Lee, Steven James, Benjamin F Cummings, and Jason Martin. "Victim Characteristics of Investment Fraud." Paper presented at the 2019 Academic Research Colloquium for Financial Planning and Related Disciplines, 2019.

Lusardi, Annamaria, and Olivia S Mitchell. "Financial Literacy and Retirement

Planning: New Evidence from the Rand American Life Panel." CFS working paper, 2007.

Mohd Padil, Hazlina, Eley Suzana Kasim, Salwa Muda, Norhidayah Ismail, and Norlaila Md Zin. "Financial Literacy and Awareness of Investment Scams among University Students." *Journal of Financial Crime* 29, no. 1 (2022): 355-67.

Murat Yıldırım, Gözde Topal Arslan. "Examining the Role of Resilience and Hope in Predicting Psychological Distress and Life Satisfaction among University Students During the Covid-19 Pandemic." *PLOS ONE* Volume 19, Issue 4 (2024).

PYMNTS. "Report: 82.9% of Young Adults Have Been Tricked by Suspicious Links.", 2025.

Rich, Michael, and Kenneth R Ginsburg. "The Reason and Rhyme of Qualitative Research: Why, When, and How to Use Qualitative Methods in the Study of Adolescent Health." *Journal of Adolescent health* 25, no. 6 (1999): 371-78.

Salahdine, Fatima, and Naima Kaabouch. "Social Engineering Attacks: A Survey." *Future internet* 11, no. 4 (2019): 89.

Särökaari, Niklas. "Phishing Attacks and Mitigation Tactics." (2020).

Steven James Lee, Benjamin F. Cummings, and Jason Martin. "Victim Characteristics of Investment Fraud." (2019).

Wash, Rick. "How Experts Detect Phishing Scam Emails." *Proceedings of the ACM on Human-Computer Interaction* 4, no. CSCW2 (2020): 1-28.