https://doi.org/10.51483/IJAIML.6.1.2026.168-184 ISSN: 2789-2557

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Cyber Fraud Awareness in Digital Social Environments: A Correlational Study Among University Students

Luo Yuchao[1] and Immanuel T. San Diego[2]

[1]Graduate School of Education Trinity University of Asia Quezon City, Philippines. E-mail: yuchaonluo@tua.edu.ph
[2]Graduate School of Education Trinity University of Asia Quezon City, Philippines. E-mail: itsandiego@tua.edu.ph

Article Info

Volume 6, Issue 1, January 2026
Received : 15 September 2025
Accepted : 11 January 2026
Published : 26 January 2026
doi: 10.51483/IJAIML.6.1.2026.168-184

Abstract

The proliferation of digital technologies has introduced unprecedented convenience but has also created a fertile ground for online fraud, making university students a particularly vulnerable demographic. This study employed a descriptive correlational design to investigate the relationship between online fraud awareness and social interaction among 381 students at Zhengzhou University of Economics and Business. Using a researcher-made questionnaire grounded in the Technology Threat Avoidance Theory and Social Engagement Theory, the research assessed students' perceptions of online fraud and their social behaviors. The findings revealed a high level of online fraud awareness among students, with no significant differences found across gender, age, or year level. However, a critical disconnect was identified between a general knowledge of cyber threats and a personal sense of susceptibility. The data also highlighted a complex relationship with social interaction: while high self-efficacy acted as a protective factor, fostering a positive social life, a heightened perception of threat was negatively correlated with the quality of social interactions. The study concludes that effective security interventions must be holistic, addressing psychological biases and behavioral habits in addition to technical knowledge. Based on these findings, the paper recommends a multi-faceted action plan that includes personalized educational strategies, user-friendly security solutions, peer-to-peer support networks, and initiatives to build psychological resilience.

Keywords: *Online Fraud Awareness, Social Interaction, University Students, Self-Efficacy, Digital Security*

Introduction

The digital age has fundamentally transformed human interaction, commerce, and financial transactions, offering unprecedented convenience and connectivity. Yet, this widespread adoption of digital technologies has created a fertile ground for the proliferation of online fraud, a pervasive and evolving threat (Drew & Webster, 2024; Vimal et al., 2021). Online fraud encompasses a wide spectrum of cybercrimes, including

phishing scams, identity theft, financial fraud, and investment schemes, all of which exploit the anonymity and borderless nature of the internet (Ansar et al., 2021). As individuals increasingly rely on digital platforms such as e-commerce sites, social media networks, and online banking systems, cybercriminals have become more adept at leveraging sophisticated tools, including artificial intelligence, to deceive unsuspecting victims (Drew & Webster, 2024; Croll, 2023). The increasing complexity of fraudulent tactics, exemplified by criminals using generative AI to create more intricate and convincing scams, presents a pervasive and growing threat to individuals across all demographics (Drew & Webster, 2024).

Online fraud is not merely a technological issue; it is a profound social and psychological one. The psychological and emotional effects on victims, such as distress, anxiety, and a loss of trust, can significantly impact their social behavior and interaction patterns, leading to a decline in social trust and a reluctance to engage in online activities (Drew & Webster, 2024). This uncertainty makes it difficult for individuals to distinguish genuine interactions from fraudulent schemes, often amplifying feelings of isolation and mistrust in the digital landscape (Ansar et al., 2021). The economic and social impact is far-reaching, with billions of dollars lost annually to cybercriminal activities, underscoring the necessity of effective countermeasures (Vishwakarma, 2017; Ali et al., 2019). While governments and businesses develop preventative measures, their effectiveness is ultimately contingent on the awareness and vigilance of individuals.

University students represent a particularly vulnerable demographic due to their high digital engagement, frequent online transactions, and often limited financial literacy (Nikitkov & Bay, 2008). Their reliance on social media, digital marketplaces, and online payment systems makes them prime targets for cybercriminals. In China, where this study is situated, students constitute a significant portion of the country's 1.1 billion internet users, and cyber fraud cases are disproportionately high among young people (Global Times, 2024; Sixth Tone, 2024; Liu, 2022). This alarming trend highlights the urgency of examining how awareness of online fraud relates to social interaction, with the ultimate goal of devising enhanced security measures to mitigate these risks. The central research problem addressed by this study is to assess the level of online fraud awareness among students, investigate its relationship with their social interactions, and provide insights for effective, evidence-based security measures. The research aims to bridge the critical gap between a cognitive understanding of cyber threats and the behavioral responses of students, contributing to a deeper understanding of how online safety and social well-being intersect.

Theoretical Framework

This study is grounded in two key theoretical frameworks that provide a conceptual lens for understanding the complex relationship between online fraud awareness and social behavior. The first is the Technology Threat Avoidance Theory (TTAT), and the second is the Social Engagement Theory. The Technology Threat Avoidance Theory (TTAT), developed by Liang and Xue (2010), provides a robust explanation for how individuals respond to cybersecurity threats by taking actions to avoid them. This theory is particularly useful for understanding why students may or may not adopt protective behaviors. The TTAT posits that an individual’s motivation and behavior to avoid a technological threat are influenced by four core constructs: Perceived Threat, Safeguard Effectiveness, Self-Efficacy, and Safeguard Cost. Perceived threat refers to an individual's evaluation of the risk of a threat, encompassing both perceived susceptibility and perceived severity. Perceived susceptibility is the belief in how likely one is to be a victim, while perceived severity is the subjective belief regarding the seriousness of the consequences (Liang & Xue, 2010). If students do not see themselves as potential victims or do not believe the consequences of fraud are severe, they may not take security measures seriously. Research shows that while students may have a high general fear of fraud, they often do not feel personally susceptible, highlighting a critical disconnect between a general understanding of the threat and an individual’s personal vulnerability (Qu et al., 2024).

Safeguard effectiveness reflects whether students believe that security measures, such as strong passwords and two-factor authentication, can effectively prevent online fraud. A high belief in the efficacy of these measures increases the likelihood of their adoption. Self-efficacy is the individual's confidence in their own ability to recognize and implement protective actions. Students who feel capable of detecting

scams and securing their accounts are more likely to take proactive measures, whereas those with low self-efficacy may avoid these measures, increasing their vulnerability. Safeguard cost refers to the perceived difficulty, time, effort, or financial burden associated with implementing security measures. If students view these measures as complicated or inconvenient, they may choose not to use them, even if they understand the risks.

The second framework, the Social Engagement Theory (Rachmad, 2022), highlights the importance of active participation in social interactions for enhancing well-being and strengthening community ties. This study utilizes this theory to examine how online fraud awareness may influence social behavior. The theory measures social engagement through three key indicators: Level of Participation in Social Activities, which reflects the frequency and extent of a student's involvement in social and community events; Quality of Social Interactions, which focuses on the depth, meaningfulness, and positivity of interpersonal relationships; and Life Satisfaction, which assesses a student's overall sense of well-being and contentment with their social and personal life. By integrating these two theories, the study seeks to understand how students' cognitive perceptions of online threats (TTAT) interact with their social behaviors and well-being (Social Engagement Theory), thereby providing a comprehensive analysis of the problem.

Literature Review

Awareness of Online Fraud

The threat of online fraud is a growing concern, with recent literature highlighting its increasing prevalence and impact (Drew & Webster, 2024; Vimal et al., 2021). Scammers leverage a combination of technological advancements, such as generative AI, and psychological manipulation to deceive victims, making the need for heightened awareness crucial (Croll, 2023; Juanda et al., 2024).

A key psychological factor in how students approach online threats is the significant disconnect between a high general fear of cyber fraud and a low belief that they are personally likely to be a victim (Qu et al., 2024). This psychological phenomenon, sometimes referred to as optimistic bias, allows individuals to acknowledge a threat intellectually while denying its relevance to their own lives, which can reduce their motivation to take adequate precautions (Akhmadieva et al., 2020). Furthermore, research suggests that gender plays a role in this perception, with female students consistently reporting a higher perceived risk and susceptibility to fraud, which translates into more cautious behavior compared to their male counterparts (Balakrishnan et al., 2025; Lee et al., 2023).

Students generally perceive the effects of online fraud as serious, particularly concerning financial and psychological harm (Qu et al., 2024). They are aware that fraud can lead to substantial financial losses and emotional distress and anxiety (Qu et al., 2024; Lyu et al., 2025). This perception is critical because a higher perceived severity is often linked to stronger protective behaviors (Lestari et al., 2024). However, a concerning aspect is the potential for the normalization of fraudulent acts, where repeated exposure to scams can reduce their perceived severity (Dias-Oliveira et al., 2024). This can lead to a cycle where justifying fraudulent actions diminishes a person's concern for the consequences, potentially increasing their vulnerability (De Oliveira et al., 2020).

While advanced technological safeguards, such as machine learning models, have been proven to be highly effective in preventing fraud with high accuracy rates (Sreekala et al., 2023; Pathan et al., 2024; Subramanian, 2024; Lenka & Tiwari, 2025; Farouk et al., 2024; Shetty et al., 2023), the adoption of personal security measures is a different matter. The literature indicates that students' trust in safeguards is shaped not only by their knowledge but also by the perceived cost of implementing them (Vanini et al., 2023). The adoption of safeguards is often hindered by non-financial burdens, with the perceived effort and inconvenience of practices like frequent password changes and two-factor authentication acting as major deterrents (Farjana et al., 2024; Ahmad et al., 2024). This means that for students, the cognitive load and time required for security are often more significant barriers than the direct financial cost of software or

services (Vanini et al., 2023). This understanding of safeguard cost is a direct application of the TTAT model and highlights the need for user-friendly and low-friction security solutions (Papasavva et al., 2024; Sharma, 2024).

A student's confidence in their ability to recognize and implement security measures—or self-efficacy—is a critical factor in online safety. Research indicates that higher self-efficacy in digital technologies leads to greater engagement and a reduced likelihood of engaging in risky online behaviors (Getenet et al., 2024). Students with a strong sense of self-efficacy are more likely to actively participate in online environments, and this confidence can enhance their ability to recognize and respond to online threats (Liu & Zhang, 2021). This suggests that effective security education should focus on empowering students with practical skills to build their confidence, rather than just raising awareness of threats (Qiu & Yang, 2021; Alivia & Anwar, 2022; Smith et al., 2024).

The Nature of Social Interaction

Social interaction is a fundamental aspect of human life, playing a central role in shaping relationships, fostering well-being, and supporting learning (Hamilton, 2024; Kapur, 2023; De Felice et al., 2022). It is an essential component of student life, contributing to academic performance and overall quality of life (Ali et al., 2024).

Active involvement in social and extracurricular activities is consistently linked to improved social skills, social competence, and a broader sense of community (Unlu & Çeviker, 2022; Wachsmuth et al., 2023). While the overall level of participation can be moderate (Ridkodubska, 2023), proactive engagement, such as joining discussions and clubs, is crucial for developing teamwork and leadership skills (Ghani et al., 2020; Díaz-Iso et al., 2020). Collaborative engagement in academic activities, in particular, has been shown to improve learning outcomes (Isohätälä et al., 2020; Vuorenmaa et al., 2024).

High-quality social interactions, characterized by positive relationships and meaningful engagement, are strongly correlated with a better quality of life and enhanced academic success (Albohnayh et al., 2024). Trust, communication, and mutual support are essential components of high-quality relationships that contribute to a strong sense of community and belonging (Sriram et al., 2020). Collaborative engagement in academic activities, in particular, has been shown to improve learning outcomes (Yedemie & Yidegi, 2020; Ong & Tangsoc, 2020). High-quality social interactions are also linked to lower rates of bullying and higher social competence (Anwar & Karneli, 2020; Magro et al., 2023).

The literature provides extensive evidence that high-quality social interactions, social support from peers and family, and a strong sense of belonging are all powerful predictors of greater life satisfaction among students (Azminudin et al., 2025; Santos et al., 2023; Vidić, 2024; Zahid et al., 2025; He et al., 2024; Xinyi et al., 2024). Students with higher social skills and social intelligence also report greater life satisfaction (Saleem, 2021; Rezaei & Jeddi, 2020). Social interaction anxiety is negatively correlated with life satisfaction, while a strong sense of belonging significantly predicts life satisfaction (Khan et al., 2021; Calleja-Núñez et al., 2023; Avcı, 2023; Duvnjak, 2020). The literature confirms that students are most satisfied in domains related to personal relationships and community (Duvnjak, 2020; Feraco et al., 2022).

The Interrelationship Between Online Fraud and Social Interaction

The impact of online fraud extends far beyond financial loss, having a significant negative effect on a victim's social and psychological well-being (Zhang et al., 2022). Victims often experience severe psychosocial effects, including shock, sadness, anger, low self-esteem, depression, and a significant loss of trust in others (Niman et al., 2023; Buse et al., 2023). Scammers often exploit social vulnerabilities, manipulating trust and urgency to carry out their schemes, leaving victims with feelings of shame, regret, and a reluctance to report the crime (Buse et al., 2023). The social context can both increase vulnerability to fraud and be a source of resilience. Some research suggests that scammers may have been previous victims themselves,

having learned manipulative tactics through a corrupted form of social learning (Stalans, 2022). This highlights how fraud can not only harm a victim but also perpetuate a cycle of deceit within the social fabric. This study's synthesis of the literature reveals a compelling argument that online fraud prevention must be reframed. It is not just about raising awareness of scams, but about recognizing and protecting the foundational role of social interaction in a student's life. The disconnect between knowing about fraud and acting on it is a critical vulnerability. The findings also reveal that online fraud is a deeply personal, social, and psychological crime that can dismantle trust and lead to severe emotional distress. Therefore, future interventions must not only focus on technical knowledge but also on building a digital literacy that empowers students to navigate the complex social landscape of the internet, understand the psychological tactics of fraudsters, and cultivate social resilience.

Methodology

Research Design

The study employed a descriptive correlational research design, a method well-suited for examining the relationship between variables without manipulating them. This design was chosen as it allowed for a systematic observation, description, and analysis of two key variables: the level of online fraud awareness and the extent of social interaction among university students. The descriptive component was crucial for providing a detailed account of the current state of these variables, capturing participants' perceptions, experiences, and behaviors in a real-world setting. The correlational aspect was used to determine whether a statistically significant relationship existed between online fraud awareness and social interaction, such as whether a higher level of awareness was associated with changes in social participation or relationship quality. This design was beneficial for exploring potential trends and associations in a natural setting and provided a solid foundation for future research.

Population, Sample, and Sampling Technique

The study's target population consisted of university students aged 18–24 at Zhengzhou University of Economics and Business, which has a total student population of approximately 36,000. A purposive sampling technique was used to select a sample of 381 participants, a size determined using a 95% confidence level and a 5% margin of error. This non-probability sampling method ensured that participants were deliberately chosen based on specific inclusion criteria relevant to the study's objectives: enrolled students at the university at the time of data collection; aged 18–24 years old, representing the demographic most likely to engage in independent online activities and be exposed to fraud risks; active internet users with frequent digital interactions, such as online transactions and social networking; and willing to participate and provide informed consent. Exclusion criteria included students under 18 or those who were not frequent internet users, as their experiences would not align with the study's focus. The purposive sampling method allowed the research to concentrate on a population with direct relevance to the topic, thereby enhancing the specificity of the findings.

Research Instrument

A researcher-made questionnaire was developed and used as the primary data collection instrument. The questionnaire was structured into three main sections to ensure a comprehensive assessment of the study's variables. The first section collected the demographic profile of the respondents, including their gender, age, and year level. The second section measured online fraud awareness using a 4-point Likert scale, with sub-dimensions aligned with the Technology Threat Avoidance Theory: Perceived Threat (including perceived susceptibility and perceived severity), Safeguard Effectiveness, Safeguard Cost, and Self-Efficacy. The third section evaluated the level of social interaction among respondents, also using a 4-point Likert scale, with indicators based on the Social Engagement Theory: Level of Participation in Social Activities, Quality of Social Interactions, and Life Satisfaction. The validity of the instrument was confirmed

by three academic experts, and its internal consistency was assessed through reliability testing using Cronbach's alpha, which yielded coefficients of 0.80 and above, demonstrating a high level of reliability. To accommodate non-English-speaking respondents and prevent misinterpretation of survey items, the questionnaire was professionally translated into Chinese.

Data Gathering and Statistical Treatment

The data gathering procedure was conducted in full compliance with ethical guidelines, with prior approval secured from the Trinity University of Asia – Institutional Ethics Review Committee (TUA-IERC). The process began with a pilot test to refine the clarity of the questions, followed by the distribution of the survey in both online and printed formats to maximize accessibility. Informed consent was obtained from all participants, and strict measures were taken to ensure the anonymity and confidentiality of their responses. Before the main analysis, a normality test was conducted on the dataset, revealing that the data did not follow a normal distribution. To ensure the accuracy and validity of the findings, nonparametric statistical techniques were employed for the analysis. Descriptive statistics, including frequency counts and percentages, were used to summarize the demographic profile of the respondents. The mean and standard deviation were used to describe the central tendency and variability of the awareness and social interaction variables. The Spearman's rank-order correlation was calculated to determine the strength and direction of the relationship between online fraud awareness and social interaction.

Results

This section presents the empirical findings of the study, providing a detailed analysis of the data collected from the survey. The results are organized into tables and a narrative interpretation to provide a clear understanding of the sample's profile, their levels of online fraud awareness and social interaction, and the relationships between these variables.

Awareness Level of the Respondents Regarding Online Fraud

Table 1 presents the mean scores, standard deviations, and verbal interpretations for the sub-dimensions of online fraud awareness. The data in Table 1 indicate that students possess a high overall awareness of online fraud, with a composite mean of 3.27 for perceived susceptibility (Very High) and 3.11 for perceived severity (High). A critical finding is the disconnect between acknowledging a universal risk ("I feel that I am just as likely as anyone else," M = 3.57) and internalizing a personal one ("I believe I am personally at risk," M = 3.01). This paradox suggests an intellectual understanding of the threat but a psychological resistance to accepting personal vulnerability.

Regarding safeguards, students' awareness of effectiveness is rated as High (M = 2.98), particularly concerning traditional measures like strong passwords. However, their appreciation for proactive behavioral measures, such as avoiding suspicious links, is comparatively lower. The perception of safeguard cost is also rated as High (M = 3.03), with the primary burdens being the inconvenience and effort required for upkeep, rather than the financial cost of tools. In terms of self-efficacy, students express a high level of confidence in their ability to recognize and avoid scams (M = 3.15), but this confidence is not equally matched by their certainty in their specific technical skills to secure accounts effectively.

Table 1: Level of Awareness of the Students Regarding Online Fraud

Indicators	Mean	SD	Verbal Interpretation
Perceived Susceptibility	**3.27**	**0.28**	**Very High**
Perceived Severity	**3.11**	**0.44**	**High**
Safeguard	**2.98**	**0.36**	**High**

Effectiveness			
Safeguard Cost	**3.03**	**0.51**	**High**
Self-Efficacy	**3.15**	**0.36**	**High**

Remarks: 1.00-1.75 - Very Low; 1.76-2.50- Low; 2.51-3.25- High; 3.26-4.00- Very High

Level of Social Interaction of the Students

Table 2 presents the mean scores, standard deviations, and verbal interpretations for the indicators of social interaction. The results in Table 3 show that students exhibit a High level of social interaction across all three dimensions. Their participation in social activities (M = 3.17) is robust, with a particular strength in active engagement with peers and group activities. The quality of their social interactions is also rated as High (M = 2.84), as they generally feel their relationships contribute positively to their well-being, though they are slightly less comfortable with expressing deep emotions. This high level of social engagement and positive experience with relationships translates into a High level of life satisfaction (M = 3.11), largely driven by a strong sense of belonging within their social groups.

Table 2: Level of Social Interaction of the Students

Indicators	Mean	SD	Verbal Interpretation
Participation in Social Activities	**3.17**	**0.43**	**High**
Quality of Social Interactions	**2.84**	**0.32**	**High**
Life Satisfaction	**3.11**	**0.25**	**High**

Relationship Between the Respondents' Awareness Level of Online Fraud and Their Social Interaction

Table 3 presents the results of the Spearman's rank-order correlation, which was used to determine the relationships between the awareness and social interaction variables. The correlational analysis reveals a complex and multifaceted relationship between online fraud awareness and social interaction. Key findings include: a positive correlation between Perceived Susceptibility and Level of Participation (rho = 0.36, p <.001); a negative correlation between Perceived Susceptibility and Life Satisfaction (rho = -0.27, p <.001); a strong negative correlation between Perceived Severity and Quality of Social Interactions (rho = -0.45, p <.001), but a strong positive correlation with Life Satisfaction (rho = 0.48, p <.001); a negative correlation between Safeguard Cost and Quality of Social Interactions (rho = -0.34, p <.001), but a positive correlation with Life Satisfaction (rho = 0.47, p <.001); and a positive correlation between Self-Efficacy and both Quality of Social Interactions (rho = 0.17, p <.001) and Life Satisfaction (rho = 0.24, p <.001), but a negative correlation with Level of Participation (rho = -0.40, p <.001). The findings also indicate that there were no significant differences in online fraud awareness when students were grouped by gender, age, or year level.

Table 3: Correlation of the Students' Awareness Level of Online Fraud and Their Social Interaction

		Perceived Susceptibility	Perceived Severity	Safeguard Effectiveness	Safeguard Cost	Self-Efficacy
Level of Participati	Spearman's rho	0.36*	0.06	0.02	0.01	−0.40*

on						
	p-value	< .001	0.253	0.648	0.786	< .001
Quality of Social Interactions	Spearman's rho	−0.04	−0.45*	−0.11*	−0.34*	0.17*
	p-value	0.45	< .001	0.037	< .001	< .001
Life Satisfaction	Spearman's rho	−0.27*	0.48*	−0.10*	0.47*	0.24*
	p-value	< .001	< .001	0.05	< .001	< .001

Remarks: *Significant at p<.05

4.0 Discussion

The findings indicate that students exhibit high awareness of online fraud, reflected in very high perceived susceptibility and high perceived severity scores. This aligns with studies showing that many student and youth populations report substantial knowledge of cybercrime threats and online scams, at least at a declarative level (Toso et al., 2023; Patel & Patel, 2023). Similar patterns of high general awareness have been observed among university students in Saudi Arabia, Nigeria, and Palestine, where most respondents state they know about phishing, cybercrime, or online fraud and basic safety rules (Akazue et al., 2022; Ahmead et al., 2024; Alharbi & Tassaddiq, 2021; Patel & Patel, 2023).

However, the key contribution of these results is the disconnect between acknowledging universal risk and accepting personal vulnerability. Students strongly agree that they are “as likely as anyone else” to be victims, yet are more hesitant to endorse the belief that they themselves are personally at risk. This mirrors the well-documented optimism bias in cybersecurity, where individuals accept that cyber threats are real and widespread but implicitly assume “it won’t happen to me,” leading to diminished motivation to adopt protective measures (Alnifie & Kim, 2023). Meta-analytic evidence shows that such cyber optimism bias is associated with weaker risk perception, reduced preventive behavior, and overconfidence in personal safety online (Alnifie & Kim, 2023).

Related work on university students’ fear and perceived risk of cyber fraud reports a similar pattern: a large proportion of students feel fearful of cyber fraud, but only a small minority judge their own likelihood of victimization as high (Qu et al., 2024). This combination of cognitive recognition of seriousness with psychological distancing from personal risk has also been framed as a “privacy paradox,” where students declare high awareness and concern yet continue behaviors that implicitly deny their own vulnerability (Melchior & Soler, 2024).

Protection Motivation Theory research further suggests that when people feel knowledgeable about cybersecurity, they may perceive cybercrime as severe but simultaneously feel less personally vulnerable and less inclined to take security actions (Kimpe et al., 2021). This may help explain the paradox in the current data: students understand the threat at an abstract level and endorse general susceptibility, yet maintain a subtle sense of invulnerability.

This pattern has important practical implications. If students intellectually accept that online fraud is serious but do not fully internalize personal susceptibility, awareness campaigns focusing only on prevalence and severity may have limited behavioral impact. Literature recommends interventions that explicitly target optimism bias and personalize risk—through vicarious victimization stories, realistic scenarios, and experiential training—to strengthen perceived personal vulnerability and translate awareness into secure behavior (Kimpe et al., 2021; Alnifie & Kim, 2023; Qu et al., 2024; Melchior & Soler, 2024; Alharbi & Tassaddiq, 2021).

The results also indicate that students report high awareness of the effectiveness of safeguards (M = 2.98),

especially traditional technical controls such as strong passwords. Similar patterns appear in prior work, where students show relatively good understanding of basic digital security tools (antivirus, passwords, backups) but important gaps in how they actually deploy them in practice (Althibyani & Al-Zahrani, 2023; Alharbi & Tassaddiq, 2021). For example, higher education students in Saudi Arabia were generally aware of digital security risks, yet still engaged in risky practices such as weak passwords and poor data protection (Althibyani & Al-Zahrani, 2023).

A notable nuance in the present findings is that students attach less value to proactive behavioral measures, such as avoiding suspicious links, than to more “static” technical measures. Studies of cybersecurity awareness among university students and trainees consistently report weak behavioral practices around email, links, and public Wi-Fi, even when conceptual knowledge is present (Alrobaian et al., 2023; Alharbi & Tassaddiq, 2021; Verma & Pawar, 2024). At Majmaah University, many students reported opening emails from unknown senders and accessing email via unsecured networks, suggesting that day-to-day behavior lags behind knowledge of what constitutes safe practice (Alharbi & Tassaddiq, 2021). This reflects broader evidence that digital literacy or security awareness alone does not guarantee secure cybersecurity behavior (Oktapiyadi et al., 2024).

Students in the current data also perceive the cost of safeguards as high (M = 3.03), with inconvenience and effort—rather than money—being the main burdens. Protection Motivation Theory research emphasizes that such response costs (time, hassle, cognitive load) can meaningfully reduce intentions to adopt cybersecurity recommendations, even when people accept their effectiveness (Dodge et al., 2023). Response costs are frequently tied to the perceived complexity and maintenance of good “cyber hygiene,” such as regularly updating software or managing multiple strong passwords (Dodge et al., 2023; Alharbi & Tassaddiq, 2021).

Finally, students express high self-efficacy in recognizing and avoiding scams (M = 3.15), but lower confidence in their specific technical skills for securing accounts. This pattern is consistent with work showing that many students feel confident in identifying threats (e.g., phishing, malware) yet lack deeper technical competencies or overestimate their protective abilities (Althibyani & Al-Zahrani, 2023; Ahamed et al., 2024; Kimpe et al., 2021). Studies on cybersecurity-specific self-efficacy find that higher self-efficacy is associated with stronger security behavior intentions and interest in cybersecurity, but also warn that overconfidence can coexist with real skill deficits (Schafeitel-Tähtinen et al., 2024; Ahamed et al., 2024; Kimpe et al., 2021).

Taken together, these findings and the literature point to an important educational implication: interventions should move beyond raising general awareness and emphasize hands-on, skills-focused training that (a) makes behavioral safeguards more convenient and routinized, and (b) calibrates students’ self-efficacy by linking confidence to demonstrated technical competence (Lui et al., 2025; Schafeitel-Tähtinen et al., 2024; Pirta-Dreimane et al., 2024; Ahamed et al., 2024; Verma & Pawar, 2024).

The relationship between online fraud awareness and social interaction is complex and, at times, paradoxical. A strong sense of self-efficacy—a student’s confidence in their ability to detect and prevent fraud—emerges as a powerful protective factor. The positive correlation between self-efficacy and both the quality of social interactions and life satisfaction suggests that feeling in control of one's online safety translates to a more open, trusting, and fulfilling social life. This reframes cybersecurity training not just as a technical skill but as an intervention for psychological resilience and social well-being (Albohnayh et al., 2024). The opposite is also true; a lack of trust in online systems can negatively impact self-confidence, leading to feelings of isolation and depression (Albohnayh et al., 2024; Ong & Tangsoc, 2020), which explains why students with low self-efficacy may withdraw from online engagement. By contrast, the negative correlation between a student’s self-efficacy and their level of participation suggests that those who lack confidence may actively withdraw from online social engagement to mitigate risk.

Perhaps the most complex finding is the paradoxical effect of perceived severity. The data show that a high perceived severity of online fraud is positively correlated with life satisfaction but negatively correlated with the quality of social interactions. This can be interpreted in two ways. The positive correlation with life

satisfaction suggests that a healthy level of caution and a serious view of the threat may motivate students to take proactive steps, providing them with a sense of control and security that improves their overall well-being. However, the negative correlation with the quality of social interactions suggests that a heightened state of vigilance and fear can erode the trust and openness necessary for building high-quality social bonds (Buse et al., 2023). The need for constant suspicion to detect sophisticated scams, particularly those leveraging AI, can make students more guarded, eroding the foundation of trust that is essential for meaningful social connections (Drew & Webster, 2024; Croll, 2023). This points to a delicate balance that interventions must strike: promoting healthy vigilance without fostering a culture of pervasive fear and mistrust. The social dimension of fraud is further complicated by the fact that perpetrators may themselves have been victims, learning manipulative tactics through a "corrupted form of social learning" within their own networks of deviant peers (Stalans, 2022). Scammers also utilize sophisticated linguistic and psychological tactics to trick and manipulate victims into complying with their aims, which can lead to severe emotional and financial harm (Juanda et al., 2024). The psychological impact extends to emotional trauma, with victims experiencing shock, anger, and loss of trust, and feeling a sense of shame that makes them reluctant to report the crime (Buse et al., 2023).

Recommendations

Based on the study's findings, the following recommendations are presented to enhance security measures against online fraud and improve the students' digital well-being.

1. ***Implement a Multi-Faceted Educational Strategy****:* To address the gap between universal awareness and personal susceptibility, educational programs should shift from generic warnings to personalized, interactive risk assessments. Workshops that use real-life case studies and gamified exercises, such as "Phishing Escape Rooms," can help students internalize their vulnerability and make learning about behavioral safeguards (e.g., spotting suspicious links) more engaging and memorable.
2. ***Reduce the Perceived Cost of Security****:* Recognizing that time and effort are greater barriers than financial cost, institutions should adopt user-friendly, low-friction security solutions. This includes implementing single sign-on (SSO) for all university services to reduce the burden of password management and providing free or subsidized access to enterprise-level security tools like antivirus software and VPNs.
3. ***Leverage Social Networks for Collective Security****:* The high level of social engagement among students presents a valuable opportunity to promote security through peer networks. Institutions should establish a "Cybersecurity Peer Mentor" program and create online forums where students can share information about fraud attempts in real-time, fostering a culture of mutual support and shared responsibility for online safety.
4. ***Foster Psychological Resilience****:* Since self-efficacy is a powerful protective factor for social well-being, interventions should be designed to build students' confidence in their ability to manage online threats. Hands-on, skills-based training on securing online accounts and a clear protocol for reporting and recovering from fraud can empower students, reducing their anxiety and encouraging them to engage more openly in digital spaces. It is also recommended to create a support system with mental health professionals who specialize in cyber-related anxiety to help students cope with the psychological impact of perceived threats.

Conclusion

The study concludes that university students possess a high, but nuanced, awareness of online fraud, with their perceptions of risk consistently strong regardless of their gender, age, or year level. A critical gap exists between a general understanding of the threat and a personal sense of vulnerability, which is compounded by the perceived time and effort required for effective safeguards. The relationship between online fraud awareness and a student's social life is complex. A strong sense of self-efficacy acts as a powerful protective factor, fostering a more open and trusting social life, while a heightened perceived threat

can erode social bonds. Effective security measures must therefore be holistic, addressing not only technical knowledge and behavioral habits but also psychological biases and the social dynamics that define the modern student experience. The study concludes that the student population is heavily male-dominated. This finding is significant for future institutional planning, as it suggests a need for strategic initiatives to promote diversity and gender balance within the student body. The study concludes that students are highly engaged in social activities and that their social interactions contribute positively to their well-being. However, there is room for improvement in fostering deeper, more emotionally supportive relationships, which can be a key area for future student development programs.

References

Ahamed, B., Polas, M., Kabir, A., Sohel-Uz-Zaman, A., Fahad, A., Chowdhury, S., & Dey, M. (2024). Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era. SAGE Open, 14. https://doi.org/10.1177/21582440241228920

Ahmad, I., Khan, S., & Iqbal, S. (2024). Guardians of the vault: unmasking online threats and fortifying e-banking security, a systematic review. Journal of Financial Crime. https://doi.org/10.1108/jfc-11-2023-0302

Ahmead, M., Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. Crime Science, 13. https://doi.org/10.1186/s40163-024-00230-w

Akazue, M., Ojugo, A., Yoro, R., Malasowe, B., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. Indonesian Journal of Electrical Engineering and Computer Science. https://doi.org/10.11591/ijeecs.v28.i3.pp1756-1765

Albohnayh, A., Alshammari, W., Aldoreeb, M., Alsubaie, M., Alismail, A., & Almulla, M. (2024). The Relative Contribution of Social Interaction in Predicting the Quality of Life Among Students of King Faisal University. Revista de Gestão Social e Ambiental. https://doi.org/10.24857/rgsa.v18n1-157

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data Cogn. Comput., 5, 23. https://doi.org/10.3390/bdcc5020023

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data Cogn. Comput., 5, 23. https://doi.org/10.3390/bdcc5020023

Ali, S., Hussain, S., Fatima, M., Arshid, M., & Ashraf, S. (2024). Impact of Social Interaction on Students' Academic Performance: An Exploratory Study of Pakistani Students. Global Social Sciences Review. https://doi.org/10.31703/gssr.2024(ix-i).20

Alivia, N., & Anwar, S. (2022). Academic Fraud Mahasiswa pada Sistem Pembelajaran Daring dengan Self-Efficacy sebagai Variabel Moderasi: Dimensi Diamond Theory dan Penyalahgunaan Teknologi Informasi. Al-Kharaj : Jurnal Ekonomi, Keuangan & Bisnis Syariah. https://doi.org/10.47467/alkharaj.v5i1.1156

Alnifie, K., & Kim, C. (2023). Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis. Journal of Information Security. https://doi.org/10.4236/jis.2023.142007

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation. Big Data Cogn. Comput., 7, 73. https://doi.org/10.3390/bdcc7020073

Althibyani, H., & Al-Zahrani, A. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. Sustainability. https://doi.org/10.3390/su151511512

Ansar, S. A., Yadav, J., Dwivedi, S. K., Pandey, A., Srivastava, S. P., Ishrat, M., Khan, M. W., Pandey, D., & Khan, R. A. (2021). A critical analysis of fraud cases on the Internet. Turkish Journal of Computer and Mathematics Education, 12(12), 424-445.

Anwar, K., & Karneli, Y. (2020). The Relationship between Bullying Behavior and Students' Social Interaction Ability. Jurnal Neo Konseling.(https://doi.org/10.24036/00327KONS2020)

Avcı, M. (2023). Belongingness, Social Connectedness, and Life Satisfaction in College Students after COVID-19 Pandemic. Journal of Happiness and Health. https://doi.org/10.47602/johah.v3i2.43

Azminudin, A., Harun, M., & Mahmud, F. (2025). The Relationship between Self-Esteem, Social Support, and Life Satisfaction among Residential College Students. International Journal of Academic Research in Business and Social Sciences. https://doi.org/10.6007/ijarbss/v15-i3/24663

Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. PLOS ONE, 20. https://doi.org/10.1371/journal.pone.0317232

Buse, C., Lee, E., Kuan, D., & Kheng, M. (2023). A qualitative study on the psychological impact of cyber scams on victims in Singapore. Psychology and Mental Health.(https://doi.org/10.13140/RG.2.2.14810.11204)

Calleja-Núñez, J., Granero-Gallegos, A., Espinoza-Gutiérrez, R., & Baños, R. (2023). Mediating effect of social interaction anxiety between emotional intelligence and life satisfaction in physical education students: post-COVID-19 study. Frontiers in Psychology, 14. https://doi.org/10.3389/fpsyg.2023.1284664

Crasta, S. (2024). ENHANCING CONSUMER VIGILANCE AND MITIGATING TACTICS AGAINST INTERNET SHOPPING FRAUD. Al-Shodhana. https://doi.org/10.70644/as.v12.i2.7

Croll, J. (2023). AI and the future of fraud. Journal of Fraud and Anti-Corruption.

De Felice, D., De Filippis, M., & Paglieri, F. (2022). Two is More Than One: The Cognitive and Neural Benefits of Social Interaction for Learning. Frontiers in Human Neuroscience, 16. https://doi.org/10.3389/fnhum.2022.905658

De Oliveira, E., Morais, C., Pasion, R., & Hodgson, J. (2020). "It is no big deal!": Fraud Diamond theory as an explanatory model to understand students' prevalence and perceptions of severity of academic fraudulent behavior. https://doi.org/10.31219/osf.io/tz4wj

Dias-Oliveira, E., Morais, C., Pasion, R., & Hodgson, J. (2024). "It Is No Big Deal!": Fraud Diamond Theory

as an Explanatory Model for Understanding Students' Academic Fraudulent Behavior. SAGE Open, 14. https://doi.org/10.1177/21582440241266091

Díaz-Iso, A., Eizaguirre, A., & García-Olalla, A. (2020). Understanding the Role of Social Interactions in the Development of an Extracurricular University Volunteer Activity in a Developing Country. International Journal of Environmental Research and Public Health, 17. https://doi.org/10.3390/ijerph17124422

Dodge, C., Fisk, N., Burruss, G., Moule, R., & Jaynes, C. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. Criminology & Public Policy. https://doi.org/10.1111/1745-9133.12641

Drew, M., & Webster, M. (2024). From Phishing to Vishing: A Comprehensive Review of Online Fraud in the Digital Era. Journal of Cybercrime and Digital Forensics, 2(1), 1-15.

Duvnjak, I. (2020). WELL-BEING AND LIFE SATISFACTION OF STUDENTS. International Journal of Advanced Research. https://doi.org/10.21474/ijar01/11772

Farjana, U., Sitaram, M., & Kumar, S. (2024). Automated Fraud Detection in Online Transaction Using Representation Learning. 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT), 1-4.(https://doi.org/10.1109/IC3IoT60325.2024.10550302)

Feraco, T., Resnati, D., Fregonese, D., Spoto, A., & Meneghetti, C. (2022). An integrated model of school students' academic achievement and life satisfaction. European Journal of Psychology of Education, 38, 109 - 130. https://doi.org/10.1007/s10212-022-00620-1

Getenet, S., Cantle, R., Redmond, P., & Albion, P. (2024). Students' digital technology attitude, literacy and self-efficacy and their effect on online learning engagement. International Journal of Educational Technology in Higher Education, 21, 1-20. https://doi.org/10.1186/s41239-023-00437-y

Ghani, S., Awang, M., Ajit, G., & Rani, M. (2020). Participation in Co-Curriculum Activities and Students' Leadership Skills. Journal of Southwest Jiaotong University, 55.((https://doi.org/10.35741/ISSN.0258-2724.55.4.48))

Hamilton, A. (2024). The neural and cognitive basis of social interaction: The four networks that make us human. Journal of the Royal Society of Medicine, 117. https://doi.org/10.1177/01410768241228221

He, Q., Tan, Y., & Cao, S. (2024). The effect of perceived social support on undergraduate nursing students' life satisfaction: A mediating model. Social Behavior and Personality: an international journal. https://doi.org/10.2224/sbp.13362

Isohätälä, J., Näykki, P., & Järvelä, S. (2020). Cognitive and Socio-Emotional Interaction in Collaborative Learning: Exploring Fluctuations in Students' Participation. Scandinavian Journal of Educational Research, 64, 831 - 851. https://doi.org/10.1080/00313831.2019.1623310

Juanda, N., Rosli, N., Anisah, N., & Azizi, N. (2024). A study on the linguistic features of online scams and their impact on victims. Journal of Applied Linguistics.

Kapur, S. (2023). The importance of social interaction and relationship management in day-to-day life. International Journal of Social Science Research and Review.

https://doi.org/10.47814/ijssrr.v6i10.1066

Khan, S., Khalid, A., Iqbal, M., & Shahzadi, N. (2021). Cognitive Distortions, Social Interaction Anxiety and Life Satisfaction among School Students. Journal of Pakistan Psychiatric Society. https://doi.org/10.63050/jpps.18.04.120

Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41, 1796 - 1808. https://doi.org/10.1080/0144929x.2021.1905066

Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41, 1796 - 1808. https://doi.org/10.1080/0144929x.2021.1905066

Kuah, N., Pang, M., & Liew, W. (2024). The Impact of Cybersecurity Knowledge, Perceived Severity and Subjective Norm on Online Financial Scams Awareness. International Journal of Social Science Research and Review. https://doi.org/10.47814/ijssrr.v7i4.1203

Lee, Y., Gan, C., & Liew, T. (2023). Susceptibility to instant messaging phishing attacks: does systematic information processing differ between genders?. Crime Prevention and Community Safety, 25, 179-203. https://doi.org/10.1057/s41300-023-00176-2

Lenka, S., & Tiwari, R. (2025). A Hybrid ML and Data Science Approach to Detect Online Fraud Transaction at Real Time. Journal of Neonatal Surgery. https://doi.org/10.52783/jns.v14.1601

Lestari, S., Adawiyah, W., Alhamidi, A., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. Safer Communities. https://doi.org/10.1108/sc-04-2024-0018

Liu, L., & Zhang, H. (2021). Financial literacy, self-efficacy and risky credit behavior among college students: Evidence from online consumer credit. Journal of Behavioral and Experimental Finance. https://doi.org/10.1016/j.jbef.2021.100569

Lui, A., Womack, C., & Orton, P. (2025). Collaborative online international learning as a third space to improve students' awareness of cybersecurity. Education and Information Technologies, 30, 13835 - 13856. https://doi.org/10.1007/s10639-025-13336-8

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. https://doi.org/10.3389/fpsyg.2025.1508363

Melchior, C., & Soler, U. (2024). Security of Personal Data in Cyberspace in the Opinion of Students of the University of Udine. Cybersecurity and Law. https://doi.org/10.35467/cal/188451

Nikitkov, A., & Bay, A. (2008). Young Adults, Digital Literacy, and Online Fraud. Journal of Consumer Affairs, 42(3), 487-509.

Niman, M., Anggraeni, S., & Guntara, A. (2023). Online Love Fraud against Indonesian Women: A Phenomenological Study of Victims' Experiences. Journal of Cybercrime and Digital Forensics. https://doi.org/10.51867/jcydif.v2i2.204

Oktapiyadi, W., Saepudin, E., & Yanto, A. (2024). HUBUNGAN LITERASI DIGITAL DENGAN PERILAKU KEAMANAN SIBER PADA MAHASISWA PERPUSTAKAAN DAN SAINS INFORMASI UNIVERSITAS PADJADJARAN. Info Bibliotheca: Jurnal Perpustakaan dan Ilmu Informasi. https://doi.org/10.24036/ib.v5i2.464

Papasavva, A., Johnson, S., Lowther, E., Lundrigan, S., Mariconti, E., Markovska, A., & Tuptuk, N. (2024). Application of AI-based Models for Online Fraud Detection and Analysis. ArXiv, abs/2409.19022. https://doi.org/10.1186/s40163-025-00248-8

Patel, D., & Patel, R. (2023). Awareness and information seeking behavior of B.Ed students: A cyber study. International Journal of Research in Library Science. https://doi.org/10.26761/ijrls.9.2.2023.1672

Pathan, S., Jadhav, A., Shaikh, M., Huke, A., Mate, G., & Prasad, C. (2024). Innovations in Safeguarding Online Financial Transactions using Ensemble Learning. 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0, 1-6.(https://doi.org/10.1109/OTCON60325.2024.10687815)

Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R., & Bonders, M. (2024). Try to esCAPE from Cybersecurity Incidents! A Technology-Enhanced Educational Approach. Technology, Knowledge and Learning, 30,1577 - 1606. https://doi.org/10.1007/s10758-024-09769-8

Qu, J., Lin, K., Wu, Y., & Sun, I. (2024). Fear and perceived risk of cyber fraud victimization among Chinese University students. Crime, Law and Social Change. https://doi.org/10.1007/s10611-024-10155-9

Qu, J., Lin, K., Wu, Y., & Sun, I. (2024). Fear and perceived risk of cyber fraud victimization among Chinese University students. Crime, Law and Social Change, 82, 543 - 562. https://doi.org/10.1007/s10611-024-10155-9

Rachmad, Y. E. (2022). Social Engagement Theory.((https://doi.org/10.17605/OSF.IO/KSR4V))

Rezaei, A., & Jeddi, E. (2020). Relationship between wisdom, perceived control of internal states, perceived stress, social intelligence, information processing styles and life satisfaction among college students. Current Psychology, 39, 927-933.((https://doi.org/10.1007/S12144-018-9804-Z))

Ridkodubska, H. (2023). THE STATE OF DEVELEPMENT STUDENTS' SOCIAL ACTIVITY. Humanitarian studies: history and pedagogy. https://doi.org/10.35774/gsip2023.02.094

Saleem, M. (2021). Relationship of Social Skills with Life Satisfaction of Public and Private Secondary School Students. **5**, 404-416.(https://doi.org/10.35484/PSSR.2021(5-III)30)

Santos, T., Turpo-Chaparro, J., Apaza-Tarqui, E., Apaza-Romero, A., & López, S. (2023). Social Support and Empathy as Predictors of Life Satisfaction in Brazilian University Students. Journal of Educational and Social Research. https://doi.org/10.36941/jesr-2023-0084

Schafeitel-Tähtinen, T., Koskinen, J., & Helenius, M. (2024). Measuring Cybersecurity Teaching: Case University Students in Finland. International Journal of Learning and Teaching. https://doi.org/10.18178/ijlt.10.4.481-490

Sharma, P. (2024). Algorithms and strategies for fraud prevention on online platforms. World Journal of Advanced Research and Reviews. https://doi.org/10.30574/wjarr.2024.23.2.2462

Shetty, V., R., P., & Malghan, R. (2023). Safeguarding against Cyber Threats: Machine Learning-Based Approaches for Real-Time Fraud Detection and Prevention. RAiSE 2023. https://doi.org/10.3390/engproc2023059111

Smith, K., Emerson, D., & Kelly, M. (2024). The role of self-efficacy and the fraud diamond on the decision to use assignment assistance websites. Current Psychology. https://doi.org/10.1007/s12144-024-06965-8

Sriram, R., Weintraub, S., Cheatle, J., Haynes, C., Murray, J., & Marquart, C. (2020). The Influence of Academic, Social, and Deeper Life Interactions on Students' Psychological Sense of Community. Journal of College Student Development, 61, 593 - 608. https://doi.org/10.1353/csd.2020.0057

Stalans, L. (2022). Scammer is a victim: The social and emotional context of internet fraud. Journal of Financial Crime. https://doi.org/10.1108/jfc-04-2022-0091

Subramanian, S. (2024). Fort-Trust: Safeguarding online transaction by machine learning. Salud, Ciencia y Tecnología - Serie de Conferencias. https://doi.org/10.56294/sctconf20241026

Toso, C., Jumalon, A., Magadan, J., Alvarico, A., & Cuevas,, J. (2023). Cybercrime Awareness Among Senior High School Students. Mediterranean Journal of Basic and Applied Sciences. https://doi.org/10.46382/mjbas.2023.7218

Unlu, C., & Çeviker, A. (2022). Examination of the Social Skills Levels of Students Participating in Recreative Activities. International Journal on Social and Education Sciences. https://doi.org/10.46328/ijonses.470

Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management. Financial Innovation, 9, 1-25. https://doi.org/10.1186/s40854-023-00470-w

Verma, V., & Pawar, J. (2024). Assessment Of Students Cybersecurity Awareness And Strategies To Safeguard Against Cyber Threats. Journal of Advanced Zoology. https://doi.org/10.53555/jaz.v45is4.4156

Vidić, T. (2024). Primary school students' perceptions of social support, school satisfaction and life satisfaction. International Journal of Emotional Education. https://doi.org/10.56300/qcbn1811

Vimal, K., Yadav, J., & Dwivedi, S. (2021). A critical analysis of fraud cases on the internet. Turkish Journal of Computer and Mathematics Education, 12(12), 424-445.

Vuorenmaa, E., Nguyen, A., & Järvelä, S. (2024). How do social interaction and group-level regulation shape task perceptions in collaborative learning task?. Scandinavian Journal of Educational Research. https://doi.org/10.1080/00313831.2024.2394409

Wachsmuth, S., Lewis, T., & Gage, N. (2023). Exploring Extracurricular Activity Participation, School Engagement, and Social Competence for Students With Emotional and Behavioral Disorders. Behavioral Disorders, 48, 255 - 268. https://doi.org/10.1177/01987429231166675

Wang, P., Shi, H., Yu, Z., & Chen, G. (2024). Exploring emotional trajectories of online fraud victims: A sentiment analysis of social media texts. Computers in Human Behavior. https://doi.org/10.1016/j.chb.2024.108398

Zahid, S., Jamal, R., & Hassan, B. (2025). Role of Perceived Social Support in Stress,Life Satisfaction and Academic Performance Among University Students. Pakistan Journal of Psychological Research. https://doi.org/10.33824/pjpr.2025.40.1.13

Zhang, H., Liu, G., Li, S., Wang, C., & Zhang, Y. (2022). Psychological and Social Mechanisms of Online Fraud Victimization in China. Frontiers in Psychology, 13. https://doi.org/10.3389/fpsyg.2022.846665

Cite this article as: Luo Yuchao and Immanuel T. San Diego (2026). The Role of Big Data in Advancing Artificial Intelligence: Methods and Case Studies. *International Journal of Artificial Intelligence and Machine Learning,* 6(1), 168-184. doi: 10.51483/IJAIML.6.1.2026.168-184.