JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(2), 1452-1462
ISSN: 2589-1316

Knowledge on Cyber Crime or 'Love Scam': How Does the Higher Education Institutions' (HEIs) Students Define Them?

Nur Hafizah Md Akhir [1], Muhamad Ali Imran Kamarudin [2*], Abdul Razak Abd Manaf [3], Wan Su Haji Haron [4]

[1]School of Applied Psychology, Social Work and Policy, Universiti Utara Malaysia, Kedah, MALAYSIA. Email: nurhafizah.md.akhir@uum.edu.my
[2] School of Business Management, Universiti Utara Malaysia, Kedah, MALAYSIA. Email: aliimran@uum.edu.my
[3]School of Applied Psychology, Social Work and Policy, Universiti Utara Malaysia, Kedah, MALAYSIA; Email: a.razak@uum.edu.my
[4] Malaysia Crime Prevention Foundation, Alor Setar, Kedah, MALAYSIA; Email: ezwans2001@yahoo.com

***Corresponding Author:** aliimran@uum.edu.my

Citation: Akhir, N. H. M., Kamarudin, M. A. I., Manaf, A. R. A. and Haron, W. S. H. (2025). Knowledge on Cyber Crime or 'Love Scam': How Does the Higher Education Institutions' (HEIs) Students Define Them?, *Journal of Cultural Analysis and Social Change*, 10(2), 1452-1462. https://doi.org/10.64753/jcasc.v10i2.1829

Published: November 14, 2025

ABSTRACT

Cybercrime is one of the hot issues that occur around the world. Society's addiction to social media and technology has been a one of contributing factors in the rise of cybercrime. Various categories of cybercrime are reported including telecommunications fraud, online purchases, personal data breaches, pornographic materials and cyber love scams are no exception. In fact, the addiction towards the usage of the internet or social media makes higher education institutions' (HEIs) students a vulnerable group towards love scam. Therefore, this study aims to explore HEI students' understanding on what constitute a cybercrime of love scam and what defines love scam from their perspective. This study exploits a qualitative study using Focus Group Discussion (FGD) approach among 12 students from various universities or HEIs in Northern Region of Malaysia. The data gathered is then analyzed using thematic analysis with the use of Nvivo12 software. The findings revealed that the students perceived that the definition of love scam can be categorized as, i) love fraud, ii) financial fraud, iii) dissemination of personal information, and iv) criminal behaviour. This study implicates the policy makers in designing the policy on community awareness for love scam to emphasize its' real definition. While practically, every community member's specially HEIs' students to be more alert and proactive and being knowledgeable on this matter.

Keywords: Cybercrime, Love Scam, Higher Education Institutions (HEIs), Knowledge, Readiness

INTRODUCTION

Malaysia's advancements in today's digital era and technology including green technology have solidified its position as a rising hub for innovation (Masood et al., 2024; Sidek et al., 2024), driving the nation's economic growth and global competitiveness in the developing world (Abaidah et al., 2024). Such development of the country's rapid digital transformation has a significant drawback (or flaw) in terms of its exposure to cyber threats and security (Mat et al., 2019), which requires a clear mitigation of such risks.

In this current fast-evolving world, crime does occur both physically and virtually (or online crime or cybercrime). It is claimed that despite a decline in physical crime cases in the country, Malaysia's number of cybercrime index cases is concerningly rising (Mohd et al., 2021). It is claimed that most reputable definition of cybercrime is by Thomas and Loader (2013) which is defined as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks (p.3).

It is further elaborated that cybercrime does not only focus on issues related to confidentiality and integrity, but also involves online fraud crimes (Graham, 2023; Tropina et al., 2015).

Background of the Study

The phenomenon of love scams which defined as a virtual (or online) fraudulent romantic relationship with the intent to deceive victims both financially and emotionally (Bidin et al., 2015; Fuad et al., 2022), has become increasingly prevalent among youth, particularly students in higher education institutions (HEIs). It is reported that love scam occurs in various Asian countries including Indonesia and Malaysia (Nomleni, 2023).

Most cybercriminals who also known as 'scammers' or 'love scammers' are members of international syndicates who disguise themselves as romantic partners by using fake profiles such as photos of models, officers or uniformed members who can attract the attention of victims (Suarez-Tangil et al., 2019; Syecha & Solihah, 2023). According to Syecha and Solihah (2023), most cybercriminals will steal other individuals' identities such as on modelling websites to attract the attention of victims. As stated by Fuad et al. (2022), victims of fraud cases not only cause losses of tens or thousands of ringgits but also have a long-lasting emotional impact.

Numerous factors have been reported to contribute to the susceptibility of victims becoming entangled in love scam incidents. In the recent studies conducted in Malaysia, Bong (2023) and Kuah et al. (2024) claimed that students, especially those in higher education, are vulnerable to romance or love scams because they were lacking in information or rather has minimal online literacy and privacy. These kinds of situations are a major factor in this group's increased online trust, disregard for privacy settings, and inadequate password management techniques (Bong, 2023; Kuah et al., 2024).

The Evolvement of Internet Technology

The evolution of internet technology has profoundly enhanced access to knowledge, communication, and educational equity, particularly for students in higher education institutions (HEIs) (Masood et al., 2024; Sidek et al., 2024). With the integration of high-speed connectivity, cloud computing, and AI-driven platforms, students now benefit from flexible, personalized learning environments that transcend traditional classroom boundaries. In Malaysia, the shift toward e-learning which accelerated by the COVID-19 pandemic, has enabled HEIs to adopt immersive tools such as learning management systems (LMS), virtual reality (VR), and digital libraries, fostering experiential and lifelong learning opportunities (MIDA, 2021).

Moreover, the internet facilitates global collaboration, allowing students to engage in cross-border research, virtual internships, and peer-to-peer learning, thereby enhancing their digital literacy and employability (Kamarudin et al, 2023; Shivam, 2025). A systematic review by Nhleko et al. (2025) further underscores that internet-based technologies significantly boost student motivation and reduce dropout rates by offering interactive and engaging content tailored to individual learning needs. Collectively, these advancements underscore the internet's pivotal role in democratizing education and preparing students for the demands of Industry 4.0.

However, such advancement has transformed interpersonal communication landscape which enabled new forms of social interaction while simultaneously exposing users to novel cyber threats. In the recent years, the global digital landscape witnessed a surge in mobile internet usage, cloud-based applications, and AI-driven platforms, all of which have reshaped how individuals connect and form relationships online.

It is notably important that the policymakers (or government) worldwide have acknowledged that the advancement of technology comes with the unintended consequences of digital proliferation, including increased vulnerability to cybercrime which exploited through real-time communication tools and deepfake technologies. Such digital shift has blurred the boundaries between virtual and real-life relationships, making it easier for scammers to impersonate identities and manipulate victims emotionally. The accessibility and anonymity of the internet have thus become critical enablers of love scams.

The Rise of Social Media and Youths' Addiction

Social media platforms such as Facebook, Instagram, and TikTok have become integral to student life, offering spaces for self-expression, networking, and emotional support. However, this ubiquity has also led to problematic usage patterns. Studies have shown that Malaysian university students spend an average of 20.9 hours per week online, with a significant portion dedicated to social networking (Fauzi, 2024; Kutti et al., 2022; Ting & Essau, 2021).

Faudzi (2024) found that excessive social media use among HEIs students correlates with lower academic performance, reduced self-esteem, and increased susceptibility to online manipulation. The addictive nature of these platforms—driven by algorithmic reinforcement and fear of missing out (FOMO) creates fertile ground for love scams, as students may seek validation or emotional connection online.

Moreover, a systematic review by Yusuf and Kadir (2024) highlighted that social media usage among Malaysian youth is linked to psychological vulnerabilities such as anxiety, depression, and distress, which can impair judgment and increase the likelihood of falling victim to scams. Put those into perspectives, it is crucial for researchers to understand how students define or perceive love scams requires contextualizing the issue within broader technological, social, and regional developments.

Problem Statement

Cyber-enabled scams, particularly romance or love scams, have surged across Asia in recent years, with Malaysia emerging as a significant hotspot. According to the State of Scam Report 2024, Malaysians suffered financial losses amounting to RM54.02 billion (USD 12.8 billion) in a single year—equivalent to approximately 3% of the national GDP. Love scams alone constituted 2.7% of all reported cybercrimes in 2023, with the majority of victims encountering perpetrators through social media platforms and messaging applications (State of Scam Report, 2024).

The proliferation of advanced technologies, especially Artificial Intelligence (AI), has further exacerbated the complexity of online scams. AI-driven deception techniques such as voice cloning, deepfake videos, and automated emotional manipulation have blurred the boundaries between genuine and fraudulent online interactions (Bilz et al., 2023; Lallie et al., 2021). Alarmingly, a recent survey revealed that 25% of Malaysian respondents were uncertain whether AI had played a role in the scams they experienced (Cyber Security Malaysia, 2024), underscoring the urgent need for public education on emerging digital threats.

Among students in higher education institutions (HEIs), the emotional and psychological impact of love scams is particularly pronounced. This demographic is often in the midst of identity formation and emotional development, making them especially susceptible to manipulation through digital intimacy and trust-based deception (Bong, 2023). A qualitative study conducted by Amerruddin (2021) at a Malaysian public university found that while students were generally aware of love scams, many had either direct or indirect experiences with such incidents. The study emphasized the necessity of targeted awareness campaigns and preventive education tailored to the unique vulnerabilities of university students.

The conceptualization of love scams among HEI students is shaped by a confluence of factors including rapid technological advancement, pervasive social media engagement, and regional trends in cybercrime. As digital relationships become increasingly normalized, students must be equipped not only with technical cybersecurity competencies but also with emotional resilience and critical digital literacy to navigate online interactions safely (Kuah et al., 2024; Tirumala et al., 2019).

Significance of the Study

This research holds significant relevance in the Malaysian context, particularly considering escalating cybercrime trends and the increasing vulnerability of youth in digital spaces. The State of Scam Report (2024) reported that Malaysia has recorded RM54.02 billion in scam-related losses in 2023 which is equivalent to 3 percent (3%) of national Gross Domestic Product (GDP). In fact, love scams have emerged as one of the most contributing cases particularly insidious form of cybercrime, exploiting emotional trust and digital intimacy. Here, HEI students who are actively engaged in identity formation and emotional development, represent a high-risk group due to their frequent use of social media and messaging platforms where such scams often originate (Bong, 2023; Bilz et al., 2023).

From a policy perspective, this study contributes to national efforts under the Malaysia Cyber Security Strategy 2020–2024, which emphasizes the need for targeted digital safety education and youth protection. By examining how students conceptualize love scams, the research offers empirical evidence to support ministries and agencies such as CyberSecurity Malaysia and the Ministry of Higher Education (MOHE) in designing culturally responsive awareness campaigns and preventive frameworks (CyberSecurity Malaysia, 2024). The findings can also inform updates to legal instruments, particularly those addressing AI-driven deception such as voice cloning and deepfake manipulation, which have complicated scam detection and enforcement (Lallie et al., 2021).

Practically, the study provides actionable insights for HEIs to strengthen institutional safeguards. Universities can use the findings to develop student-centric interventions, including counselling services, peer education programs, and curriculum-integrated digital literacy modules. These initiatives are essential for fostering emotional resilience and critical thinking skills among students, enabling them to navigate online relationships with greater awareness and caution (Amerruddin, 2021; Kuah et al., 2024). Previous research has shown that students often lack access to tailored preventive education, despite being aware of or directly affected by love scams, underscoring the need for institutional responsibility in addressing this issue (Bong, 2023).

Theoretically, the research advances understanding of how socio-technological factors shape perceptions of cybercrime among youth. It contributes to broader discourses in cyber-psychology, media ecology, and digital trust by exploring the intersection of emotional vulnerability, technological immersion, and online risk perception (Bilz et al., 2023). By situating the study within Malaysia's multicultural and digitally dynamic environment, it offers a localized lens to global scholarship on romance scams and AI-mediated deception. This not only enriches theoretical models but also positions Malaysia as a key contributor to ASEAN-wide efforts in harmonizing digital safety education and youth protection strategies (Alavi et al., 2018).

LITERATURE REVIEW

Cybersecurity and Love Scams

Cybersecurity plays a pivotal role in safeguarding individuals from online scams, including romance or love scams, which have become increasingly prevalent in the digital age. Love scams, a form of cyber-enabled fraud, typically involve perpetrators who exploit emotional vulnerabilities to gain financial or personal advantage through deceptive online relationships (Bilz et al., 2023). These scams are often facilitated through social engineering tactics, where cybercriminals manipulate victims by building trust and emotional intimacy before initiating fraudulent requests (Lallie et al., 2021).

University students are particularly vulnerable to such scams due to their high engagement with digital platforms and comparatively low levels of cybersecurity awareness. Bong (2023) conducted a study among Malaysian university students and found that many lacked fundamental knowledge in areas such as online trust, privacy settings, and password management. This deficiency significantly increased their susceptibility to romance scams, especially when interacting on social networking and dating platforms. Similarly, Kuah et al. (2024) emphasized that students in higher education institutions often underestimate the risks associated with online interactions, making them prime targets for cybercriminals.

The psychological and emotional manipulation inherent in love scams has been well-documented. According to Bilz et al. (2023), scammers often employ tactics such as flattery, fabricated personal stories, and staged crises to elicit sympathy and financial support from victims. These techniques are particularly effective among younger individuals who may be navigating emotional relationships for the first time and lack the digital literacy to detect fraudulent behavior.

In Malaysia, the issue has gained prominence due to the increasing number of reported cases among university populations. A qualitative study by Muhammad Irfan Bin Amerruddin (2021) at Universiti Teknologi MARA revealed that students were not only victims of love scams but also lacked awareness of the modus operandi used by scammers. The study recommended targeted interventions, including peer-led awareness campaigns and integration of cybersecurity modules into university curricula.

To address these vulnerabilities, scholars have advocated for comprehensive cybersecurity education programs within higher education institutions. Tirumala et al. (2019) argue that structured training in digital hygiene, privacy management, and scam recognition can significantly reduce the risk of victimization. Moreover, awareness campaigns tailored to the socio-cultural context of Malaysian students have been proposed to enhance their ability to critically assess online interactions and recognize red flags associated with romance scams (Bong, 2023; Kuah et al., 2024).

Love Scams and Definitions

Love scams, also known as romance scams, involve cybercriminals posing as romantic partners to deceive victims into financial transactions. Past studies claimed that the definition of love scams has evolved (Bilz et al., 2023; DeLiema & Witt, 2024; Muhammud & Muhammad, 2022), with recent studies categorizing them as a form of mass marketing fraud that exploits emotional vulnerabilities.

According to Bilz et al. (2023), love scams, also referred to as romance fraud, involve cybercriminals engineering a romantic relationship on online dating platforms with the intent of financial exploitation. This definition asserted that crime which emotionally manipulated, resulting in heartbreak and significant financial loss. While in a Muhammud and Muhammad (2022) posited that love scam described as a strategic manipulation and deceptive process, often targeting vulnerable groups such as women, by building false romantic relationships online to gain trust and ultimately exploit the victim.

A study conducted at Amerruddin (2021) found that students often fall victim to love scams due to trust in online relationships and lack of awareness about fraudulent tactics. Another systematic literature review highlights that scammers use persuasive techniques such as fake identities, emotional manipulation, and fabricated emergencies to extract money from victims. In Malaysia, online romance scams have been increasing, with reports indicating that financial losses from such scams have surged (Chethiyar et al., 2021; Purwaningrum et al., 2023; Wilson et al., 2024). With such a surge in the number of love scam cases, Wilson et al. (2024) highlighted the importance of higher education institutions should integrate scam awareness programs into their curriculum to educate students on identifying fraudulent online relationships.

Perspectives on Love Scam Definition

The definition of love scams varies across disciplines, reflecting different perspectives on their nature and impact. Some scholars frame love scams as a cybersecurity threat, emphasizing the technological manipulation and online deception involved (Gaviria-Marin & Cruz-Cazares, 2020; Muhammud & Muhammad, 2022). Others approach them as a form of psychological manipulation, where scammers exploit emotional vulnerabilities to gain trust and extract financial or personal benefits (Bilz et al., 2023; Artemova, 2022). This duality highlights the complexity of love scams, which operate at the intersection of digital crime and emotional exploitation.

A study conducted among students from a local public indigenous university in Malaysia revealed that victims of love scams often suffer emotional distress and financial loss, with long-term psychological consequences such as anxiety, shame, and social withdrawal (Muhammud & Muhammad, 2022). It also underscores the gendered nature of these scams, noting that women are disproportionately targeted due to societal expectations around emotional investment and trust in romantic relationships. Scammers often exploit cultural norms and relational cues to manipulate victims, making the deception more convincing and harder to detect (Hamadi & Saari, 2023).

From a legal standpoint, Malaysia has made strides in developing cybercrime legislation to address online scams, including love scams. However, enforcement remains a significant challenge due to fragmented legal frameworks and limited cross-agency coordination (Kamaruddin et al., 2022). Scholars argue that effective intervention requires collaboration between law enforcement agencies, universities, and cybersecurity experts to raise awareness, strengthen digital literacy, and improve detection mechanisms (Hamadi & Saari, 2023; Bilz et al., 2023). As love scams continue to evolve in sophistication, a multidisciplinary approach is essential to protect vulnerable populations and mitigate the social and economic impact of this growing cybercrime.

METHODOLOGY

Research Design

This study employs a qualitative research approach, specifically Focus Group Discussion (FGD), to explore how undergraduate students from various universities in Northern Malaysia define and perceive love scams. Qualitative research is suitable for capturing in-depth insights into students' experiences and perspectives, allowing for a rich exploration of themes related to online romance fraud (Abaidah et al., 2024; Kamarudin et al., 2025; 2024).

FGD is often chosen as the primary method by researchers as it facilitates interactive discussions, challenge ideas, enabling participants to share personal experiences as well as refine definitions collectively (Akyıldız & Ahmed, 2021; Bajnok et al., 2024). According to Bajnok et al. (2024), FGDs are particularly effective in higher education research, as they encourage collaborative knowledge-building among students with diverse backgrounds.

The study involves 12 undergraduate students from various universities, representing different academic programs, semesters, and states. This diversity ensures a comprehensive understanding of how love scams are perceived across different student demographics.

Data Collection

Data collection is conducted through four structured FGD sessions, each lasting approximately 90 minutes. The discussions are moderated by a trained facilitator, ensuring that participants remain engaged and that key themes are explored thoroughly. Participants are selected using purposive sampling, ensuring representation from different academic disciplines and geographical locations (Akhir, 2024; Akhir et al., 2020). This approach aligns with the recommendations of past studies by Akhir (2020) which emphasize the importance of diverse participant selection in FGD-based studies.

The discussions were focused on few important aspects of i) students' awareness of love scams (e.g., online romance fraud, financial deception), ii) personal experiences or encounters with love scams, iii) factors influencing students' vulnerability to scams, and iv) definitions and perceptions of love scams. All discussions are audio-recorded and transcribed verbatim for analysis. Ethical considerations, including informed consent and confidentiality, are strictly adhered to, following guidelines outlined as per Akhir et al. (2020) and Amerruddin (2021).

Data Analysis

The collected data is analyzed using thematic analysis, a widely used qualitative method for identifying, analyzing, and reporting patterns within data. Thematic analysis follows Braun & Clarke's (2019) six-step framework, as per exemplified in table 3.1 below,

Table 3.1. Thematic Analysis Steps in Defining the Love Scams among Higher Education Institutions' (HEIs) students

	Thematic Analysis Step	Description
1	Familiarization with data	Reviewing transcripts and identifying initial insights.
2	Generating initial codes	Systematically coding relevant features of the data.
3	Searching for themes	Grouping codes into broader themes related to love scams.
4	Reviewing themes	Refining themes to ensure coherence and relevance
5	Defining and naming themes	Clearly articulating the meaning of each theme.
6	Producing the report	Synthesizing findings into a structured analysis.

Furthermore, Shaari et al. (2019) highlight that thematic analysis is particularly effective in cybercrime research, as it allows researchers to capture nuanced perspectives on online scams. Key themes emerging from the analysis include, i) Emotional manipulation in love scams, ii) Financial exploitation and trust-based deception, iii) Students' awareness and preventive strategies, iv) Legal and institutional responses to love scams.

FINDINGS

The primary objective of this study is to explore the knowledge of university students regarding the concept of cyber romance crime, with a specific focus on their understanding of its definition. The sub sections afterwards revealed the four (4) themes identified as definition of love scam from the respondents' perspective namely, i) love fraud, ii) financial fraud, iii) dissemination of personal information, and iv) criminal behaviour.

Love Fraud

Based on the statements from R11, cyber romance crime is defined as an acquaintance that leads to a dishonest romantic relationship, not with the intention of genuine affection but rather to take advantage of the partner. Additionally, R4 states that cyber romance crime involves a relationship in which one party conceals their identity for the purpose of deception. The individuals in such relationships do not communicate transparently or meet in person, yet they maintain a romantic connection. Respondents also noted that such incidents have happened to others but not to themselves.

Furthermore, R5 describes cyber romance crime as online deception in the context of love. As noted by R4, the individuals involved have never met face-to-face. For example, a man may attempt to woo a professional woman with the intent of exploiting her trust and offering false affection. R5 also emphasizes that deception constitutes a form of crime.

R13 shared the experience of a friend who fell victim to a romance scam through a social media acquaintance. The victim was excited to talk about their partner and even planned an engagement ceremony despite never having met in person. The respondent found it unusual that their friend could decide to get engaged without a face-to-face meeting. However, in the end, the respondent discovered that their friend had been deceived and lost five thousand ringgits (RM5,000).

> "Bagi saya dia macam you kenal dengan orang tu then jalinkan hubungan dengan dia like bercinta kenal and then itu boleh membuatkan our patner menipu, dia bukan nak bercinta pun tapi ambil kesempatan kepada kita, kira banyak tipulah," (R11)

> "Jenayah cinta siber ni dia tak pernah tunjuk dia punya identiti, dia tak pernah bercakap sesama sendiri dari segi verbal, tak pernah jumpa tapi diaorang bercinta dan tahu-tahu perempuan tu kena tipu. Benda ni pernah terjadi pada orang lain cuma tak pernah terjadi lagi pada diri kita. (R4)

> "Bagi saya jenayah cinta siber ni penipuan yang berlaku antara pasangan atas talian. Contohnya macam kenal orang tu tak pernah jumpa face to face, Jenayah tu maksudnya macam tipu orang scam, contoh seorang wanita tu bekerjaya orang lelaki tu orang biasa je, so dia tahu wanita tu bekerjaya dia kenal suka2 macam tu lepas tu dia nak ambil kesempatan la bukan cinta yang sebab sayang tu". (R5)

> "….pengalaman kawan saya, dia kenal dengan lelaki tu dari sosial media, dia bercerita dengan saya, dia seronoklah sampai kata nak tunang apa semuakan, saya pun ok jela, tapi bila tanya pernah jumpa dia kata tak pernah, pelik juga tak pernah jumpa tapi dia nak tunang. Last-last saya tahu dia kena scam je, habis dalam lima ribu dekat lelaki tu." (R13)

Financial Fraud

According to respondent R10, cyber romance crime involves financial fraud, where perpetrators begin with small loan requests that gradually increase. They may deceive victims by sending items via postal services, persuading them to cover shipping costs under the pretence of financial hardship, while the funds serve the perpetrator's own interests. Additionally, respondent R6 highlights that cyber romance crime is primarily a financial scam conducted through online relationships, with most victims being women. Feelings of loneliness drive victims to engage with perpetrators, eventually trapping them in a cycle of financial exploitation.

Furthermore, respondent R8 notes that cyber romance crime is not exclusive to male perpetrators, as some women also engage in financial fraud by soliciting monetary rewards from male victims. The trust built within these relationships leads victims to provide financial assistance as requested by the female perpetrators. Similarly, respondent R12 describes cyber romance crime as a form of financial deception, where perpetrators establish relationships through social media and identify victims who are easily manipulated. Once trust is established, they exploit victims by requesting financial aid under fraudulent pretences.

> "….dia mula dengan saya tak cukup duit topup boleh tak awak bayar dulu RM5, ha dia akan mula dengan amount yang sikit, bila dah sikit dia akan mula dengan amount yang besar sikit. RM100 boleh tak pinjam lepastu dia mula la pulak saya ada benda nak hantar dekat awak tapi saya tak lepas duit shipping, boleh tak awak bayar dulu, tapi last-last duit tu dia yang ambil." (R10)
>
> "satu penipuan yang berlaku di alam maya yang melibatkan pasangan samada lelaki tu scam perempuan atau perempuan tu scam lelaki tapi kebanyakan yang kita tengok sekarang ni lelaki la yang banyak scam Perempuan. Scam tu dari segi dia nak duit. mungkin dia layankan sebab dia sunyi perempuan kan, dia sunyi dia kenal dengan seseorang tu mesti dia tertarik, lepas tu lelaki tu maybe dia nak duit la, jenayah cinta siber ni dia bercinta dengan seseorang tu sebab dia nak dapatkan keuntungan dia sendiri terutama sebab duit." (R6)
>
> "Ini contoh kes perempuan yang scam la kan, lepas tu dia macam selalu minta macam kewanganlah dengan lelaki tu. Bila kita perempuan kita ada keinginankan. Lepas tu bila dah ada enggangement tu lelaki tu dah percaya macam ada minat dekat perempuan tu so dia bagilah duit." (R8)
>
> "….dia buat connection dekat sosial media, lepas tu dia nampak orang tu senang kena game lepastu dia dia minta duit macam tu dengan perempuan tu. Saya nampak yang tu la". (R12)

Dissemination of Personal Information

According to R11, cyber romance crime involves the dissemination of victims' personal information. This situation is particularly relevant to teenagers who frequently engage in technologies such as video calls, inadvertently exposing personal details. Without realizing it, their actions can become leverage for perpetrators, who use these details as blackmail to extract something from their victims.

> *"Dari situ kita dengar banyak remaja atau any one share privacy, buat video call. Bila dah share gambar yang tak senonoh tu nanti partner tu akan ugut kalau kau buat hal aku share gambar video kau, itu part of jenayah cinta siber juga."* (R11)

Criminal Behaviour

According to R3, cyber romance crime can escalate into serious criminal behavior such as sexual assault or theft, driven by the wealth shared by victims on social media. Perpetrators may gather personal information, including home addresses, with the intent to intimidate and harass their targets.

> *"…mungkin akan timbul perkara jenayah macam mereka akan cari kita sampai jumpa ke, benda yang menakutkan. Mungkin dia akan cari alamat rumah, hari-hari datang kacau kita so nanti tak tenang. Mungkin dia nak rogol ke, mencuri ke sebab kita tunjukkan kekayaan. Bila kita tunjuk apa yang kita pakai dekat sosial media mungkin akan tarik minat dia and then diaorang akan cari kita, macam saya kata mungkin akan rogol mungkin akan mencuri."* (R3)

DISCUSSION

The analysis of respondents' understanding of cyber romance crime reveals four key themes: deception in love, financial fraud, personal data exposure, and criminal behaviour. Cyber romance crime involves fraudulent romantic relationships initiated through websites to manipulate victims financially (Coluccia et al., 2020). Additionally, romantic fraud or deception is used to gain financial rewards through intimate relationships, which, despite being dangerous, remains highly effective (Cross et al., 2023).

Love scams, particularly through the theme of love fraud, have become a growing concern among higher education students, as digital interactions and online relationships increasingly shape their social experiences. Love fraud in this context refers to deceptive romantic engagements where perpetrators manipulate victims into emotional attachment with the primary goal of financial or personal exploitation (Cross et al., 2023). Given that university students often seek companionship and meaningful relationships, they become vulnerable to fraudulent schemes, especially those exploiting loneliness and trust.

Both studies by Whitty and Buchanan (2016) and Bidin et al. (2015) highlighted that such scams involve psychological manipulation, where perpetrators craft convincing narratives and develop fictitious personas to gain their victims' trust. The anonymity provided by online platforms further exacerbates the risk, making it difficult for students to verify the authenticity of individuals they engage with (Cross et al., 2023), ultimately leading to financial and emotional distress.

Moreover, love fraud among students is particularly alarming due to their limited experience in identifying deceptive online behaviours. Whitty (2013) suggests that victims of romance scams often struggle to distinguish genuine affection from orchestrated deceit, particularly when scammers employ tactics such as grooming and emotional coercion. The financial losses associated with these scams are significant, as perpetrators gradually manipulate victims into providing financial aid under false pretences.

According to Whitty and Buchanan (2016), scammers create elaborate stories, including claims of financial emergencies or overseas hardships, to justify monetary requests. This phenomenon reveals a critical need for educational institutions to provide awareness and training on digital literacy and scam prevention, equipping students with the skills to assess online relationships critically and safeguard themselves from exploitation.

Financial fraud in the context of love scams involves perpetrators engaging in deceptive romantic interactions to exploit victims for monetary gain. Whitty and Buchanan (2012) describe this phenomenon as a systematic manipulation where scammers fabricate emotional connections to gain victims' trust before making financial demands. For students, the emotional attachment built through digital communication creates an illusion of sincerity, making them more susceptible to fraudulent requests such as emergency financial aid or investment schemes. The anonymity of online platforms exacerbates the risk, as perpetrators can easily disguise their identities and fabricate convincing narratives that persuade victims to transfer money under false pretences (Whitty, 2013).

Furthermore, financial fraud in love scams among university students reflects broader concerns about digital deception and financial exploitation. Cross et al. (2023) emphasize that scammers often adopt psychological tactics such as guilt-tripping, persuasion, and urgent requests to pressure victims into providing financial assistance. In many cases, students who lack experience in financial risk assessment unknowingly transfer significant amounts of money, believing they are helping a genuine partner. Whitty (2013) notes that perpetrators construct elaborate personas, sometimes impersonating professionals or individuals facing personal crises, further legitimizing their fraudulent claims.

On the other hand, the respondents defined love scams as a form of criminal behaviours, which involve various unpleasant acts that harm victims. This is aligned with Whitty's (2013) claimed that love scam includes deceit, coercion, and financial or psychological harm to the victims by the respondents, often targeting university students in digital spaces. Scammers manipulate victims into trust-based relationships, leading to identity theft, cyberstalking, and extortion (Whitty, 2013). The anonymity of online interactions enables emotional blackmail and fraudulent schemes (Cross et al., 2023). To combat this, higher education institutions must prioritize cybersecurity education and awareness campaigns to help students recognize and prevent digital exploitation (Whitty & Buchanan, 2016).

While prior research has primarily focused on romantic and financial fraud as central elements of cyber romance crime, the exposure of victims' personal information such as sexually explicit content which also be considered within this crime category. Cross et al. (2023) emphasize that although sextortion is often treated as a separate offense, there is a lack of comprehensive research examining its role within romance scams. Some evidence suggests that sextortion has been utilized by cyber romance criminals to extort larger sums of money from victims (Whitty, 2013). Moreover, threats to disclose intimate recordings obtained within personal relationships may serve as an effective strategy for perpetrators to coerce financial payments (Cross et al., 2023).

Thus, the definitions discussed here clearly position cyber romance crime as an illegal act. As noted by Muhammud and Muhammad (2022), the term 'cyber' in cybercrime refers to the virtual domain (the internet) where such actions are considered criminal behaviour's committed by irresponsible individuals or groups seeking profit through unethical and prohibited means under Islamic law.

CONCLUSION

This study concludes that students in Malaysian higher education institutions (HEIs) perceive love scams not merely as financial deception but as emotionally manipulative fraud that exploits trust, loneliness, and the desire for connection in digital spaces. These scams are viewed because of hyper-connected lifestyles, where social media and online dating platforms blur the lines between genuine intimacy and orchestrated deceit (Kamaruddin, 2022). Students often associate love scams with psychological manipulation, identity fabrication, and the misuse of digital communication tools to create false emotional bonds (Bilz et al., 2023). Qualitative findings from by Ameruddin (2021) further revealed that students experience emotional distress and social embarrassment due to such scams, underscoring their psychological impact. Therefore, it is imperative for policymakers and university management to enhance students' digital literacy and emotional resilience through targeted interventions, as Malaysia's current legal and educational frameworks must evolve to address the emotional and technological dimensions of love scams (Hamadi & Saari, 2023).

REFERENCES

Abaidah, T. N. A. B. T., Kamarudin, M. A. I. B., & Kamarruddin, N. N. A. B. (2024). The Model of Entrepreneurial Marketing (EM) Among Agropreneurs in the Emerging Markets: A Conceptual Framework 1. *UCJC Business and Society Review*, (80), 160-209.

Akhir, N. H. M. (2024). Motivation Toward Volunteerism in Flood Disaster Relief. *Salud, Ciencia y Tecnología-Serie de Conferencias*, *3*, 1040.

Akhir, N. M., Soh, O. K., & Akhir, N. H. M. (2020). Faktor pengaruh resiliensi mangsa banjir: Kajian kes di Kelantan (Factors influencing resilience of flood victims: a case study in Kelantan). *Jurnal Psikologi Malaysia*, *34*(2).

Akyıldız, S. T., & Ahmed, K. H. (2021). An overview of qualitative research and focus group discussion. *International Journal of Academic Research in Education*, *7*(1), 1-15.

Alavi, R., et al. (2018). Typologies of Cybercrime Victims in Selangor: A Socio-Demographic Analysis. *Asian Journal of Criminology*, 13(1), 23–41.

Amerruddin, M. I. (2021). Awareness of love scam among students of UiTM Dungun.

Bajnok, A., Kriskó, E., Korpics, F., Korpics, M. K., & Milován, A. (2024). Focus Group Discussion as a Method of Data Collection in Higher Education and Related Fields. *Pro Publico Bono–Public Administration*, *12*(2), 23-41.

Bidin, A., Nong, S. N. A. S., & Mohamad, M. A. (2015). Intipan Siber: Jenayah Baru Dalam Masyarakat Kontemporari. *Jurnal Islam dan Masyarakat Kontemporari*, *11*(S)), 12-25.

Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted love: A systematic literature review of online romance scam research. *Interacting with Computers*, *35*(6), 773-788.

Bong, X. L. (2023). *A study of awareness of cyber scams and cybersecurity among university students in Malaysia* (Doctoral dissertation, UTAR).

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health*, *11*(4), 589-597.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law, 20*(3), 261-283.

Coluccia A, Pozza A, Feretti F, et al. (2020) Online romance scams: Relational dynamics and psychological characteristics of the victims and scammer. A scoping review. *Clinical Practice and Epidemiology in Mental Health 16*, 24–35.

Cross, C., Holt, K., & Holt, T. J. (2023). To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud. *Criminology & Criminal Justice.*

Cyber Security Malaysia. (2024). AI and Scam Vulnerability Survey Report. [Unpublished internal report].

Fuad, N. S. M., Daud, M., & Yusof, A. R. M. (2022). Memahami Jenayah Siber Dan Keselamatan Siber Di Malaysia: Suatu Pemerhatian Terhadap Pandangan Sarjana Dan Intelektual: Understanding Cybercrime and Cybersecurity in Malaysia: An Observation from The Perspective of Scholars and Intellectuals. *Asian Journal of Environment, History and Heritage*, *6*(1).

Ghani, N. M., Bakar, M. A. A., & Rosli, H. (2023). Cybercrime experience's impact on women's emotions: A case study in Penang. *Malaysian Journal of Tropical Geography (MJTG)*, *49*(2), 48-67.

Graham, A. (2023). *Cybercrime: Traditional Problems and Modern Solutions* (Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington).

Hamadi, N. A. F., & Saari, C. Z. (2023). *The Love Scams Fraud Cybercrime in Malaysia: Civil Law and Syariah Perspectives*. SALAM Digest.

Kamaruddin, S., Wan Rosli, W. R., Abd Rani, A. R., Md Zaki, N. Z. A., & Omar, M. F. (2020). When love is jeopardized: Governing online love scams in Malaysia. *International Journal of Advanced Science and Technology*, *29*(6), 391-397.

Kamarudin, M. A. I., Kamarruddin, N. N. A., Ramli, A., & Murad, S. M. A. (2023). The challenges and issues faced by the new appointed academic staffs of the university in the emerging market. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(1), 20.

Kamarudin, M. A. I., Abaidah, T. N. A. T., Kamarruddin, N. N. A., & Rahim, N. A. A. (2025). The Effect of Opportunity Focus and Value Creation on the Performance of Agropreneur Small Medium Enterprises (SMEs) in the Emerging Market: The Role of Government Support Programs (GSPs) as Moderating Variable. *PaperASIA*, *41*(1b), 133-147.

Kamarudin, M. A. I., Yusof, M. S., Ramli, A., Othman, S., Hasan, H., Jaaffar, A. R., ... & Kamsani, M. J. (2024). The Issues and Challenges of Diversification Strategy in Multiple Industries: The Case of Kental Bina Sdn. Bhd. *PaperASIA*, *40*(3b), 48-58.

Kuah, C. Y., Lee, X. W., Lim, H. N., & Lim, Y. Y. V. (2024). Awareness On Online Financial Scams: A Case Study in Malaysia. *International Journal of Advanced Research in Economics and Finance*, *6*(1), 101-116.

Kutty, R. M., Mahmood, N. H. N., Masrom, M., Mohdali, R., Zakaria, W. N. W., Razak, F. A., ... & Aris, H. (2022). The influence of internet addiction and time spent on the internet towards social isolation among University students in Malaysia. *Asian Social Science*, *18*(10), 1-32.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, *105*, 102248.

Mat, B., Pero, S., Wahid, R., & Sule, B. (2019). Cybersecurity and digital economy in Malaysia: Trusted law for customer and enterprise protection. *International Journal of Innovative Technology and Exploring Engineering*, *8*(3), 214-220.

Masood, A., Zakaria, N., & Kamarudin, M. A. I. (2024). Empowering E-Learning Excellence: Unveiling the Influence of Outcome Expectation. *Learning Motivation, and Self-Efficacy in the Industrial Era*, *4*, 254-264.

Mohd, M., Abdullah, S. N. H. S., Yusof, S. B. M., Aman, J. S. J. K. B., & Kadri, A. (2021). Pemerkasaan Wanita Melalui Program Wanita Malaysia Revolusi Industri (IR 4.0) Bebas Jenayah Siber. *International Journal for Studies on Children, Women, Elderly and Disabled*, *14*.

Muhammud, F. S., & Muhammad, H. (2022). Cybercrime through love scams: What women should know?. *Journal of Contemporary Islamic Studies*, *8*(2), 41-54.

Nomleni, K. E. (2023). Analisis Fenomena Romance Scam dalam Komunikasi Interpersonal Love Scammer & Korban. *Jurnal Communio: Jurnal Jurusan Ilmu Komunikasi*, *12*(2), 202-221.

Purwaningrum, E. K., Ho, Y. M., Imawati, D., Prihadi, K. D., & Talib, M. A. (2024). Factors of susceptibility to online romance scam in Malaysia: unraveling the complex pathways. *International Journal of Public Health Science (IJPHS)*, *13*(4), 2053.

Shaari, A. H., Kamaluddin, M. R., Fauzi, W. F. P., & Mohd, M. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online Journal of Language Studies*, *19*(1).

Sidek, S., Hasbolah, H., Samad, N. S. A., Abdullah, Z., Zoraimi, N. H. N., Khadri, N. A. M., ... & Hassin, N. H. (2024). Leveraging Customer Relationship Management (CRM) for Stimulating Cyberpreneurship in Malaysia. In *Contemporary Issues in Entrepreneurship and Innovative Technology* (pp. 145-160). Cham: Springer Nature Switzerland.

State of Scam Report. (2024). Annual Cybercrime Statistics and Economic Impact in Malaysia. Ministry of Communications and Digital.

Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically dismantling online dating fraud. *IEEE Transactions on Information Forensics and Security*, *15*, 1128-1137.

Thomas, D., & Loader, B. D. (2013). Introduction: Cybercrime: Law enforcement, security and surveillance in the information age. In *Cybercrime* (pp. 1-14). Routledge.

Ting, C. H., & Essau, C. (2021). Addictive behaviours among university students in Malaysia during COVID-19 pandemic. *Addictive Behaviors Reports*, *14*, 100375.

Tirumala, S. S., et al. (2019). Cybersecurity Awareness Among Malaysian University Students. Journal of Information Security Research, 10(2), 45–58.

Tropina, T., Callanan, C., & Tropina, T. (2015). Public–private collaboration: Cybercrime, cybersecurity and national security. *Self-and co-regulation in Cybercrime, cybersecurity and national security*, 1-41.

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology, 53*(4), 665-684.

Whitty, M. T. and Buchanan T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice,16*(2),176–194.

Wilson, S., Hassan, N. A., Khor, K. K., Sinnappan, S., Abu Bakar, A. R., & Tan, S. A. (2024). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime*, *31*(5), 1140-1155.