

Unveiling the Patterns of Romance Scams in South Korea: Insights and Implications

Seoung Won Choi

 <https://orcid.org/0009-0003-2614-4723>

Chung-Ang University, South Korea

Julak Lee

 <https://orcid.org/0000-0002-1798-8671>

Chung-Ang University, South Korea

Yeon-Jun Choi

 <https://orcid.org/0009-0007-1589-6611>

Kwangju Women's University, South Korea

ABSTRACT

Romance scams, a prevalent form of cybercrime, have surged globally, with South Korea experiencing a rapid rise. Furthermore, perpetrators have adopted increasingly sophisticated tactics. However, South Korea's unique legal framework and the lack of comprehensive regional studies have led to insufficient preventive measures and responses. This research aims to elucidate the modus operandi of South Korean romance scams and highlight their distinguishing features. By employing crime script analysis and conducting interviews with investigators, this study delineated three pre-crime scripts and thirteen criminal event scripts. The research reveals distinctive features of these scams, including the extensive use of KakaoTalk for romantic communications, the significant influence of South Korean cultural norms on scam operations, and the increasing use of advanced technologies such as deepfakes. These findings provide a comprehensive understanding of the unique dynamics of romance scams in South Korea, thus facilitating the development of more effective preventive strategies and responses.

KEYWORDS

Crime Script Analysis, Criminal Investigator Interview, Cybercrime, Modus Operandi, Romance Scam, South Korean Context

INTRODUCTION

The prominence of romance scams in South Korea has garnered significant attention, with a public figure recently falling victim to the “pig butchering scam,” in which scammers established a trust relationship online and persuaded the victim to invest in a fraudulent cryptocurrency scheme (K. Lee, 2023). In addition, there was an incident in which a group, posing as “white hat” hackers and falsely claiming to assist romance scam victims, defrauded approximately 430 million in Korean won (KRW) over ten months before being brought to trial (Ryu, 2023). As such, romance scams are evolving, causing secondary victimization, and are considered a serious crime in South Korea (H. Kim & Suh, 2019). Despite the common perception that romance scams are less serious or traumatizing

DOI: 10.4018/IJCBPL.357152

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

than other forms of abuse due to their occurrence in the online realm, victims of these scams can endure not only substantial financial losses but also profound psychological trauma resulting from feelings of betrayal and deception (Wang & Topalli, 2024). Accordingly, these scams should be recognized and treated as serious criminal offenses.

A romance scam characteristically commences with establishing a romantic affiliation with a designated individual, followed by monetary solicitations (Whitty & Buchanan, 2012). Notably, the ramifications of these scams extend beyond financial repercussions; they significantly impact the psychological and emotional well-being of the victims (Buchanan & Whitty, 2014).

While the earliest romance scams relied on postal mail, their contemporary iterations exhibit far greater sophistication, with their tactics persistently evolving. Moreover, the incidence of romance scam victims in South Korea is rising, making it crucial to curtail and alleviate their subsequent repercussions. Central to dealing with the issue is the situational crime prevention theory, a leading approach to crime prevention. This theory posits that reshaping situational and environmental factors—by amplifying risks and impediments while diminishing incentives associated with illicit activities—can substantially reduce crime opportunities (Clarke, 1995). Building on this theory, any reduction in crime frequency should integrate a detailed understanding of the crime process. In this vein, crime script analysis stands out as an exemplary analytical technique (Cornish & Clarke, 2002).

Within the Korean legal context, romance scams present distinct characteristics. The Special Act on the Prevention of Loss Caused by Telecommunications-Based Financial Fraud and Refund for Loss, which provides guidance on issues such as account suspensions, damage mitigation, and responses to online fraud, excludes romance scams from its purview. Even though this legislation was crafted to curb damages from online fraud, it underscores the inadequacy of preventive and remedial measures for romance scams in South Korea.

Moreover, while global research endeavors have actively explored romance scams and their procedural intricacies, studies within the South Korean context remain limited. This research gap stems from a relatively low awareness of the severity of romance scams in South Korea (H. Kim & Suh, 2019). The current study sought to elucidate the modus operandi underlying South Korean romance scams through crime script analysis and interviews with criminal investigators. By undertaking this approach, it aimed to bridge this research gap and enrich the global understanding of romance scams by highlighting the specific characteristics and nuances of romance scams within the South Korean context.

The study addressed the following research questions:

What is the modus operandi of South Korean romance scams?

How do Korean romance scams differ from those observed in other nations?

LITERATURE REVIEW

Cybercrime

Romance scams are one of the most common types of cybercrime (Nurse, 2018). Cybercrime refers to crimes committed using special knowledge in cyberspace (Holt & Bossler, 2015). Historically, criminal activities were predominantly executed in physical space. However, advancements in computer technology have paved the way for a shift to virtual space, amplifying the urgency for in-depth research into cybercrimes. Stabek et al. (2010) categorized cybercrimes into various types: financial gain through low-level trickery, financial gain and information gathering through developed story-based applications, participation and information gathering through employment-based strategies, financial gain through implied necessary obligation, information gathering through apparently authentic appeals, financial gain through merchant- and customer-based exploitation, and financial gain and information gathering through marketing opportunities. Romance scams belong to the “financial gain and information gathering through developed story-based applications” category because perpetrators engage in detailed conversations with targets.

Definition and Characteristics of the Romance Scam

Romance scams are a relatively new type of scam that emerged around 2008 (Whitty & Buchanan, 2012). Characterized by two primary phases, they initially involve the scammer cultivating a trust-based relationship with the victim before subsequently soliciting funds under various pretexts (Whitty & Buchanan, 2012; Kopp et al., 2016; Whitty, 2018; H. Kim & Suh, 2019; Anesa, 2020). Romance scams progress to the point where the targets realize they have been deceived (Eseadi et al., 2021). Unlike other fraudulent activities, romance scams inflict a “double hit” on victims, entailing financial and relational losses (Whitty & Buchanan, 2012; Buchanan & Whitty, 2014).

Historically, before the widespread use of online technology, scams were primarily conducted through postal correspondence, such as the Nigerian mail scam (Whitty, 2015a). However, the advancement of digital technology and the emergence of various online services have engendered a significant shift. Fraudsters now exploit various digital platforms, encompassing dating websites and social media, to ensnare their victims (Chuang, 2021). As such, online romance scams now account for the majority of romance scams (Whitty, 2015b). The prevalence of romance scams is likely underrepresented in data, as victims often abstain from reporting due to the associated stigma (Whitty & Buchanan, 2012; Buchanan & Whitty, 2014).

Extant research on the progression of romance scams (Rege, 2009; Whitty & Buchanan, 2012; Whitty, 2013; Buchanan & Whitty, 2014; Whitty, 2015b; Shaari et al., 2019; Anesa, 2020) primarily focuses on a specific scenario: Typically, the scammers initiate contact on online platforms, utilizing a fabricated profile. Subsequently, they foster a romantic milieu through strategic self-presentation and calibrated dialogue, cultivating intimacy via rehearsed flattery and emotional manipulation. After establishing trust, the scammer conducts a “feasibility test,” soliciting minor financial assistance to gauge the target’s susceptibility to more significant monetary requests. As the scam escalates, the perpetrator pleads for increasingly substantial sums, allegedly for emergencies. This process persists until the victim discerns the deception. The scams culminate once the victims disclose their exploitation to the outside world.

Romance Scams in South Korea

The prevalence of romance scams has increased sharply in the United States and South Korea. Specifically, in 2022, victims in the United States reported losses amounting to \$1.3 billion in U.S. dollars, marking a 138% upsurge from \$547 million reported in 2021 (Obi, 2023). South Korea reflects a parallel trend, albeit with more pronounced growth. The financial repercussions of romance scams in 2021 were estimated at 2.07 billion KRW, up 459% from 370 million KRW in 2020 (S. Lee, 2021; J. Kim, 2022). Furthermore, reported incidents in 2021 numbered 28, tripling the nine cases registered the prior year (S. Lee, 2021).

However, in the United States and South Korea, the demographics of romance scam victims display striking differences. According to DeRoos (2022), in the United States, the primary victims are middle-aged to elderly individuals, with females representing 78% of the affected group. In contrast, data from the Korean National Police Agency’s Electronic Cybercrime Report and Management System for the first half of 2022 indicate that, in South Korea, 87.5% of victims are 30 or younger (Park & Lee, 2023). Thus, while females are predominantly targeted in both countries, these populations differ significantly by age.

Romance Scams in the South Korean Legal Context

Under the Korean legal framework, romance scams are classified as fraudulent activities. Consequently, prosecutions of these offenses fall under the purview of the fraud provisions within the South Korean Penal Code. The fraud statute aims to safeguard individuals’ property rights. The applicability of the fraud statute is contingent on the specifics of the fraudulent situation and whether it involved exploitation. Depending on the unique traits of each romance scam incident, a spectrum of legal codes might come into play beyond the traditional South Korean Penal Code. For instance,

should a victim's personal information be unlawfully gathered or deployed during the scamming process, the Personal Information Protection Act might be invoked. Similarly, if scams are orchestrated by leveraging communication platforms like the internet or mobile networks, penalties might be imposed under the Act on Promotion of Information and Communications Network Utilization and Information Protection.

In light of a marked surge in voice phishing cases, South Korea introduced the Special Act on the Prevention of Loss Caused by Telecommunications-Based Financial Fraud and Refund for Loss in 2011. This legislation facilitates the suspension of accounts, offers relief for damages, and outlines responses to telecommunication fraud incidents (Kang, 2021). Notably, these preventive measures, especially the suspension of account payments, are predominantly aimed at voice phishing incidents. Consequently, victims of romance scams find themselves in a predicament where timely relief and control of their losses are difficult to achieve. Due to these legal limitations, which fail to significantly mitigate the impact of romance scams, current debates actively contemplate extending the scope of this specific law to include romance scams, thereby offering more comprehensive protection and restitution (Y. Kim, 2023).

METHODS

The primary objective of this study was to elucidate the modus operandi of South Korean romance scams. Understanding a crime's modus operandi necessitates a detailed examination of the crime's progression; for such analysis, crime script methodology proves invaluable (Cornish & Clarke, 2002). This research employed crime script analysis on the amassed data, charting the sequential steps of romance scams. Subsequently, expert interviews were conducted to refine and hone the initially deduced scripts. This multifaceted methodological approach, encompassing multiple research techniques, is called triangulation (Flick, 2004; Leech & Onwuegbuzie, 2007). Such triangulation is instrumental in mitigating researcher biases, augmenting the validity and reliability of findings, and ensuring their comprehensive accuracy (Moon, 2019).

Data Collection

Existing literature that employs crime script analysis to scrutinize crimes (Beauregard et al., 2007; Brayley et al., 2011; Chiu et al., 2011; D. Y. Jeong, 2021) predominantly relies on data sources such as criminal interviews, investigative records, online collated criminal cases, and court transcripts. However, the unique nature of romance scams—the focal point of this study—presents challenges in obtaining criminal interviews. These challenges are attributed to the fact that many perpetrating organizations operate from foreign soil, with most perpetrators being nonnatives.

Given these constraints, the study leveraged Python's Selenium and BeautifulSoup to web crawl publicly accessible online data. We meticulously sourced articles, videos, and blog content pertinent to romance scams, using specific keyword searches: "romance scam ()," "dating app scam ()," and "chat currency exchange scam ()." This study harnessed Naver—South Korea's premier search engine (Internet Trend, 2023)—and YouTube, the platform with the highest user engagement in the region (Z. Lee, 2022). A detailed overview of the data collection methodology is presented in Table 1. As shown in Table 1, the total volume of data gathered throughout the study amounts to 437 kilobytes.

Crime Script Analysis

After data collection, the study proceeded with a crime script analysis of the amassed data. The underlying rationale of crime script analysis lies in scripting the crime process to forestall potential criminal occurrences (Leclerc, 2014). Given its encompassing nature, this analytical technique allows for identifying not just the crime category but also its specific modus operandi (Hutchings & Holt, 2015; D. Y. Jeong, 2021). Scripts, as conceptualized by Cornish (1994), comprise details regarding

Table 1. Information about the data

Keywords	romance scam (로맨스스캠), dating app scam (데이트앱사기), chat currency exchange scam (채팅환전사기).
Crawling Method	Python(www.python.org)
Website	Naver (www.naver.com), YouTube (www.youtube.com)
Data Type	News Article, Video, Blog Post
Volume	437 KB

Note. KB=kilobytes

criminal behavior, tools employed, strategies, and the like. These are fundamentally segmented into the pre-crime, criminal event, and post-offense phases (Beauregard & Leclerc, 2007).

This research undertook a focused analysis of both the pre-crime and criminal event phases intrinsic to romance scams. Ideally, we would delve into the post-offense phase; however, extracting such insights mandates interviews with actual perpetrators. Given the transnational nature of romance scams, with many culprits residing overseas, conducting such interviews presents substantial challenges. Therefore, a limitation of this study is that generalizations from the findings may be restricted due to the constraints of the current data set. Nonetheless, the study's capacity to dissect romance scam methodologies and proffer preventive strategies remains intact even without insights from the post-offense phase. This approach aligns with the primary objectives of this research, affirming its inherent academic value despite the limitations.

Expert Interviews

Expert participants were identified via snowball sampling, a prominent nonprobability sampling approach. Snowball sampling begins with the initial selection of participants who subsequently recommend other potential subjects (Etikan et al., 2016; Naderifar et al., 2017). As an inherently purposive method, snowball sampling is especially effective for data collection within qualitative research (Naderifar et al., 2017).

Consequently, five investigators, each with expertise in probing romance scams, were selected. Interviews with these experts were conducted to ascertain the modus operandi of romance scams, thereby augmenting the validity and reliability of the study's outcomes. From July 3-28, 2023, this study engaged in email interviews with the selected investigators. The scripts, derived from the crime script analysis, were shared with these investigators to obtain their feedback. Email interviews were chosen to afford the investigators ample time for reflection, ensuring their responses were more informed and reliable (K. Kim et al., 2020).

RESULTS

This research collected data on romance scams, analyzed the criminal scripts, and interviewed criminal investigators based on the initially derived script. Even if romance scams are scripted, not all progress according to script, so the interviews with criminal investigators allow us to refine our script.

The crime procedure was segmented into pre-crime and criminal event phases. Within these phases, recurrent behaviors and characteristic tactics were categorized based on the crime's progression. This categorization resulted in the derivation of three scripts for the pre-crime phase and 13 for the criminal event phase.

Modus Operandi in the Pre-Crime Phase

The pre-crime phase of a romance scam is divided into three main stages, as shown in Figure 1.

Figure 1. The pre-crime phase of romance scams



To effectively orchestrate romance scams, criminal organizations first delineate roles crucial to the scam’s success and assign members accordingly. Given the transnational and coordinated nature of these scams, role assignment is paramount. Crime investigator interviews reveal that these organizations typically operate from abroad and have a hierarchical structure comprising a target contact team, cash withdrawal team, management team, local South Korean branch, and overseas headquarters. The target contact team directly interacts with victims using messaging apps. The cash withdrawal team manages the finances, extracting funds deposited by victims. The management team, led by a “middle boss,” oversees the operations. The South Korean branch’s chief serves as the main coordinator for scams within South Korea, maintaining communication with the primary headquarters, predominantly located in West Africa.

In subsequent stages, scammers meticulously craft conversation scenarios tailored to various potential targets. These scenarios are not only designed to engage and maintain ongoing communication with the victim but also to anticipate and address any skepticism or reservations the victim might harbor. Each dialogue is structured to align with the specific interests and context of the target to increase the likelihood of resonance and continued engagement.

Romance scammers meticulously curate tools and profiles tailored to their deceptive narratives. They set up online dating and social media accounts using fake credentials, such as passports and bank statements, alongside purloined photos or videos. Scammers often populate their social media profiles—typically a victim’s first introduction to the scammer—with crafted photos, posts, and even followers to ensure credibility. Some also prepare chat platforms and sham cryptocurrency exchanges to further their schemes. A notable revelation from the study is the existence of “formats,” packaged products available for purchase, which provide ready-to-use tools and dialogue scenarios for these scams.

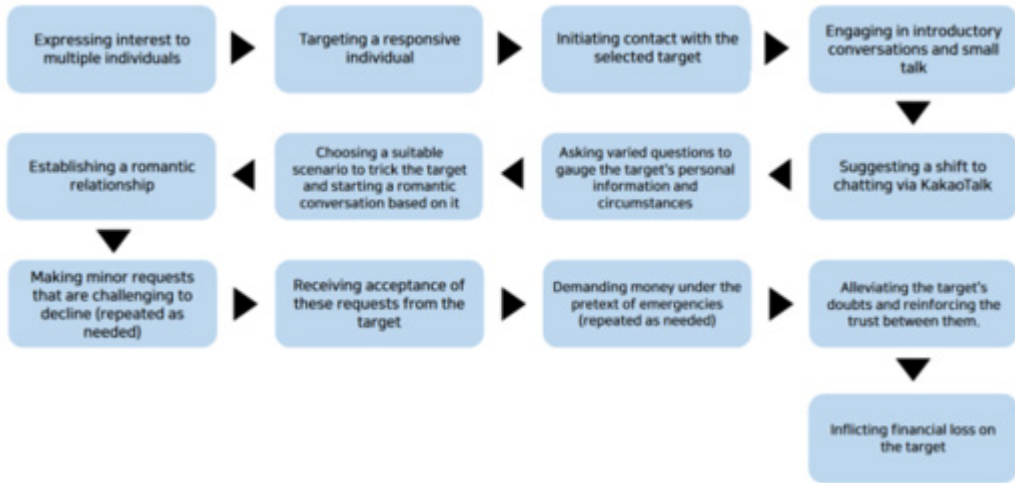
Modus Operandi in the Criminal Event Phase

The criminal event phase of a romance scam is divided into 13 main stages, as shown in Figure 2.

In the initial stage of a romance scam, perpetrators cast a wide net by expressing interest to numerous individuals and expressing romantic intent on dating platforms or engaging on social media through likes, comments, or follows. As individuals reciprocate this interest through messages or follows, scammers narrow down their targets. Typically, they initiate further communication using direct channels like dating apps or Instagram direct messages. Recent interviews with crime investigators highlight a concerning trend: Scams targeting younger individuals, particularly those in their 20s and 30s, have increased significantly since the onset of the pandemic. Furthermore, scams aimed at sexual minorities are also on the rise.

Once the targeted individual reciprocates the scammer’s outreach, the deceptive courtship truly begins. The scammers typically use a crafted online persona or social media profile to introduce themselves and briefly converse with the targets. These fraudsters often hail from foreign locations and might use online South Korean translation tools to mimic a particular accent or tone. They often masquerade as figures of authority or allure, such as members of the U.S. military, diplomats, affluent individuals, or professionals like businessmen and lawyers. To deepen the connection and further isolate the victims, scammers suggest shifting the conversation to KakaoTalk. Upon doing so, they take a more inquisitive stance, probing the targets for personal details and understanding their current circumstances. Armed with this fresh knowledge and insights from the targets’ online

Figure 2. The criminal event phase of romance scams



presence, the scammers fine-tune their approach, zeroing in on their intended victims' specific needs or vulnerabilities.

Once the typical scammers gain a foundational understanding of the target, they sift through their repertoire of preprepared dialogue scenarios, selecting the one best aligned with the target's situation. For example, should the target be a young, solitary woman experiencing loneliness, the scammer might employ frequent compliments, emphasizing her beauty and using flirtatious remarks, all with the intent to spark romantic sentiments. This approach could progress to bestowing pet names upon each other or mutually recognizing a romantic relationship. Investigative experts reported that several elements increase the scammers' allure to potential victims: the appeal of their online persona, the romantic ambiance they cultivate, and the perceived opportunity for targets to enhance language skills, particularly in English, through their exchanges. These aspects often seduce targets into believing they are in genuine romantic engagements.

Once a semblance of a romantic relationship is established, the scammer begins testing the waters by asking the target for minor favors, which are typically hard to reject given the emotional bond. If the target accedes to the scammer's requests, the scammer iterates this tactic to fortify the perceived connection. Moreover, the scammer often creates heart-wrenching tales to elicit further sympathy and make it even harder for the target to decline requests. The scammer may claim to have been orphaned at a young age, subjected to domestic or sexual abuse during childhood, or have tragically witnessed the death of close family members. These fabricated stories manipulate the target's emotions and deepen the entanglement in the scammer's web.

Building on the established relationships, the scammers request monetary assistance, presenting an emergency from their predetermined script. Reasons may range from an unjust arrest necessitating bail, unforeseen customs or shipping charges to emergencies like a sudden grave injury requiring immediate surgery they cannot afford. Investigators have noted that with increasing awareness of romance scams, potential victims have grown wary of sudden large monetary requests. Scammers have adapted their approaches to overcome this skepticism.

Scammers leverage sophisticated deepfake technology to conduct video calls, projecting the attractive faces from their profiles to deceive targets demanding visual proof of identity. Deepfakes are produced using artificial intelligence techniques that merge, combine, replace, and superimpose images and video clips to create convincingly real, deceptive videos (Maras & Alexandrou, 2019). Previously, scammers only shared stolen photos and videos or partially exposed their faces in dark

settings during video calls. However, their deceptive tactics have evolved, now employing deepfake technology to enhance their schemes. This strategic unveiling of the fake face heightens the targets' intimacy, making them more susceptible to satisfying the scammers' pleas.

Afterward, romance scammers repeatedly plead financial emergencies to the target until the latter discerns the deception. Once suspicion arises, the scammers often employ threats, even of a lethal nature, to deter the victims from reporting the crime. Furthermore, when scammers sense their current victims' utility waning, they swiftly pivot to a new target. Hence, the cycle of romance scams extends to ensnare multiple victims.

DISCUSSION AND CONCLUSION

This research delved into the *modus operandi* of South Korean romance scams, employing a multifaceted approach that combined online data mining, crime script analysis, and insights from criminal investigators. A comprehensive understanding of the scams' blueprints and methodologies was attained by integrating the preliminary scripts from the crime script analysis with insights derived from investigator interviews. Utilizing a multifaceted methodological approach known as triangulation, this study aimed to minimize researcher bias, thereby enhancing the validity and reliability of the findings and ensuring their comprehensive accuracy.

Interestingly, the *modus operandi* unearthed in this study share many similarities with the findings of prior research on romance scams. Key parallels include the utilization of social networking sites (SNSs) as initial touchpoints and a gradual escalation in demands from the scammer, starting with minor favors and culminating in significant monetary requests. Furthermore, the process of soliciting money from the other party by citing various unavoidable circumstances, thereby appealing to the victim's feelings of trust and affection for the perpetrator (Eseadi et al., 2021), is also a common pattern in romance scams. Thus, South Korean romance scams align closely with global romance scams in many aspects.

In the initial phase of garnering attention from a broad spectrum of individuals, scammers strategically engage with SNS content, notably through likes, comments, and follows. Given the conduciveness of SNS platforms for vivid self-expression and the users' heightened cognizance of societal perceptions (Ip et al., 2017), romance scammers find it propitious to exploit these platforms with minimal exertion. This approach and the behavioral patterns observed align with an array of prior scholarly investigations (Rege, 2009; Aransiola & Asindemade, 2011; Whitty & Buchanan, 2012; Whitty, 2013; Buchanan & Whitty, 2014; Whitty, 2015b; Whitty, 2018; Shaari et al., 2019; Anesa, 2020).

During the "making small requests that are hard to refuse (repeat)" phase, the scammer posits minor requests designed to be challenging for the target to decline. Each time the target accedes, the cycle persists, progressively reinforcing the bond between both parties. This tactic aligns with the framework of Cialdini (2001), which delineated six foundational dispositions prompting affirmative responses: consistency, reciprocation, social validation, liking, authority, and scarcity. Creating an environment where the targets routinely grant minor favors increases the likelihood of them complying with more significant requests in subsequent interactions. Such an approach finds echoes in prior scholarly endeavors, including Whitty (2013), Buchanan and Whitty (2014), Whitty (2015), Shaari et al. (2019), and Anesa (2020).

Conversely, examining South Korean romance scams in comparison to those abroad reveals distinguishing features. Foremost in the pre-crime phase is the commercial exchange of "formats." These are comprehensive kits encompassing social media profiles, images, scripted dialogues, and various tools pivotal for the scam's execution. Scammers shape their deceptive tactics according to the formats they procure. This approach considerably muddles the discernment process for potential victims. This observed trend points to the ease of implementing these scams, hinting at their potential future proliferation.

When delving deeper into the particularities of South Korean romance scams, significant nuances appear in the victim selection phase. A post-pandemic spike in romance scams targeting individuals in their 20s and 30s is evident, possibly because of heightened loneliness stemming from social distancing measures (Hwang et al., 2020; Li & Wang, 2020) and a surge in digital encounters (Goldstein & Flicker, 2020). This divergence in the victim demographic in South Korea is striking, especially when global studies predominantly pinpoint middle-aged, well-educated females as the primary targets (Whitty, 2018; Coluccia et al., 2020).

While it was initially postulated that individuals in their 20s and 30s, given their digital acumen, would be less susceptible, their prolonged online presence and heavy digital consumption have ironically rendered them more vulnerable. Some research suggests that this younger demographic, already comfortable with online socialization, may remain the primary target of such scams for the foreseeable future (Park & Lee, 2023).

Moreover, a marked increase in scams directed at the LGBTQ community within South Korea has emerged lately. This finding mirrors a previously observed pattern abroad, where the LGBTQ community is often preyed upon (Buchanan & Whitty, 2014). Factors such as limited offline dating avenues and a heavy dependence on specialized dating platforms, like LGBTQ dating apps, render this group particularly susceptible (Gudelunas, 2012).

A salient characteristic distinguishing South Korean romance scams is the prevalent use of KakaoTalk by scammers to engage deeply with their targets, a reflection of the app's overwhelming predominance in the South Korean messenger landscape. Recent statistics from May 2023 highlight KakaoTalk's undisputed dominance, boasting an impressive 41 million monthly active users, relegating platforms like YouTube and Naver to the second and third positions, respectively (Hong, 2023). Further reinforcing this dominance is KakaoTalk's staggering 95% market share in the South Korean messaging ecosystem (Z. Lee, 2022). In contrast, the 2021 messaging app market share in the United States reveals a different narrative: Facebook Messenger leads with 64.43%, trailed by Snapchat at 13.59% and WhatsApp at 13.56%. Similarly, in the United Kingdom, Facebook Messenger (54.90%), WhatsApp (25.59%), and Snapchat (13.09%) primarily split the market (Curry, 2023). This distinct market composition in South Korea not only underlines the uniqueness of its romance scams but also underscores how regional digital preferences can profoundly shape the modalities of online scams, distinguishing them markedly from global trends.

After transitioning to KakaoTalk, scammers endeavor to cultivate a romantic connection with the victim through affectionate dialogue. Often, as the conversation progresses, victims quickly develop strong feelings for the scammers. Notably, the scammers' expressions might appear slightly clumsy due to their reliance on translators. Several factors underpin the intensifying bond between the scammer and the victim. First and foremost, scammers deploy advanced persuasive tactics (Kopp et al., 2016; Anesa, 2020) coupled with psycholinguistic strategies that resonate with the victims' emotions and foster trust (Kopp et al., 2016; Shaari et al., 2019; Whitty, 2019). Such tactics aim to construct a hyper-personal relationship (Buchanan & Whitty, 2014; Shaari et al., 2019), causing the victims to make judgmental errors that prevent them from detecting the scams (Dreijers & Rudziša, 2020).

The extent of psychological manipulation is so profound that most victims are unable to doubt their partners and firmly believe they are in an authentic romantic relationship. While these strategies are commonly employed in romance scams, South Korean scams exhibit unique elements deeply rooted in the nation's cultural backdrop. South Korea's intense emphasis on English education (S. Kim, 2008; M. Jeong, 2011) has historically driven many to adopt English via email exchanges with foreigners (Cho, 1998). However, technological advancements have precipitated a significant shift toward language exchange apps, with individuals preferring messengers over traditional emails for language learning (S. Lee, 2018; Heo & Bae, 2021). Given this context, numerous South Koreans feel comfortable communicating with foreigners through apps. This cultural inclination might inadvertently make them more susceptible to romance scams by causing them to feel an even closer connection to the scammers.

In addition, targets have grown more cautious and skeptical before remitting substantial amounts to fraudsters. However, potential victims' escalating skepticism has catalyzed fraudsters to refine their deceptive tactics, ensuring their fabrications remain credible. A primary factor intensifying victims' vulnerability is cognitive destabilization resulting from sustained manipulation, particularly through gaslighting (Nataraj-Hansen, 2023). Gaslighting, a tactic where victims are made to question their memories or sanity, makes them increasingly dependent on the scammers' narratives. This vulnerability is further amplified by confirmation bias, where individuals favor information that resonates with their existing beliefs, overlooking conflicting data (Williams et al., 2017).

Faced with the increasing demand for tangible evidence of their legitimacy, scammers have resorted to more sophisticated methods. Where they previously may have avoided video calls or obscured their visibility, they now employ deepfake technologies to create a believable facade. Such advancements bolster the scammers' trustworthiness in the eyes of the targets, culminating in financial exploitation.

With advancements in translation tools and the rise of artificial intelligence technologies, scammers can fabricate highly believable images and videos of appealing individuals. Moreover, with innovations in generative AI, like Chat GPT, the dialogues used in romance scams could become more diverse and compelling. Indeed, the embrace of cutting-edge technologies in romance scams underscores the urgent need for studies focused on new counterstrategies (Whitty & Buchanan, 2012; Eseadi et al., 2021). Based on the findings, suggestions to mitigate the detrimental effects of romance scams are presented.

This study reveals a recent uptick in romance scams aimed at individuals under 30. These scams often originate from interactions on social media or online dating platforms, predominantly used by this age group. Hence, offering educational resources to this demographic is imperative. Such resources can include comprehensive workshops, informative pamphlets, and interactive online modules. These materials would enlighten them about common scammer tactics, victim profiles, and typical dialogue scenarios, ultimately equipping them with the knowledge to identify and avoid potential scams. Moreover, given that the KakaoTalk Messenger app is the primary communication channel for these scams within the South Korean context, collaborating with national agencies to proactively implement measures is essential. By informing and notifying users about romance scam prevention, these collaborative efforts can help significantly mitigate the harm caused by these scams.

Moreover, as previously highlighted, South Korea's distinct legal context significantly impedes efforts to curtail romance scams. This impediment stems from the fact that the Special Act on the Prevention of Telecommunications-Based Financial Fraud and Refund for Loss—which provides guidance on issues such as account freezes, reparations for victims, and responses to virtual deceit—does not encompass romance scams. Even though these scams unequivocally fall under the umbrella of online fraud, the law's exclusive focus on voice phishing proves to create a bottleneck in anti-scam endeavors. While entities such as the Online Damage 365 Center offer guidance on recuperating from romance scams and provide psychological support via counseling, anticipating the potency of any legal sanctions against a scam's perpetrators or meaningful compensation for its victims remains challenging under the current law. Given the widespread underreporting and the feelings of shame associated with victims of this crime worldwide (Kassem & Carter, 2024), extending the application of this special act to encompass romance scams can provide significant benefits, addressing these challenges and offering more comprehensive protection and restitution.

By undertaking research on romance scams within the South Korean context, a more comprehensive and nuanced understanding of the methodologies and strategies employed in these scams was obtained. This study enriches the existing body of knowledge while holding significant value for future research in different regional contexts, providing a foundational framework for comparative analyses and the development of targeted prevention strategies.

However, given the limitations of the current data set, future research should conduct longitudinal studies to track the long-term impacts of romance scams on victims. Moreover, incorporating a diverse

data set and cross-cultural comparisons would improve the applicability of the findings and provide a comprehensive understanding of patterns and differences. This approach would inform more effective prevention and support strategies, making it a highly effective research direction.

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

PROCESS DATES

09, 2024

This manuscript was initially received for consideration for the journal on 07/07/2024, revisions were received for the manuscript following the double-anonymized peer review on 09/06/2024, the manuscript was formally accepted on 09/05/2024, and the manuscript was finalized for publication on 09/19/2024

CORRESPONDING AUTHOR

Correspondence should be addressed to Julak Lee; julaklee71@cau.ac.kr

FUNDING

This study was supported by the BK21 FOUR program (Education and Research Center for Securing Cyber-Physical Space) through the National Research Foundation funded by the Ministry of Education of Korea (5199990314137).

REFERENCES

- Anesa, P. (2020). Lovextortion: Persuasion strategies in romance cybercrime. *Discourse, Context & Media*, 35, 100398. DOI: 10.1016/j.dcm.2020.100398
- Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. DOI: 10.1089/cyber.2010.0307 PMID: 22007957
- Beauregard, E., & Leclerc, B. (2007). An application of the rational choice approach to the offending process of sex offenders: A closer look at the decision-making. *Sexual Abuse*, 19(2), 115–133. DOI: 10.1177/107906320701900204 PMID: 17541744
- Beauregard, E., Proulx, J., Rossmo, K., Leclerc, B., & Allaire, J. F. (2007). Script analysis of the hunting process of serial sex offenders. *Criminal Justice and Behavior*, 34(8), 1069–1084. DOI: 10.1177/0093854807300851
- Brayley, H., Cockbain, E., & Laycock, G. (2011). The value of crime scripting: Deconstructing internal child sex trafficking. *Policing, Policing (Oxford, England)*, 5(2), 132–143. DOI: 10.1093/police/par024
- Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, 20(3), 261–283. DOI: 10.1080/1068316X.2013.772180
- Chiu, Y. N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *British Journal of Criminology*, 51(2), 355–374. DOI: 10.1093/bjcr/azr005
- Cho, S. (1998). The applications of electronic mail to English education. *Multimedia-Assisted Language Learning*, 1(1), 213–227.
- Chuang, J. Y. (2021). Romance scams: Romantic imagery and transcranial direct current stimulation. *Frontiers in Psychiatry*, 12, 738874. DOI: 10.3389/fpsyt.2021.738874 PMID: 34707523
- Cialdini, R. B. (2001). The science of persuasion. *Scientific American*, 284(2), 76–81. DOI: 10.1038/scientificamerican0201-76
- Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice*, 19, 91–150. DOI: 10.1086/449230
- Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice and Epidemiology in Mental Health*, 16(1), 24–35. DOI: 10.2174/1745017902016010024 PMID: 32508967
- Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies*, 3(1), 151–196. <https://www.semanticscholar.org/paper/THE-PROCEDURAL-ANALYSIS-OF-OFFENDING-AND-ITS-FOR-Cornish/6dddc49c32701d682e4c4714d0299bcb7887327>
- Cornish, D. B., & Clarke, R. V. (2002). Analyzing organized crimes. In Piquero, A. R., & Tibbets, S. G. (Eds.), *Rational choice and criminal behavior: Recent research and future challenges* (pp. 41–63). Routledge.
- Curry, D. (2023, January 9). Messaging app revenue and usage statistics (2023). *Business of Apps*. <https://www.businessofapps.com/data/messaging-app-market/>
- DeRoos, D. (2022, October 20). Think all “catfish” victims are easily fooled? Think again. *19 News*. <https://www.cleveland19.com/2022/10/19/think-all-catfish-victims-are-easily-fooled-think-again/>
- Dreijers, G., & Rudziša, V. (2020). Devices of textual illusion: Victimization in romance scam e-letters. *Research in Language*, 18(1), 1–13. DOI: 10.18778/1731-7533.18.1.01
- Eseadi, C., Ogbonna, C. S., Otu, M. S., & Ede, M. O. (2021). Hello pretty, hello handsome! Exploring the menace of online dating and romance scams in Africa. In Chan, H. C., & Adjorlolo, S. (Eds.), *Crime, mental health and the criminal justice system in Africa: A psycho-criminological perspective* (pp. 63–87). DOI: 10.1007/978-3-030-71024-8_4
- Etikan, I., Alkassim, R., & Abubakar, S. (2016). Comparison of snowball sampling and sequential sampling technique. *Biometrics and Biostatistics International Journal*, 3(1), 55. DOI: 10.15406/bbij.2016.03.00055

- Flick, U. (2004). Triangulation in qualitative research. In Flick, U., von Kardoff, E., & Steinke, I. (Eds.), *A companion to qualitative research* (pp. 178–183). Sage.
- Goldstein, A., & Flicker, S. (2020). “Some things just won’t go back”: Teen girls’ online dating relationships during COVID-19. *Girlhood Studies*, 13(3), 64–78. DOI: 10.3167/ghs.2020.130306
- Gudelunas, D. (2012). There’s an app for that: The uses and gratifications of online social networks for gay men. *Sexuality & Culture*, 16(4), 347–365. DOI: 10.1007/s12119-012-9127-4
- Heo, S., & Bae, S. (2021). The study of using Kakao talk on TOEIC speaking. *Korean Journal of General Education*, 15(2), 57–67. DOI: 10.46392/kjge.2021.15.2.57
- Holt, T., & Bossler, A. (2015). (Manuscript submitted for publication). [*Theory and prevention of technology-enabled offenses*. Routledge.]. *Cybercrime*.
- Hong, K. (2023, June 5). KakaoTalk and Naver “falter” as Google advances: YouTube is on the verge of becoming number one in terms of number of users for the first time. *Yonhap News*. <https://www.yna.co.kr/view/AKR20230604052751017>
- Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, 55(3), 596–614. DOI: 10.1093/bjc/azu106
- Hwang, T. J., Rabheru, K., Peisah, C., Reichman, W., & Ikeda, M. (2020). Loneliness and social isolation during the COVID-19 pandemic. *International Psychogeriatrics*, 32(10), 1217–1220. DOI: 10.1017/S1041610220000988 PMID: 32450943
- Internet Trend. (2023, June 18). Search Engine. *Internet Trend*. <http://www.internettrend.co.kr/trendForward.tsp>
- Ip, R. K., Pang, P. P., & Wu, M. X. (2017, January). What drives people to flaunt in social networking sites? In *Proceedings of the 8th international conference on e-education, e-business, e-management and e-learning* (pp. 76–80). DOI: 10.1145/3026480.3026483
- Jeong, D. Y. (2021). A study on the sextortion M.O. (modus operandi) using crime script analysis. *The Journal of Police Science*, 21(3), 5–30. DOI: 10.22816/polsci.2021.21.3.001
- Jeong, M. (2011). Social conditions of English fever and its harmful effects for universities since the 1990s in Korea. *Social History*, (92), 131–168. <https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001625099>
- Kang, J. (2021, February 16.). Why is my account suspended for voice phishing, but not for romance scams and reading scams? *Digital Today*. <https://www.digitaltoday.co.kr/news/articleView.html?idxno=263858>
- Kassem, R., & Carter, E. (2024). Mapping romance fraud research—a systematic review. *Journal of Financial Crime*, 31(4), 974–992. DOI: 10.1108/JFC-06-2023-0160
- Kim, H., & Suh, J. (2019). A study on romance scams: The current situation and effective countermeasures. *The Police Science Journal*, 14(3), 117–146. DOI: 10.16961/polips.2019.14.3.117
- Kim, J. (2022, September 17). If you meet someone on a chat app and they ask you to invest, be suspicious of a “romance scam.” *Dongailbo*. <https://www.donga.com/news/Economy/article/all/20220916/115492108/1>
- Kim, K., Cho, Y., & Bae, J. (2020). Exploratory study on countering Internet hate speech: Focusing on case study of exposure to internet hate speech and experts’ in-depth interview. *The Journal of the Korea Contents Association*, 20(2), 499–510. DOI: 10.5392/JKCA.2020.20.02.499
- Kim, S. (2008). Television discourse on English education fever: Narrative analyses of twelve current-affairs documentaries. *Korean Journal of Broadcasting and Telecommunication Studies*, 22(5), 7–52. <https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001281746>
- Kim, Y. (2023). *Current status of online service damage counseling and support and issues for improvement: Focusing on the “Online Damage 365 Center.”*. National Assembly Research Service.
- Kopp, C., Sillitoe, J., Gondal, I., & Layton, R. (2016). The online romance scam: A complex two-layer scam. *Journal of Psychological and Educational Research*, 24(2), 144–161. <https://www.ceeol.com/search/article-detail?id=461681>

- Leclerc, B. (2014). Script analysis for crime controllers: Extending the reach of situational crime prevention. In Caneppele, S., & Calderoni, F. (Eds.), *Organized crime, corruption and crime prevention: Essays in honor of Ernesto U. Savona* (pp. 13–20). Springer. DOI: 10.1007/978-3-319-01839-3_2
- Lee, K. (2023, January 25). “I lost 20 million won in a coin scam”: The new “romance scam” that Kim Sang-hyuk also fell victim to. *Chosunilbo*. https://www.chosun.com/national/national_general/2023/01/25/A5ZT6M7DTZAH5LIC3WED46JA4Q/
- Lee, M. (2022, October 31). Find a replacement for “the exclusive messenger” KakaoTalk. *Hankyung*. <https://magazine.hankyung.com/business/article/202210265444b>
- Lee, S. (2018, October 12). Four new global social chat apps for learning a language and making foreign friends. *Kukminilbo*. <http://news.kmib.co.kr/article/view.asp?arcid=0012755207&code=61151411&cp=nv>
- Lee, S. (2021, December 8). Deepfake, fake bank: Cryptocurrency investment, “Honey, I’m in a hurry...” *NTN*. <https://www.intn.co.kr/news/articleView.html?idxno=2019763>
- Lee, Z. (2022, November 23). 200 Mobile apps loved by Koreans in 2022: 2023 new trends predicted by app rankings. *Forbes Korea*. <https://jmagazine.joins.com/forbes/view/337083>
- Leech, N. L., & Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: A call for data analysis triangulation. *School Psychology Quarterly*, 22(4), 557–584. DOI: 10.1037/1045-3830.22.4.557
- Li, L. Z., & Wang, S. (2020). Prevalence and predictors of general psychiatric disorders and loneliness during COVID-19 in the United Kingdom. *Psychiatry Research*, 291, 113267. DOI: 10.1016/j.psychres.2020.113267 PMID: 32623266
- Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. *The International Journal of Evidence & Proof*, 23(3), 255–262. DOI: 10.1177/1365712718807226
- Moon, M. D. (2019). Triangulation: A method to increase validity, reliability, and legitimation in clinical research. *Journal of Emergency Nursing: JEN*, 45(1), 103–105. DOI: 10.1016/j.jen.2018.11.004 PMID: 30616761
- Naderifar, M., Goli, H., & Ghaljaie, F. (2017). Snowball sampling: A purposeful method of sampling in qualitative research. *Strides in Development of Medical Education*, 14(3), e67670. DOI: 10.5812/sdme.67670
- Nataraj-Hansen, S. (2023). “Should’ve known better”: Using Lerner’s belief in a just world to understand how the Fraud Justice Network observe victims of online romance and investment frauds. *International Review of Victimology*, 02697580231167901. Advance online publication. DOI: 10.1177/026975802311679
- Nurse, J. R. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. In Attrill-Smith, A., Fullwood, C., Keep, M., & Kuss, D. J. (Eds.), *The Oxford handbook of cyberpsychology* (pp. 663–690). Oxford University Press.
- Obi, O. (2023, June 5). States with the most and least romance scams. *Social Catfish*. <https://socialcatfish.com/scamfish/states-with-the-most-and-least-romance-scams/>
- Park, B., & Lee, S. (2023). Current status of romance scams and countermeasures. *Journal of Digital Forensics*, 3(17), 95–116. DOI: 10.22798/kdfs.2023.17.1.95
- Rege, A. (2009). What’s love got to do with It? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology*, 3(2), 494–512. https://www.researchgate.net/publication/228373590_What’s_Love_Got_to_Do_with_It_Exploring_Online_Dating_Scams_and_Identity_Fraud
- Ryu, W. (2023, June 12). “We’ll find you your money”: The gang who scammed victims of a “romance scam” again. *Moneytoday*. <https://news.mt.co.kr/mtview.php?no=2023061210110870790>
- 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), 97–115. DOI: 10.17576/gema-2019-1901-06
- Stabek, A., Watters, P., & Layton, R. (2010, July). The seven scam types: Mapping the terrain of cybercrime. In *2010 second cybercrime and trustworthy computing workshop* (pp. 41-51). IEEE.

- Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: Qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, 49(1), 145–181. DOI: 10.1007/s12103-022-09706-4
- 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. DOI: 10.1093/bjc/azt009
- Whitty, M. T. (2015a). Anatomy of the online dating romance scam. *Security Journal*, 28(4), 443–455. DOI: 10.1057/sj.2012.57
- Whitty, M. T. (2015b). Mass-marketing fraud: A growing concern. *IEEE Security and Privacy*, 13(4), 84–87. DOI: 10.1109/MSP.2015.85
- Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 105–109. DOI: 10.1089/cyber.2016.0729 PMID: 28657792
- Whitty, M. T. (2019). Who can spot an online romance scam? *Journal of Financial Crime*, 26(2), 623–633. DOI: 10.1108/JFC-06-2018-0053
- Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking*, 15(3), 181–183. DOI: 10.1089/cyber.2011.0352 PMID: 22304401
- Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412–421. DOI: 10.1016/j.chb.2017.03.002

Seoung Won Choi is a Ph.D. candidate in Security Convergence at Chung-Ang University. Research interests encompass security convergence, cybercrime, and risk management, with a focus on examining and addressing contemporary challenges within these domains.

Julak Lee is a professor of Security Convergence at Chung-Ang University. Research interests span criminal justice, criminology, and security convergence, with a strong focus on exploring and resolving modern challenges in these disciplines.

Yeon-Jun Choi is a distinguished professor at Kwangju Women's University, specializing in Aviation Security Protection. Research interests encompass criminology, physical security, and aviation security.