Journal of Criminology and Criminal Justice Studies
Vol. 3, No. 1, 2025, pp. 85-104 • ISSN: 2583-9918

URL: www.arfjournals.com
https://doi.org/10.47509/JCCJS.2025.v03i01.04

Digital Romance Scams: A Transnational Threat

Mark S. Johnson and Mkay Bonner
Department of Criminal Justice, University of Louisiana Monroe

To Cite this Article

Mark S. Johnson & Mkay Bonner (2025). Digital Romance Scams: A Transnational Threat. *Journal of Criminology and Criminal Justice Studies,* 3: 1, pp. 85-104. *https://doi.org/10.47509/JCCJS.2025.v03i01.04*

Abstract: Digital romance scams are a global threat and have been increasing exponentially in numbers of scammers and amounts stolen over recent years. With digital dating, worldwide internet access, and emotion-based schemes, no person or nation is safe from the impact of romance fraud and cybercriminals. Offenders use identified tactics and justifications for their actions. Victims have differing characteristics but the impact of the exploitation always includes psychological and financial damage. Several researchers have been investigating this topic with increased attention since 2020. Current challenges and future trends that are interconnected with online romance scams include human trafficking, face to face ploys, the digital cloud, and artificial intelligence technology. These new iterations can create a physical danger that has not been associated with cyber romance scams before. Nations, corporations, and law enforcement agencies have devoted resources and personnel to try to stem the tide of cyberfraud including online romance scams. Links to many of these global resources are provided as well as recommendations from researchers in an attempt to reduce, and hopefully, eliminate digital romance scams as a transnational threat.

***Keywords*:** digital romance scams, online scams, transnational scams, global cyberfraud, cyberfraud prevention

Introduction

Cyber romance scams are a worldwide problem. They are not new. However, they have been increasing in number and damage, especially since 2020.

According to the United States Department of Justice (DOJ) in 2022, the number one type of transnational cyberfraud was Online Romance Scams and the occurrences were increasing. In 2023, the United States Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) received almost 900,000 cybercrime reports which included online romance scams. Recently, an article in *The Economic Times of India* reported that 43% of Indians became victims of romance scams last year.

Received : 18 April 2025 • **Revised :** 22 May 2025 • **Accepted :** 09 June 2025 • **Published :** 25 June 2025

Background

Historically, romance scams have been known by several names such as Sentimental Scams, Love Scams, Sweetheart Swindles, and Confidence Schemes (see D'Ambrosia & Barba, 2023; FBI, 2024b; Whitty, 2013). The perpetrators of these scams intentionally use peoples' emotions to victimize with no concern for the devastation and pain that they inflict.

Lazarus *et al.* (2022) defined romance scams as "the deployment of fake romantic relationships primarily for material ends" (p. 387). Romance scams use the vulnerability of loneliness and the psychological variable of fear in order to obtain money or other benefits while avoiding capture. Emotional manipulation is foundational in all romance scams including those that are online (Lazarus *et al.*, 2023b). The illusion of a relationship is inviting and comforting to the potential victim.

Before the internet, romance scammers, or confidence schemers, had to have extensive interpersonal skills in persuasion to be successful. Most often, the fraudulent relationship would require a lengthy time to develop necessitating the scammer to always be in character. With the global reach of the internet, one romance scammer can be involved in multiple online relationships at the same time. Fewer interpersonal skills are required because the mechanism of deceit is shrouded in digital interactions. The advantage goes to the criminal to the detriment of the unsuspecting victim.

Another advantage for online romance scammers is that cybercrimes are easy to set up. Digital access exists for the worldwide population (DOJ, 2022; and Sharma, 2023). Many people distrust their governments, so people do not follow online safety guidelines or they do not report being victimized. In addition, cybercrimes may be relatively anonymous (DOJ, 2021). Cybercrimes are difficult to investigate and prosecute especially if they cross international borders. And, most cybercrimes are transnational.

For the individuals who may become victims, online romantic relationships can provide several benefits. As mentioned for the criminals, the online environment can also allow some measure of anonymity for those seeking a romantic relationship. Anonymity may be helpful in mitigating possible judgment from friends and rejection from potential love interests (Coluccia *et al.*, 2020). The individuals may want privacy, may be seeking a thrill, or may just be curious. The digital environment also allows the person to create their ideal self, including dynamics such as how they look or what they do.

Digital Dating

The modern digital age influences almost every aspect of life. Interpersonal connections have become dominated by digital communications. The days of meeting a new love interest at a social or work function is becoming rare (D'Ambrosia & Barba, 2023).

Increasingly, people have started to turn to different forms of social media to meet someone new (Kwok and Wescott, 2020; and Sharma, 2023). As a result, digital dating platforms are flourishing (Vogels & McClain, 2023). Many online daters are enticed by the suggestion that the scientific platforms will provide a perfect connection for them (Coluzzia *et al.*, 2020). Over 40% of digital daters state that it is easier to find someone online as compared to face-to-face interactions. Interestingly, nearly 50% of single people in an Indian study would not date someone who did not use some form of social media (Times of India, 2024). Overall, approximately half of the online daters believe that this method is safe while half believe this may not be a safe way to date.

Based on Pew Research data, Vogels (2023) stated that 52% of U.S. citizens who have never been married have used online dating sites. According to this data, the rates are relatively the same when comparing data from 2019 and 2022.

Digital dating is not exclusively for millennials. There are some age differences among digital daters. Comparatively, only about 17% of U.S. citizens who are over 50 and dating have used a dating site regardless of marital status (Sidoti & Faverio, 2023). Almost half of the adults over 50 who have participated in online dating platforms do so to find a long-term relationship, while 36% of this demographic are only interested in casual dating. Within the 50 to 64 age demographic, over 50% of the online daters believe that they have encountered a scammer. This percentage decreases to approximately 40% for those over 65. Across young and old, men and women, the data indicates that older women are more likely to rate their online dating experiences as negative.

Digital Fraud and Transnational Romance Scams

At the beginning of the COVID-19 pandemic, many countries documented a surge in all types of online scams (e.g. Nolte *et al.*, 2021a, and Federal Trade Commission, 2020). For example, in Singapore, there was a 163% increase in online scams (Bose, 2021). In Italy, even physical mail scams related to romance increased over 100% (D'Ambrosia & Barba, 2023). Walstad (2021) analyzed worldwide data specifically for "catfishing scams" which can refer to romance scams. The data documented a large increase in online romance scams during the pandemic. Many crucial psychological elements were occurring at that time: fear, isolation, and loneliness.

According to Walstad (2021), the top ten countries with the most online romance scammers, in order, were the Philippines, Nigeria, Canada, United Kingdom, Turkey, Ghana, Afghanistan, Germany, Morocco, and Mexico. In contrast, the most money was stolen by cyber romance scammers who were in the United Kingdom, Turkey, Nigeria, China, and Ghana, respectively.

Monetary losses related to romance scams in the United States increased dramatically during the pandemic. From 2020 to 2021, the losses increased by 80% (Fletcher, 2021). Between 2017 and 2021, almost $600 million U.S. dollars was scammed from unsuspecting individuals who believed they were in a loving online relationship. However, from 2021 to 2023, online romance or confidence scams decreased in the United States (FBI, 2024b).

In 2021, the monetary loss from online romance scams was almost $1 billion U.S. dollars. By the end of 2023, the amount had decreased to approximately $650 million U.S. dollars which is close to the pre-pandemic numbers (FBI, 2024b). The number of complaints in the United States also decreased from over 24,000 in 2021 to slightly under 18,000 in 2023. These decreases are encouraging. The hope is that some of the preventative measures are effective instead of the alternative – fewer people are making reports but the victimization has continued at the same rate or has increased. To accurately answer this question, more research must be conducted.

Romance Scam Commonalities

Several characteristics are common to romance scams whether they are in person or online. These commonalities provide broad indicators that the person may be a fraudster. (Please note: These commonalities have been compiled from multiple sources. For examples, refer to Bonner & Johnson, 2023; DOJ, 2022; Lu *et al.*, 2020; Neo, 2020; Payne, 2020; Senior Medical Patrol, 2021; Sharma, 2023; and Skiba, 2021):

- Fake vulnerability: The scammer states their love of 20 years (or more) has recently died or ended their relationship. Or, they have never had someone who loved them.
- Whirlwind relationship: Everything happens very quickly. They state their need to connect. They emphasize their special feelings and undying love in a very short amount of time. They state they have never experienced anything like this relationship.
- Spiritual connection: They may use religion or spirituality to emphasize the love is real, special, ordained by the universe.
- Money problems: They state they want to be with the person, but they do not have the money to travel or they need to pay some debts first. Some scammers even suggest they will be put in jail if they do not have a certain amount of money by a specific date.
- Different geographical locations: They request the money to be wired to a different region or country than expected.

- Contradictory stories: They tell a different story or provide inconsistent information. They may be particularly adept at explaining these contradictions.
- Avoiding contact: They have many excuses of why they cannot meet in person. However, there is a particularly dangerous type of scammer who wants to meet in person (see Challenges and Future Trends).

These characteristics can be very effective within the online environment. The digital modality makes the scam process faster, cheaper, and easier.

Research

A recent literature search for *online romance scams* provided more documents than might be expected. Some of these are advertisements and some are relatively short opinion pieces. However, several articles are research based and include quantitative methods, qualitative methods, and mixed methods. Regular contributors to the online romance scams academic literature include Aborisade, Buchanan, Cross, Fletcher, Lazarus, Topalli, Wang, Whittaker, and Whitty. Some documents related to digital romance scams were published almost 20 years ago. Within the past two to three years, the number of publications has steadily increased. The literature also provided a broad view with many different countries represented. Because of the transnational nature of online scams, any consideration of this topic should include a global perspective.

Lazarus *et al.* (2023b) conducted a systematic review of international research on digital romance fraud. They found that most of the studies focused on the victims; however, a few of the articles considered the offenders. As a result, more information herein will be presented on the offenders instead of the victims. References will be presented to obtain more comprehensive information regarding victims. Overall, the research literature has identified both males and females as offenders. The victims are also males and females, wealthy and financially challenged, and display a range of intellectual abilities.

Offenders, Tactics, and Justifications

According to the World Health Organization (2018), cybercriminals considered loneliness and isolation when identifying their targets. Scammers preyed upon the weak and defenseless especially through fear and emotional connections. The most common scam victims tended to be teenagers, elderly people, persons with a mental illness (PMI), and persons with a recent major life change.

Cyber romance scams are not accidental. Wang and Zhou (2023) documented criminal premeditation while they were investigating the *Sha Zhu Pan* ("Pig-Butchering"

scam) in China. This scam uses persuasive techniques to target victims who speak Chinese.

In the scoping review by Coluccia *et al.* (2020), digital romance scammers tended to reference their relationship as "eternal". Consistently, the scammers used fictional tragedies that required critical deadlines to receive money. If the money was not received, they would face dire consequences. Therefore, if the potential victim really loved the scammer, the victim must send money as quickly as possible.

Cross and Holt (2021) found an increase in the use of military profiles as the narrative to lure unsuspecting victims. They stated that this scheme follows the typical pattern of using a trustworthy profile to enhance believability in online romance scams. Other common profiles have included doctors and clergy. Criminals have used the military profiles and included actual events to enhance believability.

Within West Africa, criminals using digital fraud techniques have been prolific (Cretu-Adotte *et al.*, 2024). Many of these scammers are part of a criminal organization instead of being solitary con-artists. They have been very adaptable within the online environment. Because of the global reach of the internet, these criminal enterprises have become formidable.

The glamour of wealth and luxury were documented as important motivators for West African romance scammers (Lazarus *et al.*, 2023b). Within the studies from West Africa, the scammers were found to be revered by their communities for being clever instead of being ostracized for their criminal activities. Many of the criminals were considered virtuous because their actions were seen as a form of reparation for past injustices.

To appear more trustworthy, many scammers have assumed an elitist profile and stated they are already wealthy (Lazarus *et al.*, 2023b). In this scenario, they cannot access their money at a specific time so they need the victim to give them some money for a short time. Other cyberscammers have presented themselves as having royal lineage. With experience, the romance fraudster can easily adjust their profile and online interactions to entice both the unsuspecting and the skeptical victim. Scripts have been written to help these criminals provide a convincing story to their victims.

Throughout many of these ploys by cyberscammers, classic psychological marketing techniques are found. Examples include the foot in the door technique (i.e. ask for something small first and then slowly increase the requests) and the door in the face technique (i.e. ask for something really big at first; after being denied, ask for something smaller). In addition, they frequently rely on the truth bias (some people tend to believe what others tell them) and the confirmation bias (some people only pay attention to information that confirms what they want to believe).

Another tactic within cyber romance scams is related to sextortion (Cretu-Adatte *et al*., 2024; and Cross *et al*., 2022). The term sextortion may be more typically associated with the online fraud and victimization of teenagers. The unsuspecting individual begins an online relationship with the cybercriminal. After developing an online relationship with a semblance of trust and deep emotions, the scammer requests nude or compromising pictures or videos (Coluccia *et al*., 2020). Once the scammer has the explicit materials, they threaten to expose the trusting victim in social media venues or directly to loved ones unless they receive a certain amount of money. Instead of money, the request may be to meet face to face (F2F) for sex or other nefarious purposes. Regrettably, several teenage suicides have been attributed to sextortion in the U.S. (OffenderWatch, 2023). This tactic has also been used with adults. Cross *et al*. (2023) found indications that there are some slight differences between sextortion and online romance scams but stated that further investigation is necessary for definitive statements.

Sometimes romance scams involve identity theft (DOJ, 2022). The cybercriminal will assume the identity of someone and use their name, picture, and other information. This tactic is less difficult than some might imagine because of the modern digital world. Many social media platforms exist from which someone may steal an identity and then create their own account to use for fraudulent activities. Almost every platform states they will confirm an individual's identity when they open an account, but this does not always happen.

Regardless of the technique, at some point, a crisis is created and the scammer desperately needs the help, and money, of the romantically committed target. Because of their love, concern, and fear of what might happen if they do not meet the requests, the target (who is now the victim) sends the money. In contrast, the victims may be asked to receive money and then send it to someone else. If they comply, they have become a money mule. This scheme of using victims as money mules is a method of money laundering used within the digital romance scam environment (DOJ, 2022).

Online romance scammers employed several methods to justify their actions. Whether these methods were conscious or unconscious, most revolved around blaming the victim (see Lazarus *et al*., 2023b; and Meikle & Cross, 2024). The victims were viewed as too wealthy, too privileged, or too stupid. Another common tactic was to dehumanize the victim. Victims have been dehumanized in music while the criminal was exalted and justified by the lyrics (Lazarus *et al*., 2023a). Whitaker *et al*. (2024) posited that the Chinese pig butchering (Sha Zhu Pan) scam is dehumanizing because the victims are reduced to the level of nothing more than animals, i.e. pigs. Another

factor that helps the criminals justify their actions is the physical distance between the scammer and the victim. This distance has provided a psychological defense for some of these fraudsters. These scammers do not know the victims and are not psychologically connected. As a result, the cyberscammers have no sympathy or compassion; for them, it is just a job. They may also view the scam process as a challenge of their skills and count all obtained monies as an indication of personal success.

Nigeria was documented as having the second highest number of online romance scammers in country and the third highest amount of money stolen in the world (Walstad, 2021). In efforts to justify their criminal actions, many of these scammers said they were doing it to make money for their children (Aborisade *et al.*, 2024). They sought sympathy instead of sanctions. Some parents even used their children to perpetuate the scams.

Many romance scammers erroneously believed that their actions were not dangerous and should not be considered a crime (Lazarus *et al.*, 2023b). They justified what they do by emphasizing that no one is physically hurt. They dismissed the idea that financial losses can be devastating for individuals. They also ignored the emotional impact that can be worse than the financial impact. The dire consequences of being a victim of online romance scams have included mental health issues, suicide, and homelessness.

Victims, Impact, and Vulnerability

People like to believe others and to think that they are wise enough to spot a scam. Considering the popularity of dating apps, many believe in the personal fable: It will not happen to me. Based on one study, dating app scammers constituted up to 39% of the romantic connections made (Times of India, 2024).

Fraud exploitation occurs with many different types of people. Overall fraud victimization has been linked with multiple characteristics including gullibility and gender. Some studies have identified gullibility as an enduring personality trait (Teunisse *et al.*, 2020,). Other researchers have documented females as more susceptible to fraud. In a research study in Japan by Ueno *et al.* (2022), loneliness and isolation in elderly women exacerbated fraud susceptibility and dangerous decisions (letting unknown subjects in their homes). Additionally, elderly individuals who were depressed and had insufficient social interactions were more susceptible to financial fraud (DOJ, 2022). Yet another study found that 75% of the people recognized an online scam but 43% were still willing to respond (Nolte *et al.*, 2021b).

The psychological impact resulting from fraud and victimization is powerful and can be devastating. Examples of the identifiable impact have included shame and guilt,

embarrassment, anger, loss of self-confidence, and exacerbated psychological disorders (Aborisade, Ocheja, & Okuneye, 2024; Bonner & Johnson, 2023; Coluccia *et al.*; and DOJ, 2022). Importantly, people do have differing psychological responses and are unlikely to experience all of these examples. Or, they may experience these responses in different phases instead of all at the same time.

Coluccia *et al.* (2020) emphasized the impact of romance scams on the victim as threefold: the loss of economic resources, the loss of a relationship (even though it was fictitious), and the shame of being a victim (see also Meikle & Cross, 2024). They found the additional reactions of shock and denial. They also identified some interesting victimization characteristics such as a tendency toward dependency and thrill seeking. Additional individual characteristics included impulsiveness, lack of self-control, advanced education, and middle-aged individuals (Whitty, 2013).

Over a decade ago, Whitty (2013) developed a five-stage process model associated with cyber romance scams. More recently, Wang and Topalli (2022) used qualitative methods to identify a reciprocal model that considers the interactions between the victims and the offenders. In their model, they presented the victimization process as having four phases. Impression management and interpersonal deception theory are important model components that they identified.

There are several screeners and vulnerability assessments that may prove beneficial when considering the possibility that someone may be an easy target for scammers. With this awareness of possible vulnerability, family, friends, and the individuals themselves can make plans and create barriers to help prevent scamming success. A discussion of these tools is beyond the scope of this article but some information may be found in *Cybercriminals and COVID-19 Scams: Cognitive Vulnerabilities Leading to Scam Susceptibility and Victimization, Prevention, and Future Directions* (Bonner & Johnson, 2023).

Challenges and Future Trends

Virtual crime including online romance scams is no different than any other property crime. As long as the profits are good and the probabilities of being caught and prosecuted are low, these crimes will continue and flourish. Online scammers will continue to improve their cyber profiles and imitate legitimate people or official government agencies to gain confidence and access to unsuspecting victims. The fraudsters will also continue to adjust their schemes. The following are some of the newer challenges, extensions, and predicted future trends within the online romance scam environment.

Human Trafficking

According to the International Justice Mission (2024), some agencies in Asia reported increases in human trafficking where the victims were forced to engage in online scamming. This scam strategy uses social media to entice unsuspecting victims by advertising professional jobs that provide good pay and benefits. Once committed, the victims are forced to engage in digital scams including those focused on romance. Often, the victims are forced to work long hours, are provided only small amounts of food, and are punished if they do not meet required quotas of cybercrime. There are estimates that hundreds of thousands of individuals may have fallen victim to this vicious cycle of the scammed being forced to scam others. Data indicate that $12 billion in U.S. dollars is generated every year through this illegal human trafficking activity in Asia. It is not unreasonable to hypothesize that this scam strategy is occurring in more areas of the world or may start soon.

Previously, human trafficking related to cybercrime increased dramatically within Latin America (Kobek, 2017). Mexico is one example of a country whose economy and geographic location make it a target for these criminals. Research documented that Mexico has had a 40% increase in the number of cybercrimes since 2013 with an estimated 10 million victims. Many of these victims can be connected to the human trafficking epidemic occurring in that area of the world (Corral *et al.*, 2023).

Further, the U.S. Department of State 2023 Trafficking in Persons Report noted that the decline of human trafficking in Mexico is hampered by corruption and the lack of prosecutions, particularly as it applies to cybercrimes. Cyber-trafficking and scamming are transnational crimes which increase the difficulty of combatting these criminal activities. Major challenges are associated with compliance of international laws and protocols. Tracking transnational criminals is extremely difficult which provides an advantage for these cybercriminals. To complicate the situation, many law enforcement agencies lack the training, equipment, and support to stay abreast of technological advances in cybersecurity and enforcement.

Face to Face (F2F) Ploy

The model online romance scam often will include making plans for the victim and the fraudster to meet in person. This plan can be one of the methods the scammer uses to lure the victim into sending money. The scammer will suggest they meet but then the scammer cannot meet because they do not have enough money to travel, or they have a bill to pay first, or they have not received their inheritance yet, or a similar story. The victim is desperate to meet their romantic interest in person so they send money.

A new twist to this scheme is for the criminal to actually go to meet them face to face (F2F). These encounters are particularly dangerous. Instead of only being able to do financial damage, the criminals can now physically attack the victim. Extreme caution is advised whenever meeting with anyone, especially if the relationship started online (DOJ, 2022).

Technology and Apps

The digital cloud is increasingly being used to store information electronically (Microsoft, 2023). This vast repository is a prime hunting ground for cybercriminals and their organizations. In addition, they use the cloud to facilitate and conduct their ongoing illegal enterprises. The more skillful the hacker, the more the cloud data will be used for cybercrimes including digital romance scams.

Scammers will continue to utilize online platforms to facilitate their illegal operations. Cybercriminals have proven they can recruit and lure unsuspecting victims into romance scams, human trafficking traps, and other nefarious activities through websites and applications such as Facebook, Twitter, Instagram, and chat rooms. While encrypted tools and sites are intended to increase protection for legal users, they also make accessing and tracing these cybercriminals even more challenging. Mobile apps such as Whatsapp can be expected to be utilized. Even more sophisticated and secure communication platforms will continue to be developed but they will help both legal users and criminal endeavors (Corral *et al.*, 2023).

Artificial Intelligence

With the explosion of the usage of Artificial Intelligence (AI), even more innocent people may be exploited. The advances with chatbots allow criminals to work faster and more efficiently when implementing an online romance scam (Fletcher *et al.*, 2024). Cybercriminals can use deepfake technology to quickly and easily create a multitude of images to enhance their fraudulent activities which includes online romance scams. In one survey, approximately 77% of persons using dating apps stated they had encountered fake profiles and pictures that looked like they were created by AI (Times of India, 2024). Of the study respondents, 26% believed they had communicated with a bot that they initially believed to be a potential romantic interest. Most of the public are just beginning to notice the trend of AI. However, the cyberworld has been developing AI for some time and the applications, both good and bad, are staggering. AI will be a prominent factor in the future cyberworld including online romance scams.

Recommendations

Any wise guidance must begin with admonitions to those who believe they have been scammed to contact the appropriate authorities. To try to stop crime, the law enforcement agencies must know about it. Reporting online romance scams is critical. After this, a more broad discussion is warranted that includes possible actions by countries, governments, and law enforcement. Individual specific recommendations have been comprehensively presented in other articles. Please refer to these references, among others, for details and suggestions on protecting individuals from fraud and online romance scams (e.g. Bonner & Johnson, 2023; DOJ, 2022; and Singapore Ministry of Health, 2022).

Reporting Options

Once an individual has been scammed or believes that someone is trying to scam them, it is critical that they contact the appropriate authorities. There are many options available to report cyberfraud around the world. A few examples are listed below:

In Australia, a reporting system entitled *Scamwatch* was used for some time (Meikle & Cross, 2024). The Australian Competition & Consumer Commission (ACCC) of the Australian Government is now funding a new centre entitled The National Anti-Scam Centre to collaborate between government and private entities (ACCC, 2024). They continue to use *Scamwatch* (https://www.scamwatch.gov.au/) as the direct reporting and educational mechanism for cybercrimes (Australian Government, 2024).

In Canada, the government maintains the Canadian Anti-Fraud Centre (Government of Canada, 2024). Victims can report fraud on this site, find information regarding new scams and threats, or connect directly with different law enforcement agencies (https://antifraudcentre-centreantifraude.ca/index-eng.htm).

In Europe, victims can contact the Consumer Centers Network of the European Union. There is a webpage for Victim Support Europe (https://victim-support.eu/help-for-victims/info-on-specific-types-of-victims/fraud-victims/). There is also a webpage with direct links to the reporting websites of Member States which is managed by EUROPOL, the European Union Agency for Law Enforcement Cooperation (https://www.europol.europa.eu/report-a-crime/report-cybercrime-online). In April of 2024, this webpage included 28 links to report cybercrimes by country. The countries are listed in alphabetical order from Austria through the United Kingdom.

Additionally, in Europe, the European Commission maintains a European Anti-Fraud Office, which is also referred to as OLAF (European Commission, 2024). A link to report fraud is provided as well as general fraud information and what to expect once a report has been made (https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en).

In South Africa, the Southern African Fraud Prevention Service (SAFPS, 2024) is a non-profit organization that helps with fraud prevention. They provide links and phone numbers to help individuals protect themselves from fraud (https://www.safps.org.za/Home/FraudPrevention). However, SAFPS appears more focused on identity fraud protection instead of other forms of fraud such as online romance scams.

In South Korea, The Office of Criminal Justice Information System unites their four agencies within criminal justice (2024). The Korea Ministry of Justice maintains the criminal justice portal where fraud can be reported (as well as other crimes) and the status of cases can be requested. The portal can be found at https://fgn.kics.go.kr/en/jsp/forum/crimeReport01.jsp.

In the United States, the Federal Bureau of Investigation (FBI, 2024a) developed the Internet Crime Complaint Center (IC3). On this site, all cybercrimes can be reported, not just online romance scams (https://www.ic3.gov/). In addition, the IC3 site provides an educational function by presenting information about the latest cyber threats and scams.

Of special note, if someone is in a foreign country in which they are not a citizen, they should always contact their local embassy or consulate and report that they have been victimized. This procedure will allow the victim's representative to contact the local authorities and make certain the crime is reported correctly based on local laws and procedures.

For Countries, Companies, and Law Enforcement

Cybercriminals and online romance scams cannot be stopped with one or two brief interventions. To have a measurable impact, many countries, companies, and individuals must work together. An interdisciplinary and cooperative plan will be necessary to make a difference in this ongoing transnational threat. The following are some recommendations for consideration that have been adapted from the indicated references.

Aborisade *et al.* (2024) conducted a qualitative study focusing on the lived experiences of the victims. They provided some suggestions for helping the victims which includes aggressive prosecution of the criminals. Without appropriate consequences for the offenders, the deterrents to these criminal behaviors do not exist. Additionally, people are less likely to report they have been victimized if their reports are not investigated and appropriate action taken.

In a focus on safety, a majority of U.S. digital daters who were surveyed believed that a background check should be required before someone could create a profile on a

dating platform (Vogels & McClain, 2023). This is an interesting suggestion but would likely be hard to implement. There are many complexities with background checks in the United States. Based on the specific type and coverage area of the check, the results may not be as comprehensive or accurate as digital daters would expect. Another complication involves the computer skills of the cybercriminals. If they can already digitally manipulate their images and narratives, they can be expected to be able to manipulate their background checks. Most likely, this suggestion would only stop the most primitive of online romance scammers.

One private investigation company in the U.K. specializes in investigations of individuals to determine if they are an online predator. They refer to this as relationship investigations and discuss the protective value these services can provide (Aretheysafe.co.uk, 2024). Another private international company, the Blockchain Intelligence Group, investigates cryptocurrency scams within cases of crypto dating fraud. This investigation is very specialized which requires skilled professionals to complete the work (Marzouk, 2023).

Coluccia *et al*. (2020) emphasized the overall value of awareness of online romance scams as a tactic to prevent victimization. Cross *et al*. (2023) as well as Wang and Topalli (2022) emphasized the importance of awareness campaigns provided by the dating platforms. Cross and Holt (2021) also mentioned the importance of prevention. They stated that preventative messages should include examples of common scams, an emphasis on skepticism, and a focus on critical thinking skills. In addition to prevention, they commented on using disruption measures when the damage had already begun.

Wang & Topalli (2022) also promoted the further development of algorithms to identify attempted online romance scams. The identification of credit card fraud provides a successful proof of theory. However, some people can be expected to be against this process considering it an invasion of privacy and an overreach of corporate and governmental authority.

Whittaker *et al*. (2024) encouraged law enforcement personnel to avoid shaming and blaming the victims. Commonly, blaming and shaming utilize metaphors in language to provide visual imagery. This imagery can alter the perception of individuals and their lived reality. Blaming the victims perpetuates the reluctance of victims to report the crimes. They make a case for compassion when anyone is dealing with a fraud victim.

Corral *et al*. (2023) emphasized increasing the access to the necessities of life and basic resources for countries which should ultimately benefit their citizens. They suggested incorporating public and private partnerships to improve security and citizen

development. They also promoted the sharing of information between law enforcement entities across territorial borders.

Additionally, collaborations should be created between apps and social media websites to develop anti-human trafficking campaigns and anti-cybercrime education (Corral *et al.*, 2023). These collaborations should include criminal tactics as well as methods to avoid being scammed. Further, these campaigns could educate users on how to recognize when a loved one or friend may be an unknowing victim and provide them with access to resources to stop the victimization. These messages may be especially useful to younger people who are often the main audience on social media platforms. These companies can also help law enforcement stay current on updates and innovative changes in the industry. And, Cretu-Adatte *et al.* (2024) suggested the development of scripts or other training devices to assist financial institutions and internet banking users to be more aware of cybercrime and digital romance scams.

Lazarus *et al.* (2023b) highlighted the need for increased empirical research into online romance fraud from both the victim and offender perspectives. They stated that strong theoretical foundations should be required in this research. They emphasized the importance of a truly global approach because of the nature of the online environment which crosses territorial borders worldwide.

Regulations and rules should be improved, specifically those that authorize the disclosure of electronic information during emergency investigations where lives are imminently in danger (Microsoft, 2023). Law Enforcement and governments should continue to only have access to cloud information through due process, but some exceptions are appropriate such as when access is needed to avoid death or great bodily harm. In an emergency, this type of exception can be vital for law enforcement and the protection of the public.

Rules should be modernized regarding cloud services and law enforcement to allow access to the evidence of illegal activities (Microsoft, 2023). Regulations and laws need to be established to allow digital evidence to be obtained from companies most directly involved with suspected scammers and cybercriminals. Past cases have documented that a company is the data controller and not the cloud service. Increased training for law enforcement and the inclusion of technology experts can greatly enhance the probability of gaining information without jeopardizing an investigation.

Please note, The Microsoft Corporation has provided a submission to the Cybercrime Convention Negotiations that is worth reviewing. The pdf can be found at https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/Microsoft_submission_to_AHC_third_substantive_session_002.pdf

Conclusions

Digital romance scams are abundant and global. The proliferation of online dating creates a rich hunting ground for cybercriminals. The psychological vulnerability of people can make them easy targets for exploitation in the digital dating environment. Many of the tactics employed by online romance scammers utilize classic psychologically informed marketing techniques. The offenders are skilled cybercriminals with many of them working within cybercriminal enterprises. Researchers have documented scammer tactics, methods, and justifications of these fraudsters. Countries have been identified with percentages of scammers within their borders and the amount of money stolen. Victims and victimization have been studied.

The current state of online romance scams appears to be fairly well documented, especially from 2020 to 2024. However, schemes and tactics continue to evolve. Of particular concern for the present and the future are the relationships between online romance scams and human trafficking, F2F meetings, cloud data, and AI technology.

Without question, empirical research must be conducted with AI and its impact on crimes and online romance scams. AI technology is increasing exponentially but the research is very limited (Fletcher *et al.*, 2024). Because it is relatively new, the negative side of deepfake technology and AI does not appear to have been given adequate consideration at this time. The full impact of AI on cybercrime and online romance scams has yet to be identified.

Several recommendations have been provided through research, corporations, governmental entities, and law enforcement agencies. Importantly, to reduce and ultimately eliminate digital romance scams, consistent transnational enforcement and global cooperation will be required.

References

Aborisade, R., Ocheja, A., & Okuneye, B. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters, *Journal of Economic Criminology, 3*, 100044. https://doi.org/10.1016/j.jeconc.2023.100044.

Are They Safe. (2024). Online dating fraud investigators. https://artheysafe.co.uk.

Australian Competition & Consumer Commission (ACCC). (2024). *The National Anti-Scam Centre*. The Australian Government. https://www.accc.gov.au/national-anti-scam-centre

Australian Government. (2024). *Scamwatch. The National Anti-Scam Centre*. https://www.scamwatch.gov.au/

Bonner, M., & Johnson, M. (2023). Cybercriminals and COVID-19 scams: Cognitive vulnerabilities leading to scam susceptibility and victimization, prevention, and future directions. In *Home Team Journal & the Ministry of Home Affairs of Singapore, Singapore Home Team Academy, 12,* 85-99.

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 & Epidemiology in Mental Health, 16*, 24. http://dx.doi.org/10.2174/1745017902016010024

Corral, R., Hussein, M., & Zia, M. (2023). Cyber-trafficking in Mexico. *The International Affairs Review*. The George Washington University's Elliott School of International Affairs, Washington, D.C. https://www.iar-gwu.org/print-archive/cyber-trafficking-in-mexico

Cretu-Adatte, C., Azi, J., Beaudet-Labrecque, O., Bunning, H., Brunoni, L, & Zbinden, R. (2024). Unravelling the organisation of ivorian cyberfraudsters: Criminal networks or organised crime? *Journal of Economic Criminology, 3(100056-)*. https://doi.org/10.1016/j.jeconc.2024.100056

Cross, C., & Holt, T. J. (2021). The Use of Military Profiles in Romance Fraud Schemes. Victims & Offenders, 16(3), 385–406. https://doi.org/10.1080/15564886.2020.1850582

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: An International Journal, 1*. https://doi-org.ulm.idm.oclc.org/10.1177/1748895822114958

Cross, C., Holt, K., & O'Malley, R. (2022). "if u don't pay they will share the pics': Exploring sextortion in the context of romance fraud. *Victims & Offenders,* https://doi-org.ulm.idm.oclc.org/10.1080/15564886.2022.2075064

D'Ambrosio, M., & Barba, D. (2023). Il bisogno affettivo e l'inganno dei social: i presupposti e le pratiche del Romance Scam. (The affective need and the social illusion: The assumptions and the practices of Romance Scam). Rivista Di Criminologia, Vittimologia e Sicurezza, (17, 74–87. https://doi.org/10.14664/rcvs/235 The original language is Italian but is translated.

European Commission. (2024). How to report fraud. *European Anti-Fraud Office*. https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en

European Union. (2024). *Victim Support Europe: Help for Victims*. https://victim-support.eu/help-for-victims/info-on-specific-types-of-victims/fraud-victims/

European Union Agency for Law Enforcement Cooperation (EUROPOL). (2022). *Report Cybercrime Online*. https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

Federal Bureau of Investigation (2024a). *Internet Crime Complaint Center (IC3)*. U.S. FBI. https://www.ic3.gov/

Federal Bureau of Investigation (2024b). *The FBI 2023 Internet Crime Report (IC3)*. U.S. FBI. p 1-34. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Fletcher, E. (2021). Social media a gold mine for scammers in 2021. *Federal Trade Commission*. https://www.ftc.gov/news-events/blogs/dataspotlight/2022/01/social-media-gold-mine-scammers-2021

Fletcher, R., Tzani, C., & Ioannou, M. (2024). The dark side of Artificial Intelligence – Risks arising in dating applications. *Assessment & Development Matters, 16*(1), 17–23. https://doi-org.ulm.idm.oclc.org/10.53841/bpsadm.2024.16.1.17

Government of Canada. (2024). Report fraud. *Canadian Anti-Fraud Centre*. https://antifraudcentre-centreantifraude.ca/index-eng.htm

The Economic Times (2024). When Mr. Right turns into Mr. Hyde: 43% of Indians have fallen prey to romantic scams online! *India Times. Panache.* https://economictimes.indiatimes.com/magazines/panache/when-mr-right-turns-into-mr-hyde-43-of-indians-have-fallen-prey-to-romantic-scams-online/articleshow/107660603.cms?from=mdr

International Justice Mission. (2024). Forced scamming. *IJM*. https://www.ijm.org/our-work/trafficking-slavery/forced-scamming

Kobek, L. (2017). The state of cybersecurity in Mexico: An overview. *The Wilson Center's Mexico Institute*. https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview

Korea Ministry of Justice. (2024). The Criminal Justice Portal. *Korea Information System of Criminal Justice Services*. https://fgn.kics.go.kr/en/jsp/forum/crimeReport01.jsp

Kwok, I., & Wescott A. (2020). Cyberintimacy: A scoping review of technology-mediated romance in the digital age. *Cyberpsychology, Behavior, and Social Networking, 23*(10), 657-667. https://www.liebertpub.com/doi/10.1089/cyber.2019.0764

Lazarus, S., Button, M., & Kopend, R. (2022). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice, 61:*381-398. https://doi.org/10.1111/hojo.12485

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E., & Okolorie, G. (2023a). Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. *Journal of Economic Criminology, 2, 100033*. https://doaj.org/article/d2e19ce114854e248c2a37f494c8aae6

Lazarus, S., Whittaker, J., McGuire, M., & Platt, L. (2023b). What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). *Journal of Economic Criminology, 2, 100013*. https://doi.org/10.1016/j.jeconc.2023.100013

Marzouk, O. (2023). Everything you need to know to investigate romance scams. BIG Investigations. https://blockchaingroup.io/everything-you-need-to-know-to-investigate-romance-scams/

Meikle, W., & Cross, C. (2024). "What action should l take?": Help-seeking behaviours of those targeted by romance fraud. *Journal of Economic Criminology, 3*(100054-). https://doi-org.ulm.idm.oclc.org/10.1016/j.jeconc.2024.100054

Microsoft. (2023). Cybercrime convention negotiations. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/Microsoft_submission_to_AHC_third_substantive_session_002.pdf

Neo, L. (2020). Leveraging on digital footprints to identify potential security threats: Insights from the behavioral sciences perspective. In M. Khosrow-Pour's (Ed.) *Encyclopedia of Criminal Activities and the Deep Web, Volume 3*.

Nolte, J., Hanoch, Y., Wood, S., & Hengerer, D. (2021a). Susceptibility to COVID-19 scams: The roles of age, individual difference measures, and scam-related perceptions. *Frontiers in Psychology, 12*, pp 789-883.

Nolte, J., Hanoch, Y., Wood, S., & Reyna, V. (2021b). Compliance with mass marketing solicitation: The role of verbatim and gist processing. *Brain and Behavior, 11*(11).

OffenderWatch (2023). Sextortion increasing suicide rates among teens. *GSA Resources, National Sex Offender Registry Network*. https://www.offenderwatch.com/post/sextortion-increasing-suicide-rates-among-teens

Senior Medical Patrol. (2021, August). *SMP Consumer Fraud Alert: COVID-19.* https://www.smpresource.org/Content/Medicare-Fraud/SMP-Consumer-Fraud-Alerts/SMP-Consumer-Fraud-Alert-COVID-19.aspx

Sharma, B.S. (2023). Romance scams: The rise of cybercrime in India's quest for love. Linkedin. https://www.linkedin.com/pulse/romance-scams-rise-cybercrime-indias-quest-love-sharma

Sidoti, O., & Faverio, M. (2023). Dating at 50 and up: Older Americans' experiences with online dating. *Pew Research Center*. https://pewrsr.ch/3q02RPr

Singapore Ministry of Health, (2022). *What to do in case of Cyberattack?* https://www.moh.gov.sg/licensing-and-regulation/cybersecurity

Southern African Fraud Prevention Service (SAFPS). (2024). Fraud Prevention. *SAFPS*. https://www.safps.org.za/Home/FraudPrevention.

Times of India. (2024). 39% connections on dating apps are scammers: Study. *India Times*. https://timesofindia.indiatimes.com/city/kolkata/39-connections-on-dating-apps-are-scammers-study/articleshow/107768119.cms

U.S. Department of State. (2023). *2023 Trafficking in persons report*. Office to Monitor and Combat Trafficking in Persons. https://www.state.gov/reports/2023-trafficking-in-persons-report/

Vogels, E. (2023). About half of never-married Americans have used an online dating site or app. *Pew Research Center*. https://pewrsr.ch/41qDd4c

Vogels, E., & McClain, C. (2023). Key findings about online dating in the U.S. *Pew Research Center*. https://pewrsr.ch/3HulOib

Walstad, L. (2021). Catfish analysis: The countries with the highest rates. *TechShielder. Blog*. https://techshielder.com/catfish-analysis-the-countries-with-the-highest-rates

Wang, F., & Topalli, V. (2022). 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*. https://doi-org.ulm.idm.oclc.org/10.1007/s12103-022-09706-4

Wang, F., & Zhou, X. (2023). Persuasive schemes for financial exploitation in online romance scam: An anatomy on Sha Zhu Pan (杀猪盘) in China. *Victims & Offenders, 18*(5), 915–942. https://doi-org.ulm.idm.oclc.org/10.1080/15564886.2022.2051109

Whittaker, J., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). Journal of Economic Criminology, 3(100052-). https://doi.org/10.1016/j.jeconc.2024.100052

Whitty, M. (2013). The scammers persuasive techniques model. *The British Journal of Criminology, 53*, 665-684.

World Health Organization. (2018). Mental health of older adults. Fact Sheet. The World Health Organization. Retrieved from http://www.who.int/en/news-room/fact-sheets/detail/mental-health-of-older-adults