
The Journal of Information Systems Security is a publication of the Information Institute. The JISSec's mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

Editor-in-Chief
Gurpreet Dhillon
University of Nebraska Omaha, USA

Managing Editor
Filipe de Sá-Soares
University of Minho, Portugal

Publishing Manager
Roderick Reid
ISEG, Universidade de Lisboa, Portugal

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 22, Issue 1

www.jissec.org

SOCIAL ENGINEERING THREATS: ONLINE ROMANCE SCAMS AND BEYOND

Gurpreet Dhillon

University of Nebraska Omaha, USA

Romance scams exploit human emotions, trust, and authority to manipulate victims into financial loss, identity theft, or even criminal activity. From traditional dating sites like eHarmony and Match.com to social media-based services like Bumble and Facebook Dating, these scams typically begin on dating platforms. Scammers have also infiltrated ethnically oriented dating sites, such as InterracialMatch and InternationalCupid, targeting individuals who are socially or geographically isolated.

Targeted Demographics and Psychological Manipulation

Victims are often over 40 years old, with the 50-59 age group being the most vulnerable. Research indicates that financial losses in these scams increase with age, and women tend to suffer more significant monetary losses. The success of these scams hinges on the perpetrator's ability to create an illusion of trust, authenticity, and authority. This is done by leveraging cognitive biases and decision-making errors. Scammers meticulously craft their schemes to exploit deeply ingrained psychological tendencies, such as the *halo effect*, where individuals associate positive traits with perceived authority figures. In addition, victims interpret information in a way that confirms their pre-existing beliefs. For example, a scammer posing as a bank representative might use official-sounding language, logos, and even spoof phone numbers to create a facade of legitimacy. This manipulation of trust is further amplified by *urgency bias*. This is where the scammer creates a sense of immediate threat or opportunity, pressuring the victim to act quickly without critical evaluation.

Scammers also exploit *social proof*, a cognitive bias in which people are influenced by the actions of others. An example of a phishing email would say that thousands of customers have already updated their accounts, encouraging the recipients to do the same. It is also reinforced by *authority bias*, when people comply with requests from

perceived authority figures, such as government officials, tech support agents, or corporate executives. With the help of sophisticated technical methods, like spoofed emails, fake websites, or deepfake technology, scammers create a convincing and multifaceted deception.

As a result of these strategies, human cognition is exploited, and rational thought processes are bypassed while emotional responses are triggered. In order to avoid falling victim to such scams, cybersecurity awareness and critical thinking are essential. The psychological mechanisms involved can assist individuals and organizations in recognizing red flags and taking proactive measures to protect themselves.

How Manipulation Led to Victimization

Human vulnerabilities are exploited by scammers, and psychological tactics are used to manipulate victims into compliance. Individuals are more likely to be deceived when their strategies bypass rational thinking and trigger emotional responses. In creating illusions that lead to victimization, three key tactics are particularly effective: authority exploitation, social engineering via familiarity, and urgency of emotional triggers.

Often, scammers exploit authority bias by posing as figures of trust and credibility, such as doctors, military personnel, or business executives. As a result, victims are more likely to comply with requests without questioning their authenticity in these roles. An impersonator who poses as a bank manager may use the perceived authority of their position to convince someone to reveal sensitive account information. Despite red flags, this tactic takes advantage of the human tendency to trust and obey those in power.

In addition, scammers build false connections with their targets by using social engineering through familiarity. Social media and other sources of public information are used to invent shared interests, mutual acquaintances, and personal ties. This creates a sense of trust and rapport, making victims more likely to lower their guard. To appear credible and relatable, scammers might mention a victim's recent vacation or a family member's name. This tactic exploits the human desire for connection and belonging, turning social bonds into tools for manipulation.

Finally, scammers pressure victims into making quick, irrational decisions by creating a sense of urgency and emotional triggers. Inventing crises that trigger fear, panic, or empathy, they cloud judgment and force an immediate response. An example would be claiming a loved one is in danger and demanding immediate payment to protect them. Overriding logical reasoning and compelling victims to act impulsively, this tactic capitalizes on the brain's fighter-flight response.

Human psychology is exploited by scammers because we trust authority, crave connection, and are vulnerable to emotional manipulation. It is important to understand these tactics to build resilience against scams. A person can better protect himself or herself from falling victim to these deceptive schemes by cultivating awareness, critical thinking, and skepticism.

A Tale of Deception

One of the predominant ways in which scammers collect personally identifiable information and engage in deception through the “abuse of authority” attack. In this case the perpetrator impersonates influential individuals and those with credibility to manipulate the victims. This may include impersonating military officials or public figures. Interestingly military officials stationed abroad stands out as a particularly insidious tactic. Even though there have been extensive public awareness campaigns, this scam continues to ensnare victims.

One example is a scammer who pretended to be a nurse at a military base in the Middle East¹. The interaction with the victim began as a seemingly harmless contact on social media. But very quickly it transformed into a friendship where both the perpetrator and the victim shared details about each other. However, the perpetrator carefully curated photos and shared only the pertinent details to sound convincing. In addition, she posted photos of herself wearing scrubs and army uniforms, as well as photos of someone she claimed was an army general. Paired with detailed stories about her military service and overseas hardships, these images created a convincing and believable narrative. This made it difficult for the victim to question her authenticity.

The scammer's story became increasingly elaborate over time, further gaining the victim's trust. According to the scammer, she had been in contact with a high-ranking army general who was helping her navigate life on a military base. To make the story more believable, she shared fake documents and messages with the general. The involvement of an authoritative figure gives the story credibility. This made it even harder for the victim to question what she was being told.

The deception reached its turning point when the scammer claimed that the general had arranged for a large sum of money to be transferred to her. According to her story, military regulations and bureaucratic delays prevented her from accessing the funds. She asked the victim to help her by covering various fees. She promised that the money would be repaid and that the victim would receive a generous share once the transfer was completed. At this stage, the victim had become emotionally invested

¹ While this is written as a fictitious case, many real cases exist. See: <https://lovescammer.com/lovescam-blog/un-doctor-in-syria-could-be-a-scammer/>

in the relationship and believed in the scammer's account. Trusting both the scammer and the supposed authority of the general, the victim sent the requested funds. However, the victim discovered later that the entire story had been fabricated.

This case illustrates the powerful influence of perceived authority and how easily it can be manipulated by skilled scammers. Through carefully staged photographs, forged documents, and emotionally compelling stories, the scammer constructed a believable narrative that discouraged skepticism. This narrative overrode the victim's critical judgment. The case serves as a reminder that authority can be manufactured as convincingly as identity itself. This underlines the importance of verifying claims independently and remaining cautious, even when a story appears credible and is supported by seemingly authoritative figures.

The Illusion of Connection

In the world of online scams, credibility is often the scammer's utmost valuable asset. One of the most effective ways to establish that credibility is by exploiting the psychological principle of social proof. It is an individual's tendency to trust information or people that appear to be endorsed by someone we already admire or respect. By creating the illusion that they are connected to celebrities, politicians, business leaders, or other public figures, scammers convince victims that they can trust them. Creating these fake associations lends credibility to the deception, making it more convincing.

Imagine Linda, a middle-aged woman who had long admired a well-known Hollywood actor². As many fans, she kept up with news about the actor's films and charitable efforts. Suddenly, she received a message on social media from someone claiming to be a close friend of the actor. There was little reason to be suspicious at first glance. There were photos of the individual with the actor at movie premieres, charity events, and private gatherings on the profile, which appeared to be authentic. Public information about the actor's recent projects aligned with mutual connections, regular posts, and conversations. Everything about the profile appeared credible.

During the following weeks, the scammer patiently built a relationship with Linda. The conversations did not immediately ask for money but instead stayed friendly and informal. In addition to sharing anecdotes about working on a film set with the actor, the scammer mentioned charitable initiatives that the actor supposedly preferred to keep private. The details were consistent with information available online, so Linda

² The story is based on real cases. See <https://www.security-everywhere.com/the-psychology-behind-scams-unraveling-the-minds-vulnerabilities/>

had little reason to doubt their authenticity. During each interaction, she felt as if she was interacting with a genuine member of the actor's inner circle.

It was only after establishing this foundation of trust that the scammer revealed his true purpose. A charitable initiative that had encountered unexpected financial difficulties was being privately supported by the actor. Since the project had not yet been publicly announced, financial assistance was sought discreetly from a small group of trusted supporters. The request seemed plausible. Linda admired the actor, believed she was contributing to a worthy cause, and felt privileged to be included. As a result of both her generosity and her trust, she provided a substantial contribution to the fund.

Several weeks passed before Linda began to question what had happened. Attempts to verify the charity led nowhere. Neither the organization nor a fundraising campaign existed, and the actor had no connection to the project. It soon became clear that the photographs she had initially believed had been digitally manipulated, the stories fabricated, and the online identity itself had been deleted.

This case illustrates the persuasive power of social proof in online deception. The scam succeeded not because the victim lacked intelligence or judgment, but because the scammer deliberately exploited an existing source of trust. Linda's skepticism was reduced and every subsequent interaction became more credible because of the scammer's apparent relationship with a respected public figure.

It has become easier than ever to create convincing false associations thanks to advances in artificial intelligence and image-generation technologies. Photographs, videos, and even voice recordings can now be manipulated with remarkable realism. Consequently, individuals should not assume that online images or claimed affiliations constitute reliable evidence of authenticity. This increasingly sophisticated form of social engineering can be defeated by verifying claims through independent and trusted sources.

The Illusion of Love

Among the most damaging forms of social engineering are online romance scams. Even though financial losses can be substantial, trust betrayal often causes more damage. Unlike many other scams that rely on urgency or fear, romance scams unfold gradually. The scammer patiently cultivates a relationship, creating an emotional bond before introducing financial requests or other forms of exploitation. In doing so, they capitalize on one of the most fundamental human needs - the desire for companionship, affection, and belonging.

Whenever an online relationship involves requests for money, financial information, or personal documents, it is imperative to pause and verify the individual's identity through independent sources. Legitimate relationships develop through mutual trust and openness, not through financial dependence or emotional pressure. Reverse image searches, independent verification of employment claims, and healthy skepticism about unexpected requests are simple but powerful safeguards.

The internet has transformed how people meet, communicate, and build relationships. These opportunities should not be viewed with suspicion, but neither should they be approached without caution. Romance scams remind us that social engineering is ultimately less about technology than human psychology. Scammers succeed because they understand how trust develops, how emotions influence decision-making, and how easily credibility can be manufactured in a digital world. Recognizing these psychological dynamics remains one of the most effective defenses against online deception.

Gurpreet Dhillon is the John Becker Dean of the College of Business Administration at the University of Nebraska Omaha, and a Professor of Management as well as a Professor of Information Systems and Quantitative Analysis. He previously held an endowed chair in Artificial Intelligence and Cybersecurity and has served in multiple academic leadership roles internationally. Gurpreet earned his Ph.D. from the London School of Economics and received an Honorary Doctorate from Örebro University, Sweden, in 2019. His research has appeared in several FT50 journals, and he is the author of more than a dozen books, including a best selling graduate level cybersecurity textbook. His expertise has been featured in major media outlets such as the Wall Street Journal, the New York Times, USA Today, BusinessWeek, CNN, NBC News, NPR, and TEDx, among others..