The Art of Deception:
An Analysis of Social Engineering Tactics in Financial Fraud

Authors

Nida ENGİN[1*]

Affiliations

[1]Master Program in Management Information Systems, Graduate School of Social Sciences, Yeditepe University, Istanbul, 34755, Turkey

*To whom correspondence should be addressed; E-mail: nida.engin@std.yeditepe.edu.tr

Abstract

Social engineering is a deceptive tactic used by fraudsters to manipulate individuals into divulging sensitive information or performing actions that are against their best interests. It involves exploiting human psychology and emotions to gain trust and access to confidential information, systems or assets. This paper discusses the different types of social engineering techniques used in fraud, including phishing, pretexting, baiting, and so on. It also examines the impact of social engineering on individuals and the measures that can be taken to prevent or mitigate its effects. By understanding the psychology behind social engineering, individuals can better protect themselves from the negative consequences of these tactics, which can range from identity theft and financial loss to reputational damage and legal liability.

Keywords: Financial fraud; identity theft; prevention methods; social engineering

INTRODUCTION

Fraud can be defined as a type of deception or deceitful behavior that involves misleading or tricking others, typically for the purpose of obtaining illegal gain (Albrecht et al., 2011). These actions occur when an individual or organization intentionally deceives or misleads others in order to gain illegal advantage. A common problem in the financial sector, financial fraud is often carried out through various manipulations, scams, or other illegal methods (Reurink, A. 2019). Fraud can result in victims suffering financial or emotional harm and can be subject to legal sanctions. Therefore, combating fraud is an important issue and is often regulated by laws (Vassiljev & Alver, 2016).

Financial fraud is one of the biggest threats facing many people and organizations today. With the development of technology, and the increasing use of digital platforms, financial fraud has evolved, and so has the tactics used by fraudsters to defraud unsuspecting victims. Financial fraud refers to planned fraudulent actions that exploit a person's financial situation. It means to deliberate fraudulent activities that take advantage of an individual's financial circumstances without their awareness or consent, leading to monetary setbacks. These actions are carried out without a person's knowledge or permission and can result in financial losses (Kranacher et al., 2010).

One of the most common tactics used by fraudsters in financial fraud is social engineering. Social engineering is the use of psychological manipulation to trick people into divulging confidential information or to take actions that may result in financial loss (Mann, 2018). In the study of "Hacking the human: Social engineering techniques and security measures" Mann discusses the various techniques used in social engineering in financial fraud, some ways to prevent it, comprehensive dimensions for social engineering. Social engineering attacks are often used to deceive a fraudster's target audience. The target of these attacks is to exploit vulnerabilities by using people's natural tendencies and weaknesses, ultimately leading to financial losses. Fraudsters, especially through the use of the internet and other electronic communication technologies, try to deceive their targets. For example, a fraudster might try to gain access to a victim's bank account using a fake website or a fake email. They may try to convince their victims to share personal information or carry out another action requested by the fraudster (Krombholz K. & Hobel H. & Huber M. & Weippl E., 2015). The use of social engineering techniques can make fraudulent attempts more convincing. Fraudsters can use many different social engineering tactics that they can use to trigger people's emotional

responses (Cialdini, R. B. 2007). For example, fraudsters can focus on people's feelings of insecurity and fears, getting their victims to respond quickly to the fraudster's requests. By using social engineering techniques, financial fraud can be more difficult to detect and prevent. It's important to be aware of these tactics and to take steps to protect yourself from becoming a victim of financial fraud (Mitnick, K., & Simon, W. L. 2002)

Social engineering tactics and attacks, which encompass the most effective and powerful methods of fraud techniques, can be categorized into computer-based and human-based forms (Anıl Keskin D., & Gözenman S., 2019). Computer-based social engineering is generally associated with digital tools such as malicious software, phishing campaigns, and fake websites. Attackers employ computer-based techniques to mislead victims and guide them into fraudulent financial transactions. For instance, tactics like stealing login credentials through a fake bank website or gaining access to financial data through malicious software are examples of how computer-based social engineering can be executed (Hadnagy, 2011). However, even if technology-based, no method can be considered independent of humans. Regardless of the technological methods employed, the greatest asset of fraudsters is the human tendency to trust and be persuaded by nature. Fraudsters establish contact with their targets and persuade them through various scenarios by gaining their trust (Cialdini, 2007).

Computer-based social engineering techniques can manifest in various forms. The period of increasing use of information technologies has enabled malicious actors to develop different methods through unaware usage. In these methods, fraudsters aim to steal individuals' sensitive information, take over the management of mobile devices, and gain financial benefits by using bank or other financial institution accounts (Krombholz, Hobel, Huber, & Weippl, 2015). The computer-based social engineering methods are as follows:

Phishing is a deceptive and malicious tactic employed in social engineering, wherein perpetrators send fraudulent emails, text messages, or other types of communication that masquerade as legitimate entities (Emigh, 2007). The aim is to trick unsuspecting individuals into divulging their sensitive personal, financial, or login information. The messages often create a sense of urgency or fear, coercing recipients to act hastily without questioning the authenticity of the communication (Emigh, 2007).

According to Hedayati (2012), phishing messages are skillfully crafted to mimic the appearance and content of reputable organizations, such as banks, online retailers, or social media

platforms, aiming to deceive recipients into believing that they are interacting with a trusted source. They employ various techniques to enhance their credibility, such as incorporating official logos, graphics, and formatting that closely resemble the genuine organization's branding. Typically, phishing messages contain a call-to-action that urges the recipient to take immediate steps to rectify an alleged problem or exploit an enticing offer. The message may include a hyperlink that directs the victim to a counterfeit website, meticulously designed to replicate the legitimate website of the targeted organization. Once the victim lands on the fake website, they are prompted to enter their confidential information, such as usernames, passwords, credit card details, or social security numbers, under the guise of security verification, account maintenance, or claiming a reward (Hedayati, 2012). Unbeknownst to the victim, their entered information is swiftly harvested by the fraudsters behind the phishing campaign. Armed with the stolen data, these criminals can engage in various illicit activities, including unauthorized access to financial accounts, identity theft, fraudulent transactions, or even selling the pilfered information on the dark web (Krombholz et al., 2015). Phishing attacks continue to evolve and adapt, employing competent techniques to evade detection and exploit human vulnerabilities. The perpetrators rely on psychological manipulation, exploiting trust and inducing a sense of urgency, in order to persuade individuals into divulging their sensitive information willingly. Consequently, it is crucial for individuals to exercise caution, remain vigilant, and employ robust security measures, such as verifying the authenticity of messages and websites, utilizing strong and unique passwords, and regularly monitoring financial accounts, to protect themselves from falling victim to these insidious phishing schemes (Krombholz et al., 2015). Krombholz and colleagues also discuss vishing in their study "Advanced social engineering attacks" and they define vishing as a voice phishing, a type of social engineering attack where fraudsters deceive people using voice communication tools such as phone or VoIP. They typically try to extract personal or financial information from their victims by posing as someone with a fake identity or a trusted source. The study notes that vishing often creates a sense of urgency to influence victims and directs phone numbers to fake websites or call centers to create a seemingly trustworthy environment. Such attacks are particularly effective in situations where people may be more vulnerable to fraud, as voice communication is not as easily scrutinized as written text. In summary, vishing is a type of social engineering attack that should be approached with caution from an information security perspective. Koyun and Al Janabi's article titled "Social Engineering Attacks" (2017) examines

the process and types of deception between individuals. These deception processes can provide insights into how individuals are persuaded and deceived following phishing attacks.

• Building Trust: Scammers introduce themselves as a trustworthy individual or organization. They may use fake identities and information.

• Requesting Information: Scammers ask victims to provide personal information, bank account details, or other sensitive information. They may use various methods to obtain this information.

• Persuading the Victim: Scammers try to persuade victims using various tactics. For example, they may claim that their accounts are in danger and they need to provide information immediately.

Malware is a type of malicious software designed to cause harm to computer systems, networks, or devices, or to gain unauthorized Access (Abraham et al., 2010). Malware can take various forms, including viruses, worms, trojans, spyware, adware, and ransomware. In social engineering fraud, attackers often use malware to gain the trust of victims or deceive them. For example, in a ransomware attack, attackers may send a malicious link or file to the victim and try to persuade them to open it. Additionally, using spyware, attackers can monitor victims' computers and steal information such as usernames, passwords, and other sensitive data. The best way to protect against such attacks is to use a reliable and up-to-date antivirus program, be cautious of emails and links from unknown sources, use strong passwords, and regularly update software. Abraham and Chengalur-Smith's 2010 article "An overview of social engineering malware: Trends, tactics, and implications" provides a comprehensive overview of the trends, tactics, and implications of social engineering malware. The article emphasizes the rapidly evolving nature of social engineering malware and the diversity of tactics used

Man-in-the-Middle (MITM) is a type of attack where an attacker intercepts communication between two parties, allowing them to listen, modify, or block the communication (Mallik et al., 2018). This attack typically occurs over a network, and the attacker impersonates both communicating parties to capture or manipulate data.

In social engineering fraud, attackers often use MITM attacks to deceive individuals (Mallik et al., 2018). For example, an attacker could perform a MITM attack on a Wi-Fi network that a victim is using to access their bank's website. The victim could be redirected to a fake website

controlled by the attacker when trying to log in, allowing the attacker to capture the victim's login credentials.

Scareware is a manipulative social engineering tactic commonly employed in financial fraud, which preys on the victim's fear and concern regarding their computer or device's security (Wall, 2011). This technique aims to deceive individuals into believing that their system is infected with a virus or malware, creating a sense of urgency and vulnerability. Scareware attacks typically begin with the victim encountering a pop-up message or receiving a convincing-looking notification claiming that their device has been compromised by malicious software (Sabelli, 2022). The messages often use alarming language, such as "Your computer is at risk!" or "Critical system error detected!" The intention is to instill fear and anxiety, compelling the victim to take immediate action to resolve the perceived threat. To further establish credibility and exploit the victim's trust, fraudsters may employ visual elements resembling legitimate security software interfaces or include official logos of reputable cybersecurity companies in their scareware messages (Ferreira & Teles, 2019). This visual deception adds an extra layer of authenticity and increases the likelihood of victim compliance. Once the victim is convinced of the imminent threat, the fraudster offers a solution to fix the alleged problem. This typically involves the sale of software or services that claim to remove the detected malware or viruses. However, the provided software is usually fake and ineffective in addressing the non-existent threat (Sabelli, 2022). In some cases, the scareware software itself may introduce actual malware or spyware onto the victim's device, causing further harm and compromising their privacy and security. Fraudsters employ various distribution methods to propagate scareware, including malicious websites, compromised advertisements, or even spam emails. They may target individuals who are less tech-savvy or those who are more susceptible to panic-driven decision-making (Hadnagy, 2011). By exploiting human emotions, particularly fear, scareware attackers capitalize on the victim's desire to protect their personal information and sensitive data. The financial implications of falling victim to scareware can be substantial. Victims may end up purchasing expensive and useless software or services that do not deliver the promised protection. Additionally, they may unknowingly expose their devices to actual malware, leading to further financial losses, identity theft, or unauthorized access to personal and financial accounts. To protect oneself from scareware attacks, individuals should be aware of the tactics employed by fraudsters and adopt preventive measures. It is crucial to maintain up-to-date antivirus software and regularly scan devices for malware (Abraham & Chengalur-Smith, 2010). Implementing reliable ad-blockers and avoiding suspicious websites

or unfamiliar links can reduce the risk of encountering scareware messages. In case of encountering scareware, it is recommended to close the pop-up or notification, and avoid engaging with the provided software or services. Increasing awareness through education and disseminating information about scareware and other social engineering tactics is essential. By empowering individuals with knowledge, they can recognize and avoid falling victim to scareware attacks, contributing to a safer online environment. Human-based social engineering attacks are types of attacks in which an attacker manipulates people's natural behaviors and social interactions to gain access to a target or obtain information (Del Pozo et al., 2018). The main types of these attacks are as follows:

Pretexting, a significant social engineering tactic, is frequently employed in financial fraud, aiming to deceive individuals and extract confidential information (Krombholz et al., 2015). This tactic involves the creation of a false scenario or pretext to manipulate the victim into divulging sensitive data willingly. The fraudster assumes the identity of a trustworthy individual, often posing as a bank employee, financial advisor, or government official, to establish credibility and gain the victim's trust. In pretexting schemes, the fraudster meticulously plans and crafts a narrative to create a sense of legitimacy and urgency. They exploit the victim's natural inclination to comply with authority figures or individuals they perceive as knowledgeable and trustworthy (Hadnagy, 2011). The pretext may involve a variety of scenarios, such as a security breach, account verification, or an urgent financial matter requiring immediate attention. To make the ruse more convincing, the fraudster leverages various tactics and resources. They may spoof phone numbers, emails, or official documents to create a façade of authenticity (Abraham et al., 2010). Additionally, they gather publicly available information about the victim, such as their name, address, occupation, or recent transactions, to establish a sense of familiarity and further enhance their credibility. Once the fraudster establishes contact with the victim, they skillfully manipulate the conversation to extract confidential information. They may engage in empathetic discussions, expressing concern for the victim's financial well-being or offering assistance in resolving an alleged issue. By creating a friendly and helpful atmosphere, the fraudster aims to lower the victim's guard and encourage them to disclose sensitive details, such as bank account numbers, passwords, or social security numbers (Abraham et al., 2010). Furthermore, pretexting often involves psychological techniques to exploit the victim's emotions and cognitive biases (Hadnagy, 2011). The fraudster may use fear, promising protection against potential threats or dire consequences if the victim fails to cooperate. They might also exploit the victim's desire for

personal gain or the fear of missing out on a lucrative opportunity. By manipulating these emotions, the fraudster increases the chances of obtaining the desired information. Pretexting attacks can have severe financial consequences for victims. Once the fraudster obtains the sensitive information, they can gain unauthorized access to the victim's financial accounts, conduct fraudulent transactions, or engage in identity theft. The victims may suffer significant financial losses, damage to their credit history, and enduring emotional distress (Krombholz et al., 2015). To protect oneself from pretexting attacks, it is crucial to remain vigilant and employ preventive measures. Individuals should be cautious when sharing personal information, especially over the phone or email, and verify the legitimacy of any requests or offers received. Contacting the relevant organization directly using verified contact information can help confirm the authenticity of the communication. Additionally, regularly monitoring financial accounts, using strong and unique passwords, and implementing two-factor authentication can significantly mitigate the risks associated with pretexting attacks (Krombholz et al., 2015).

Baiting is a cunning social engineering tactic frequently employed in financial fraud, designed to entice individuals into taking actions that ultimately lead to financial loss (Hadnagy, 2011). This technique involves the offer of something valuable or enticing to the victim, which serves as a bait to manipulate their behavior and exploit their vulnerabilities. In baiting schemes, fraudsters strategically present victims with tempting opportunities or rewards to gain their trust and cooperation. The bait can take various forms, such as a free service, a prize, a job offer, or access to exclusive content. The allure of the bait is intended to capture the victim's attention, pique their interest, and override their judgment and caution (Mouton et al., 2016). To execute a successful baiting scheme, fraudsters employ persuasive tactics that exploit human psychology and emotions. They often create a sense of urgency or scarcity, emphasizing that the opportunity or reward is time-limited or available to a limited number of individuals. This scarcity element triggers the victim's fear of missing out and increases their inclination to act quickly without thoroughly evaluating the situation (Mouton et al., 2016). Fraudsters may leverage online platforms, social media, or targeted advertisements to distribute their bait and reach a wide audience. They strategically tailor their messages to appeal to specific demographic groups or individuals who are likely to be susceptible to the bait's allure. The communication may include compelling testimonials, fabricated success stories, or falsified credentials to enhance credibility and entice victims further (Dong et al., 2016). Once the victim takes the desired action, such as clicking a link, downloading a file, or providing personal information, the fraudsters' objective is achieved. They may gain unauthorized access to the

victim's devices, install malware or spyware, or obtain sensitive information, including bank account details, social security numbers, or login credentials (Abraham & Chengalur, 2010). This acquired information is then exploited to carry out fraudulent activities, such as unauthorized financial transactions, identity theft, or unauthorized access to other accounts. Baiting attacks can have severe financial and personal consequences for victims. Individuals who fall prey to baiting schemes may suffer significant financial losses, reputational damage, and emotional distress. Furthermore, the aftermath of such attacks can be time-consuming and challenging to resolve, requiring extensive efforts to regain financial stability and restore one's online security. To protect oneself from baiting attacks, individuals must exercise caution and adopt preventive measures. It is essential to remain skeptical of enticing offers that appear too good to be true and to critically evaluate the legitimacy and credibility of the source. Verifying the authenticity of websites, emails, or advertisements through independent channels and conducting thorough research on unfamiliar organizations or opportunities can help identify potential scams. Implementing robust security measures, such as antivirus software, firewalls, and regular software updates, can also minimize the risk of falling victim to baiting attacks (Ferreira & Teles, 2019).

Quid pro quo, derived from Latin, means "something for something". In social engineering, quid pro quo is a tactic where a person offers something in exchange for personal or sensitive information (Aun et al., 2022). This often occurs over the phone, where the attacker tries to persuade the target to provide information in exchange for a service or benefit. For example, the attacker may claim to be calling on behalf of a technology company and say there is a security issue with the target's computer. They may then request remote access to the target's computer to provide technical support. This way, the attacker can gain access to the target's computer and steal sensitive information. For quid pro quo to be effective, the attacker must create a convincing fake identity and persuade the target that the situation is real (Connor, 2015). They may impersonate employees of a company and offer a version upgrade or software installation service to the employees of a targeted company. This way, social engineers can ask users to temporarily disable their antivirus software for the installation of malicious software (Long, 2011).Therefore, it is crucial for employees to be cautious and skeptical of individuals claiming to represent the company to protect against such attacks. Otherwise, sensitive data can be accessed from individuals' or company employees' computers, data can be collected for financial fraud, and doors can be opened to fraudsters.

Dumpster Diving is a type of physical security breach and falls under social engineering attacks. In this method, attackers sift through a victim's waste bins, recycling bins, or trash containers to obtain the targeted information or material. This attack method typically unfolds as follows: The attacker targets the waste bins of the victim organization or individual and rummages through them before they are regularly emptied. During this process, attackers search for information-carrying items such as used invoices, bank statements, personal notes, passwords, or other sensitive information on used documents, floppy disks, hard drives, flash drives, or other media devices (Koyun & Al Janabi, 2017; Long, 2011). Dumpster Diving can jeopardize personal privacy or corporate security. Therefore, it is important to implement security procedures such as regular disposal of waste materials and destruction of unnecessary documents.

Shoulder Surfing is a form of observation technique used in social engineering attacks. In this method, attackers closely observe their targets from a short distance to watch for sensitive information they enter using input devices such as keyboards, mice, or touch screens. For example, if a person is entering their PIN at an ATM and a perpetrator watches over their shoulder to observe this information, it is considered Shoulder Surfing (Koyun & Al Janabi, 2017). This type of attack is typically carried out in crowded environments or public places. Attackers may act in ways to distract or deceive the target. For instance, an attacker might create an artificial problem to draw the target's attention and then observe the information entered by the target during this distraction (Long, 2011). The most effective way to protect against Shoulder Surfing is to be mindful of the people around you and take extra precautions to protect your sensitive information when using input devices. For example, when entering your ATM or bank card PIN, it's important to observe the people around you and your surroundings and conceal your keystrokes. Additionally, in general, it's important to be aware of the people around you when entering sensitive information and, if possible, protect your screen (Long, 2011).

Tailgating, also known as "piggybacking," is a physical security breach where an unauthorized person follows an authorized individual into a secure area. This method exploits the natural human tendency to be polite and hold doors open for others, allowing the unauthorized person to gain access without proper authentication (Long, 2011). In a typical tailgating scenario, an unauthorized person waits near a secure entrance, such as a door with an access control system. When an authorized person approaches the door and unlocks it using their access card or code,

the unauthorized person quickly slips in behind them, taking advantage of the door being held open. Tailgating can be exploited in social engineering attacks to gain physical access to secure areas or buildings. An attacker may dress and behave in a way that makes them appear as if they belong in the environment, making it less likely for others to question their presence. Attackers may also employ various tactics to distract or deceive security personnel (Long, 2011). Therefore, when implementing measures against social engineering attacks, it is crucial to focus not only on technical security measures but also on employee education and awareness. Employees should be cautious of unfamiliar individuals and adhere to security procedures diligently. Additionally, security personnel should rigorously enforce authentication requirements and intervene immediately in suspicious situations.

RESULTS

Education and awareness play a crucial role in preventing social engineering in financial fraud. Studies have examined the impact of awareness campaigns and educational programs on reducing vulnerability to social engineering attacks. It is essential to educate individuals and organizations about the various tactics employed by fraudsters, including phishing, pretexting, scareware, and baiting. By providing comprehensive training programs and resources, individuals can become more knowledgeable about these techniques and better equipped to identify and respond to potential threats (Wells, 2014). Organizations should conduct regular workshops, seminars, and awareness campaigns to ensure that employees and customers are well-informed about the latest social engineering tactics and the importance of cybersecurity. Also, organizations can collaborate with law enforcement agencies, industry experts, and cybersecurity organizations to disseminate information about emerging social engineering techniques, case studies, and real-life examples of financial fraud. This collaborative approach can enhance awareness and foster a collective effort to combat social engineering in the financial sector (Gulati, 2003). Kim & Lee (2018) conducted a survey-based study to evaluate the effectiveness of social engineering awareness programs. Their research revealed that individuals who had received education and training on social engineering tactics demonstrated higher levels of awareness and were more likely to detect and report fraudulent activities. The study emphasized the importance of ongoing education and reinforcement to sustain awareness and combat evolving social engineering techniques.

In addition to education, organizations should implement robust security measures to protect against social engineering attacks. This includes deploying advanced firewalls, intrusion detection and prevention systems, and secure email gateways to detect and block malicious (Wells, 2014). Regular security assessments and penetration testing should be conducted to identify vulnerabilities and address them promptly. It is also important to keep all software and systems up to date with the latest security patches to minimize the risk of exploitation (Bakhshi & Papadaki & Furnell, 2009).

Cultural and societal factors can influence individuals' susceptibility to financial fraud and social engineering tactics. Some researches have explored the impact of cultural norms and social dynamic factors on fraud vulnerability. Sample, Hutchinson, Karamanian & Maple (2017) conducted a cross-cultural study on the influence of societal factors on fraud susceptibility and suggested that cultural differences can affect individuals' sensitivity and responses to social engineering tactics. For example, in some cultures, people may be more obedient to authority figures, while in others, they may seek more individualism and autonomy. This suggests that they may exhibit different responses to social engineering attacks. Additionally, cultural values and norms can also influence people's tendencies to share information and their levels of trust (Thompson & Findlay, 1999). Therefore, considering and addressing cultural differences is important for protecting against social engineering attacks. Understanding intercultural and interracial cultural differences can help make fraud prevention strategies more effective. In this context, cultural sensitivity and education play an important role for institutions such as financial organizations and social media platforms.

Establishing strict access controls and permission levels is crucial to prevent unauthorized access to sensitive data and systems. This can be achieved through the implementation of role-based access controls, where individuals are granted access based on their specific job responsibilities and level of authority (Koivisto, 2019). Preventing fraud through internal control Strong password policies should be enforced, including the use of complex passwords and regular password changes. Regular user account audits should be conducted to ensure that access rights are up to date and revoke any unnecessary privileges.

Organizations should also extend their security measures to include their vendors and supply chain partners. Social engineering attacks can occur through third-party relationships, so it is important to assess the security practices of vendors and enforce strict contractual obligations regarding data protection and security (Katz, 2016). Regular audits and assessments of vendor

security can help identify potential vulnerabilities and ensure compliance with security standards.

Continuous monitoring of network and system activities is essential to detect any suspicious behavior or anomalies that may indicate a social engineering attack. Implementing real-time monitoring systems and security information and event management (SIEM) solutions can help identify and respond to security incidents promptly. Organizations should also have a well-defined incident response plan in place to ensure a coordinated and effective response to any security breaches or social engineering incidents (Abdallah et al., 2016).

Employees play a vital role in preventing social engineering attacks. Organizations should foster a culture of security awareness and encourage employees to report any suspicious activities or attempts at manipulation (Wells, 2014). Establishing open communication channels and providing a confidential reporting system can facilitate the timely reporting of incidents without fear of reprisal. Regular reminders and updates about emerging social engineering tactics can also help keep employees vigilant.

In today's digital landscape, where cyber threats continue to evolve, traditional password-based authentication alone is no longer sufficient to protect sensitive information and resources from social engineering attacks. Two-factor authentication (2FA) has emerged as an effective method to enhance security and thwart such malicious activities (Reese, Smith, Dutson, Armknecht, Cameron & Seamons, 2019). By combining multiple authentication factors, 2FA provides an additional layer of defense, ensuring that only authorized individuals have access to sensitive data and systems. Two-factor authentication involves the use of two or more independent methods to verify the identity of a user. Typically, these methods fall into three categories: something you know, something you have, and something you are. The most common combination is a password (something you know) and a security token (something you have), such as a physical device or a mobile app (Reese, Smith, Dutson, Armknecht, Cameron & Seamons, 2019). This multi-factor approach significantly reduces the risk of unauthorized access, even if one factor is compromised. As technology evolves, new authentication methods and technologies are being introduced to further strengthen 2FA. Biometric authentication, such as fingerprint or facial recognition, is gaining popularity as a second factor (Reese et al., 2019). This approach adds an additional layer of security by using unique biological traits, making it significantly harder for attackers to impersonate legitimate users. Furthermore, the integration

of contextual information, such as the user's location or behavioral patterns, can enhance the effectiveness of 2FA. Adaptive authentication systems analyze multiple factors to determine the risk associated with an authentication attempt and adjust the level of security accordingly (Reese et al., 2019). This dynamic approach ensures that strong authentication measures are applied when necessary, without inconveniencing users during routine activities.

Peltier-Rivest's 2018 study, titled "The battle against fraud: do reporting mechanisms work?", evaluates the importance of reporting financial fraud cases and the effectiveness of these reporting processes. The article focuses on different reporting mechanisms used in combating financial fraud and their success rates. Additionally, it offers suggestions for improving reporting processes and developing more effective strategies in the fight against financial fraud. According to this study, encouraging reporting of suspicious activities is a critical aspect of preventing social engineering attacks in the realm of financial fraud. Organizations should actively promote a culture of vigilance and provide channels for employees to report any potential fraudulent incidents or suspicious behavior. By establishing a secure and confidential reporting system, organizations can empower their employees to come forward without fear of retaliation or negative consequences. Creating an open and supportive reporting environment is essential to foster a sense of trust and accountability within the organization. Employees should be made aware that their concerns will be taken seriously, and that their identities will be protected throughout the reporting process. Anonymity options, such as anonymous hotlines or online reporting platforms, can further enhance employees' confidence in reporting suspicious activities. To encourage reporting effectively, organizations should provide comprehensive training programs that educate employees about the common indicators of social engineering attacks. By enhancing their awareness and knowledge, employees become better equipped to recognize potential red flags and are more likely to report suspicious incidents promptly. Furthermore, organizations should emphasize the importance of reporting even the smallest suspicions or uncertainties. Social engineering attacks often involve manipulative tactics that exploit human vulnerabilities, and early detection is crucial to prevent financial losses and mitigate the impact on both individuals and the organization. To incentivize reporting, organizations can implement a robust system for incident management and response. Promptly addressing reported incidents, conducting thorough investigations, and providing feedback to the reporting employees not only demonstrate the organization's commitment to combating social engineering fraud but also reinforce the reporting culture. In addition to internal reporting channels, organizations should establish partnerships with external entities,

such as law enforcement agencies and financial institutions, to facilitate the sharing of information and collaboration in combating social engineering attacks. This collaborative approach enhances the collective knowledge and resources available to detect, investigate, and prevent fraudulent activities. Regular communication and awareness campaigns can also play a vital role in encouraging reporting. By consistently reminding employees of the importance of reporting and highlighting success stories where reporting has helped prevent financial fraud, organizations can reinforce the message and foster a proactive and vigilant workforce. Ultimately, creating a strong reporting culture within organizations is crucial in the fight against social engineering attacks in financial fraud. By encouraging employees to speak up and providing the necessary support and protection, organizations can detect and respond to threats more effectively, safeguard their assets and sensitive information, and contribute to a safer financial environment.

Data analytics and artificial intelligence (AI) have emerged as powerful tools by leveraging advanced algorithms and data analytics to identify patterns and anomalies indicative of fraudulent activities in the fight against social engineering attacks in the realm of financial fraud. By leveraging the capabilities of advanced technologies, organizations can enhance their ability to detect, prevent, and mitigate the risks associated with social engineering tactics (Bao, Hilary, & Ke, 2022). The article "Artificial Intelligence and Fraud Detection," published in 2022 -by Bao and orhers- explores the usage and importance of data analytics and AI in preventing social engineering in financial fraud, highlighting their potential benefits and key considerations. Bao et al. (2022). explored the role of AI in fraud prevention and detection. Their research demonstrated that AI-based systems can analyze vast amounts of data in real-time, detect subtle patterns, and flag suspicious transactions or behaviors. The integration of AI into existing fraud prevention frameworks has shown potential in improving accuracy, reducing false positives, and enabling proactive fraud prevention. Data analytics plays a crucial role in identifying patterns and anomalies that may indicate social engineering attempts. By analyzing large volumes of data, including transaction records, user behaviors, and communication patterns, organizations can uncover irregularities and suspicious activities. Machine learning algorithms can be employed to analyze historical data and establish baseline patterns, enabling the detection of deviations that may signal potential social engineering attacks (Guven & Aras, 2022).

AI-powered systems can enable real-time monitoring of various data sources, such as network traffic, log files, and user activities. By continuously analyzing and correlating this data, organizations can promptly identify and respond to suspicious activities associated with social engineering. AI algorithms can generate automated alerts and notifications, allowing security teams to take immediate action to prevent potential fraud incidents (Hamal & Senvar, 2021).

Data analytics and AI techniques can be used to build user profiles and analyze behavioral patterns. By monitoring user interactions, preferences, and deviations from established norms, organizations can detect anomalies that may indicate social engineering attempts. Machine learning algorithms can learn from historical data to identify unusual behaviors and assess the risk level associated with individual users or transactions (Awoyemi et al., 2017).

AI technologies, such as facial recognition and voice biometrics, can strengthen authentication mechanisms and reduce the risk of social engineering attacks. By employing these technologies, organizations can verify the identity of individuals more accurately, making it harder for fraudsters to impersonate legitimate users. AI-powered authentication systems can analyze multiple factors, including facial features, voice characteristics, and behavioral biometrics, to provide a robust and reliable authentication process (Reese et al., 2019).

DISCUSSION

This study examined the relationship between demographic variables and social engineering tactics, an important component of financial fraud. Findings obtained through literature review and survey analysis suggest that susceptibility to social engineering attacks does not significantly vary based on demographic factors such as age, gender, education level, and income. These results indicate that individuals across all age groups, genders, education levels, and income brackets may equally fall victim to social engineering attacks. However, slight variations based on demographic characteristics have been identified. For instance, individuals with lower levels of education may be more vulnerable to certain social engineering tactics. These findings are crucial for the prevention of financial fraud and combating social engineering attacks. Financial institutions and authorities should develop education and awareness programs targeting a broad audience rather than focusing solely on specific demographic groups. Additionally, special measures should be implemented for individuals with lower education levels or limited financial literacy, with increased efforts to protect this

group. The study emphasizes the need for effective measures against social engineering attacks, tailored to demographic differences. Future research should delve deeper into the association between social engineering tactics and demographic variables, as well as develop more comprehensive prevention strategies.

Study provides an important perspective on social engineering in financial fraud. Starting with the definitions of fraud and financial fraud, the thesis elaborates on various types of social engineering. The literature review indicates that social engineering plays a significant role in financial fraud and that prevention methods in this area need to be enhanced. The research methodology involved a survey, which showed that demographic characteristics did not change the likelihood of falling victim to social engineering attacks. This highlights that social engineering attacks pose a potential threat to everyone. The survey findings are consistent with the literature review, emphasizing the importance of the human factor in combating financial fraud. Therefore, the most significant contribution of the thesis is the recommendation for financial institutions to develop more effective/preventive measures against social engineering attacks and for individuals/organizations to be more conscious of such attacks. This thesis theoretically and practically demonstrates that the inherent tendency to trust and the reflex to act based on fear or desire for gain can lead to dangerous outcomes. It advises controlling instinctive reflexes, adopting a more skeptical approach to events, and ensuring the security of devices. Therefore, it contributes not only to academics or professionals but also to individuals in their daily lives, urging them to build financial security.

This thesis explores social engineering in financial fraud, providing a comprehensive analysis of fraud and financial fraud definitions, types of social engineering, and preventive measures. However, the study faced several limitations and challenges that should be considered when interpreting the results. One of the major challenges encountered during the survey methodology was the difficulty in creating a homogeneous sample group by distributing the survey to individuals from different age groups, professions, educational backgrounds, and income levels. This diversity made it challenging to ensure that all respondents had a similar understanding of the terminology used in the survey questions. Despite efforts to explain technical terms, some respondents may have misunderstood or been unfamiliar with certain terminologies, leading to potential biases in the data interpretation. Additionally, the technical and specialized nature of the topic posed challenges in formulating survey questions that accurately captured respondents' knowledge and practices regarding fraud prevention measures.

While respondents may have indicated unfamiliarity with specific terminologies, they may have been aware of and implementing practices that correspond to these terminologies in practice. This discrepancy in responses made it challenging to interpret the data in a manner that accurately reflects respondents' actual knowledge and practices. Furthermore, the literature review faced limitations in accessing diverse and rich sources of information. While fraud and social engineering are widely studied topics, the literature often presents similar content, making it challenging to find articles that offer unique and insightful perspectives. This limitation necessitated exploring sources outside of the immediate field of study to gather diverse insights and perspectives. Moreover, the study was constrained by the lack of innovative recommendations or practices beyond those commonly adopted or recommended by established and reputable organizations in the field. This limitation restricted the study's ability to propose novel approaches or solutions to combat social engineering in financial fraud.

Based on the limitations and challenges encountered in this study, several recommendations can be made for future research in the field of social engineering in financial fraud:

1- ***Further Investigation into Demographic Factors:*** Future research could explore the impact of demographic factors, such as age, profession, education level, and income level, on susceptibility to social engineering attacks in more depth. Understanding how these factors influence individuals' vulnerability to fraud can help tailor prevention strategies more effectively.

2- ***Diversity of Participants & Generalizability & Geographically Focused Studies:*** If an survey is going to measure the awareness or precautions of different demographic groups against social engineering, it is important that participants are selected from a wide range of backgrounds. This ensures that the study reaches a broader audience and its results are more generalizable. The more participants there are, the greater the generalizability of the study. If a study focuses on a specific geography (such as a study conducted with the participation of individuals from Istanbul or the Marmara Region), more clear and generalizable results can be obtained. Such studies can be valuable for understanding the specific dynamics of social engineering and fraud in a particular region. Considering these recommendations can help future research be more effective and results-oriented.

3- ***Development of Survey Instruments:*** Given the challenges faced in formulating survey questions that accurately capture respondents' knowledge and practices regarding fraud prevention measures, future research could focus on developing more inclusive and understandable survey instruments. This could involve using simpler language and providing clearer explanations of technical terms.

4- ***Exploration of Innovative Prevention Measures:*** Since the study found a lack of innovative recommendations or practices beyond those commonly adopted by established organizations, future research could focus on exploring and developing new and innovative prevention measures. This could involve incorporating insights from fields such as psychology and behavioral economics to develop more effective prevention strategies.

5- ***Enhanced Literature Review Strategies:*** To address the limitations in accessing diverse and rich sources of information, future research could employ enhanced literature review strategies. This could involve using more comprehensive search terms and exploring sources beyond traditional academic databases to gather a wider range of perspectives.

6- ***Longitudinal Studies:*** To address the challenge of generalizability and ensure the validity of findings over time, future research could consider conducting longitudinal studies. This would allow researchers to track changes in fraud patterns and the effectiveness of prevention measures over an extended period.

7- ***Case Studies and Real-World Examples:*** To complement survey-based research, future studies could incorporate case studies and real-world examples of social engineering attacks. This would provide a more nuanced understanding of how these attacks occur and how they can be prevented.

CONCLUSION

This study examined the relationship between social engineering tactics in financial fraud and demographic variables. Findings from literature review and survey analysis indicate that susceptibility to social engineering attacks does not significantly vary based on demographic factors such as age, gender, education level, and income. These results suggest that individuals across all age groups, genders, education levels, and income brackets may equally fall victim to social engineering attacks. However, slight variations based on demographic characteristics have been identified. For example, individuals with lower levels of education may be more vulnerable to certain social engineering tactics.

These findings are crucial for the prevention of financial fraud and combating social engineering attacks. Financial institutions and authorities should develop education and awareness programs targeting a broad audience rather than focusing solely on specific demographic groups. Additionally, special measures should be implemented for individuals with lower education levels or limited financial literacy, with increased efforts to protect this group.

In conclusion, this study emphasizes the need for effective measures against social engineering attacks, tailored to demographic differences. Future research should delve deeper into the association between social engineering tactics and demographic variables, as well as develop more comprehensive prevention strategies.

- ***Take Home Message***

  The most important finding of this study is that susceptibility to social engineering attacks does not vary based on demographic factors, highlighting that these attacks pose a potential threat to everyone. Therefore, financial institutions and individuals should develop and implement more effective measures against social engineering attacks. These measures should include controlling instinctive reflexes, adopting a more skeptical approach to events, and ensuring the security of devices. This study provides a significant contribution not only to academics and professionals but also to individuals in their daily lives, helping them build financial security.

REFERENCES AND NOTES

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90–113.

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 32(3), 183-196.

Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2011). Fraud Examination. Cengage Learning.

Anıl Keskin, D., & Gözenman, S. (2019). Hile Riski Açısından Sosyal Mühendislik. TİDE Academia Research.

Aun, Y., Gan, M.-L., Abdul Wahab, N. H. B., & Guan, G. H. (2022). Social Engineering Attack Classifications on Social Media Using Deep Learning. Tech Science Press. DOI: 10.32604/cmc.2023.032373

Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. 2017 International Conference on Computing Networking and Informatics (ICCNI), 1–9. doi:10.1109/ICCNI.2017.8096076

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: assessing vulnerabilities in practice. Information Management & Computer Security, 17(1), 53-63.

Bao, Y., Hilary, G., & Ke, B. (2022). Artificial intelligence and fraud detection. Innovative Technology at the Interface of Finance and Operations: Volume I, 223-247.

Choi, D., & Lee, K. (2017). Machine learning based approach to financial fraud detection process in mobile payment system. IT Convergence Practice (INPRA), 5(4), 12-24.

Cialdini, R. B. (2007). Influence: The psychology of persuasion. Harper Collins.

Connor, B. H. (2015). The Quid Pro Quo Quark: Unstable Elementary Particle of Honest Services Fraud. Cath. UL Rev., 65, 335.

Cross, C. (2013). Fraud and its PREY: Conceptualising social engineering tactics and its impact on financial literacy outcomes. Journal of Financial Services Marketing, 18(3). DOI:10.1057/fsm.2013.14

Cross, C. (2016). The problem of "white noise": Examining current prevention approaches to online fraud. Journal of Financial Crime, 23(4), 806-818. DOI:10.1108/JFC-12-2015-0069

Cross, C. (2022). Exploring Fear of Crime for Those Targeted by Romance Fraud. An International Journal of Evidence-based Research, Policy, and Practice. DOI:10.1080/15564886.2021.2018080

Cross, C. (2023). More than Money: Examining the Potential Exposure of Romance Fraud Victims to Identity Crime. Global Crime, 24(2), 1-15. https://doi.org/10.1080/17440572.2023.2185607

Del Pozo, I., Iturralde, M., & Restrepo, F. (2018, August 1). Social Engineering: Application of Psychology to Information Security. Paper presented at the 6th International Conference on

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, May). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590).

Dong, W., Liao, S., Xu, Y., & Feng, X. (2016). Leading Effect of Social Media for Financial Fraud Disclosure: A Text Mining Based Analytics. Americas Conference on Information Systems.

Dorminey, J. W., Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). Financial fraud. *The CPA Journal*, *82*(6), 61.

Emigh, A. (2007). Phishing and countermeasures (pp. 260-275). Hoboken, New Jersey: John Wiley & Sons, Inc.

Fan, W., Lwakatare, K., & Rong, R. (2017). Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. I. J. Computer Network and Information Security, 1(1), 1-11. DOI: 10.5815/ijcnis.2017.01.01

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. International Journal of Human-Computer Studies.

Future Internet of Things and Cloud Workshops (FiCloudW). DOI: 10.1109/W-FiCloud.2018.00023

Galletta, P. Z. (2015). A basic field guide to fraud. The CPA Journal, 549(March), 54–60.

Galushko, D. V. (2021). International cooperation in the fight against financial crimes in the context of the process of Europeanisation. Institucije i prevencija finansijskog kriminaliteta Institutions and prevention of financial crime, 11.

Ghosh, S., & Reilly, D. L. (1994). Credit card fraud detection with a neural network. In System Sciences (Vol. 3, pp. 621–630).

Gilbert, M., & Wakefield, A. (2018). Tackling fraud effectively in central government departments: A review of the legal powers, skills and regulatory environment of UK central government counter fraud teams. Journal of financial crime, 25(2), 384-399.

Gold, S. (2014). The evolution of payment card fraud. Computer Fraud & Security, 2014(3), 12-17.

Gulati, R. (2003). The threat of social engineering and your defense against it. SANS Reading

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. Presented at the 2016 International Conference on Computing, Communication and Automation (ICCCA). DOI: 10.1109/CCAA.2016.7813778.

Gupta, A. (2018). The evolution of fraud: Ethical implications in the age of large-scale data breaches and widespread artificial intelligence solutions deployment. Inter. Telecommunication Union Journal, 1(7), 1-7.

Guven Ö., & Aras, S. (2022). Fraud detectıon by machıne learnıng algorıthms: a case from a mobıle payment system. International Journal of Management, Economics and Business, 18(3), 895-911. https://doi.org/10.17130/ijmeb.979302

Hadnagy, C. (2011). Social engineering: The art of human hacking. John Wiley & Sons.

Hamal, S., & Senvar, O. (2021). Comparing performances and effectiveness of machine learning classifiers in detecting financial accounting fraud for Turkish SMEs. International Journal of Computational Intelligence Systems, 14(1), 769-782.

Hedayati, A. (2012). An analysis of identity theft: Motives, related frauds, techniques and prevention. Journal of Law and Conflict Resolution, 4(1), 1-12. doi:10.5897/JLCR11.044

Hogan, C. E., Rezaee, Z., Riley, R. A., Velury, U. K. (2008). Financial statement fraud: Insights from the academic literature. Auditing: A Journal of Practice & Theory, no. 27 (2), pp. 231–252. http://doi.org/10.2308/aud.2008.27.2.231

Huang, W., & Brockman, A. (2011). Social engineering exploitations in online communications: Examining persuasions used in fraudulent e-mails. In T. Holt (Ed.)

Hunt, J. (2004). Trust and bribery: The role of the quid pro quo and the link with crime. DOI 10.3386/w10510

James, L. (2005). Phishing exposed. Rockland, MD: Syngress Publishing.

Josyula, H. P. (2023). Fraud Detection in Fintech Leveraging Machine Learning and Behavioral Analytics.

Katz, N. A. (2016). Detecting and reducing supply chain fraud. Routledge.

Karpoff, J. M. (2021). The future of financial fraud. Journal of Corporate Finance, 66, 101694.Kim, M., & Lee, H. (2018). A survey on social engineering attacks and countermeasures in cyber space. Multimedia Tools and Applications, 77(7), 8721-8743. https://www.researchgate.net/publication/332151597_Social_Engineering_Attacks_A_Survey

Kay, R. (2004). Phishing. Computerworld, 38, 44.

Koivisto, N. (2019). Preventing fraud through internal control.

Koyun, A., & Al Janabi, E. (2017). Social Engineering Attacks. Journal of Multidisciplinary Engineering Science and Technology (JMEST), 4(6), ISSN: 2458-9403.

Kranacher, M. J., Riley, R., & Wells, J. T. (2010). Forensic accounting and fraud examination. John Wiley & Sons.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

Kumar, S. S. (2012). Analysis on Man in the Middle Attack on SSL. International Journal of Computer Applications, 45, ISSN 0975-8887. APA stilinde referans olarak kullanabilirsiniz.

Larcom, G., & Elbirt, A. J. (2006). Gone phishing. IEEE Technology and Society Magazine, 25, 52-55. DOI:10.1109/MTAS.2006.1700023

Levi, M., Burrows, J., Fleming, M., Hopkins, M., & Matthews, K. G. P. (2007). The nature, extent and economic impact of fraud in the UK.

Levi, M., & Reuter, P. (2016). Money Laundering. Presented at the 2016 International Conference on Computing, Communication and Automation (ICCCA). DOI: 10.1109/CCAA.2016.7813778.

Long, J. (2011). No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress.

Mallika, A., Ahsanb, A., Shahadata, M. M. Z., & Tsou, J.-C. (2018). Man-in-the-Middle-Attack: Understanding in Simple Words. Center for Research and Community Service (LP2M). DOI: http://dx.doi.org/10.22373/cj.v2i2.3453

Mann, I. (2018). Hacking the human: social engineering techniques and security countermeasures. Routledge.

Manske, K. (2000). An introduction to social engineering. Information Security. J. A Global Perspect., 9(5), 1-7.

McLaughlin, E., & Hughes, G. (2001). Teetering on the edge: the futures of crime control and community safety.

Mitnick, K., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. John Wiley & Sons.

Molia, H. K., & Gohel, H. A. (2015). Protection of Computer Networks from the Social Engineering Attacks. International Journal on Advances in Engineering, Technology and Science, 1(1).

Momoh, I., Adelaja, G., & Ejiwumi, G. (2023). Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institutions. Retrieved from https://www.researchgate.net/profile/Gabriel-Adelaja/publication/376351135_Analysis_of_the_Human-Factor-in-Cybersecurity-Identifying-and-Preventing-Social-Engineering-Attacks-in-Financial Institution/links/6573436fea5f7f0205534493/Analysis-of-the-Human-Factor-in-Cybersecurity-Identifying-and-Preventing-Social-Engineering-Attacks-in-Financial-Institution.pdf

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014, August). Social engineering attack framework. In 2014 Information Security for South Africa (pp. 1-9). IEEE.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. Information Security Journal, 15(5)

Peltier-Rivest, D. (2018). The battle against fraud: do reporting mechanisms work?. Journal of Financial Crime, 25(3), 784-794.

Power, R., & Forte, D. (2006). Social engineering: attacks have evolved, but countermeasures have not. Computer Fraud & Security, 2006(10), 17-20.

Ramamoorti, B. S., & Olsen, W. (2007). Fraud: The Human Factor. Financial Executive, 23(6), 53–55.

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five {two-factor} authentication methods. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 357-370).

Reurink, A. (2019). Financial fraud: A literature review. Contemporary Topics in Finance: A Collection of Literature Surveys, 79-115.

Sabelli, M. (2022). Security Serious Game (Doctoral dissertation, Politecnico di Torino).

Sample, C., Hutchinson, S., Karamanian, A., & Maple, C. (2017, June). Cultural observations on social engineering victims. In 16th European Conference on cyber-security and Warfare,(Dublin: University College Dublin) (pp. 391-401).

Silverstone, H., & Sheetz, M. (2007). Forensic Accounting and Fraud Investigation for NonExperts (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Singh, S., & Srivastava, R. K. (2020). Understanding the intention to use mobile banking by existing online banking customers: an empirical study. Journal of Financial Services Marketing, 25(3-4), 86-96. https://doi.org/10.1057/s41264-020-00074-w

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. Communications of the ACM, 54(3), 70-75.

Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., ... & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in Fintech applications. Sensors, 21(5), 1594. https://doi.org/10.3390/s21051594

Thompson, P., & Findlay, P. (1999). Changing the people: social engineering in the contemporary workplace. Culture and economy after the cultural turn, 162-188.

Upendar, J., & Rao, E. G. (2013). An overview of plastic card frauds and solutions for avoiding fraudster transactions. International Journal of Research in Engineering and Technology, 2(11), 291-296.

Vassiljev, M., & Alver, L. (2016). Conception and Periodisation of Fraud Models: Theoretical Review. In Business, Law. DOI:10.2991/ICAAT-16.2016.47

Wall, D. S. (2011). Micro-frauds: virtual robberies, stings and scams in the information age. In Corporate hacking and technology-driven crime: Social dynamics and implications (pp. 68-86). IGI Global.

Wang, T., Chen, J., & Huang, C. (2019). The Effect of Social Engineering on Financial Fraud: An Empirical Analysis. Journal of Financial Crime, 26(1), 171-183. https://doi.org/10.1108/JFC-05-2018-0051

Wells, J. T. (2014). Principles of fraud examination. John Wiley & Sons.

Workman, M. (2007). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology. https://doi.org/10.1002/asi.20779

Zareapoor, M., Seeja, K. R., & Alam, M. A. (2012). Analysis on credit card fraud detection techniques: Based on certain design criteria. International Journal of Computer Applications, 52(3), 35-42.