International Journal of Circuit, Computing and Networking

E-ISSN: 2707-5931
P-ISSN: 2707-5923
Impact Factor (RJIF): 5.64
Journal's Website
IJCCN 2025; 6(2): 01-06
Received: 10-04-2025
Accepted: 15-05-2025

Maicon Pinheiro Santana
Student, Federal Institute of Education, Science and Technology of São Paulo (IFSP), Bragança Paulista, São Paulo, Brazil

Flavio Cezar Amate
Professor, Federal Institute of Education, Science and Technology of São Paulo (IFSP), Bragança Paulista, São Paulo, Brazil

Clayton Eduardo dos Santos
Professor, Federal Institute of Education, Science and Technology of São Paulo (IFSP), Bragança Paulista, São Paulo, Brazil

Corresponding Author:
Clayton Eduardo dos Santos
Professor, Federal Institute of Education, Science and Technology of São Paulo (IFSP), Bragança Paulista, São Paulo, Brazil

Preventing social engineering attacks: A case study of a financial scam in Brazil

Maicon Pinheiro Santana, Flavio Cezar Amate and Clayton Eduardo dos Santos

DOI: https://www.doi.org/10.33545/27075923.2025.v6.i2a.93

Abstract
This study presents an investigation into preventive practices against social engineering attacks, with a focus on raising awareness and training users to mitigate cybersecurity risks. The research was conducted through a case study applied to an organization through an ex post facto analysis to examine past incidents and identify vulnerabilities exploited by attackers. Published records, together with documentary interviews and observations, were analyzed to provide insights into the context and circumstances that facilitated fraud attempts. Based on the findings, guidelines and best practices tailored to the institution's reality were established, drawing on specialized literature and the evidence obtained in the analysis. The study demonstrated that the systematic application of educational initiatives, clear security protocols, and the continuous updating of internal policies has the potential to reduce the attack surface and enhance the resilience of both users and organizations against social engineering threats.

Keywords: Social engineering, information security, fraud prevention, ex post facto, financial scams, cybersecurity awareness

1. Introduction
Social engineering is an attack vector that exploits human vulnerabilities to gain unauthorized access to information, systems, or resources, relying on techniques of persuasion, psychological manipulation, and the exploitation of trust. As highlighted in recent studies, it is one of the most effective and persistent threats in the field of information security, since it targets the most susceptible link in the protection chain: the user [1, 2].

In the current digital era, in which information has become a highly valuable strategic asset, social engineering incidents can compromise sensitive data and generate operational, financial, and reputational impacts. Research by Jang-Jaccard and Nepal [3] and Heartfield *et al.* [4] shows that, even in the face of technological advances in security, the effectiveness of these attacks stems from their ability to bypass technical barriers by exploiting the behavioral and cognitive aspects of victims.

A variety of methods are employed to carry out such actions, ranging from traditional approaches (such as phishing, pretexting, and baiting) to more sophisticated techniques that incorporate artificial intelligence resources to personalize messages and increase their credibility[2,4]. The collection of preliminary information about the victim or target organization, often from public sources or reverse engineering of exposed data, is a critical step in constructing convincing narratives [5].

Trust-building, a central element in social engineering, reduces the victim's perception of risk, thereby increasing the likelihood of a successful attack. This process can be further reinforced through techniques such as social profiling, behavioral pattern analysis, and the use of data obtained from social networks or other digital environments. In this context, understanding the strategies employed by malicious actors and the recommended practices to mitigate them is essential for the development of effective prevention policies and mechanisms.

2. Theoretical Framework
Social engineering is widely recognized as one of the most effective and persistent threats in the field of information security, exploiting human vulnerabilities through psychological manipulation and persuasion strategies [4]. Unlike purely technical attacks, these offensives

exploit behavioral principles, often grounded in cognitive biases and heuristics, to induce individuals to compromise organizational data, systems, or assets [6].

Evolution and Types of Attacks

Historically, social engineering attacks have ranged from in-person scams — such as the famous case of the "sale" of the Eiffel Tower in 1925 — to sophisticated digital campaigns involving phishing, spear phishing, and vishing [2]. In recent years, the popularization of social media and the abundance of online data have intensified the personalization capacity of these attacks, enabling adversaries to craft more convincing and targeted narratives [7].

The literature indicates that the evolution of these techniques is marked by the convergence between traditional methods and emerging technologies, such as deepfakes, generative artificial intelligence, and automated data harvesting [8]. This combination increases the potential impact, as it expands the scale and sophistication of the approaches, reduces attackers' costs, and makes detection more challenging [1].

Psychological Factors and Cognitive Biases

The effectiveness of social engineering is deeply rooted in psychological aspects. According to Coatesworth [6], principles described by Cialdini — such as reciprocity, commitment/consistency, social proof, authority, liking, scarcity, and unity — are systematically exploited to induce rapid and uncritical decisions. Biases such as anchoring, confirmation bias, and availability directly influence victims' responses, making them more likely to accept false information when it confirms pre-existing expectations [6].

These human factors make the exclusive adoption of technological barriers insufficient. Even in organizations with robust security policies, the absence of continuous awareness and training programs increases the risk of incidents [4].

Emerging Techniques and Artificial Intelligence

Recent studies highlight the growing role of artificial intelligence in enhancing social engineering attacks [8]. Generative AI tools allow the creation of highly personalized messages that mimic the linguistic and emotional patterns of real individuals, thereby increasing the success rate of phishing and other fraudulent schemes [1]. In addition, malicious chatbots and machine learning algorithms have been employed to automate the reconnaissance phase, reducing the time required to identify human vulnerabilities [8].

Prevention and Best Practices

Mitigating this type of threat requires a holistic approach that integrates technical measures, organizational policies, and behavioral interventions [2]. Models such as Zero Trust - which eliminate implicit trust and continuously validate digital interactions — have been increasingly recommended [6]. Furthermore, Security Orchestration, Automation, and Response (SOAR) platforms have been adopted to coordinate incident response, reducing reaction time and increasing the effectiveness of countermeasures [6, 7].

Systematic literature reviews highlight that successful prevention strategies include gamified training, regular attack simulations, segmentation of sensitive information, and behavioral anomaly monitoring [2, 4, 9]. The integration of awareness and technology, therefore, constitutes the foundation of an adaptive defense against social engineering.

3. Methodology

This study adopts the ex post facto approach, characterized as a type of observational research applied after the occurrence of the investigated events. In this design, the researcher does not exercise control or manipulation over the independent variables, being limited to the analysis of effects resulting from pre-existing conditions or previously established facts.

The data analyzed were obtained from a documentary interview extracted from the episode "Débito ou Crédito?" [Credit or Debit?] of the series Realidade Violada [Violated Reality], produced by NZN and broadcast on the TechMundo portal. The choice of this methodological design aimed to identify and understand possible cause-and-effect relationships between a previously observed fact and subsequent phenomena.

The main characteristic of this approach lies in the fact that data collection occurs only after the events have taken place, which makes it appropriate in situations where it is neither feasible nor ethically acceptable to conduct controlled experiments. As pointed out by [10], ex post facto research is particularly useful when manipulation of the variables required for the investigation is impracticable, while still allowing for the analysis of interrelationships between presumed causes and their observable effects.

3.1 Currency Conversion Note

To ensure clarity for international readers, all monetary values originally presented in Brazilian Reais (BRL, symbol: R$) were converted to U.S. Dollars (USD) using the average official exchange rate for the year 2020, which was approximately 1 USD = 5.18 BRL, as reported by the Central Bank of Brazil. Whenever possible, both currencies are displayed to maintain precision and facilitate interpretation of the financial figures throughout the manuscript.

3.2 Case Study

Among the numerous strategies exploited by criminals, one that stands out is the scheme known as Carder fraud, which is strongly associated with social engineering practices. In this modality, the victim is induced to voluntarily hand over their credit or debit card to the fraudster, granting illicit access to financial resources and sensitive information.

The term Carder designates an individual engaged in illicit schemes involving credit or debit card fraud. Common techniques employed by these criminals include phishing, the deployment of malware, and the use of skimming devices: all aimed at capturing sensitive data such as card numbers, expiration dates, and security codes (CVV). These data can then be exploited to conduct fraudulent purchases, clone cards, or be traded in illegal markets.

The episode analyzed in this study was extracted from the documentary *Realidade Violada*: EP #01 - "Débito ou Crédito?", released on the TechMundo portal on May 23, 2020 [11]. The case involves Marieta Pereira, a housewife who fell victim to a "fake call center" scam. The fraud began with a phone call from an individual posing as a representative of "Bank C" (name omitted for ethical reasons). During the conversation, the scammer alleged that

purchases amounting to R$1,000 (≈ USD 190) had been made, in addition to a recent attempt at a cash withdrawal. Marieta denied the transactions, emphasizing that she had not left her home for two weeks due to health issues.

According to Fidel Beraldi, Risk Director at Wirecard Brazil, one of the methods reportedly used by fraudsters to obtain card CVVs involves bots that execute automated attempts across multiple websites to verify code validity - a technique cited in the context of highlighting vulnerabilities that financial institutions must address. Through this brute-force technique, low-value transactions - usually between R$ 50 and R$ 100 (≈ USD 9.65 to 19.30, respectively) - are carried out to avoid detection. If the transaction is authorized, fraudsters confirm that the card is active and then proceed with higher-value schemes.

As the interaction progressed, the scammer validated some of the victim's personal information, reinforcing the credibility of the narrative. He then provided a phone number and instructed Marieta to contact a supposed representative of "Bank C", consolidating the fraudulent script and maintaining control over the situation. Fig. 1 illustrates the attacker leaving on a motorcycle after successfully deceiving the victim. This type of vehicle is commonly used for fast, small-scale deliveries, which may have added further plausibility to the scam scenario.

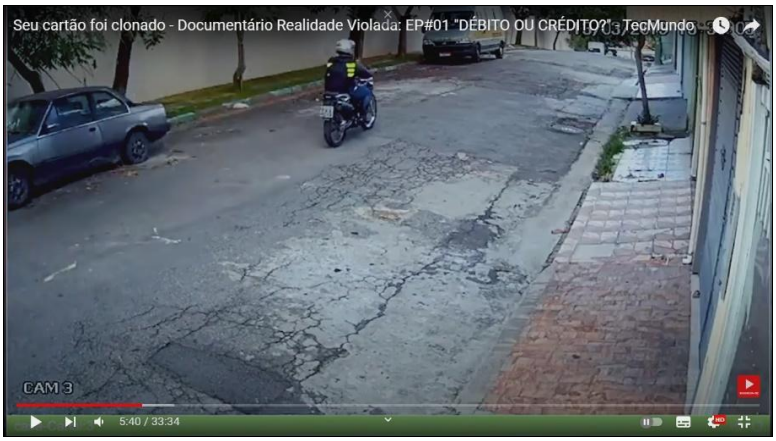

Fig 1: Security camera footage showing the arrival of the fake delivery rider to collect the victim's bank card, as part of a *Carder*-type social engineering scam (*Realidade Violada: Debit or Credit?*, Adapted from [11]

The supposed representative, continuing the conversation, reiterated the claims regarding the unauthorized purchases and the attempted withdrawal, stating that a motorcyclist would be dispatched to collect the credit card for a so-called "security verification." As part of the procedure, Marieta was instructed to handwrite a letter including her address and to place the card inside a sealed envelope. She was also told to remain on the phone line until the courier arrived.

When the motorcyclist arrived, he introduced himself and provided a prearranged password that had been established during the call, a detail that further reinforced the credibility of the scheme. Convinced that this was a legitimate procedure, Marieta handed over the envelope, after which the individual departed with the card.

Frauds of this nature, such as the one perpetrated against Marieta, are more common than generally assumed. Criminals rely on social engineering techniques to exploit vulnerabilities in society, impersonating financial institutions and instilling fear and uncertainty. These tactics particularly affect older individuals who are less socially integrated into technological environments. By gaining their trust, attackers manipulate victims into disclosing sensitive data, thereby bypassing authentication processes and achieving their objectives: the theft and control of information for personal gain.

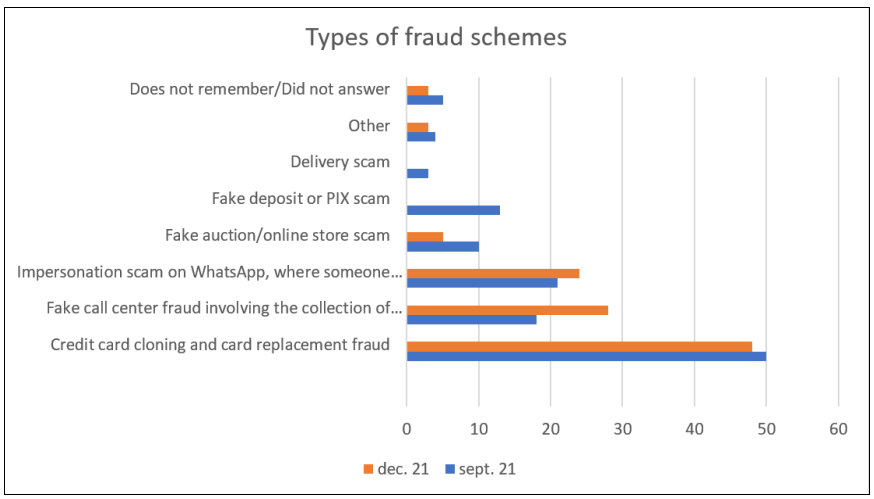

Fig 2: Comparative percentages of different types of scams and attempted scams reported by victims in September and December 2021, according to the Radar Febraban survey. Adapted from [12].

A survey conducted by RADAR Febraban, released by the Brazilian Federation of Banks and published on the Tudo Celular portal on December 29, 2021 [12], revealed a significant increase in scams involving fraudulent customer service centers. In the last quarter analyzed, this type of fraud recorded a rise of 10 percentage points, as illustrated in Fig. 2.

The data indicate that, although card cloning remains the most frequent occurrence, its incidence showed a slight decline, decreasing from 50% to 48%. Conversely, cases in which fraudsters impersonate known contacts on WhatsApp to request money transfers increased from 21% in September to 24% in December. Among individuals aged 18 to 24, scams involving fake online auction stores were also reported, accounting for 5% of cases.

The most significant increase, however, was observed in scams involving fraudulent call centers, where criminals request personal information by telephone. The prevalence of this type of fraud rose from 18% in September to 28% in December, being most common among individuals aged 45 to 59, who accounted for 39% of the incidents.

According to complementary data published by[12] during the same period, the statistics confirm an overall increase in crimes committed through social engineering compared to the previous year, as shown in Table 1. This modality is widely used by criminals because it exploits victims' careless behavior, inducing them to take risky actions such as clicking on malicious links, making unverified transactions, or disclosing sensitive information (including passwords and credit card details).

Table 1: Distribution of scam and attempted scam types by gender, age group, education level, and household income, based on the *Radar Febraban* survey [12].

Security issue	Total	Sex		Age (years)				Education level			Household income (MW)		
		M	F	18-24	25-44	45--59	More than 60	Elementary School	High School	Higher Education	Up to 2	2-5	More than 5
Credit card cloning and card replacement fraud	48	47	49	41	63	45	43	47	45	54	50	48	44
Fake call center fraud involving the collection of personal data via phone call	28	24	31	21	23	39	28	29	30	24	29	29	26
Impersonation scam on WhatsApp, where someone poses as a known contact to request money	24	29	21	33	24	22	23	21	27	27	18	29	32
Fake auction/online store scam	5	8	2	14	6	1	2	3	7	5	5	5	3
Others	3	4	2	1	2	1	6	3	2	5	3	2	6
Does not remember/Did not answer	3	1	4	3	2	2	4	3	3	2	2	5	2

Although it was already a known practice, the "fraudulent call center" scam experienced strong growth in the first half of 2021. According to a study by the Brazilian Federation of Banks (Febraban), the incidence of this type of fraud increased by 165% compared to the previous semester. Some specific modalities showed even more significant increases, such as the fake delivery rider scam, which rose by 271%. There was also a 62% increase in cases involving fake attendants and fraudulent telephone service centers.

Another method that gained prominence during the period was phishing, an electronic fraud that uses fraudulent emails, websites, or applications (often replicas of legitimate platforms) to capture victims' personal and financial data. According to the most recent surveys, this practice grew by 26% in the first six months of the year.

The WhatsApp scam also remained highly prevalent: in this scheme, criminals impersonate a known contact to request money transfers. The occurrence of this fraud increased by 24% during the period, representing three percentage points above the figure recorded in September. It was observed that the highest incidence occurred among individuals with an income above five minimum wages, accounting for 32% of reported cases.

With regard to Marieta's case, a victim of a Carder-type scam, she filed a lawsuit against Bank C, alleging negligence in fraud prevention, particularly for failing to block a high-value withdrawal. According to the NZN report, the court ruling was favorable to the victim, but the compensation was only partial: of the R$ 13,800.00 (≈ USD 2,660.00) stolen, approximately R$ 10,000.00 (≈ USD 1,930.00) were reimbursed, in addition to moral damages of just over R$ 4,000.00 (≈ USD 770.00). Nevertheless, Marieta still reported a loss exceeding R$ 4,000.00 (≈ USD 770.00).

4. Best Practices for Prevention

Prevention against social engineering attacks requires a combination of technical measures, organizational procedures, and security habits adopted by individuals. Several international bodies, such as ISO/IEC 27001 [13] on information security management, and NIST SP 800-53 [14] on security controls, as well as national initiatives in Brazil

such as CERT.br [15] and its Internet Security Handbook, emphasize that continuous awareness is the most effective tool to reduce human vulnerabilities.

Based on the case study analyzed, the Febraban statistics [12], and best practices described by security organizations, Table 2 presents preventive measures directly related to the main attack vectors identified.

Table 2: Preventive Measures Against Social Engineering Attack Vectors

Preventive Measure	Mitigated Attack Vector	Case Study Example
Never hand over cards or passwords to third parties	Carder, Fake delivery rider, Physical card cloning	Marieta handed the physical card to the scammer posing as an authorized delivery rider
Avoid making consecutive calls to the same number provided by the alleged attendant	Fake call center, Vishing	The victim was induced to call a fraudulent number, reinforcing the criminal narrative
Do not share personal data (phone number, address, CPF) with strangers	Pretexting, Vishing, Smishing	The scammer obtained confirmation of personal data during the call
Use distinct and complex passwords for each service	Credential stuffing, Unauthorized access to multiple accounts	Protects against cascading effects in case of credential leaks
Enable two-factor authentication (2FA)	Phishing, Unauthorized remote access	Adds a protection layer even if the password is stolen
Be skeptical of promotions, offers, or contacts outside official channels	Baiting, Phishing, Smishing	Prevents victims from being lured by false benefits or fabricated urgency
Keep antivirus software updated and operating systems patched	Malware, Trojan Horse	Prevents infection by malicious files received via email, USB drives, or links
Regularly monitor bank accounts and credit score	Misuse of financial data	Allows early detection of unauthorized transactions
Use temporary virtual cards for online purchases	E-commerce fraud	Limits card data exposure to a single transaction
Verify identity through official channels before providing any information	Vishing, Pretexting, Phishing	Could have prevented the disclosure of personal data and the physical card in the analyzed case
Conduct periodic training and simulations (organizations)	All attack vectors	Companies can test employee resilience against simulated attacks
Establish formal incident response policies	Post-attack	Ensures quick action to minimize losses and recover systems or credentials

The application of these practices, both by individuals and organizations, significantly reduces the attack surface exploitable by social engineers. It is essential that awareness efforts are not limited to isolated campaigns but rather become a continuous part of the security culture. Furthermore, it is recommended that training programs be tailored to the profile of the target audience, particularly for more vulnerable groups such as the elderly or individuals with limited familiarity with technology.

5. Conclusions

The analysis confirmed that social engineering remains one of the most effective threats to information security, exploiting the human factor through psychological manipulation, inducement to error, and the exploitation of gaps in organizational procedures. Based on the ex post facto approach and the real case study “Debit or Credit?” from the series Realidade Violada, it was possible to map the stages of the scam, identify vulnerabilities, and correlate them with statistical data from Febraban as well as internationally recognized guidelines such as ISO/IEC 27001, NIST SP 800-53, and CERT.br recommendations.

The consolidation of this evidence resulted in a set of best practices presented in Chapter 4, encompassing awareness measures, the use of multi-factor authentication, the creation of strong passwords, regular system updates, the definition of formal security policies, and the periodic execution of incident simulations. When systematically applied, these actions have the potential to significantly reduce the attack surface and enhance the resilience of users and organizations against increasingly sophisticated scams.

Thus, this study contributes both to the academic understanding of the impact of social engineering and to the provision of practical, applicable recommendations, reinforcing that protection against such threats requires the integration of technological, procedural, and behavioral aspects.

References

1. Coatesworth B. The psychology of social engineering. Cyber Secur A Peer-Rev J. 2023;6(3):261-274.
2. Nonum EO, Avwokuruaye O, Umar AM. Social engineering: Understanding human factors in cyber security. Int J Converg Informat Sci Res. 2025.
3. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. J Comput Syst Sci. 2014;80(5):973-93.
4. Schmitt M, Flechais I. Digital deception: Generative artificial intelligence in social engineering and phishing. Artif Intell Rev. 2024;57(12):324.
5. Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol. 2014;33(3):237-248.
6. Waelchli S, Walter Y. Reducing the risk of social engineering attacks using SOAR measures in a real world environment: A case study. Comput Secur. 2025;148:104137.
7. Syafitri W, Kusumawardhany G, Pratama G, Saputra R, Kim KH, Lee HJ. Social engineering attacks prevention: A systematic literature review. IEEE

Access. 2022;10:39325-39343.
8. Akeiber HJ. The evolution of social engineering attacks: A cybersecurity engineering perspective. Al-Rafidain J Eng Sci. 2025:294-316.
9. Heartfield R, Loukas G, Budka M, Bezemskij A, Panaousis E, Roeschlin M. Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning. IEEE Trans Inf Forensics Secur. 2020;16:1720-1735.
10. Rohwer D. Designing ex post facto and experimental studies. In: Inquiry in music education. New York: Routledge; 2022. p. 230-52.
11. TecMundo. Veja como funciona um ataque de engenharia social [See how a social engineering attack works] [Internet]. 2020 [cited 2025 Aug 27]. Available from: https://www.tecmundo.com.br
12. FEBRABAN. Pesquisa FEBRABAN de tecnologia bancária 2021 [FEBRABAN Banking Technology Survey 2021]. São Paulo: Federação Brasileira de Bancos; 2021.
13. International Organization for Standardization. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO; 2022.
14. National Institute of Standards and Technology (NIST). Security and privacy controls for information systems and organizations. NIST Special Publication 800-53, Revision 5 [Internet]. 2020 [cited 2025 Aug 27]. Available from: https://doi.org/10.6028/NIST.SP.800-53r5
15. CERT.br. Cartilha de segurança para internet [Internet Security Handbook] [Internet]. São Paulo: Comitê Gestor da Internet no Brasil; 2022 [cited 2025 Aug 27]. Available from: https://cartilha.cert.br