Analysis of Consumer Financial Fraud and Prevention Strategies

CIS 3319: Wireless Networks and Security / CIS 4378: Computer and Network Security
Lab 1: Consumer Financial Fraud Investigation

Group Members:
Aaron Jefferson

01-Feb-2024

Abstract

This report provides an analysis of consumer financial fraud, including key findings and conclusions drawn from studying various cases and prevention strategies. The cases were selected from the Darknet Diaries podcast.

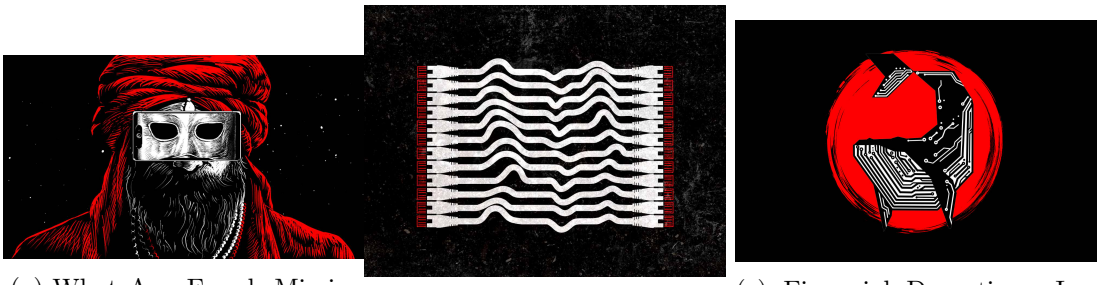
Contents

1 Introduction

The landscape of Consumer Financial Fraud is constantly evolving and becoming more sophisticated. This report aims to provide a focused, high-level analysis, showing the intricacies of how these instances of fraud are orchestrated and the methods used in their execution. To address these threats this report employs two cybersecurity frameworks: CIA (Confidendtiality, Integrity, Availibility) and STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). The CIA triad is a staple in cybersecurity offering an approach to understanding the protective measures essential in safeguarding information. STRIDE on the other hand, provides a lens to dissect and understand the nature of attacks a system might face. By analyzing three cases through these lenses, I hope to show how these occur and the vulnerabilitiesthey exploit, as well as offer some potential strategies for mitigation.

2 Exploration of Consumer Financial Fraud

2.1 Examples and Analysis



(a) WhatsApp Fraud: Mimics

(b) Stock Market Manipulation: Newswires

(c) Financial Deception: Impersonation and fake invoices

Figure 1: Visual Representations of Financial Fraud Cases

Case Study	**Brief Description**	**STRIDE Analysis**	**CIA Analysis**
WhatsApp Fraud	Social engineering through WhatsApp communications.	Spoofing: Impersonation Repudiation: Potential denial Information Disclosure: Personal data exposure Elevation of Privilege: Identity assumption	Confidentiality: Social engineering breach Integrity: False information Availability: Urgency manipulation
Stock Market Manipulation	Hackers infiltrated newswire services for insider trading.	Spoofing: Company impersonation Tampering: Invoice alteration Repudiation: Denial of actions Information Disclosure: Financial data access Elevation of Privilege: Insider information access	Confidentiality: Data breach Integrity: Fake invoice creation Availability: Financial process manipulation
Financial Deception	Fake invoices lead to unauthorized transfers.	Spoofing: System infiltration Tampering: Information alteration Repudiation: Denial of hacking Information Disclosure: Financial data release Elevation of Privilege: Unauthorized access	Confidentiality: Press release breach Integrity: Misused financial data Availability: Insider trading misuse

Discuss each example in detail, focusing on how the fraud was perpetrated.

Impersonation, Communications Fraud and Phishing In the Jalandhar region, a new fraud has emerged where victims receive WhatsApp communications from individuals posing as distant relatives in urgent need of financial aid. The scammers meticulously craft scenarios involving the relative facing legal trouble abroad, compelling the victim to act swiftly. In one case, a woman received a call from a person claiming to be her nephew in Canada, who supposedly had been arrested after an altercation and needed funds for legal fees. Despite initial doubts, she was persuaded by the urgency of the situation and the familiar details provided, leading to a significant financial loss.

Over the span of one week, multiple residents have reported cumulative losses exceeding Rs 5 lakh. Even with reports filed with the Punjab Cyber Cell, recovery of the funds remains uncertain.

Cybersecurity experts suggest that these scams might be the result of a data breach, as scammers appear to have detailed information about the targets. Over a hundred individuals have reported receiving similar calls, pointing to a large-scale operation involving domestic and international perpetrators.

Newswires Evaldas Rimasauskas crafted a scheme that exploited the trust and financial flows between large corporations and their suppliers. By establishing a company with the same name as a legitimate supplier and meticulously creating counterfeit invoices, he tricked companies into rerouting payments to bank accounts under his control. His deep understanding of corporate financial processes and the use of social engineering allowed him to bypass existing security measures and accumulate vast sums before detection.

Over two years, Rimasauskas siphoned 23 million from Google and 98 million from Facebook, demonstrating the profound impact that well-planned financial deception can have on even the most technologically advanced firms. While the majority of the stolen funds were eventually recovered, the case highlights the necessity for robust financial controls and the continuous reassessment of security protocols to prevent similar BEC scams.

For further information and to explore the episode, you can visit the Darknet Diaries website.

Financial Deception In the "Newswires" case, Arkadiy Dubovoy, a stockbroker, together with a group of traders and hackers, orchestrated a scheme to hack into the systems of major newswire agencies, extracting unpublished press releases containing critical financial data. These documents, containing earnings reports and other market-impacting information, were used to conduct informed trades before the data became public, yielding substantial profits. The operation was sophisticated, utilizing offshore accounts and anonymizing techniques to mask the illicit activities. However, the scheme eventually came undone when U.S. authorities detected the unusual trading patterns, leading to arrests and legal proceedings.

2.2 Common Vulnerabilities and Attack Vectors

In the cases examined, common vulnerabilities include exploitation of trust, social engineering, and security gaps within digital communication platforms and financial transaction systems. The attack vectors range from impersonation and phishing to complex intrusions into secure databases.

3 Prevention Advice Analysis

3.1 Examples of Advice

Source	Advice
https://darknetdiaries.com/episode/141/	1. Educate about phishing scams and social engineering tactics.
https://darknetdiaries.com/episode/124/	2. Implement robust verification processes for financial transactio
https://darknetdiaries.com/episode/123/	3. Adopt multi-factor authentication and strong cybersecurity me

Discuss each piece of advice, ensuring clarity for a general audience.

Phishing

verification for financial transactions

multi-factor authentication

3.2 Summary of Common Advice

Common advice includes continuous awareness training for potential scams, enhanced verification procedures for transactions, and improved cybersecurity infrastructure to prevent unauthorized access.

4 Effectiveness of Prevention Strategies

4.1 Analysis of Advice Against Vulnerabilities

Assess how each piece of advice addresses the vulnerabilities and attack vectors.

4.2 Limitations and Unaddressed Threats

Identify any advice that does not target vulnerabilities or attack vectors, and highlight any attacks not defended by the advice.

4.3 Tailoring Advice for Specific Populations

Discuss how advice might need modification for older adults, non-native English speakers, visually impaired users, etc.

5 Conclusion

Summarize the key findings, the effectiveness of current advice, and any recommendations for improvement.

6 References

List all sources used in your report.

- Darknet Diaries Podcast Episodes.
- Relevant case law and SEC filings.
- Cybersecurity best practices from authoritative sources.