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.

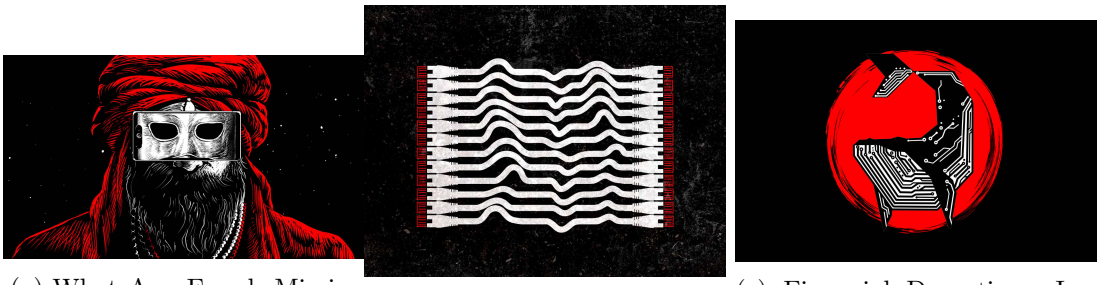
Contents

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

2.2 Detailed Case Analyses and Security Framework Application

Impersonation, Communications Fraud, and Phishing in the Jalandhar Region

Case Description: Victims in the Jalandhar region received WhatsApp messages from individuals posing as distant relatives in urgent need of financial aid. The scammers crafted scenarios where the relative was in legal trouble abroad, compelling the victim to send money.

CIA Analysis:

- *Confidentiality:* Personal conversations and trust were manipulated, leading to the sharing of sensitive information.
- *Integrity:* The integrity of information was compromised as scammers provided false narratives and impersonated family members.
- *Availability:* Scammers used the availability of instant communication to create a sense of urgency, prompting victims to act swiftly and without proper verification.

STRIDE Analysis:

- *Spoofing:* Impersonation of a family member.
- *Repudiation:* Scammers could easily deny involvement due to the anonymity of digital communication.
- *Information Disclosure:* Personal information of the victims was at risk.

Newswires: Evaldas Rimasauskas Scheme

Case Description: Evaldas Rimasauskas created a fraudulent company with a name similar to a legitimate supplier. He sent counterfeit invoices to major corporations, redirecting payments to his controlled bank accounts.

CIA Analysis:

- *Confidentiality:* Corporate financial processes were exploited.
- *Integrity:* Data integrity was breached through the creation of fake invoices.
- *Availability:* Legitimate financial processes were manipulated for fraudulent activities.

STRIDE Analysis:

- *Spoofing:* Creating a company with a similar name to a legitimate supplier.
- *Tampering:* Altering invoice details to redirect funds.
- *Repudiation:* Potential denial of fraudulent activities.
- *Information Disclosure:* Access to confidential corporate financial information.

Financial Deception: Newswires Case - Arkadiy Dubovoy and Co.

Case Description: Arkadiy Dubovoy, along with traders and hackers, hacked major newswire agencies, accessing unpublished press releases with market-sensitive information for insider trading.

CIA Analysis:

- *Confidentiality:* Breach through unauthorized access to unpublished press releases.

- *Integrity:* Misuse of financial information for insider trading.
- *Availability:* Exploitation of information for financial gain before public release.

STRIDE Analysis:

- *Spoofing:* Hackers posed as legitimate users to infiltrate newswire systems.
- *Tampering:* Unauthorized access to and use of financial data.
- *Repudiation:* Hackers and traders could deny their involvement.
- *Information Disclosure:* Release of sensitive financial information before scheduled publication.

2.3 Common Vulnerabilities and Attack Vectors

- *Exploitation of Trust:* Key in all three cases, targeting individual trust in personal relationships or corporate trust in business processes.
- *Social Engineering:* A primary tactic used in WhatsApp fraud and the Newswires case, manipulating human psychology to achieve the desired outcome.
- *Security Gaps:* In digital communication platforms (WhatsApp case) and financial transaction systems (Newswires case), allowing unauthorized access and misuse of information.

3 Prevention Advice Analysis

3.1 Examples of Advice

This section discusses the prevention advice drawn from the Darknet Diaries episodes, linking it to the CIA and STRIDE frameworks and incorporating standards from NIST and ISO.

1. **Educate about Phishing Scams and Social Engineering Tactics (Episode 141):** This advice is crucial for addressing the 'Spoofing' and 'Information Disclosure' aspects in STRIDE. Educating users about recognizing and responding to phishing attempts can preserve the 'Confidentiality' and 'Integrity' of information, as defined in the CIA triad.
2. **Implement Robust Verification Processes for Financial Transactions (Episode 124):** This step targets the 'Tampering' and 'Repudiation' aspects in STRIDE. By ensuring robust verification, organizations can maintain the 'Integrity' and 'Availability' of their financial transactions. This aligns with NIST's recommendation for strong access control measures.
3. **Adopt Multi-Factor Authentication and Strong Cybersecurity Measures (Episode 123):** Multi-factor authentication (MFA) is a critical tool for addressing 'Spoofing' and 'Elevation of Privilege' in STRIDE. It directly enhances 'Confidentiality' and 'Integrity' as per the CIA model. MFA is also a key recommendation in ISO/IEC 27001 for information security management.

Each piece of advice is discussed in detail, ensuring clarity for a general audience and linking back to the respected cybersecurity frameworks.

This subsection summarizes the common pieces of advice identified across the episodes, highlighting their relevance to cybersecurity principles and best practices. The advice aligns with the CIA and STRIDE frameworks, reflecting best practices as recommended by NIST and ISO standards.

4 Effectiveness of Prevention Strategies

4.1 Analysis of Advice Against Vulnerabilities

In this section, we critically assess the advice provided against the vulnerabilities and attack vectors identified in our examples. By applying the STRIDE and CIA frameworks, we can better understand the depth and coverage of the advice.

1. **Phishing Scams and Social Engineering:** Education about these scams addresses the 'Spoofing' and 'Information Disclosure' elements of STRIDE. By increasing awareness, individuals are better equipped to recognize and avoid these threats, thereby preserving the 'Confidentiality' and 'Integrity' aspects of the CIA triad.

2. **Robust Verification Processes for Financial Transactions:** Implementing these processes directly combats the 'Tampering' and 'Repudiation' aspects of STRIDE. It strengthens the 'Integrity' of financial transactions, ensuring the authenticity of the transaction data.

3. **Multi-Factor Authentication (MFA):** MFA is an effective tool against 'Spoofing' and 'Elevation of Privilege'. It enhances 'Confidentiality' and adds an extra layer of security, ensuring that access to sensitive information is strictly controlled.

4.2 Limitations and Unaddressed Threats

Despite the effectiveness of the advised strategies, there are limitations and potential threats that remain unaddressed. For instance:

1. **Emerging Techniques:** Fraudsters continuously evolve their strategies. Therefore, staying updated with the latest fraud tactics is crucial. Current advice may not fully cover novel or sophisticated attack methods that bypass traditional security measures.

2. **Psychological Manipulation:** Much of the advice focuses on technological solutions, but human factors like psychological manipulation often play a significant role in successful fraud. Developing strategies to counteract these tactics is equally important.

4.3 Tailoring Advice for Specific Populations

The effectiveness of fraud prevention advice can be significantly enhanced by tailoring it to specific groups:

1. **Non-Native English Speakers:** Simplifying the language used in fraud prevention materials or providing translations can greatly assist those who might otherwise miss critical information.

2. **Visually Impaired Users:** Integrating screen readers or audio descriptions into security tools can make fraud prevention more accessible, ensuring equal protection for all users.

5 References

Guidance on structuring the content was obtained through an interaction with an LLM.

Podcasts:

1. Darknet Diaries. (n.d.). Episode 123: Newswires.
   Retrieved from https://darknetdiaries.com/episode/123/

2. Darknet Diaries. (n.d.). Episode 124: Evaldas Rimasauskas.
   Retrieved from https://darknetdiaries.com/episode/124/

3. Darknet Diaries. (n.d.). Episode 138: Insider.
   Retrieved from https://darknetdiaries.com/episode/138/

Online Articles and Reports:

1. Greenberg, A. (2018, August 22). How an International Hacker Network Turned Stolen Press Releases Into 100 Million. The Verge.
   Retrieved from https://www.theverge.com/2018/8/22/17716622.

2. United States Department of Justice. (n.d.). [Press Release on Hacking Scheme].
   Retrieved from https://www.justice.gov/usao-nj/file/765216/download

3. United States Department of Justice. (n.d.). [Press Release on Fraud Case].
   Retrieved from https://www.justice.gov/usao-nj/file/705916/download

4. Securities and Exchange Commission v. Dubovoy, et al. (2016).
   Retrieved from https://casetext.com/case/sec-exch-commn-v-dubovoy-1/

5. Securities and Exchange Commission. (2018). Litigation Release No. 24193.
   Retrieved from https://www.sec.gov/litigation/litreleases/2018/lr24193.htm

News Articles:

1. BBC News. (2018, April 23). Man fooled Facebook and Google out of 100m.
   Retrieved from https://www.bbc.co.uk/news/uk-43823962

2. CNBC. (2015, August 11). Five arrested in insider trading hacking scheme: FBI.
   Retrieved from https://www.cnbc.com/2015/08/11

3. Investopedia. (n.d.). Public Company.
   Retrieved from https://www.investopedia.com/terms/p/publiccompany.asp

4. The Register. (2019, December 20). Facebook, Google scammer gets just five years in clink for 121m heist.
   Retrieved from https://www.theregister.com/2019/12/20

5. The Tribune India. (n.d.). 3 lose over 5L in WhatsApp call scam.
   Retrieved from https://www.tribuneindia.com/news/jalandhar/3-lose-over-5l-in-whatsapp-call-scam-387050