

Cyber vs Regular: Understanding the State of Consumer Fraud in America

Mohammad Taha Khan and Chris Kanich

Department of Computer Science, University of Illinois at Chicago

taha@cs.uic.edu, ckanich@uic.edu

Abstract—The abstract goes here.

I. INTRODUCTION

the main contributions: Understanding the differences in the nature of cyber and regular frauds in the United States. Exploring if certain demographics are more susceptible to cybercrime Suggesting improvements that might be the right way to create more awareness and campaigns.

Fraud and and deceptive practices have been around since the establishment of

The FTC and the FBI

According to a recent FTC survey report[13] shows that Internet fraud had doubled within the past 6 years and now is the top most source of frauds within the the US.

Explain regular and cyber fraud... dive details in categorization

II. RELATED WORK

As our work evaluates both cyber as well as regular frauds, we provide related work that encompasses both of these categories. However, we elaborate more on recent research that focuses on cyber frauds due to the increased Internet usage trends for sensitive activities leading to more individuals being victims of online frauds [13]. Before the Internet became a primary source of economic and social activity, researchers measured [9] and developed techniques based on statistical models [10], [11], [12] to detect phone and credit card based frauds. In the past few years, most research has shifted focus towards cyber activity [4], [5], [3], [7] due to its high potential for harm.

Even though, term "cyber" is usually associated with Computer Science, due to its recent socio-economic impact, researchers in Economics, Law and Finance have also explored for solutions to this problem by incorporating methodologies specific to their areas. Ionescu et. al [3] characterize the types and sources cyber frauds in global digital networks. The authors link the exponential increase of cyber fraud to increased Internet usage for financial management and transactions, especially in financial markets. They suggest the involvement of all stakeholders and employees through awareness and training for containing and mitigating this type of fraud. Similarly, Howard et. al [7] study malicious code attacks against financial networks and suggest technical detection and mitigation techniques for financial infrastructure. [5] studies how the cyber criminals have several potential

advantages over the law enforcement agencies that they are opposing them. They suggest some practical steps to even out the differential gap.

Due to an increase in overall concern for online criminal activity, there have also been state sponsored research that look at Fra have Smyth et. al [8] measured the extent of cyber fraud in Canada in 2011. Their work indicated that a major chunk of frauds do not get recorded and suggested a need of a sentinel to record fraud data similar to the FTC complaint center in the US.

Another significant area of research focuses on understanding the underlying demographics of victims of these frauds. A recent FTC Report [14] use complaint data to evaluate quantify complaint rates and nature across different ethnic and education groups. Researchers in [4] provide a comprehensive survey report collected from individuals that were victims of an online data breach. They categorize their results in different income, education, age and ethnic groups. Such research aims at allowing organizations to better develop policies and create awareness among for consumer rights protections.

In comparison to previous research which study either cyber or regular fraud, our work provides a different angle of evaluation by characterizing both types of frauds and provide distinctions for each category based on popular demographics.

Our study mainly fo

III. DATA COLLECTION

IV. EVALUATION

V. DISCUSSION

VI. CONCLUSION

The conclusion goes here.

ACKNOWLEDGMENT

The authors would like to thank...

REFERENCES

- [1] H. Kopka and P. W. Daly, *A Guide to L^AT_EX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.
- [2] pete snyder affiliate fraud
- [3] cyberfraud in a global digital network
- [4] Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information
- [5] An Uneven Playing Field: The Advantages of the Cyber Criminal vs. Law Enforcement-and Some Practical
- [6] Identity Theft as a Teachable Moment
- [7] Cyber Fraud Trends and Mitigation
- [8] Cyberfraud in Canada

- [9] Controlling Cell Phone Fraud in the US: Lessons for the UK Foresight Prevention Initiative
- [10] Neural data mining for credit card fraud detection
- [11] Detection of mobile phone fraud using supervised neural networks: A first prototype
- [12] Statistical Fraud Detection: A Review
- [13] <http://gotaclassaction.com/wp-content/uploads/2013/05/FTC-Fraud-Survey.pdf>
- [14] complaints ftc