Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U.S. Seniors: A Short Review

Niroop Sugunaraj , Akshay Ram Ramchandra , and Prakash Ranganathan3
School of Electrical Engineering and Computer Science (SEECS)
University of North Dakota
Grand Forks, USA

Abstract

Abstract—Cyber fraud has become increasingly common as it can be easily carried out with relative ease through multiple mediums. Particularly, the elderly population aged 60 and above seniors, are more vulnerable to such fraud/scams as they generally lack the know-how for such fraudulent activities. This paper briefly addresses the various types of fraud/scams, apparent early warning signs, and potential preventive tips before falling victim of cyber fraud. Additionally, sophisticated scam methods are also highlighted, and resources available to report/inform the general public is documented.

Index Terms—cyber fraud, exploitation, scams, resources.

Introduction

The global digital footprint has been steadily rising due to the emergence of consumer devices such as smartphones, tablets, personal computers (PCs), and the growth of the world-wide web (WWW). While these digital devices have provided greater access to information to the Internet's large consumer base, and more accessible networking capabilities through social media platforms and e-commerce, these digital devices have also become targets or sources to increase in cyber-fraud incidents. According to the Federal Trade Commission (FTC) [1], the most common cyber frauds are computer support, fake checks, check or money order solicitation, and sweepstakes scams.

Elder fraud is a subset of a broader class of abuse called elder exploitation or elder abuse. The United States Government Accountability Office (GAO) [2] defines elder exploitation as the "illegal or improper use of an older adult's funds, property, or assets". Financial exploitation of seniors is one aspect of elder fraud that is gaining much traction among threat actors and is called the fraud of the 21st century [3]. Elder fraud is targeted at cohorts of the population aged 60 years or above, referred to as seniors. Statistics from the Survey of Consumer Finances (SCF) [4] indicate that seniors, on average, have a reported income of $46,800 (before tax).

Recognizing Elder Fraud

Fraud Vectors

1) Voice calls.
2) Email.
3) Short message service (SMS).
4) Letters.
5) Internet pop-ups.

B. Fraud Types

Types of elder fraud:

1) Sweepstakes: Threat actors notify victims of free prizes and gifts that are offered on the basis of a lottery win.
2) Technical support: Victims are contacted by "qualified" technicians who troubleshoot technical issues in the victims' personal computers.
3) Confidence/sweetheart/romance endeavors: Overly friendly or suspicious interactions from recently met persons.
4) Phishing: Victims are threatened by scammers who pose as law enforcement personnel.
5) Identity theft: Victims are solicited for personally identifiable information (PII).
6) Overpayment: Counterfeit checks or money orders are offered by phony buyers as overpayments.

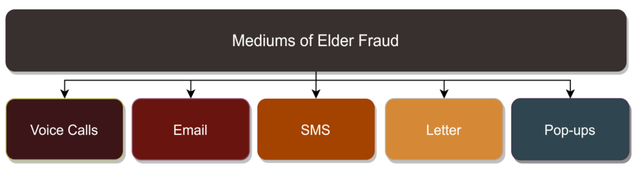

Figure 3: Vectors of Elder Fraud

In 2021 alone, there were 92,371 reports from elderly fraud victims with $1.7 billion in losses. The financial losses due to elder fraud have steadily increased over the past five years, only with a recent drop in 2021.

The majority of the reported cases were from victims based in California (see Figs. 1 and 2).

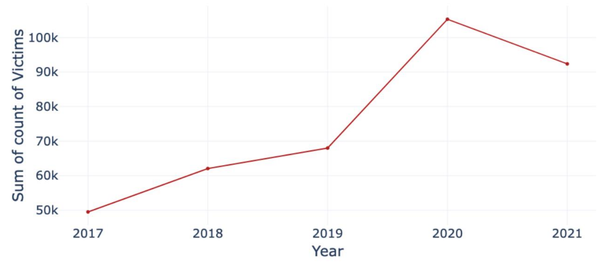

Figure 1: Victims of elder fraud from 2017 – 2021.

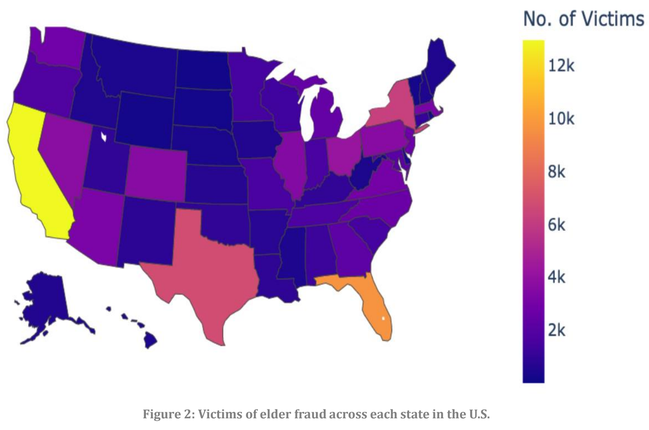

Figure 2: Victims of elder fraud across each state in the U.S.

Advanced Threats

Artificial Intelligence (AI) can be used in generative adversarial networks (GANs) to generate fake audio that sounds remarkably like a human impersonation: GANs can be used to aurally impersonate a loved one or a law enforcement official to commit financial fraud. GANs can also be trained to misclassify malicious data as benign samples to evade detection.

Social Engineering tactics from skilled attackers can effectively condition the psyche of a victim into giving what the attack wants through manipulation, guilt trips, or fear instillation.

28% of financial losses due to cyber fraud in 2020 were experienced by seniors with 14.7% of these losses attributed to social engineering

Fraudulent Surveys are carried out by deploying fraudulent surveys that primarily look to exploit the victims' PII and finances. Hackers may also use fake survey pages that are hypertext transfer protocol secured (HTTPS) to bait a doubtful user in thinking the site is legitimate. An HTTPS connection indicates that communicated data is free from prying eyes but does not say anything about the legitimacy of the webpage's content

Prevention and Mitigation Strategies and Resources

Strong Passwords are at least 12 characters long, does not include any personal information, is a combination of uppercase and lowercase characters, numbers and alphabets, and is as unique as possible. Password managers can also be used to securely store passwords, particularly if a user maintains many login accounts.

Multi-factor Authentication (MFA) is authentication using two or more different ways to validate authentication. Validation methods include something you know (e.g., PIN, password), something you have (e.g., cryptographic dentification device, token), or something you are (e.g., biometric)."

Antivirus Software is a program that scans one's computer for potential threats while keeping itself updated with the latest virus signatures from databases that may be privately owned or open-source. Antivirus software primarily function by detecting malicious software / activity by monitoring signatures and behavior of software.

Pop-up Blockers

It is recommended to install add-ons (provided by all the major browsers such as Chrome, Mozilla Firefox, Edge, etc.) that automatically filter pop-ups. However, legitimate websites use pop-ups to communicate with users and can be allowed to pass through the pop-up blocker.

Table 1
ELDER FRAUD RESOURCES FOR SENIORS

Resource	Service
Office for victims of Crime	Helpline
American Association of Retired Persons	Helpline
Internet Crime and complaint Center	Reporting
Federal Trade Commission	Reporting
National Center on Elder Abuse	Assistive
Office of Inspector General	Reporting

Conclusions

Elder fraud is becoming a widely-spread threat to seniors who are typically at or above the retirement age. Elder fraud is primarily carried out through five communication mediums (voice calls, email, SMS, pop-ups, and letters). The commonly sought after details or interests that are included in such communication mediums are sweepstakes, technical support, confidence/romance endeavors, phishing attempts, identity theft, and overpayment scams. There are typical signs that an elder is being exploited financially through cyber threat actors, but increased sophistication due to tactics such as artificial intelligence, social engineering techniques, and fake surveys has led to greater success in carrying out frauds. However, simple prevention and mitigation strategies can help to reduce the likelihood of being defrauded.

Contact Information

Akshay Ram Ramchandra
Graduate Research Assistant(DECS)
akshay.ramchandra@und.edu

Citation

This paper was published in the 22nd Annual IEEE International EIT Conference.
N. Sugunaraj, A. R. Ramchandra and P. Ranganathan, "Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U.S. Seniors: A Short Review," 2022 IEEE International Conference on Electro Information Technology (eIT), 2022, pp. 623-627, doi: 10.1109/eIT53891.2022.9813960.

References

[1] U. S. Government, "Report scams and frauds," Scams and Frauds, 2022.
[2] G. A. Office, "Elder justice - stronger federal leadership could enhance national response to elder abuse," 2011. https://www.sec.gov/files/elder-financial-exploitation.pdf.
[3] Consumer Financial Bureau Protection, "Money Smart for Older Adults (Resource Guide)," no. June, 2021.
[4] T. F. Reserve, "Survey of Consumer Finances (SCF) (1929 - 2019," 2019.
[5] T. C. Truong, Q. B. Diep, and I. Zelinka, "Artificial intelligence in the cyber domain: Offense and defense," Symmetry, vol. 12, no. 3, p. 410, 2020

UNIVERSITY OF NORTH DAKOTA.

UND SCHOOL OF ELECTRICAL ENGINEERING & COMPUTER SCIENCE
UNIVERSITY OF NORTH DAKOTA

C2SR
CENTER FOR CYBER SECURITY RESEARCH

DECS