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

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

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.

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

Advanced Threats

Artificial Intelligence (AI) can be used to generate adversarial networks (GANs) to generate fake audio that sounds remarkably like a human impersonation: GANs can be used to audially 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 victim's PII and finances. Hackers may also use fake survey pages that are hypertex转移 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 log-in 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 authentication 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.

Conclusion

Elder fraud is becoming a widespread 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, computer support, fraud/scams, and sweepstakes 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 to greater success in carrying out frauds. However, simple prevention and mitigation strategies can help to reduce the likelihood of being defrauded.

Acknowledgments

This paper was published in the 22nd Annual IEEE International EIT Conference.


References