Applicable Mitigation Strategies and Technology Propositions: Preventing Scamming in Marginalized Populations

Grace Nicole Sandhofer-Adams
Old Dominion University

Applicable Mitigation Strategies and Technology Propositions:

Preventing Scamming in Marginalized Populations

Grace Nicole Sandhofer-Adams

School of Cybersecurity, Old Dominion University

COVA CCI Undergraduate Research

April 14, 2022

Table of Contents

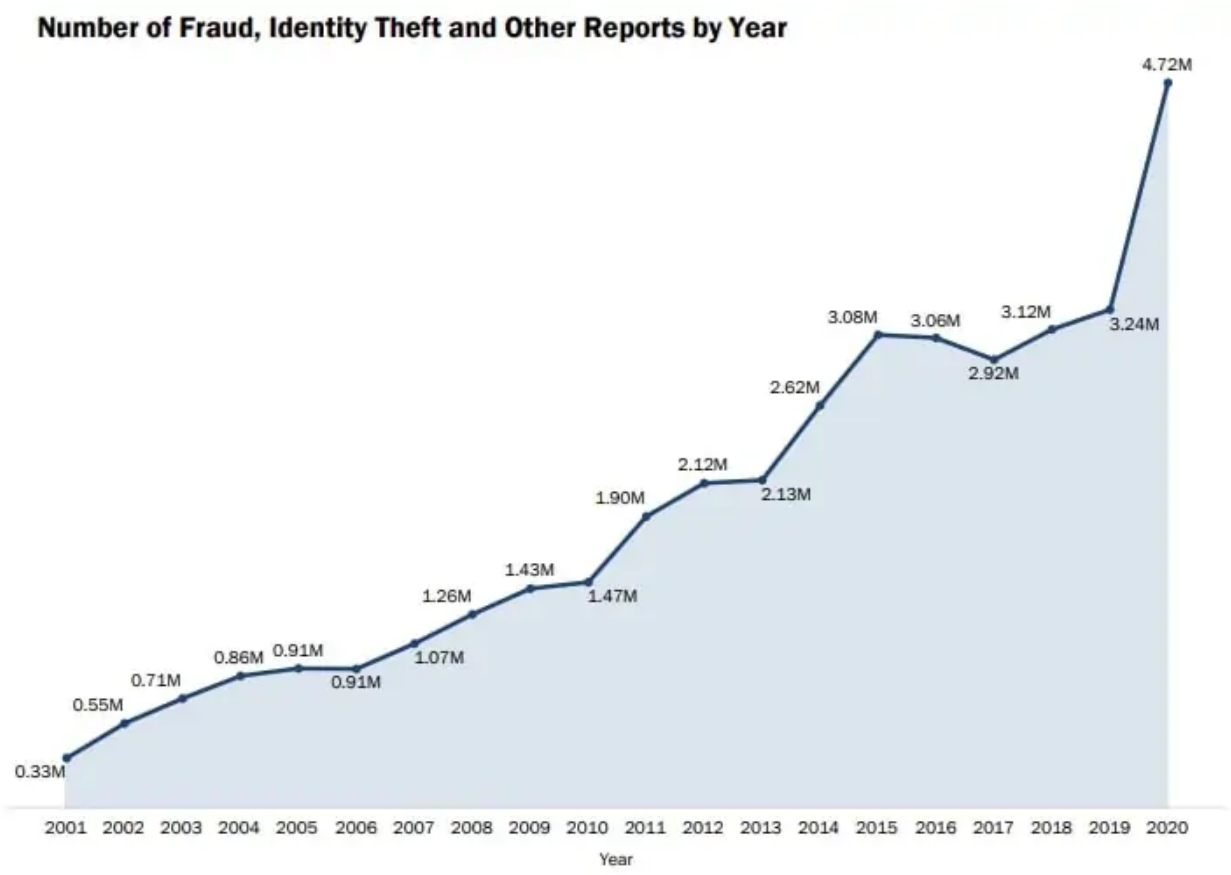
ABSTRACT

This essay serves as a proposal for new technology and mitigation against the scamming of marginalized individuals (i.e., those over the age of 65). Research supports this outline, giving background to the types of scams, and prevention strategies currently seen in the cybersecurity landscape. It is evident that the methods we currently use to combat scamming attacks are not effective, therefore, I propose a new solution. This proposed telecommunications strategy is necessary to prevent scamming of all internet users, no matter the device. This telecommunication strategy would use artificial intelligence and machine learning to constantly improve its detection over time, nullifying the scamming issue that plagues senior citizens.

Keywords: Artificial Intelligence, Machine Learning, Telecommunication Leverage, Senior Adults, Educational Mitigation, Technological Mitigation, Scam-Prevention, Scamming

I. INTRODUCTION

I am an undergraduate student writing to bring attention to a marginalized group of people that disproportionately fall victim to scams. I believe that adults over the age of 65 can implement simple security tips that will decrease the likelihood of cyber-attacks stemming from the user domain. Moreover, my overarching research question for my topic of user domain security is what simple, applicable security tips can we teach and apply to the mentioned marginalized demographics, to help lessen the statistic of cybersecurity incidents and scamming attacks?



(Gill, 2022)

I have a hard time hearing of marginalized individuals' life savings being taken away by people who have no displayed ethics. Before I had an interest in cybersecurity, I would find myself frequenting videos of people in America wasting scammers' time with silly impractical stunts, like putting on a grandma voice to stall scammers. Not only was this entertaining, but I knew it was one less scammer having the chance to trick an unsuspecting individual, that could not defend themselves.

Many foreign call centers contracted to specifically target the age group of 65 and over to reach older individuals, who usually have more empathy for others and less to do with their money. The primary reason for targeting this age group is that their demographic, statistically, is less technologically savvy. Unfortunately, scammers resort to verbally berating and victimizing these individuals, causing them to break down under pressure. Due to this social engineering, scammers can retrieve sensitive information through the user domain. These scams can range from robotic phone calls to elaborate computer schemes where individuals take remote access of an elder's computer (Special Committee on Aging United States Senate, 2016, pp. 7-10). These companies will pose as a familiar company like Microsoft or Amazon to create familiarity and authority, creating a greater sense of persuasion (Wang, Zhu, & Sun, 2021, p. 11897).

Because the usual weak point in a system is usually located in the user domain, we can decrease that vulnerability by educating users. Unfortunately, in the world of information security, the risk level of an attack is never zero. But we can do our best to educate others and implement techniques that lower the chance of an attack. The more informed people are about possible threats and the damage that they can do, the more likely they are to be concerned about issues that affect them directly and put measures in place to protect themselves.

II. SOCIAL ENGINEERING

When we begin to analyze the threats to data security, the most common liability seen is the human factor. This threat comes in the form of social engineering. In an article supported by the National Key Research and Development Program of China, authors define social engineering as follows: “In the context of computer and cyber security, social engineering describes a type of attack in which the attacker exploit human vulnerabilities by means such as influence, persuasion, deception, manipulation and inducing, so as to […] breach the security goals” (Wang, Zhu, & Sun, 2021, p. 11895). I believe this definition is critical for understanding the context of social engineering when it comes to system security, as it gives a base definition for the term throughout this research.

In social engineering, generally, there are a few effective mechanisms used to infiltrate the user domain. First, we see that similarity invites liking, and dissimilarity leads to dislike (2021, p. 11897). Often, social engineers, or attackers, will use this to their advantage and try to relate to the victim, so the victim will feel more inclined to be empathetic toward them (2021, p. 11897). The second tactic used is distraction in persuasion and manipulation. The human brain is wired to focus on one thing at a time without pressure, so when social engineers use blaring alerts or strong verbal commands to invoke a sense of panic and confusion, individuals’ first response is to do whatever necessary to exit the situation (2021, p. 11897). The third mechanism in this type of social engineering is source credibility and the theory of obeying authority (2021, p. 11897). Attackers will use this by claiming they are from a large, reputable company, such as Amazon or Microsoft, to trick victims into believing they are communicating directly with the company.

Even in 2022, the most common causes of cybersecurity breaches are malware at 22 percent and phishing at 20 percent (Jakkal, 2022). Malware attacks are often executed because of individuals opening or downloading files or links with malicious software inside. Depending on the coding in the malware, this code can cause irreversible damage to systems. Phishing, on the other hand, is the process of fishing for people to click on links, download files, or give away credentials. These statistics remain so high because attackers continue to use the social engineering mechanisms previously mentioned.

III. APPLICATION AND BACKGROUND

In the middle of the workday in the United States, your phone begins to ring. You pick it up, not knowing the caller. The 'voice' on the other line is a robotic one, reading, "This is Amazon.com. You have been charged three hundred and seventy-nine dollars—" before you abruptly end the call (Rober, 2021). Most Americans are familiar with this scenario, but "behind this harmless sounding call is a 20-billion-dollar scam industry" (Rober, 2021, & Denver7, 2018).

This is one of the most popular, and effective, scams in the United States. Victims believe that this phone call is true, so they listen to the rest of the call, which gives them directions on how to "get their money back." Essentially, the victim's phone call is transferred to a real person working for a fraudulent company. The scammer gives directions on installing a software on the victim's computer, so they can take control over their screen—their justification is that this is to assist the victim.

The scammer will, first, have the victim log into their bank account. They then turn off the victim's screen, so they cannot see what is happening, and use the "inspect" tool on Google

to make the website look like thousands of dollars has been added to their account. The victim has not seen this page, keep this in mind.

The scammer will explain that they could not process the refund, so they have one more option. Then, the scammer will prompt the victim to type in some personal information and the amount they are meant to be refunded in a "permanent system." This "permanent system" is a text box, but the victim believes this is a permanent system that cannot be altered after they input the refund amount. As the victim is carefully typing the return amount, the scammer adds an extra zero on the end of the amount in this "permanent system." The scammer then reveals the edited bank account page, showing that they now have thousands of dollars in their account that should not be there. Now we begin to see how these marginalized individuals who do not understand this technology are willing to send thousands of dollars to these companies because they believe this is their mistake (Rober, 2022). This is another big reason that these individuals do not disclose this to their families or the authorities—they believe they are fixing their mistake.

IV. EDUCATIONAL MITIGATION

Denver7 explains that scammers have a 'suckers list'-- a collection of individuals' information created for the use of scamming (Denver7, 2018). This list is a compilation of information from individuals that have bought from catalogs, entered sweepstakes, or fallen for solicitations in the past-- even those who give to charities (Denver7, 2018). The main demographic on this list are older individuals who participate in the activities previously stated. Because the elderly are often very empathetic and not very technologically savvy, this makes them the most susceptible to scamming. It is also common knowledge that these individuals are

probably living off retirement funds and might have social security checks as well, making them the perfect, unknowing target.

An article published by Nina Klimburg-Witjes and Alexander Wentland reiterates that social engineering is the most common way of committing cybercrime (Kilmburg-Witjes & Wentland, 2021, 1316). Since elderly individuals are the most vulnerable to these attacks, we must find easily implementable mitigations to deter scamming in their demographic. A great way to prevent scamming, especially the aforementioned refund scams, is getting a second opinion. Simply double-checking the email or source of the email can save thousands of dollars. This can be having a second party check the email or reaching out directly to the company through their website to make sure the email came from them. The victim also needs to check their bank account though a different device if they are in the process of being scammed, as the scammer can alter the appearance of their bank account page. Even just being informed of this scam and suspicious behavior can save many elders their life's savings. No reputable company will require a customer to send them thousands of dollars in a suspicious way (i.e., wrapping money in cling wrap for smell-proofing and tin foil for X-Ray-proofing, sending gift card codes, putting money in the pages of books). Potential victims should also be aware that no reputable company should require them to download a software in order to process a refund. The safest way to double-check these emails is to contact the company directly from their website or ask a more tech-savvy individual, generally someone not in their demographic.

V. TECHNOLOGICAL MITIGATIONS

Even with the solution of education, there are still many victims of this scam. This has been a fairly well-known scam for a few years as of 2023, so it is clear that just education is not a

viable solution. We are currently on the brink of a technology explosion, as artificial intelligence (AI), quantum computing, and blockchain technologies are all emerging into the public eye. I believe that with the use of AI and machine learning, there could be a very effective technological mitigation.

I believe this technology would pull some inspiration from the retail browser extension Honey, a couponing platform with over 17 million users (Sherman, 2019). There is no guessing why this PayPal sponsored couponing-helper is worth over 4 billion USD (Sherman, 2019). It is incredibly user-friendly, giving coupon help only when necessary and notifying the user of price drops on items. I believe this technology could be immensely helpful when assessing websites.

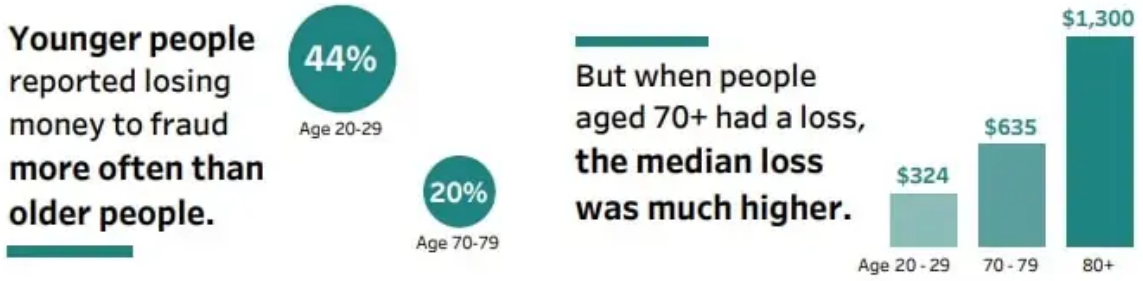
Similar to Honey, this proposed browser extension would pop up when necessary. In the same user-friendly manner, the extension would warn the user if they are on a seemingly fraudulent website. The detection system would check for spelling errors, expired certificates, similar, more reputable websites using AI technology and machine learning– the system would only get more accurate with time. To account for the margin of error and liability, the browser extension would read a risk percentage of scam, rather than block access to the site. The extension would give reason to why it thinks it has detected a fraudulent website.

The problem when it comes to browser extensions lies in the usage by users and careful curation by distributors. Moreover, for the browser extension to prevent scams, it must be installed and executed by the user. In addition to this, browser extensions, some meant for scam prevention, have turned out to be scams, as browsers like Google Chrome do not curate what browser extensions are available to add to their browser. Chrome extensions were to blame for an affiliate payment scam, affecting 1.4 million users (Sims, 2022).

Browsers, like Google Chrome, have instead opted for built-in scam protection, offered by the browser. However, this is a relatively new feature and the user must navigate through settings to remove malicious software. When accessing a suspicious website, the user will receive a large red warning sign saying “Deceptive site ahead” with only one option– “Back to safety” (Google, n.d.). This warning gives no explanation to why the website might be fraudulent, or how much of a risk it is. This solution gives no choice to the user either, even though the fraudulent flagging could be a result of an expired certificate and the website is harmless.

VI. LEVERAGING TELECOMMUNICATION PROTOCOLS

Therefore, I propose a new telecommunication protocol, similar to IP or TCP, as not all browsers will have this built in, and it is not a thought through system yet, even when built into browsers. Just as the Domain Name System has its purpose as the “phone book of the internet,” there could be a similar, parallel IP, ensuring the website you are attempting to access is trusted. The same aforementioned AI and machine learning algorithms would detect the fraudulent site, along with IP addresses reported to be fraudulent. Before connecting to the site, a disclaimer would be posted, showing the user what risks lie ahead and how likely the site is to be fraudulent. The user would have the option to proceed forward or return to safety. This solution would not only help marginalized individuals, but it would be a standard practice, helping to ensure internet safety for users of all ages.



(Gill, 2022)

It is evident that the solutions we are currently using are not working– an infrastructure-based solution would solve many of the problems we are facing. The solutions currently being used are all optional, and that is what makes them dangerous. Solutions like browser extensions are not regulated by reputable companies, causing more incidents of scamming. Browsers with built-in software only protect the user when using that browser, and the technology they use is hardly user-friendly. A telecommunications protocol solution makes this solution permanent for all users.

This solution will not be perfect, and in its infancy there will be false positives and false negatives. However, with AI and machine learning, the longer this system is in place, the more accurate the detection becomes. The process refines over time and the algorithm improves with every detection.

VII. CONCLUSION

Nino, Enström, and Davidson (2017) reiterate that "[f]raud over the Internet is an increasingly common phenomenon and very common in the form of emails." Not only are elderly individuals being targeted over the phone, but by email as well. Just like the phone call

scams, these emails lead thousands of marginalized individuals to become victims of scams. Nino, Enström, and Davidson's (2017) research found that respondents, born between 1928 and 1951, had "primarily been poor at identifying technical factors in the fraudulent email." They concluded that the demographic group they studied is more vulnerable to these types of scams (Nino, Enström, & Davidson, 2017).

I believe that the best mitigation to combat these scamming attempts is a technological solution. This is most likely the most simple, effective solution to the impersonation fraud common today. The best solution, while waiting for updated technology, would be to install a browser with built-in scam detection. This may not be the most user-friendly solution, but it beats no technological solution. In addition, the receiver of this phone call or email should either go directly to the source company, through their official website, or get a second opinion from a more technologically savvy individual. This second-glance can be the difference between an individual having a retirement fund or inheritance or having it go into the hands of someone who does not deserve it.

It is no secret that these scammers are good at what they do. Wang, Zhu, and Sun (2021) write about how effective these tactics are and that the "social engineering threat is increasingly serious." It is becoming exponentially important that we protect our elders and assist them with online communication and interactions. With the increasing number of devices we have connected to the internet, we have to remember that each of those systems need to be secured. This threat only becomes larger as the Internet of Things (IoT) continues to expand. I believe it should be the younger generations' mission to guide elders in this changing world, and help to ensure them with the security they deserve by using the new technology we are discovering.

VIII. REFERENCES

Denver7 – The Denver Channel (2018, August 8). *Scammers use lists to target vulnerable people*. YouTube. https://www.youtube.com/watch?v=A_4x65zEJ3E

Gill, M. (2022, October 7). *Senior scam statistics 2023: Is elder fraud on the rise?* Comparitech. Retrieved April 12, 2023, from https://www.comparitech.com/identity-theft-protection/senior-scam-statistics/

Google. (n.d.). Chrome Privacy & Security Settings - Google Safety Center. Retrieved April 3, 2023, from https://safety.google/chrome/#:~:text=Security%20you&text=Make%20the%20most%20of%20your,from%20malware%20and%20dangerous%20sites.

Jakkal, V. (2022, October 4). *Cybersecurity awareness tips from Microsoft to empower your team to #becybersmart*. Microsoft. https://www.microsoft.com/security/blog/2022/10/04/cybersecurity-awareness-tips-from-microsoft-to-empower-your-team-to-becybersmart/

Klimburg-Witjes, N. & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "deficient user" in cybersecurity discourses, *Science, technology, & human values, 46*(6), 1316-1339. https://doi-org.proxy.lib.odu.edu/10.1177/0162243921992844

Nino, JR., Enström, G., Davidson, A.R. (2017). Factors in fraudulent emails that deceive elderly people. In: Zhou, J., Salvendy, G. (eds) Human Aspects of IT for the Aged Population.

Aging, Design and User Experience. ITAP 2017. Lecture Notes in Computer Science(), vol 10297. Springer, Cham. https://doi.org/10.1007/978-3-319-58530-7_28

Rober, M. (2021, March 18). *Glitterbomb trap catches phone scammer (who gets arrested)*. YouTube. https://www.youtube.com/watch?v=VrKW58MS12g&t=710s

Rober, M. (2022, May 8). *Pranks destroy scam callers- glitterbomb payback*. YouTube. https://www.youtuabe.com/watch?v=xsLJZyih3A

Sherman, E. (2019, November 22). *PayPal's $4 billion acquisition of Honey could 'pay for itself in a few years'*. Fortune. Retrieved March 7, 2023, from https://fortune.com/2019/11/21/paypal-honey-acquisition-worth-4-billion/

Sims, D. (2022, September 1). *Chrome extensions with 1.4 million installs track users for affiliate payment scam*. TechSpot. Retrieved April 3, 2023, from https://www.techspot.com/news/95831-chrome-extensions-14-million-installs-track-users-affiliate.html

Special Committee on Aging United States Senate (2016, February 11). Fighting fraud: U.S. senate aging committee identifies top 10 scams targeting our nation's seniors. *U.S. Government Publishing Office*. https://www.govinfo.gov/content/pkg/CRPT-114srpt208/pdf/CRPT-114srpt208.pdf

Wang, Z., Zhu, H., & Sun, L. (2021, January 14). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, 9, 11895-11910. https://doi.org/10.1109/ACCESS.2021.3051633