The Struggle Between the Scammer and Technology: An Evolving Balance of Power

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Andrew Cornfeld
March 13, 2024

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignment.

Andrew Cornfeld

STS Advisor: Peter Norton

Preface

How can machine learning systems improve safety and other performance criteria?

How can machine learning be used to predict the admission and seeding of the NCAA basketball tournament? Bracketology is the process of predicting and creating the March Madness tournament bracket, which is not well understood and complex. The March Madness bracket is selected by a committee of twelve members. To predict tournament bids and their respective seeds, I utilized Machine Learning techniques to create a model which analyzes a team's resume to determine its seed placement. Based on the model, any team looking to receive an at-large bid must evaluate the strength of their conference schedule (the last 16-20 games of their 30-game schedule) to make decisions about how difficult their non-conference schedule must be.

In the US, how do telecom companies, federal agencies and scammers compete to protect or subvert telecommunications security? Telecommunications scams have existed for decades, and unaware victims have lost $8.8 billion dollars in just 2022 to these scams. User training cannot prevent all online scams, and law enforcement often cannot recover victims' losses. Because telecom companies and government agencies cannot thwart all scammers, users must learn how to protect themselves.

The Struggle Between the Scammer and Technology: An Evolving Balance of Power

Telecommunications scams have existed for decades, and unaware victims have lost $8.8 billion dollars in just 2022 to these scams (Mayfield, 2023). Scams can devastate people who rely on government services, exacerbating their disadvantages. Scams cost businesses and individuals opportunities, and can cause emotional and even physical stress (Commonwealth of Australia, 2020).

Machine learning engineers, telecom companies, federal agencies, mobile phone carriers, scam-savvy mobile phone users, naive users, and scammers compete to perpetrate or to thwart scams. Engineers train models on caller data and use them to detect potential fraud (Rudolph, 2022). Motivated by their business interests, telecom companies want to prevent fraudulent accounts from stealing from other customers (Apple, 2023). The Federal Communications Commission (FCC) asks phone companies to apply call analytics to block unwanted calls (FCC, 2023).

Scam-savvy mobile users know how to thwart scams and can educate others in scam prevention. They recognize threats but may not help others recognize them. One scam-savvy mobile user, Cameron Huddleston, recalled that a scammer told her mother, who was suffering from Alzheimer's, to wire money to claim a prize (2023). Huddleston said: "That was a wake-up call for me. If you have any cognitive decline, you don't see those red flags anymore."

T-Mobile offers users Scam Shield, an app that protects users and lets them change their number as needed (T-Mobile, 2023). To retain users in their network, some carriers offer users free devices. The devices collect user data from other personal devices. While telecom companies and federal agencies in the US try to thwart scams, scammers develop new attacks. Users must therefore learn how to protect themselves.

Review of Research

Scammers use technical, social, and physical methods of social engineering to trick victims into revealing sensitive information (Salahdine, 2019). Examples of a technical attack include creating a fake banking website and requesting credit card information, or creating a virus pop-up alerting the user of a computer virus (which doesn't exist) and they must call the scammer to fix it. A social attack could be calling as tech support to fix a computer bug, and connecting to the computer to steal information. Examples of physical attacks include walking into locked buildings behind people with access, or dumpster diving through ineffectively destroyed documents.

Truecaller, a spam call blocking app, estimates scammers have made nearly $40 billion in 2022 from nearly 70 million victims (Truecaller, 2022). The average reported loss has increased since 2021, and the percentage of people reporting being scammed has increased. Rachit Agarwal from Beebom details alternative apps to Truecaller that have been developed, such as T-Mobile's Scam Shield and Robokiller. Each has unique issues, including missing legitimate calls due to inaccurate spam filtering (Agarwal, 2022). Intuition is insufficient to discern scams. Scammers are quickly improving at posing as real companies, coworkers, and family to steal information and money. Machine Learning can detect scams so Americans don't have to waste time engaging with them.

Li et al. (2018) developed a mobile app called TouchPal, which collects minimal amounts of data from calls and requires users to tag calls. Kubilay et al. (2023) created an experiment analyzing the public's ability to classify scams from genuine messages. They noticed age and higher than secondary education were positively correlated with correct identification. Mahoney analyzes the "Do Not Call List" and attributes its failure to scammers' ability to "spoof" their

numbers and make calls from overseas (Mahoney, 2015). Scammers disregard the Do Not Call List and aren't afraid to get caught. Many works in this field attempt to analyze or develop specific solutions for techniques scammers use. These solutions have flaws that scammers can exploit. Although developers can respond, this paper argues that this conflict is not solvable for developers.

History of Scams

Scams have existed long before telephones or email. 16th century Spanish criminals used trade directories to mail contacts in richer countries (Okosun, 2022). They would send letters about huge stashes of gold or money, but they had a loved one held hostage. After getting the victim's financial help, the scammer would send information about the money's location. The Nigerian prince scam is a similar scam that exists today. Both scams praise the victim's character, which selected them to receive the money. All scams require victims to keep information private. Through the scam's evolution, the general principles of an enticing reward and a call for help still remain today.

TeamViewer

Most scams involve scammers connecting to the victim's computer through remote access. TeamViewer allows the remote user to control the other person's screen. Legitimate companies use this for tech support and software setup. However, scammers trick victims into downloading TeamViewer and allowing them connection, letting the scammer access sensitive information. The remote user can blank the screen and disable input, which was implemented for security purposes in legitimate workplaces, but scammers misuse it to steal information.

TeamViewer recognized that scammers use their software and implemented preventative security measures. Computer can't be controlled unknowingly. A textbox will appear if someone is controlling your computer. This prevents scammers from lingering after a victim closes the connection with the scammer. Also, passwords are regenerated each time users open TeamViewer, preventing scammers from saving victims' passwords. File transfers and other encryption protocols require confirmation. Users can create a block list. Commercial users must purchase TeamViewer subscriptions. Blanking the screen and blocking remote output are paid features(Jackins, 2023).

Romance Scams

In romance scams, scammers pretend to initiate relationships with victims to steal money. Scammers use fake profiles on dating sites with stolen pictures and fake identities. Monica Whitty, in Volume 21 of the Cyberpsychology, Behavior, and Social Networking journal claims that middle-aged people are more susceptible to romance scams because they are more likely to seek out partners on dating sites compared to other age groups (Whitty, 2018). Women fall victim to these scams more often than men, and those with less cybersecurity education are more susceptible.

Incognia, a company which solves fraud and authentication challenges across industries, notes that dating apps like Bumble, Tinder, Hinge, OkCupid, and HER have required ID verification to confirm the new users' identity (Incognia, 2024). This could be through a government ID, a matching selfie, or a third-party verification solution. This creates a conflict of interest for the companies, which are scam averse, but also want low barriers of entry for regular users. Some apps implement backend profile approval processes to ensure profile legitimacy.

This is automated using machine learning, but can be checked by employees. Apps verify location with the phone's GPS coordinates.

Other Impersonation Scams

Regardless of technologies implemented to prevent scammers, scammers will find new social engineering tactics. Some scammers impersonate the government, and tell the victim they owe taxes and will be arrested if they don't pay. Baiting is where scammers offer a large reward in exchange for money, such as the cash flip scam. Scammers convince victims they can turn money into more money, usually $100 into $1000. They will provide evidence in fake testimonials to entice the user. Once scammers receive the initial money, they will disappear or block the victim. Scammers create urgency in the victim, whether to avoid punishment or convincing them the offer has a time limit. This decreases the victim's likelihood of talking to others who might alert them of the scam.

UPS delivery scams are common while awaiting a package. A text message tells the victim the delivery needs to be changed, and requires confirmation by clicking a link, as UPS displays on their scam information page (UPS, 2024). These links are illegitimate sites with random character URLs, or a UPS URL with extra characters. These scams call for action by telling the victim their package will be sent back without action. UPS's website lists all legitimate phone numbers and email addresses.

Phishing

Phishing is a common type of scam where scammers will send emails or other messages claiming authority and request personal information. Sometimes these are distinguishable by the

sender email being outside the company domain (ex: a claimed US government employee requesting other employees to change their password, but the email is from a hotmail account). More recently, scammers can spoof a domain name on email addresses, so accurate domain names do not necessarily mean legitimate emails. These emails typically contain a threat and a call to immediate action. Common signs of phishing include spelling or grammatical mistakes, a poor signature, a phone number from the wrong area code, or an offer too good to be true.

Email clients like Gmail have implemented advanced security settings to make phishing attempts more obvious to potential victims (Google, 2024). This includes protection from attachments that are uncommon for the domain. Clicking on attachments from unknown domains gives a warning message to ensure they trust the sender. Shortened links and images are identified and scanned, and Gmail also gives a warning for links that send you outside the domain. Gmail also offers protection against spoofing domain names, and unauthenticated emails appear with a question mark by the sender's name.

Methods of Scam Prevention

Hanaa Alghamdi's attempt to educate potential victims on scams was to create a phishing quiz app for mobile devices (Alghamdi, 2017). The app gives you a pre-test with twelve questions asking the user to identify a phishing scam or a legitimate form of communication. It gives the user a risk level and suggests the user areas they can learn more about through the learning resources center. The user can then take a posttest to evaluate their learning through the modules. This method did not show any significant risk decrease on the post test, which shows that although education is a good idea, it alone will not make victims immune from scams.

Fraud has a very low rate of reporting, which can be attributed to several factors, including the belief that nothing can be done, and the stigma and shame associated with victimization. The victim's attitude towards police, previous victim history, opportunity for compensation, and time and effort involved in reporting the scam can attract or deter a victim from reporting the scam. Those who felt responsibility for becoming a victim were less likely to report the scam. Victims who lost more money were more likely to report the scam.

Some actions that scammers take that lead to victims reporting them include money requests. One victim said, "Early on he asked for phone vouchers which I sent. Two weeks ago he asked for $41,000. I knew it was a scam." The payment type also influenced victims to report scammers, saying "He had me buy him iTunes till I caught on and sent him used ones that didn't work." Others were clued in by threats, saying "He has threatened my life and my children's," and even "She said that she was willing to commit suicide if I didn't pay her the money." Other victims realized their mistakes when scammers were not paying money back when promised, they were told by a third party (bank, police, family member, etc.), or searching about the fraud on the internet.

Scambaiters

Another group that is important to stopping scammers are called scambaiters. These are usually internet personalities who make content on websites like YouTube and Twitch where they call a scammer and attempt to waste as much of their time as possible and possibly expose the scammer's personal information. Notable scambaiters include Kitboga, Jim Browning, Scammer Payback, and Trilogy Media. These scambaiters use voice modulation software to

sound like an elderly man or woman and can spend upwards of ten hours across multiple days wasting a scammer's time.

While this is effective to stop one scammer for a period of time, dozens of scammers could be working in the same call center, and hundreds of these call centers are operating daily. Some of these scambaiters look to involve local authorities to shut down the call centers, but this is very difficult to do. Local authorities will ask for evidence from the scambaiters of people being scammed, which is difficult to prove. Authorities don't have proper protocol on how to punish scammers, which usually results in minimal punishment, the money made being kept, and a group of scammers setting up a new call center again somewhere else.

Scambaiting is very dangerous for those involved, because they can easily become victims to the scammers if they aren't careful. In the same way that potential victims can recognize a scam, some scammers can recognize a scambaiter and try other approaches to steal a scambaiter's information. Scammers may be able to get your location or IP address and target you through attacks like swatting. Because there is little legislation on scambaiting, the legality of scambaiting is questionable, and certain scambaiting techniques could put scambaiters in legal trouble.

Legislation

The US has enacted the Computer Fraud and Abuse Act, which protects against accessing digital information without authorization (U.S. Department of Justice, 2022). This is defined as the defendant not being authorized to access the computer by anyone with authority to grant authorization, and the defendant knowingly accessing without authorization. The act protects against exceeding authorized access, which is defined as using a protected computer divided into

areas in a computational sense. The defendant must be authorized to access some areas, but not others, and the defendant must have knowingly accessed an area they were not authorized to access. Given these laws, it is difficult to deem a scammer as breaking these laws, as a scammer could argue that when a victim allows access to their computer, they are authorizing them to use any part of their computer. The legality of scambaiting is also called into question, especially if the scambaiter deletes files from the scammer's computer.

Scammers are competing with local governments to remain hidden or bribing them to let them stay in business. In Nigeria, 40% of people live below the poverty line, and the gap between rich and poor is so large that the only efficient way to make money is through scamming. Some scammers justify their actions by referencing the slave trade and colonial rule, and consider it "taking back what belonged to our forefathers". Scammers learn that to stay untouchable they need the right social and political connections to those in power, and they won't be held accountable.

Banks and Money Transfer

Some banks have implemented fraud detection systems to protect victims from scammers (Repin et al, 2017). These banks perform fast processing, which is real time and does not require deep analysis. This includes common check rules for all bank accounts, profiled check rules, which are rules specific to your type of bank account, and a probabilistic logic model. This model learns payment characteristics for a client, so longtime bank users get more protection, and the algorithm is more suspicious of newer users. If new payment patterns are detected, a suspension and detailed analysis will take place. The algorithm will run through fraud scenarios,

and the account owner will be notified. If fraud is not detected, the algorithm will account for the new type of payment. Otherwise, corrections will be made.

In order to subvert bank safeguards, scammers use money laundering, which is making lots of money and falsely representing it as generated from legitimate sources. The money is obtained through various victims, moved around through people called money mules, and finally transported to the scammers (Stapleton, 2023). If the scammers live outside the US, money mules could be people in on the scam or victims who are promised some of the money they help send overseas. Scammers might require them to send the money as cash overseas with other items in boxes to ensure security cannot detect it.

Scammers also use gift cards as a money medium, where they request victims to buy hundreds of dollars of gift cards from the store and read the codes to the scammers. They might use these cards as their own, liquidate them to get the money directly, or even create accounts with the cards loaded and sell the accounts. Retail employees are trained to notice someone buying large sums of gift cards and ask them questions about what they are using the gift cards for. On gift cards, they recommend the customer keep their receipt and use the cards quickly to prevent scammers accessing them.

Conclusion

Though companies will advertise their products as “scam-proof”, there is no way to fully make a product scam-proof. Along with law enforcement being relatively ineffective, with lots of documentation and evidence required to make any convictions, as well as it being almost impossible to recover lost money, scams will not go away. Scammers are crafty and innovative. With any blocker, effective scammers will find a new way around it. Although it was believed

that education can prevent potential victims from falling for scams, this will not entirely prevent people from falling for scams. People need to be alert and question the legitimacy of all telecommunication. Another false perception of scams is that there is always an obvious sign, such as a misspelling or poor grammar. Efficient scammers will begin to use AI tools to correct these obvious signs, requiring potential victims to be more careful. Researchers should next look into ways to build effective reporting mediums. If a text message or phone call is labeled “Scam Likely”, users are much less likely to interact with it. If other methods cannot detect the scam, other users reporting the scam could be an effective option. More research could be done in understanding and fixing the inefficiencies of law enforcement in taking action against scammers. This is difficult to research and would require several case studies, as data on police reports is rarely released, usually for the scammer’s privacy. If police release this data, scammers may catch on to the techniques the police use. The findings in this paper could also be applied to computer viruses and malware, where designers of malware will continue to evolve and find ways around antivirus programs.

References

Agarwal, R. (2018, September 18). Top 10 Truecaller Alternatives You Can Use. Best Truecaller Alternatives for Android and iPhone (2022). beebom.com/truecaller-alternatives

Alghamdi, H. (2017) Can Phishing Education Enable Users To Recognize Phishing Attacks?. Masters dissertation, Technological University Dublin, 2017. doi:10.21427/D7DK8T

Buxton, O. (2023, Dec. 14). Cash app scams and how to detect them. LifeLock. lifelock.norton.com/learn/fraud/cash-app-scams#:~:text=Cash%20flipping%20scams%20on%20Cash,and%20X%20(formerly%20Twitter)

CBS Interactive. (2023, April 10). How to protect elderly parents from financial scams. CBS News. cbsnews.com/news/money-scams-elder-fraud-abuse

Commonwealth of Australia. (2020, July 20). The total impacts of fraud. Commonwealth Fraud Prevention Centre. counterfraud.gov.au/total-impacts-fraud#:~:text=Human%20impact&text=Fraud%20can%20have%20a%20devastating,opportunities%20for%20individuals%20and%20businesses

Dema, A. (2023, Aug. 28). App Store stopped more than $2 billion in fraudulent transactions in 2022. Apple Newsroom. apple.com/newsroom/2023/05/app-store-stopped-more-than-2-billion-in-fraudulent-transactions-in-2022/#:~:text=For%20example%2C%20with%20Apple%20Pay,714%2C000%20accounts%20from%20transacting%20again

Google. (2024). Advanced phishing and malware protection. Google Workspace Admin Help. support.google.com/a/answer/9157861?hl=en

Halladay, K. (2022, October 6). How do phones identify potential spam calls?. Built In. builtin.com/machine-learning/spam-calls

Help with scams, Spam, and fraud. T-Mobile. (2023). t-mobile.com/support/plans-features/help-with-scams-spam-and-fraud#:~:text=call%20is%20about!-,Scam%20Shield%20app,Store%20or%20Apple%20App%20Store

Higgins, M. (2023, Oct. 20). What is scambaiting? Everything you need to know. NordVPN. nordvpn.com/blog/scambaiting

Incognia. (2024). Online Dating Identity Verification. incognia.com/use-case/online-dating-identity-verification

Jackins, T. (2023, Oct. 31). TeamViewer Free Version Limitations. Splashtop. splashtop.com/blog/teamviewer-free-version-limitations

Kubilay, Raiber, Spantig, Cahlíková, and Kaaria (2023, Feb. 2). Can You Spot a Scam? Measuring and Improving Scam Identification Ability. SSRN. papers.ssrn.com/sol3/papers.cfm?abstract_id=4344411

Li, Xu, Liu, Ren, Wu, Cao, Zhang, Yu, and Song (2018, July 26). A Machine Learning Approach to Prevent Malicious Calls over Telephony Networks. *2018 IEEE Symposium on Security and Privacy*. IEEE Xplore. ieeexplore.ieee.org/abstract/document/8418596

Mahoney, M. (2015, Nov.). Dialing Back: How Phone Companies Can End Unwanted Robocalls. Consumers Union. advocacy.consumerreports.org/wp-content/uploads/2015/02/Dialing-Back-Complete-Report-11.16.2015.pdf

Mayfield, J. (2023, Feb. 23). New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022. Federal Trade Commission. ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

Okosun, O., and Ilo, U. (2022). The evolution of the Nigerian prince scam. *Journal of Financial Crime*, 30(6), 1653–1663. https://doi.org/10.1108/jfc-08-2022-0185

Repin, M., Mikhalsky, O., & Pshehotskaya, E. (2017). Architecture of Transaction Monitoring System of Central Banks. *Proceedings of the International Conference "Actual Issues of Mechanical Engineering"* 2017 (AIME 2017). https://doi.org/10.2991/aime-17.2017.106

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 89. doi.org/10.3390/fi11040089

Stapleton, C. (2023, July 22). What methods are used to launder money?. Investopedia. https://www.investopedia.com/ask/answers/022015/what-methods-are-used-launder-money.asp

Stop Unwanted Robocalls and Texts. Federal Communications Commission. (2024, Jan. 30). fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts#:~:text=Under%20the%20Truth%20in%20Caller,to%20%2410%2C000%20for%20each%20violation

Truecaller. (2022). Truecaller insights 2022 U.S. Spam & Scam Report. Truecaller Blog. truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report

UPS. (2024). Protect Yourself From Fraud and Scams. UPS. ups.com/us/en/support/shipping-support/legal-terms-conditions/fight-fraud.page

U.S. Department of Justice. (2022, May 19). 9-48.000 - Computer Fraud and Abuse Act. Justice Manual | 9-48.000 - Computer Fraud and Abuse Act | United States Department of Justice. justice.gov/jm/jm-9-48000-computer-fraud

Whitty, M. T. (2018). Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 105–109. doi.org/10.1089/cyber.2016.0729

Wilson, Hassan, Khor, Sinnappan, Abu Bakar, and Tan (2023). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime*. https://doi.org/10.1108/jfc-06-2023-0151