The Eternal Struggle between Social Engineering Attackers and Their Targets

An STS Research Paper

presented to the faculty of the

School of Engineering and Applied Science

University of Virginia

by

Anmol Sandhu

March 14, 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 Assignments.

Anmol Sandhu

STS Advisor: Peter Norton

The Eternal Struggle between Social Engineering Attackers and Their Targets

Computer users are susceptible to a variety of attack vectors, including malicious code, unpatched vulnerabilities, and weak encryption. Research is constantly being performed to make computers more robust against these types of attacks from malicious actors. Companies and government agencies strive to improve the security of their own devices and of the products or services they provide. The most common type of cyberattacks are social engineering attacks, such as phishing scams (Klimburg-Witjes & Wentland, 2021). In such an attack, the attacker seeks to bypass security features by exploiting vulnerabilities in user psychology, such as trust or the hope of a large reward (Salahdine & Kaabouch, 2019). In a common kind of attack, the victim receives a phone call from a supposed wealthy foreigner who purports to offer a large sum of money and needs their banking information to wire it. In such an attack, the bank's security systems against malicious code or hacking do not matter. If the target grants the scammer the requested information, the attack succeeds. Victims' hope for promised money can overcome their caution. Variations of this scam persist today. Training can prepare users to resist social engineering attacks. Like other types of cyberattacks, social engineering attacks evolve to adapt to and overcome evolving defenses. Engaged in this evolving arms race are attackers, targets, security system vendors, and government agencies. Social engineering attacks exploit users' cognitive heuristics and hopes.

Review of Research

There has been considerable research already done to determine how social engineering attacks exploit their targets (specifically individuals), the most prominent being Montañez et al.

(2020). This paper provides a framework to understand “human cognition through the lens of social engineering attacks.” While not the first paper to attempt to explain social engineering attacks, it is the first to provide such a framework. Social engineering attacks can bypass the security features programmed into devices by relying on vulnerabilities in human psychology such as trust or the promise of a large reward (Salahdine & Kaabouch, 2019). There tends to be a general agreement in existing research that human nature is a weakness that is readily exploited in these types of attacks. However, there is some disagreement on whether the responsibility for the attack is being properly attributed. Placing the blame on human nature creates an idea of a “deficient user” in discourse (Klimburg-Witjes & Wentland, 2021). This idea gives an institution a way to avoid responsibility, “Our findings suggest a redistribution of institutional responsibility to the individual user through three distinct social engineering story lines—'the oblivious employee,’ ‘speaking code and social,’ and ‘fixing human flaws.’” A possible solution is to change how the discussion on social engineering attacks is done, “we propose to open up the discourse on social engineering and its inscribed politics of deficit construction and securitization and advocate for companies and policy makers to establish and foster a culture of collective cyber in/security and corporate responsibility.” There is definitely a strong argument that the “deficient user” is an accurate term, designed to pass the buck. However, the user remains a possible attack vector and while “deficient” might not be the right term to describe it, human nature must be understood when designing or improving security systems.

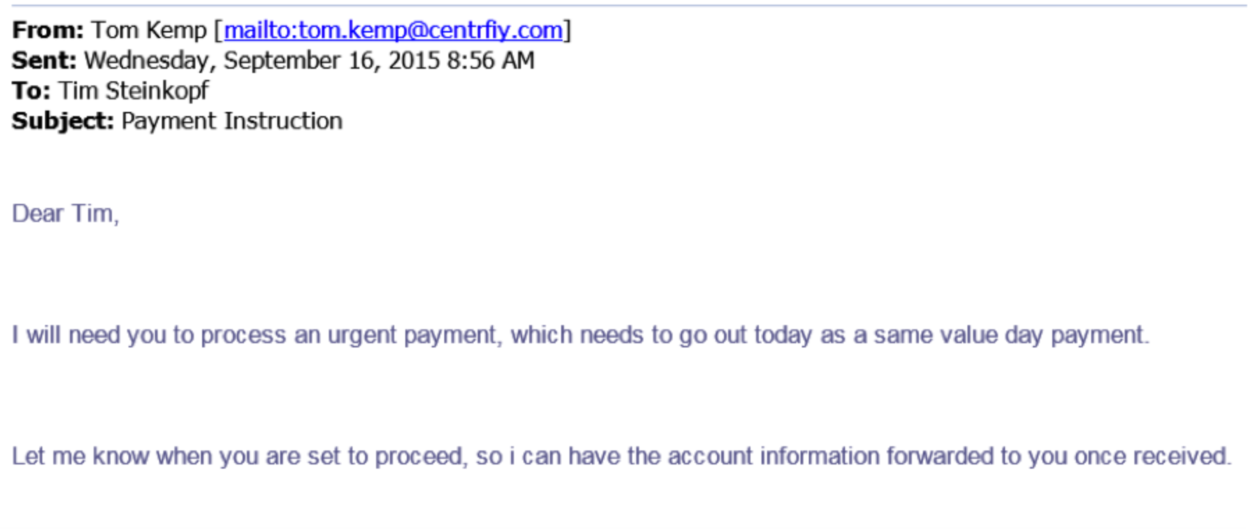
Attackers

Unlike the other participant groups, attackers are not willing to share their stories or motivations. This somewhat complicates trying to understand them, beyond a general idea of them wanting useful information. It also made getting direct quotes and sources from them difficult. However, many victims and news agencies report on social engineering attacks and from these reports, it is possible to understand the attackers' agenda. By far the most common type of social engineering attack is phishing. There are, broadly speaking, two types of phishing attacks: wide and spear. Wide phishing attacks, as the name suggests, focus on casting a wide net in hopes of targeting as many victims as possible. In either case, the attacker does not particularly care which of the targets responds, so long as a few do so. From these few responses, attackers can get valuable information about their targets. In spear phishing, the attacker spends significant time gathering publicly available information about their target. From this, they can craft highly personalized attacks meant only to target that specific person. These targets are usually people in some privileged position who have access to much more valuable information than the average person or are significantly wealthier than average. Since these attacks are personalized, they have a higher chance of success. Some tactics used include inducing a false sense of urgency, pretending to be a figure of authority, and promising a reward in exchange for information. The first and second of these are especially effective. Four of the five largest phishing attacks in history involved the attacker pretending to be the CEO or another high-level executive and ordering employees to transfer money (Check Point Software, n.d.). The fifth of these attacks, and the largest of them all, was slightly different since the attacker pretended to be Quanta, a company that works with Facebook and Google, and created fake invoices, tricking the companies into paying them $100 million dollars in total (Check Point Software, n.d.). Though this was slightly different, the general idea of pretending to have some kind of authority and requesting money is still there and is clearly highly effective. Imitating a figure of authority has become so popular that it has received its own designation: CEO fraud. Even in smaller attacks, pretending to be someone with authority over the target is a common tactic since it requires little technical expertise and creates a sense of urgency in the target.

The other popular tactic is to promise a reward to the target. Being given such an incentive, the target is more likely to fall for the attack. There are numerous other strategies that attackers use to take advantage of their victims, such as using a fake URL, but these are some of the most successful ones. A common trend in these methods is their usage of the target's heuristics and hopes. Most people are not going to question a somewhat convincing order from their boss, and everyone wants easy rewards. This is combined with exploiting a "fear of missing out" or FOMO to further incentivize targets to comply. Attackers know this and carefully design their attacks to exploit these vulnerabilities. If it were not for the mental shortcuts that we as humans naturally make, these scams would not be as effective, as most phishing attempts have very clear signs of their deceit. Figure 1 is an excellent demonstration of this. This is a screenshot of a real phishing attack. It utilizes a false sense of urgency and fake authority to compel the target to give money to the attacker. The name of this company was Centrify, but the email address says "centrfiy.com" (Dyckman, 2017). A human is going to have difficulty recognizing that, especially with the urgency from someone who is pretending to be part of the company. These types of phishing attacks are effective on companies of every size, from smaller ones like Centrify to massive corporations like Facebook and Google.

Figure 1

Screenshot of CEO fraud phishing attack



From: Tom Kemp [mailto:tom.kemp@centrfiy.com]
Sent: Wednesday, September 16, 2015 8:56 AM
To: Tim Steinkopf
Subject: Payment Instruction

Dear Tim,

I will need you to process an urgent payment, which needs to go out today as a same value day payment.

Let me know when you are set to proceed, so i can have the account information forwarded to you once received.

Targets

There are two broad categories of targets: individuals and organizations. Both can fall vulnerable to attacks due to human nature seeking shortcuts and rewards. When individuals are targeted, it is often a wide attack designed to go as far as possible and gather the maximum number of victims. Through sheer probability, at least a few are going to fall for the attack, so even if the majority do not, it is no concern to the attacker. Certain individuals can be specially targeted, but they are usually those with close ties to an organization. A normal person is unlikely to be targeted in such a way. There are many different types of targets, and each can fall victim to an attack. Some major categories are naïve or hopeful users and ironically tech-savvy users. The naïve are the more understandable category. The Australian government has gathered real stories from victims to keep their citizens better informed about potential scams. Many of the stories are very clearly of attackers preying on people's hopes and dreams, such as "Investment scam: I lost $50,000 in fake online trading" and "Dating and romance scam: my brother lost $20,000 looking for love" (Australian Competition and Consumer Commission, 2019). Both these stories are real events from one or more victims, which some information omitted to preserve privacy. In both cases, the attacker relied on a person's desire for something, be it money or love, to convince the target to give them a large amount of money. As mentioned earlier, FOMO is a major part of the target's psychology. A chance at making guaranteed returns or finding happiness is motivating, but the true motivator is the fear that this opportunity will pass them by. People are not driven completely by logic. They can fall vulnerable to their desires and not truly consider that the offer they are receiving is too good to be true.

The more confusing category of users are the tech-savvy. It seems almost paradoxical that tech-savvy users are more likely to fall victim to these attacks, but interestingly 34% of Gen Z admitted to being phished versus only 12% of Baby Boomers, though the older generation does lose more money per attack (National Cybersecurity Alliance, 2022). There are two primary reasons for this supposed paradox. Firstly, Gen Z users and tech-savvy users in general spend considerably more time on the internet than others and thus are exposed to many more scams (National Cybersecurity Alliance, 2022). It would make sense then, that they fall victim to more scams. Secondly, just because these users regularly use technology does not inherently make them any wiser to the tactics that attackers might use. They can be just as gullible as anyone else and possibly even more so due to their self-confidence. The former of these explanations is a popular explanation given in articles and studies and makes sense, simply due to laws of probability. Interestingly, while there were several articles and studies that espoused potential explanations for this paradox, there was little insight from Gen Z victims in them. However, there were posts from such victims on Reddit. The posts there, while not too numerous, show a common trend among victims: they believed themselves to be resistant to tech scams as seen in "considered myself pretty savvy with combatting scams" (peopleloveourpatties, 2023) and "As an 18 year old girl who grew up social media savvy I have no excuse for getting fooled" (Reddit,

2023) and “I consider myself internet and somewhat tech savvy” (moonchilleddd, 2023). These quotes seem to indicate that the latter possible explanation for the paradox holds merit. Gen Z appears to consider themselves more resistant to tech-based scams and may not do their due diligence when they face a scam, ironically making them more vulnerable to such a scam. This can be applied to tech-savvy users in general, not just Gen Z, as seen here where the user was not explicitly Gen Z, “ig i wasn't aware of how good scammers are these days or i thought i that i was too savvy to fall for one” (st15rm_, 2023). There has not been a complete study investigating tech-savvy victims and their stories, as far as my search could find, and so this might be a meaningful thing to research in the future to come to a more conclusive explanation for this paradox. However, the posts from victims do suggest that overconfidence is a likely explanation.

Beyond individuals, organizations are the other type of target. There is an additional weakness to be considered when thinking of people in an organization: susceptibility to false authority. False authority is a consistently effective tactic to get targets to comply. This plays into the heuristics of the human mind. Most employees are not going to deeply consider an order that appears to be from their boss, they will simply try to complete the instruction. Unfortunately, organizations are somewhat hesitant to release images of phishing emails. Figure 1 was the only real-life example easily available. There were other examples, but they were mostly fake examples designed for training or just for illustrative purposes. However, organizations do often release apologies when they are the victims of phishing attacks, explaining what was stolen and that they intend to do better, giving insight to their thought processes. In 2016, Snapchat and Seagate Technology were both victims of phishing attacks that cost them their employees’ W-2 data. Their official responses were “We’re a company that takes privacy and security seriously.

So, it’s with real remorse–and embarrassment–that one of our employees fell for a phishing scam and revealed some payroll information about our employees. The good news is that our servers were not breached, and our users’ data was totally unaffected by this. The bad news is that a number of our employees have now had their identity compromised. And for that, we’re just impossibly sorry” (Trendmicro.com, 2016) and “When we learned about it, we immediately notified federal authorities who are now actively investigating it. We deeply regret this mistake and we offer our sincerest apologies to everyone affected. Seagate is aggressively analyzing where process changes are needed and we will implement those changes as quickly as we can” (Krebs on Security, 2016). These attacks both operated on the same tactic that was mentioned in the attacker section, where the attacker pretended to be the CEO of a company to get useful information. While organizations give these apologies, they are still hesitant to release much more information, as Seagate refused to give specific data about how many employees were affected to anyone but federal authorities (Krebs on Security, 2016). Additionally, Google and Facebook, after dealing with the largest phishing scam in history, both gave short press statements that addressed the situation but failed to offer meaningful improvements to their defense against social engineering attacks. These statements were “We detected this fraud and promptly alerted the authorities. We recouped the funds and we’re pleased this matter is resolved” from Google and “Facebook recovered the bulk of the funds shortly after the incident and has been cooperating with law enforcement in its investigation” (Huddleston, 2019). While organizations would obviously prefer that data breaches never occur, it can be surmised that they face a serious problem when dealing with social engineering attacks. Keeping data secure and patching existing vulnerabilities is ultimately fruitless if a careless employee with the right information falls victim to a phishing attack. Whenever an attack is successful, companies insist that they are making improvements, but considering the frequency of data breaches, it does raise concern as to what their employees are being taught regarding anti-phishing techniques. This further highlights the danger of mental heuristics in social engineering attacks. Employees should follow instructions from their boss, but they often do not do the necessary work to make sure that an order is truly from their boss.

Law Enforcement

The last participant group to discuss are law enforcement agencies. In essence, these agencies are another type of organization, but with significantly more data and connections than a typical one. Naturally, this also makes them a bigger target. Furthermore, they also have the responsibility of protecting its citizens and organizations from social engineering attacks. Therefore, law enforcement works to understand potential vulnerabilities in personal and national security and works to protect against such threats. One of the ways they do this is by creating policies and regulations. The Securities and Exchange Commission's (SEC) policy states that "Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its Nature, scope, and timing; and Impact or reasonably likely impact" (Securities and Exchange Commission [SEC], 2023). The goal of this policy is clearly to encourage transparency when dealing with cyberattacks, with some exceptions for sensitive data, "A registrant may delay filing as described below, if the United States Attorney General ("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public safety" (SEC, 2023). This increase in transparency is designed to both hold companies accountable for data breaches and to keep the public informed so they can hopefully be better prepared. Furthermore, the government also takes actual data breaches very seriously. In the Google and Facebook phishing attack, the attacker was a Lithuanian citizen, normally rendering him immune from American prosecution. Additionally, he had placed the money he stole in bank accounts around the world, making it nearly impossible to recover the money (U.S. Attorney's Office, Southern District of New York, 2019). However, the government was able to arrest him, after which Geoffrey Berman, a US attorney, said, "As Evaldas Rimasauskas admitted today, he devised a blatant scheme to fleece U.S. companies out of $100 million, and then siphoned those funds to bank accounts around the globe. Rimasauskas thought he could hide behind a computer screen halfway across the world while he conducted his fraudulent scheme, but as he has learned, the arms of American justice are long, and he now faces significant time in a U.S. prison" (U.S. Attorney's Office, Southern District of New York, 2019). Approximately half the money was recovered (Check Point Software, n.d.). The government clearly has the tools to investigate attacks of this scale and by showing the lengths they are willing to go to in pursuing attackers, they clearly hope to dissuade potential attackers from even attempting such schemes in fear of retribution. This also serves to reinsure the public, ideally fostering greater trust in the government. Furthering this trust is also accomplished by providing resources to keep citizens safe from attacks. Both the NSA and FBI have webpages where they explain what phishing and spoofing attacks are and how to stay safe. The FBI also says, "If you believe you are a victim of an online scam, contact your local FBI office. Victims are also encouraged to report the incident to the FBI's Internet Crime Center at www.ic3.gov" (Federal Bureau of Investigation, 2021). By offering guidance, encouraging reporting, and vigorously pursuing attackers, law enforcement agencies improve users' security and discourages attackers, reducing the number of social engineering attacks and their success rates.

Conclusion

Beyond the participant groups mentioned here, there are other groups that have an interest in social engineering attacks, such as security providers like DUO. Social engineering attacks are a constantly evolving field with many participants. The three primary participants groups are the attackers, the targets, and law enforcement. Each group's agenda interacts with or conflicts with the other groups. Attackers want to gain valuable data or money from their targets, targets want to keep their data secure against attacks, and governments want to prevent attackers from succeeding. The success of social engineering attacks is largely based on the exploiting of the heuristics and hopes of the targets. Humans are not completely logical creatures and often do not put in the necessary work to ensure that communications are legitimate. They may take mental shortcuts in verifying the validity of a text or email they received and simply assume it is valid, ignoring a sign that it was not. Furthermore, FOMO plays a large role in the design of social engineering attacks. By promising their targets a reward, but giving it a false sense of urgency, social engineering attacks make them even less likely to validate the communication they receive, increasing the attack's success rate. Attackers and governments understand this and work to use this knowledge for their own agendas. Individual targets are less likely to be aware of these weaknesses, thus making them more vulnerable. Organizational targets are also vulnerable to these attacks, as at its core, an organization consists of individuals with the same weaknesses as independent targets. Since social engineering attacks rely so heavily on human nature, it is difficult to design policies that prevent them. However, always doing due diligence when encountering communications that seem strange would be an excellent way to reduce their success. Social engineering attacks will always be a problem as there is no way to design a system for humans that does not have the weaknesses of human nature, but always being cautious and skeptical will massively improve security.

References

Australian Competition and Consumer Commission. (2019, August 15). *Scam victims tell us their stories*. Www.scamwatch.gov.au. https://www.scamwatch.gov.au/protect-yourself/real-life-stories/scam-victims-tell-us-their-stories

Dyckman, C. (2017, July). *Beware of This Email: The boss email scam that could cost your company thousands*. Www.trustbgw.com. https://www.trustbgw.com/blog/2017/07/28/boss-email-scam

Federal Bureau of Investigation. (2021, June 22). *FBI Tech Tuesday: Protecting Yourself from Spoofing and Phishing Scams*. Federal Bureau of Investigation. https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-protecting-yourself-from-spoofing-and-phishing-scams

Huddleston, T. (2019, March 27). *How this scammer used phishing emails to steal over $100 million from Google and Facebook.* CNBC; CNBC. https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

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. Web of Science

Krebs on Security. (2016, March 6). *Seagate Phish Exposes All Employee W-2's — Krebs on Security*. https://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/

Montañez, R., Golob, E., & Xu, S. (2020). *Human Cognition Through the Lens of Social Engineering Cyberattacks. Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.01755

moonchilleddd. (2023, December 14). *I've (27M) always considered myself internet savvy but yesterday I got scammed.* https://www.reddit.com/r/Scams/comments/18im5yn/ive_27m_always_considered_myself_internet_savvy/

National Cybersecurity Alliance. (2022). *Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022.* https://20740408.fs1.hubspotusercontent-na1.net/hubfs/20740408/CYBSAFE-Oh%20behave%20report%202022-220927%20MS%20-%20V1.pdf

peopleloveourpatties. (2023, April 19). *I'm a Gen Z who fell for a USPS scam* 🤦‍♀️. https://www.reddit.com/r/Scams/comments/12scrne/im_a_gen_z_who_fell_for_a_usps_scam/

Reddit. (2023, August 4). *"I got tricked by a fake check scam. I'm only 18 and it lost me the majority of my savings. I'm devastated."*.

https://www.reddit.com/r/Scams/comments/15hmltt/i_got_tricked_by_a_fake_check_scam_im_only_18_and/

Salahdine, F., & Kaabouch, N. (2019). *Social Engineering Attacks: A Survey*. Future Internet, 11(4), 89. Web of Science

Securities and Exchange Commission. (2023). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure [Review of Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure]*. Www.sec.gov. https://www.sec.gov/files/rules/final/2023/33-11216.pdf

Snapchat Employees Fell for a Phishing Scam, Here's How They Responded - Security News. (2016, March 1). Www.trendmicro.com. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/snapchat-employees-fell-for-a-phishing-scam-here-s-how-they-responded

st15rm_. (2023, December 30). *i fell for a record scam*. https://www.reddit.com/r/Scams/comments/18u2l48/i_fell_for_a_record_scam/

The Top 5 Phishing Scams of all Time. (n.d.). Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/

U.S. Attorney's Office, Southern District of New York. (2019, March 20.) *Lithuanian Man Pleads Guilty To Wire Fraud For Theft Of Over $100 Million In Fraudulent Business Email Compromise Scheme*. Www.justice.gov. https://www.justice.gov/usao-sdny/pr/lithuanian-man-pleads-guilty-wire-fraud-theft-over-100-million-fraudulent-business