

SOCIAL ENGINEERING STUDY:  
EXAMINING THE INFLUENCE OF CHOICE ARCHITECTURES ON TRUST AND  
PASSWORD PRIVACY

By

JEREMY DAVID BERNICK

---

A Thesis Submitted To The Honors College  
In Partial Fulfillment of A Bachelor's Degree in  
PPEL

THE UNIVERSITY OF ARIZONA

M A Y 2 0 2 0

Approved By:

---

Dr. Brandimarte  
Department of Management & Information Systems

## **Abstract**

Social engineering is a popular and dangerous method of attack in computer security and privacy studies. Even with the public rise of privacy education and computer security literature, there still remains a gap in the human elements of security. In this study, researchers from the University of Arizona designed an experiment to detect whether individuals would give away personally sensitive information to a stranger and whether the presentation style of the attack would influence the propensity of an individual would give that information away. More data will have to be collected in order to determine whether the presentation of choice in a social engineering attack influences the victim's likelihood to trust and give away information.

## **Introduction**

Online privacy is quickly becoming one of the most sought after rights in the 21st-century. As cryptography, privacy education, and policy continue to improve, the need for a better understanding of the behavioral and psychological antecedents of trust and security are urgent (Rosenzweig). Without patching this part of our own biological software, trust and the human element of security will continue to fail even under the most rigorous security systems. In our research study, we observe the intersections between social psychology, choice behaviors, privacy, and whether these decisions to disclose personally identifiable information are affected by the attacker's presentation of choices.

The practice of convincing individuals to give away sensitive information is better known as social engineering. It is often said that humans are the weakest link in regard to information protection and the study is designed to examine how format of the survey (online or on paper), perceived security of data transmission, and familiarity with one's own device might allow a hacker or fraudster to persuade an individual to provide information that may be sensitive. By understanding more closely how these factors affect the decision-making process, we will be able to better educate the public about what types of information requests they should be more suspicious of.

Social engineering attacks have only continued to increase year over year (FireEye Threat Report, 2019). In 2019, over four billion dollars had been lost, stolen, or captured by hackers as a result of cyberattacks (Su, 1). While this is a massive number, the true implications of social engineering go much deeper than just financial loss. In 2016, a social engineering attack had geopolitical consequences and threatened general global security. The site of the attack was the U.S. Democratic Party, which was successfully socially engineered by hackers during the 2016 presidential primary (Levy, 1). The social engineering hack led to both the resignation and upheaval of the Democratic Party just four months before one of the largest elections in U.S. history. As a result, the United States' parties and citizens are still seeing the ramifications and fear that simple social engineering attacks can incur. From the privacy research side, teams like ours are hoping to close the gap to stop these malicious and dangerous attacks and better educate colleagues on these failings.

## **Literature Review**

Social engineering is a broad field that includes and intersects elements of human psychology, sociology, experimental economics, and privacy/cybersecurity fields. Due to its breadth, it's important to narrow down what considerations and related literature our

team used to orient our study in the field broadly. Social engineering, by definition, is the ability to manipulate individuals through social actions to alter their behaviors, usually in order to do something that they wouldn't ordinarily consent to under normal psychological circumstances ((Nohlberg, Kowalski). In social engineering experiments, various psychological vulnerabilities and triggers are used by social engineers to gain influence over an individual's emotional state and cognitive abilities to obtain information. Theoretically, to successfully defend against these psychological triggers, the individual needs to have a clear understanding of the triggers to recognize them during a social engineering attack. What are the most common vulnerabilities that are exploited during social engineering studies? Several psychological vulnerabilities exist, of which the most common ones are defined as strong affect, overloading, reciprocation, diffusion of responsibility and moral duty, integrity and consistency, authority, and deceptive relationships (Mouton, Malan, Venter). These conditions are the most target because they are often the most affected. They play into our mind's natural heuristics, biases, and trust weaknesses. Observing these and other conditions, social engineering teams can understand exactly what makes an attack most potent and debilitating to their victim.

In social engineering exercises, victims are exploited because of their reliance on the implicit trust they hold in the person or system they are working on. As humans, in the face of technology, we often believe the machines to be more trustworthy than their human counterparts (Logg, Minson, Moore). As most in the security and privacy community know though, this is a dangerously false notion. On both the machine and human side, there are endless malicious agents, security holes, and adverse interests that make comprehensive security tough. With experiments like this, we aim to both aid and better understand the underlying mechanisms by which trust is given and why. Particularly for our experiment, we used the way choices were presented and the appearance of the security of said choice. In the following sections, I will be connecting important works in the field to orient our study to the broader literature.

People can fail to be trustworthy when it comes to protecting private systems. This is often due to inadequate education, negligence, and various social pressures (Nohlberg, Kowalski). People are often the weakest link in an otherwise secure computer system and, consequently, are targeted most easily for social engineering attacks (Kearney, Kruger). Social engineering is a technique used by hackers outside of the common software-only hacking techniques like brute force or keystroke methods. Such attacks can occur on both a physical and psychological level (Nohlberg, Kowlaski). The

physical setting for these attacks occurs where a victim often feels secure: often the workplace, the phone, and particularly online or on social media (Huber, et. al).

Psychology is often used to create a rushed or pleasant ambiance that helps the social engineer to convince the victim to relinquish sensitive information about accessing the system.

There are other related experiments in user agent trust games that help inform our work on games and economic behavior. User agent trust games are a popular mode of experimental economics research by which researchers can understand the decision-making in games or exchanges amongst players. In our case, we are interested in the trust exchanges between two parties who hold valuable information.

In our study, our research team tested three variables all related to the way in which the attack was presented. The first manipulated dimension was the format of the survey: online or on paper. Second, in the online condition, participants were either asked to take the survey on their personal device or on a tablet provided to them. Finally, the online survey contained a "Submit securely" button, which had an image of a lock (to give a higher perception of security) or a simple "Submit" button. The corresponding manipulation for the paper format was submission into a closed and locked or open and unlocked ballot box.

For the online versions, we developed a survey in Qualtrics, an online survey builder. Importantly, none of the information requested via the online survey was actually stored. Our research team programmed the Qualtrics survey so that only a binary variable would be stored: 0 if the participant decided not to provide the requested information, 1 if they did provide it. This was to ensure that no sensitive information would be put at risk. Normatively, these different options would have limited influence on the participants' choice to relinquish sensitive information (Venkatanathan, et.al). However, based on evidence from the behavioral economics, psychology, and decision making literature, it is possible that different presentation styles might affect participants' likelihood to give away sensitive information. There are no known forms of habituation that take place in our experiment that may make participants have proactive or adaptive behaviors to recognize stimuli. This is because it is a one-time experiment with each participant. Based on the basis of trust alone, our team expects people to be influenced by visual stimuli like a lock on the box, which aims to potentially provide a subliminal illusion of security to the victim, plaintext security prompts, and other mechanisms for establishing trust. In enough cases, these variables may cause a greater influence on subjects than alternative methods.

## **Experiment Procedure**

Our experiment procedure is straightforward and replicable across other environments. First, our team would select a busy and well-trafficked area around campus in order to get a random and varied demographic sample. Once a location was established, the research team, composed of two individuals, would set up a booth. The booth consisted of a black box that contains all of our forms and an insertable sign that stated that we were a club on campus focused on cybersecurity. Once the booth was set, with all the appropriate conditions made ready, our team would randomly select a treatment condition to test. Every time a new data point was successfully collected, this step would be repeated to provide enough data on each treatment condition. To ensure pseudo-randomness, we would generate a random number between one and six (six conditions to test in total). Once a treatment condition was selected, one of the research team members would approach every third person, dependent on the crowd density. Importantly, our team made the decision that we would never approach any individual who was in a group. This is because of all the literature done on norm compliance and peer pressure and how it can deeply influence decision-making under uncertainty. Under conditions of peer or social group pressures, victims will often make choices under the

consultation of the other opinions of the group. This is not an accurate representation of the victim's actual propensity to relinquish sensitive information.

When the person is approached, the other member of the team takes note of the gender, age, and ethnicity of the customer. The confederate will start with stating s/he is part of the Wildcats Cybersecurity Club, and ask if they are interested in having a security assessment of the strength of their University of Arizona password. If they say yes, continue along with the experiment if the party is interested. Offer the potential subjects the chance to enter into a raffle for two \$50 Amazon gift cards (approximately 1 in 100 chance of winning). If the potential subject decides to participate, then the confederate will direct them to complete the form. Depending on the random condition picked, that person participates in the survey. After the survey, we will also ask participants if we can take a photo of them to showcase everyone we helped with our security review. When the participant is done: for paper conditions, the participant personally slips the sheet in the ballot box; for electronic conditions, simply move to the survey end. Then the confederate will direct the subject to the research assistant. Next, the research assistant will debrief the subject about the purpose of the research and show them the consent form. Exit questions will be asked at this point. For the paper conditions, the research assistant will receive the responses from the confederate,

transform them into a binary variable equal to 1, if the participant provided an answer and 0, if otherwise. The paper form is then immediately shredded and in sight of the participant. For the online form, we query and show the participant that only 0 and 1 are stored and nothing else. Once the subject has completed the exit survey, the experiment will have ended. The exit survey will ask the participant for a selfie, their demographic data, and whether they gave a true password.

### **Challenges During Research**

There were many challenges faced by the research team on this social engineering study. Many challenges arose due to the quantity of time it takes to get a statistically significant amount of participants for 6 variables being studied. In our initial conversations, the research team had determined that 40 positive (successfully engineered attacks) were needed for every variable. This meant that the team had to collect up to at least 240 positives and consented to tests. Each test, when administered and done successfully takes up to 10 minutes minimum. With the average testing session being an hour to 2 hours at a time, it was a very successful research day if the team had successfully received 5-10 new data points. As a result, the experiment ran for over a year and a half with various rotating team members in the field. One of the resultant

factors to be examined is that there were multiple presenters of different ages and sexes. The influence of the human presenter in social engineering experiments is statistically significant (Albladi & Weir). Without consistency across the presenter variable, our data must be taken with this as a consideration. Additionally, we were only able to collect 150 data points over the course of the experiment's trial. This fell below our desired mark of 240 total data points.

Another limitation of our research was the limited demographic diversity. Most of our study's observations focused unintentionally on students, which was our primary testing group age/demographic. In an experimental economics meta-analysis, studies found that, "while students are a convenient and frequently employed sample for behavioral laboratory experiments, the external validity of using student subjects has been criticized because it is not a representative sample of the general population. Students are on average younger than random samples of the population and some research has found that relatively older subjects exhibit less trust behavior in the trust game than student participants" (Guth). While not conclusive, this evidence suggests that trust in students takes on different qualities than that of other demographics tested. While we did not have the intention to test subjects outside the university, other corroborating

social engineering studies in the future could be a way to better provide improved insights into the influence of the students in our dataset.

### **Future Work**

There are many future directions for modelings of trust and choice in social engineering experiments. With trust and relationships manifesting differently across cultures, the way in which human security evolves will be varied. The first step to advance this work could be to look at other cultures, specifically other cultures where trust, community, and individual privacy are held and valued differently. For our study, a group in Israel at the Ben Gurion Institute in the Negev region of Israel is replicating the procedure of our study. Our research team is interested in the geographical and cultural nature of security. These implications can hold weight towards the future of our global understanding of human trust. On another note, it could be used to craft more specialized and bespoke policies by governments or other entities. Finally, further interest in the domain of experimental economics and behavioral economics may provide insights into ways by which nudges and other proactive measures could generate net security and privacy benefit to individuals.

Across the world, individuals display unique preferences and inclinations towards privacy and security. While there are no meta-analyses on contemporary comparisons cross-culturally or cross-regionally in regard to privacy and trusts in the experimental economics domain. However, due to historic factors and implicit assumptions based on authority, our team sees this study having wildly different results across different areas and cultures of the world. With insights like these, we may be able to begin to piece together a more universal understanding behind providing empirically backed policies for regions and governments. Off the tailwinds of the European Union data protection laws of the past decade, the research of this experiment and many others could enable more motivated public policies that better the state of security for the public. This is important, more than ever because our reliance on digital and insecure systems only begins to grow. To reduce the asymmetry in knowledge and potential for exploitation by bad actors, policymakers must close some relevant gaps in the public's security knowledge. As in the European Union, a general data protection law is likely on the horizon globally. Whether it is effective or not is reliant on the datasets, studies, and derived data that is used to motivate these policies. With a better understanding of the common pitfalls, heuristics, and other irrational behaviors we as people exhibit, these policymakers could nudge us

subliminally towards better and more secure choices for us all. In some sense, these protection laws can act as an invisible hand in the privacy market.

With a plethora of choices, we can motivate people towards choosing the best of their presented options. With increasing knowledge of the implicit effects of choice architectures on trust and privacy, we may be able to craft lasting changes to consumer's overall safety and privacy.

## References:

Albladi, S.M., Weir, G.R.S. User characteristics that influence judgment of social engineering attacks in social networks. *Hum. Cent. Comput. Inf. Sci.* 8, 5 (2018).

Guth W, Kocher MG. 2014. More than thirty years of ultimatum bargaining experiments: motives, variations, and a survey of the recent literature”. *J. Econ. Behav. Organ.* 108:396–409.

M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa. Towards automating social engineering using social networking sites. *Computational Science and Engineering, IEEE International Conference on*, 3:117–124, 2009.

W. Kearney and H. Kruger, "Considering the influence of human trust in practical social engineering exercises," *2014 Information Security for South Africa*, Johannesburg, 2014, pp. 1-6.

F. Mouton, M. Malan, and H. Venter, “Development of cognitive functioning psychological measures for the seadm,” in *Human Aspects of Information Security & Assurance*, Crete, Greece, June 2012, pp. 40–51.

M. Nohlberg and S. Kowalski, "The Cycle of Deception-A Model of Social Engineering Attacks, Defenses and Victims," in Proceedings of the Second International

Levy, Nat. "Q&A: Cybersecurity Expert Explains the DNC Email Hack, and How You Can Prevent a Similar Attack." *GeekWire*, 25 July 2016, [www.geekwire.com/2016/a-cyber-security-experts-explains-the-dnc-email-hack/](http://www.geekwire.com/2016/a-cyber-security-experts-explains-the-dnc-email-hack/).

Logg, Jennifer M., Julia A. Minson, and Don A. Moore. "Algorithm Appreciation: People Prefer Algorithmic to Human Judgment." Harvard Business School Working Paper, No. 17-086, March 2017.

P. Rosenzweig, "Is Cybersecurity Improving?" *Lawfare*, 31 Oct. 2019, [www.lawfareblog.com/cybersecurity-improving](http://www.lawfareblog.com/cybersecurity-improving).

Su, Jeb. "Hackers Stole Over \$4 Billion From Crypto Crimes In 2019 So Far, Up From \$1.7 Billion In All Of 2018." *Forbes*, Forbes Magazine, 16 Aug. 2019, [www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/#70fadd7355f5](http://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/#70fadd7355f5).

J. Venkatanathan, V. Kostakos, E. Karapanos and J. Gonçalves, "Online Disclosure of Personally Identifiable Information with Strangers: Effects of Public and Private Sharing," in *Interacting with Computers*, vol. 26, no. 6, pp. 614-626, Nov. 2014.

"New FireEye Email Threat Report Reveals Increase in Social Engineering Attacks." *FireEye*,  
[www.fireeye.com/company/press-releases/2019/new-fireeye-email-threat-report-reveals-increase-in-social-engine.html](http://www.fireeye.com/company/press-releases/2019/new-fireeye-email-threat-report-reveals-increase-in-social-engine.html).