# Analyzing Social Engineering Techniques in Cyber Attacks

Robert Harry, Information Technology, College of Engineering and Computer science

## Project Objectives

The objective of this research project is to analyze the effectiveness of social engineering tactics utilized by threat actors and potential countermeasures. To accomplish this, we will analyze the content of current reports and statistics available on the topic of social engineering. Utilizing this information, we will run simulated social engineering attacks and record the results to demonstrate the true scale of the threat. Next, we will compare the effectiveness of each type of attack and the current industry preventive measure associated with it. Finally, we will arm our simulated cyber victims with implementable security measures based on industry standard practices and run the simulated attacks again at an unannounced time. We will compare both rounds of tests to determine the effectiveness of both the threat type and the current industry preventative measures, while offering possible substitute methods where the current measures are insufficient.

## Introduction/Literature Review

According to Carnegie Mellon University, social engineering can be defined as “the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information.” (n.d.) Today social engineering continues to be one of the biggest threats facing individuals and corporations alike. The fix to this issue is a combination of proper implementation of preventative measures and cyber literacy. There are many different types of attacks utilized by threat actors, the most common among them being phishing, baiting, pretexting and tailgating. Phishing is the act of sending fraudulent emails or texts to deceive a victim into clicking on malicious links or revealing confidential information such as passwords. Baiting is where threat actors make false promises to convince the victim to reveal their personal information. Pretexting is when a threat actor creates scenarios to convince the victim to share sensitive information. Unlike the previously described actions, tailgating is a physical breach where a person gains access to a restricted location by preying on another’s good nature by asking them to let them in or simply hold the door. With an understanding of the intrusions, we can see that the level of threat these actions pose is not negligible in the slightest. In 2019, Google and Facebook were targeted with a 100-million-dollar phishing scam back. If tech giants like Google and Facebook are at risk of social engineering what is the state of cyber literacy of companies and individuals who can’t afford an entire cybersecurity division? While researching the core message of all the documents, I found that many pointed to the idea that social engineering continues to not only be the most prevalent form of cyber-attack but also the most effective. Currently, industry preventative measures consist of employee training and company policy. Unfortunately, both measures exist solely on the prerogative of the individual company, and many smaller organizations won’t implement anything until it’s too late. In response to this issue, this project will allow us to bridge this gap by providing research-backed data and ready-to-implement solutions that will improve individuals and companies alike.

## Research Methods

Our research method is comprised of five stages: initial research, a first round of simulated attacks, an analysis of the results of the first round, a second round of simulated attacks after potential victims are given anti-social engineering information, a final analysis comparing both simulations, and a publication of findings and recommendations to improve current preventive measures. The initial research phase will be comprised of reviewing the documentation cited in the literature citation. Based on the reading, we will choose which forms of social engineering will be included in our simulation to ensure that our research is current and impactful to individuals and industries alike. Then, after receiving the proper permissions from the IRB to conduct simulations, we will form groups of volunteers for a social engineering experience. These simulations will be comprised of pseudo-social engineering attacks upon the individuals who have agreed to participate in this experiment. To not potentially corrupt the data of the first round of testing, we will keep specifics of the simulation private but give participants necessary information and have sign proper documentation to not accidentally infringe on their right to privacy. We want to source volunteers early, as expecting a potential attack may affect the outcome of the simulations. After the first round of simulations, a complete analysis of the results will begin. Depending on the outcome of the simulation, we will tailor our informational documentation to address any areas that are especially vulnerable in our test group. This will allow us to maximize the results of our second simulation and really see how impactful, if at all, proper cyber literacy is in preventing social engineering attacks. Once the second round of simulations is complete and analysis of the combined simulations is underway, we will begin to make our writeup on the overall outcome of the research project. Subsequently, we will compound our results and address any potential issues that persisted through both simulations in order to bring more awareness of social engineering threats to the public and improve upon the pre-existing preventative measures currently in place.

## IRB/IACUC Statement

As this research requires interaction and study of human subjects, we will need approval from the Institutional Review Board. Approval will be obtained before any interaction with volunteers is initiated.

## Expected Outcomes

After the completion of this research project, we look forward to providing the community with a white paper that details the findings of our research and the necessary steps that need to be taken by users to protect themselves from potential social engineering. We plan to submit our white paper to scientific journals and local sources of information dispersal, as we believe people at all levels of cyber literacy can benefit from research and findings conducted here. This knowledge will allow us to better address the current climate of cyber literacy with real data of the threat that social engineering poses. The insight that will be gained from conducting this research will help us to implement community and industry-wide preventative measures to prevent future attacks. As a student studying information technology who hopes to one day pursue a career in cybersecurity, being able to have hands-on experience with these methods of cyber attack will

give the next generation of cybersecurity professionals a true and applicable understanding of one of the most prevalent types of cyber intrusions. Recently, there have been several phishing emails have been appearing in student and faculty email inboxes, as individuals claiming to be from the university have asked users for confidential information, including student numbers and login-in credentials as well as other compromising information. As members of the UCF community, it is our responsibility to look out for the well-being of all that call the University Central Florida home. These threats continue to pose a danger to countless individuals, and action must be taken to improve the situation. There is never truly a fix-all in situations like this, but with proper awareness of cyber literacy and researched-backed preventative measures, we can usher in a new era of cyber safety for the UCF community and the world at large.

## Literature Citation


Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Siami Namin, A. (2020). How social engineers use persuasion principles during vishing attacks. *Information & Computer Security*, *29*(2), 314–331. https://doi.org/10.1108/ics-07-2020-0113

Karadsheh, L., Alryalat, H., Alqatawna, J., Alhawari, S. F., & Jarrah, M. A. (2021). The impact of social engineer attack phases on improved security countermeasures. *International Journal of Digital Crime and Forensics*, *14*(1), 1–26. https://doi.org/10.4018/ijdcf.286762

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/10.1177/0162243921992844

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Social Engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

University, C. M. (n.d.). Social Engineering - Information Security Office - Computing Services - Carnegie Mellon University. https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

## Plan of Work Timeline

- **Week 1 (May 17-23): Initial Research Phase**
  - Review relevant documentation on social engineering tactics and cybersecurity measures.
  - Select specific social engineering tactics to include in the simulation based on research findings.
- **Week 2-3 (May 24 - June 6): Preparation and Volunteer Recruitment**
  - Obtain permissions from the Institutional Review Board (IRB) to conduct simulations involving human subjects.
  - Recruit volunteers for participation in the social engineering simulations.
  - Provide volunteers with necessary information and obtain signed documentation to ensure privacy and consent.
- **Week 4-5 (June 7 - June 20): First Round of Simulated Attacks**
  - Conduct the first round of simulated social engineering attacks on volunteers.
  - Ensure that the specifics of the simulations are kept private to avoid bias in results.
  - Collect data on the effectiveness of each type of attack and participant responses.
- **Week 6-7 (June 21 - July 4): Analysis of Results and Preparation for Second Round**
  - Analyze the results of the first round of simulated attacks to identify vulnerabilities and areas for improvement.
  - Tailor informational documentation to address vulnerabilities identified in the first round.
  - Prepare volunteers with anti-social engineering information for the second round of simulations.
- **Week 8-9 (July 5 - July 18): Second Round of Simulated Attacks and Final Analysis**
  - Conduct the second round of simulated social engineering attacks after volunteers have been provided with anti-social engineering information.
  - Compare the results of both rounds of simulations to assess the effectiveness of the threat types and current industry preventive measures.
  - Begin compiling research findings and recommendations into a white paper for publication.
- **Week 10 (July 19): Publication of Findings**
  - Finalize the white paper detailing the findings of the research project and recommendations for improving current preventive measures.
  - Submit the white paper to scientific journals and local sources of information dissemination.