An Examination in Social Engineering: The Susceptibility of Disclosing Private Security Information in College Students

Rachel Bleiman, Aunshul Rege
Temple University, Philadelphia, USA
Rachel.bleiman@temple.edu
Rege@temple.edu

Abstract

While security technology can be nearly impenetrable, the people behind the computer screens are often easily manipulated, which makes the human factor the biggest threat to cybersecurity. This study examined whether college students disclosed private information about themselves, and what type of information they shared. The study utilized pretexting, in which attackers impersonate individuals in certain roles and often involves extensive research to ensure credibility. The goal of pretexting is to create situations where individuals feel safe releasing information that they otherwise might not. The pretexts used for this study were based on the *natural inclination to help*, where people tend to want to help those in need, and *reciprocity*, where people tend to return favors given to them. Participants (N=51) answered survey questions that they thought were for a good cause or that would result in a reward. This survey asked for increasingly sensitive information that could be used maliciously to gain access to identification, passwords, or security questions. Upon completing the survey, participants were debriefed on the true nature of the study and were interviewed about why they were willing to share information via the survey. Some of the most commonly skipped questions included "Student ID number" and "What is your mother's maiden name?". General themes identified from the interviews included the importance of similarities between the researcher and the subject, the researcher's adherence to the character role, the subject's awareness of question sensitivity, and the overall differences between online and offline disclosure. Findings suggest that college students are more likely to disclose private information if the attacker shares a similar trait with the target or if the attacker adheres to the character role they are impersonating. Additionally, this study sheds light on the research limitations, emphasizes the relevance of the human factor in security and privacy, and offers recommendations for future research.

Keywords

Social engineering; pretexting; disclosure rates; security questions

1. Introduction

In 2016, the United States Department of Justice (DOJ) was the target of a cyber-attack during which 20,000 Federal Bureau of Investigation and 9,000 Department of Homeland Security employees' personal details were leaked. A hacker accessed an employee's email account, pretended to be a new employee, and manipulated the department into granting him access to the system (*The Top Ten* 2019). This type of cyber-attack is a form of social engineering (SE), which is "any act that influences a person to take an action that may or may not be in his or her best interests" (Hadnagy 2018, p.7). In the DOJ's case, that action was granting the attacker access to their system; however, SE can take many forms to exploit sensitive information.

Consider the 2007 case of the then Republican vice-presidential nominee and Governor of Alaska, Sarah Palin. Her Yahoo! Mail account was compromised. All the hacker needed to gain access to her account was the answer to four security questions: birthdate, country of residence, postal code, and where she met her spouse. All of this information was available to the hacker on Google (Shea 2017), showing the extreme vulnerability of security questions and the lack of awareness people have for how their information can be used against them. As seen over the span of a decade, exploiting sensitive information through SE has remained prevalent, especially with the rise in technology.

In fact, a 2009 research study measured the reliability and security of personal questions as secondary authentication for passwords for AOL, Google, Yahoo!, and Microsoft (Schechter, Brush, and Egelman 2009). Acquaintances of the participants were able to guess nearly 20% of the answers, and 13% of the answers could be guessed within five attempts when guessing the most popular answers from other participants. Users

readily choose security questions that will be easy for them to answer and remember. Because people are not cognizant of how they share or choose their answers, their online safety is at a higher risk. It is not just online that people risk disclosing their private information, but also in-person. It is even possible for people with malicious intent to create circumstances where people will disclose their information. Because of the uncertainty of the human factor involved in security, it is necessary to study SE. Focusing solely on technological enhancements to improve cybersecurity, without regard to the human factors, is futile, because it lacks the necessary holistic approach.

Therefore, the purpose of this study is to observe and identify the pretexts, or false motives people use to obtain information, that make college students susceptible to disclosing their private information. This study additionally aims to identify the type of private information college students are susceptible to disclosing and examine their awareness regarding disclosure of private information. The hypothesis to be tested is that college students' susceptibility to disclose private information changes depending on the pretext to which they are introduced. Further expectations of this study are discussed in section 3.4. The researchers aim to utilize the known information on pretexting, disclosure, and psychological influences to examine these questions.

This paper is structured as follows. First, this paper details the literature on SE attack types, psychological manipulation, and the effects of pretexting on disclosure rates of private information. Second, the study design and methodology outlines the procedures of the study. Third, the study results and analysis are shared. The last section discusses implications, takeaways, and future research trajectories.

2. Social engineering

SE attacks have a low cost to set up, a low risk of being caught, and a high reward, making it a very popular attack style and leading it to becoming the easiest attack route with the largest payload for scammers to use (Hadnagy and Wozniak, 2018). Its popularity and success has been steadily increasing every year, rising from a 62% to 79% success rate from 2014 to 2017 (Lopez 2018). Nearly 70% of US organizations experienced SE attacks in 2017, costing the country approximately $2.76 million and each instance taking approximately 20 days to resolve (Richards, Dool, and Kennedy-White 2017).These SE attacks can be executed through a variety of methods, which are discussed next.

2.1 Attack types

Some of the most common attack styles are *phishing*, *vishing*, and *impersonation.*

Phishing is the act of sending emails appearing or claiming to be from a reputable source, with the intention of gaining private information. Phishing attacks have become increasingly sophisticated, with targeted phishing attacks utilizing known personal information about the target to seem more legitimate. *Vishing* is similar to phishing; however, it occurs over the phone (Tiwari 2018).

Impersonation is an in-person attack style where attackers attempt to gain access to private information, usually by creating a pretext. Pretexting involves attackers impersonating individuals in certain roles and often involves extensive research to ensure credibility. The goal is to create situations where individuals feel safe or comfortable releasing information that they otherwise might not and relies on the victims to disclose their own information. Humans tend to be trusting by nature, which leaves people susceptible to SE attacks and because of this, attackers may take advantage of the biases in society, such as age, gender, or ethnicity, depending on the pretext (Hadnagy and Wozniak 2019).

2.2 Disclosure and privacy

In a 2017 study measuring disclosure rates with the use of pretexts, research found that 79.1% of subjects disclosed their email address and 43.5% disclosed bank account information (Junger, Montoya, and Overink 2017). Research has also examined what factors affects disclosure rates.

A 2010 study used a survey and experiment to find that disclosure rates decreased with weaker privacy policies and low trust (Joinson et al, 2019). Furthermore, when people felt more trusting towards the attacker, they more willingly disclosed information, regardless of the type of information being disclosed.

A 2012 study ran experiments to measure disclosure online and found that cueing subjects to think about privacy decreased disclosure rates (Acquisti, John, and Loewenstein 2012). Additionally, when subjects were not cued to think about privacy, asking questions in an increasingly intrusive order produced lower disclosure rates than when asking them in a decreasingly intrusive order.

A 2018 study analyzed individuals' reading behavior for terms of service (TOS) and privacy policies (PP) used to sign up for a social networking service (Obar and Oeldorf-Hirsch 2018). Most people skipped reading PP (74%). The few people who did read PP had an average reading time of 73 seconds, instead of the 30-minute expected reading time. Similar results were found for TOS; the average reading time was 50 seconds, compared to the 15-minute expected reading time. These results showed that the majority of people did not read PP or TOS documents, yet still consented to all clauses in the documents, demonstrating a major vulnerability for attackers to target, concerning the human side of cybersecurity.

2.3 Psychological influences

There are several principles of influence often associated with cyber-attacks through SE, which involve influencing or manipulating people with the aim to access private data (Uebelacker and Quiel 2014; Rege, Williams, and Mendlein in-press). The principles consist of (i) *Authority*, in which people are likely to follow the requests of authority figures, (ii) *Commitment and Consistency*, in which people behave in a way that aligns with their beliefs, (iii) *Reciprocity*, in which people tend to return favors given to them, (iv) *Likeness*, in which people comply with others they like or with whom they share similarities, (v) *Social Proof*, in which people are likely to comply if other people have also complied, (vi) *Scarcity*, in which people will comply when they believe an opportunity is scarcely available, and (vii) *Natural Inclination to Help*, in which people tend to want to help those in need. When aligned with a relevant pretext, these principles can be used as tools of persuasion in SE attacks.

Additionally, there are techniques of SE, focusing on pretexting, which discuss personality traits associated with SE. They explain how exploiting specific psychological phenomena can help trigger a SE attack (Luo et al, 2011). Such phenomena include (i) *diffusion of responsibility*, in which attackers acting alone are held more responsible for negative behavior, (ii) *chance for ingratiation*, in which victims believe their obedience will heighten their chances of receiving a benefit, (iii) *trust relationship*, in which humans naturally trust others until they are proven untrustworthy, and lastly, (iv) *feelings of guilt and sympathy,* in which people tend to feel sympathy for others in order to avoid feelings of guilt. These phenomena leave the victims vulnerable, which allows SE attackers to exploit these phenomena to initiate and carry out attacks.

Building on this foundation, the current study uses pretexting and psychological influences to examine college students' susceptibility to disclosing their private information.

3. Study design and methodology

3.1. Participants

51 college students were recruited via a convenience sampling strategy to participate in this four-week study. The researchers chose college students for several reasons. First, college students tend to post information online, and are thus a relevant group to study (Crawford 2016; Madden et al, 2014). Second, college students have been known to seek opportunities that offer some reward (*How can paid* 2019) and have also been known to be helpful and sympathetic towards others (Glassner and Schapiro 2018). As such, the two logical principles of persuasion used for this study were *reciprocity* and *natural inclination to help*, which aligned with college students' behavior. Third, college students are the next generation work force, so examining their awareness and susceptibility is essential. Finally, this group was chosen because of its alignment with the researchers' education and study interests.

3.2. Design and procedure

During this study, subjects were asked to complete a short survey (Appendix A) that asked for information commonly used for online personal security questions (Fotre 2016). Data collection occurred on campus, with a weekly rotation around four populated areas. The survey remained the same throughout the duration of this study, with questions asked in an increasingly sensitive order. Each week utilized a different pretext, which provided the subjects with a reason to take the survey and a reason those particular questions were asked. To make the subjects more vulnerable to revealing their information, each pretext targeted one of two specific

emotions: (i) *reciprocity*, the occurrence that people tend to return favors when one is given to them and (ii) *the natural inclination to help* others when they are in need. One researcher, a female undergraduate student, conducted the pretexts. During each pretext, the researcher wore the same clothing style, tee shirts and shorts, to fit in with the college student population. This project was approved by the ethics board at the researchers' home institution.

3.2.1. Pretexts

Week 1, Pretext 1 (student helping student): This pretext targeted people's *natural inclination to help*. The researcher posed as a student in a summer Research Methods class, analyzing students' demographics and preferences. She targeted the emotion by emphasizing her need for participants to take the survey in order to get a good grade on the assignment. This pretext was chosen because of the similarities between the subject and the researcher. The similarity would give the pretext credibility and also elicit a sympathetic response from the subject because of possible past similar experiences.

Week 2, Pretext 2 (raffle): This pretext targeted the emotion derived from the principle of *reciprocity*. During this pretext, the researcher posed as a representative for a new (fake) apartment complex near campus who surveyed students on their interests and demographics to determine what retail or food shops should be put on the ground level. She enticed subjects with a monetary reward by telling them that if they completed the survey, they would be entered into a free raffle drawing for a $50 Visa gift card, and three winners were to be drawn by the end of the week. The researcher created this pretext because college students often volunteer to participate in research for money, making the pretext seem believable and enticing students to participate (*How can paid* 2019).

Week 3, Pretext 3 (student helping niece): This pretext targeted people's *natural inclination to help*. In this pretext, the researcher created a story that her young niece was doing a summer project to compare the similarities and differences between college students and elementary school students in their preferences and how much they know about themselves. The researcher claimed that the 'niece' asked her to help her by surveying college students on her behalf. While the subjects were not able to see the 'niece' who they were helping, this pretext elicited a sympathetic response by having people believe they were helping a child.

Week 4, Pretext 4 (therapy dog): This pretext targeted the emotion derived from the principle of *reciprocity*. During this pretext, the researcher had a therapy dog with her; she allowed people to pet the dog and asked them to complete the survey. She posed as a student working to start a therapy dog club on campus, and the purpose for the survey was to find out what people were interested in doing or talking about during club gatherings. The researcher chose this pretext as a way to entice students to approach her as well as to distract the subjects from questioning the credibility of the pretext.

3.2.2 Post-survey disclosure

After the completion of the survey, the true nature of the research was revealed to the subjects, and they were informed that the pretext was not real. Due to the sensitivity of their answers, the researcher only took record of which questions they answered, not their actual answers, using Appendix B. Subjects were allowed to keep the paper survey that they completed, which was the only record of the answers to their private information. 48 out of the 51 subjects consented to partake in an interview (Appendix C) about their involvement in the study.

3.3. Expected outcomes

As previously mentioned, the main expectation of this study was that the students' susceptibility to disclose private information would change depending on the pretext. More specifically, it was expected that pretext 4 (therapy dog) would be the most successful pretext, as it would attract the most amount of people and distract them from questioning the sincerity of the pretext. The researchers expected to seem more trusting and approachable with a dog.

It was also expected that pretext 2 (raffle) would be the least successful pretext, because, of the four pretexts, it seemed to be the weakest explanation for why the researchers wanted the information asked for on the survey.

Another expectation was that the majority of potential subjects would decline taking the survey or would answer only the less sensitive questions. It was expected that subjects would become uncomfortable once asked for more personal ones. It was for this reason that the questions were asked in an increasingly sensitive order.

While there was no expectation that campus location would play a role in subjects' responses, it was expected that gender would be a relevant factor. The researcher expected that more females than males would participate, and that both genders would trust the researcher more because of her gender (Steinmetz 2010).

4. Results and analysis

Overall, this study showed that college students were trusting and willingly disclosed sensitive information, unaware of how this could be used maliciously. When given the right combination of pretexts and persuasion principles, students were extremely susceptible and easily manipulated.

4.1. Sample size per pretext

In total, 51 students fell target to all of the SE pretexts; 17 with the first pretext (student helping student), 7 with the second (raffle), 11 with the third (student helping niece), and 16 with the fourth (therapy dog).

Two subjects declined to interview with the first pretext (student helping student), and one subject declined to interview with the fourth pretext (dog), which lowered the sample sizes for those two pretexts down to 15 for both. These differences in sample sizes were not necessarily a product of the pretexts, but may have been due to the time factor, as there were less students on campus for the middle two weeks/pretexts.

4.2. Pretext-based findings

Despite the differences in the number of subjects surveyed and interviewed for each pretext, subjects answered approximately the *same number of questions regardless of which pretext was used*. Out of 16 questions, the median number of questions answered from each subject per pretext was as follows: 14 for the first pretext (student helping student), 14 for the second pretext (raffle), 13 for the third pretext (student helping niece), and 14 for the fourth pretext (therapy dog). This suggests that the pretexts may have impacted how many people agreed to participate but did not have a great impact on how much information subjects were willing to disclose. This finding did not support the researchers' hypothesis that the pretext would change students' susceptibility. A possible explanation is that students may have a maximum trust threshold, wherein some information is considered so sensitive that they would not disclose it to anybody, no matter how much they trust the other person. As such, some survey questions received lower response rates than others.

The survey asked for five pieces of contact information and an additional ten questions. Table 1 details the overall response rates among all 51 subjects.

Table 1: Overall response rates

Questions with Lowest Response Rates:	3: Student ID 32/51, 63%	4: Phone Number 34/51, 67%	10: Favorite Book 33/51, 65%	14: Mother's Maiden Name 33/51, 65%
All other questions had at least a 74% response rate				

However, as seen in Tables 2-5 below, commonly omitted questions and response rates differed for each pretext. Figure 1 below offers more details for the response rates of each question per pretext.

Table 2: Pretext 1 (student helping student) response rates

Questions with Lowest Response Rates:	4: Phone Number 8/17, 47%	3: Student ID 9/17, 53%	
All other questions had at least a 76% response rate			
Questions with 100% response rate:	7: Favorite Sports Team	8: Favorite Food	12: Favorite Number

Table 3: Pretext 2 (raffle) response rates

Questions with Lowest Response Rates:	14: Mother's Maiden Name 4/7, 57%		
All other questions had at least a 71% response rate			
Questions with 100% response rate:	6: City of Origin	8: Favorite Food	1: First Name

Table 4: Pretext 3 (student helping niece) response rates

Questions with Lowest Response Rates:	14: Mother's Maiden Name 5/11, 45%	3: Student ID 6/11, 55%	10: Favorite Book 6/11, 55%	4: Phone Number 7/11, 64%
All other questions had at least a 73% response rate				
Questions with 100% response rate:	6: City of Origin	7: Favorite Sports Team	8: Favorite Food	12: Favorite Number

Table 5: Pretext 4 (therapy dog) response rates

Questions with Lowest Response Rates:	10: Favorite Book 9/16, 56%	9: Favorite Movie 11/16, 69%	14: Mother's Maiden Name 11/16, 69%	15: Street Name 11/16, 69%
All other questions had at least a 75% response rate				
Questions with 100% response rate:	1: First Name	1.2: Last Name	2: Email	5: Birthdate

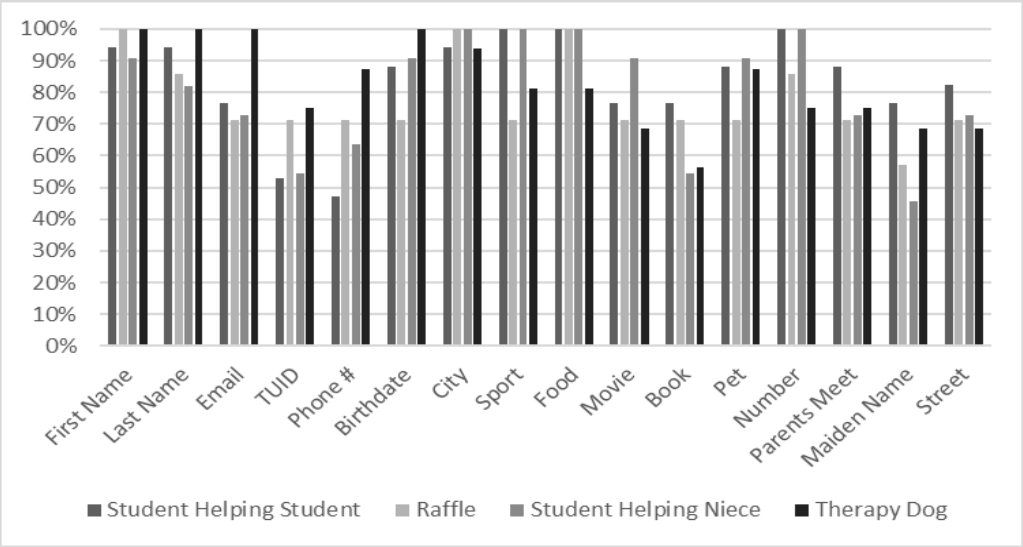

Figure 1: Question response rates per pretext

4.3. Disclosure-based findings

Overall, most subjects reported that they were able to identify that the questions on the survey asked for sensitive information, despite subjects answering the majority of them. The following sections outline the general themes identified during the post-disclosure interviews with participants for each pretext.

4.3.1 Likeness

Across all pretexts, subjects reported trusting the researcher because of shared attributes between the two, including age, gender, or life experiences; these similarities led subjects to feel more sympathetic towards the researcher. In pretext 1 (student helping student), subjects reported feeling inclined to help for reasons including having had similar experiences in their own lives. For example, Subject 3 agreed to participate because "it was for a class, and I know how hard it is to get people to actually take surveys for classes". They related to her as a college student, or had some experience trying to get people to participate in surveys, making them feel higher levels of trust and a greater inclination to help. Subject 23 explained that "if I know it's a fellow temple student, I'm more likely to give them my time".

Interestingly in pretext 2 (raffle), which aimed to target *reciprocity*, subjects revealed that the pretext triggered a *natural inclination to help*, instead. This unexpected response was a result of the likeness factor. Of the seven subjects surveyed and interviewed for this pretext, not a single one reported that they participated for the chance to win the raffle prize. Rather, each subject reported that they initially agreed to take the survey either out of sympathy towards the researcher or because of their inclination to help. The sympathetic responses were derived from subjects experiencing similar life events. For example, Subject 21 stated that "I've been on the other end, and I always feel bad […] [when] people […] are rude and walk away". Subject 23 reported that

the chance to win money did not entirely impact their decision; instead, they reported, "I just like helping out people because I see them get turned down all the time, and I know I want to be a researcher one day too, so I know one day I'm going to be turned down all the time, so that was more being nice than the money itself."

Meanwhile in pretext 3 (student helping niece), Subject 31 stated that she trusted the researcher because "you're a young woman, I'm a young woman. Definitely more comfortable than if a grown man came over and asked me". Overall, subjects felt inclined to help when they were able to relate to the researcher and understand the experience.

4.3.2 "College student" stereotype

Approximately 26 subjects out of the 34 subjects who were interviewed with the first three pretexts reported that they trusted the researcher because they assumed that she was a student, based on her appearances or how she acted. The researcher fit the physical appearance of the stereotypical college student, with attributes such as "college shirt and younger [looking]," according to Subject 30, who also stated that they trust people who "come forward and say they're a college student". Subject 26 explained that they could assume the researcher was a student and trust her because "you look like you fit the demographic, like the way you dress and the youth in your face". Many other students trusted the researcher because she "seemed friendly". Subject 21 explained "I think if you were like super young or even super old, and you said you were with the [university's] marketing team, I wouldn't really believe you, just because I know it's geared more towards actual students. But, because you actually look like you're within the range of a student here, I believed you".

4.3.3 Awareness of question sensitivity

Approximately 26 subjects of the 34 subjects who were interviewed with the first three pretexts reported that they realized while taking the survey that answers to the questions could be used to access passwords or answers to security questions. Many said they did not currently use any of the answers for security questions, so they did not mind disclosing the information; however, they did recognize them as common security questions. Students were most uncomfortable answering questions that they had commonly seen or used for security purposes. In particular, those questions consisted primarily of "what is your mother's maiden name?", "what street did you grow up on?", and "what is the name of your favorite pet?". Alarmingly though, many still gave accurate answers despite being aware of the question sensitivity, even writing down answers that they use currently for passwords or security questions. For example, Subject 21 stated, "when I started putting down all my [contact information], I was like wait, I probably shouldn't put that down, but I was already half-way done with it, so I was like, whatever." Subject 30 disclosed their favorite food, for example, which they stated that they use frequently for passwords. When asked if they were aware of the sensitivity of the questions while taking the survey, Subject 19 reported "I thought about it, but I just felt like maybe I'm overthinking it. Maybe it's not that big of a deal". Subject 31, under the premise of pretext 3 (student helping niece), said that "I didn't look at everything first. Because you have the questions structured, I'm like, yeah that's what a second grader would ask […] then towards the end I'm like what?".

In pretext 3 (student helping niece) several subjects confirmed their awareness of the invasive nature of the questions and expressed their doubt that it was really for the researcher's niece. However, these subjects still disclosed their information because they trusted the researcher. While the majority of the subjects realized the information was sensitive, some did not realize that until the debriefing, during which they agreed on the sensitive nature of the questions. However, even after the debriefing, two subjects did not agree that the questions were inquiring about sensitive information at all. For example, Subject 17 stated that the information was not private, but was general, albeit personal information, and agreed that they would have been comfortable giving the information to anyone that asked for it. They reported "you have my general information but not sensitive [information]". Despite Subject 17 believing this information to be public and non-sensitive, some of it, primarily the SID (student identification) number, is objectively sensitive on a college campus; that number allows access to grades and acts as a payment method.

4.3.4 Online vs. in-person

As noted earlier, most college-aged students today are aware of what they are posting online and who can view it (Madden et al., 2014). However, students are less cautious and more trusting when it comes to

disclosing information in-person. While it is not necessary to be distrustful to everyone, it is important to be aware of how well you know the person and what information you are giving them. Subjects reported being cautious of disclosing information online, such as on public social media pages, but were much less suspicious when talking to people in person, especially those that seem trusting. Subject 30 reported that they would be more aware of how they disclosed information, because "you never know who can sweet-talk you into giving you the last little bit of information they need". Most subjects felt that after participating in this research, they would be more cautious and aware of where they were posting their information online and, more specifically, to whom they disclose it in-person. Subject 31 even stated that participating in this research was "a wake-up call".

Subject 37 said "I give that [information] for so many people, so at this point trying to limit that by refusing one person, especially in a face to face contact situation, just didn't really seem necessary to me". After taking this survey, all of the subjects who reported not already being wary of what they post online responded that they would be more mindful when disclosing information in the future. Subject 43 reported that "definitely filling out stuff like this [in-person] I'm going to take a little more caution, just because it was so easy for you to get a lot of stuff". Subject 44 reported that they would be more cautious regarding "definitely what I give out to people […] I think I need to be more careful maybe".

4.3.5 Therapy dog

In the fourth pretext (therapy dog), subjects were eager to pet the dog the researcher had. The researcher waited until the students were already petting the dog to offer the survey. Because of this, the students were willing to take the survey as a way to return the favor of petting the dog; they also received the added benefit of inclusion into a club that suited their interests. This pretext differed from the others, because people did not disclose their information to help the researcher or because they related to the researcher in such a way that they felt trusting. Rather, when asked why the subjects initially agreed to take the survey, 15 out of 15 subjects that were interviewed reported that they did it to keep petting the dog; they were gaining some advantage from participating. For example, Subject 36 agreed to take the survey "because there was a dog"; most of the subjects in this pretext had similar responses. After agreeing to participate, 10 out of 15 subjects reported trusting the researcher almost solely because of the dog. Most stated that they would have trusted her no matter her appearance, age, or gender, as long as she had a dog with her. Subjects explained that in general, they trust people more if they have dogs with them. Subject 39 stated "anybody who walks around with a dog probably isn't part of a phishing scam". Subject 44 reported "dogs, man. I'll do anything for them". Subject 38 explained "it doesn't surprise me that this worked. It's something about the dog. Dogs are approachable. They're more approachable than people, and you offered for me to pet the dog, which is more enticing".

5. Discussion, lessons learned and future work

One study limitation was the timing during which data was collected. There were fewer students on campus during the summertime, which made it difficult to obtain a larger sample size. Second, students were varyingly present on campus during certain weeks/pretexts, contributing to the disparity between the number of subjects per pretext. There were more students on campus during the first week and the last week. Finally, construction on campus created noise pollution and impeded on the crowded target areas on campus. Because of this, students were dispersed across more areas, which also contributed to the varied sample sizes for the pretexts.

This study suggests that the *type of pretext in a SE attack is fairly insignificant*, as long as the attacker meets one of two conditions that makes the pretext believable and gains the target's trust: 1. *The adherence to the character role*: the person creating and initializing the pretext needs to fit into the character role for the age, gender, race, etc. of the person they are aiming to impersonate. For example, the researcher in this study fit into how an expected college student would appear, mainly based on age and clothing choice. 2. *A likeness factor*: there must be similarities between the person implementing the pretext and the target, which creates an aura of ease and comfort, with possible similarities including age, gender, or similar interests. Additionally, it is evident that a pretext can target more than a single psychological persuasion principle. As seen in this study, a single pretext (raffle) was able to target *reciprocity*, *natural inclination to help*, and inadvertently, *likeness*.

While these findings may hold true for a population on an urban college campus, other settings may differ. College students have a sense of unity, which could explain why the large number of subjects felt more inclined to help. A college campus is also separated from the dangers and chaos of the rest of the city, creating a safe space where people are more trusting; they are more accustomed to being approached by strangers. Researchers are encouraged to try (variations of) these pretexts in different settings. Also, future work could examine the importance of the likeness factor combined with the adherence to the character role in eliciting the most information in a SE experiment. It would also be beneficial to examine the other principles of persuasion and psychological phenomena mentioned in section 2.3 and the different types of SE tactics mentioned in section 2.1. Lastly, this studied examined in-person disclosure rates; future work could conduct a comparative study between online versus offline disclosure.

References

Acquisti, A., John, L.K. and Loewenstein, G. (2012) 'The Impact of Relative Standards on the Propensity to Disclose', *Journal of Marketing Research*, 49(2), pp.160–174.

Crawford, C. (2016) 'The Risks To the Privacy of the 'Like' on Facebook', *Social Media Today*, <https://www.socialmediatoday.com/social-networks/risks-privacy-facebook>.

Fotre, G. (2016) 'The 10 Most Common Password Security Questions', *Stumble Forward*, <https://stumbleforward.com/2012/08/20/the-10-most-common-password-security-questions/>.

Glassner, B. and Schapiro, M. (2018) 'Op-Ed: College kids aren't 'supercilious snowflakes'', *Los Angeles Times*, <https://www.latimes.com/opinion/op-ed/la-oe-glassner-schapiro-snowflakes-20180820-story.html>.

Hadnagy, C. and Wozniak, S. (2018) *Social Engineering The Science of Human Hacking*, Newark: John Wiley & Sons, Incorporated.

How can paid surveys help college students? 2019, *Opinion Outpost*, <https://www.opinionoutpost.com/en/blog/how-can-paid-surveys-help-college-students#.XYp0oyhJHqY>.

Joinson, A., Reips, U., Buchanan, T., and Schofield, C. (2010) 'Privacy, trust, and self-disclosure online', *Human-Computer Interaction*, vol. 25, no. 1, pp. 1-24.

Junger, M., Montoya, L. and Overink, F.-J. (2017) 'Priming and warnings are not effective to prevent social engineering attacks', *Computers in Human Behavior*, 66, pp.75–87.

Lopez, C (2018) 'Social Engineering Attacks by the Numbers: Prevalence, Costs, & Impact', *Datafloq*.

Luo, X. et al. (2011) 'Social Engineering: the neglected human factor for information security management', *Information Resources Management Journal*, 24(3), pp.1–8.

Madden, M. et al. (2019) 'Teens, Social Media, and Privacy', *Pew Research Center: Internet, Science & Tech*, <https://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>.

Obar, J., and Oeldorf-Hirsch, A. (2018) 'The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services', *Information, Communication & Society.*

Rege, A., Williams, K. and Mendlein, A. (in-press) 'A Social Engineering Course Project for Undergraduate Students Across Multiple Disciplines', *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*.

Richards, K., Dool, F., and Kennedy-White, J. (2017) 'Cost of Cyber Crime Study', *Accenture*, <https://www.accenture.com/t20170926t072837z_w_/us-en/_acnmedia/pdf-61/accenture-2017-costcybercrimestudy.pdf>.

Schechter, S., Brush, A.B. and Egelman, S. (2009) 'It's No Secret. Measuring the Security and Reliability of Authentication via "Secret" Questions"', *2009 30th IEEE Symposium on Security and Privacy*.

Shea, D. (2017) 'Sarah Palin's E-Mail Hacked: How It Was Done', *HuffPost*, <https://www.huffpost.com/entry/sarah-palins-e-mail-hacke_n_127553>.

Steinmetz, K. (2010) 'Study: Why We Think Women Are More Trustworthy Than Men', *Time*, <http://healthland.time.com/2010/12/13/study-why-we-think-women-are-more-trustworthy-than-men/?xid=huffpo-direct>.

Tiwari, A. (2018) 'What Is Social Engineering? What Are Different Types Of Social Engineering Attacks?', *Fossbytes*, < https://fossbytes.com/what-is-social-engineering-types-techniques/>.

The Top Ten Most Famous Social Engineering Attacks 2019, *Infosec Resources*, <https://resources.infosecinstitute.com/the-top-ten-most-famous-social-engineering-attacks/#gref>.

Uebelacker, S. and Quiel, S. (2014) 'The Social Engineering Personality Framework', *2014 Workshop on Socio-Technical Aspects in Security and Trust*.

Appendix A: Survey Administered to Subjects (Subjects Keep After Completion)

Please answer the following questions as applicable. You DO NOT have to answer every question.

1. Name: _____
2. Email Address: tu_____@temple.edu
3. TUID: 915_____
4. Phone Number: (_____) -_____ - _____

Are you 18 years or older? (check one): Yes_____ No_____

5. Birthdate: ____/_____/_____

Tell us about yourself!

6. What city are you from? _____
7. What is your favorite sports team?_____
8. What is your favorite food? _____
9. What is your favorite movie? _____
10. What is your favorite book? _____
11. What is the name of your favorite pet? _____
12. What Is your favorite number? _____
13. In what city did your parents meet? _____
14. What is your mother's maiden name?_____
15. What is the name of the street you grew up on?_____

Appendix B: Data Collection Instrument

Subject #:

Pretext Used:

Questions answered: (Y/N)

___1 First Name
___1.2 Last Name
___2 Email
___3 TUID
___4 Phone Number
___5 Birthdate
___6 City
___7 Sport
___8 Food
___9 Movie
___10 Book
___11 Pet
___12 Number
___13 Parents Meet
___14 Maiden Name
___15 Street

Appendix C: Post-disclosure Interview Questions

Subject # _____

Pretext # _____

1. Why did you initially agree to take the survey?
2. When taking the survey, did you realize that your answers could have been used to access your private information, such as passwords, login information, or security questions?
3. Why did you think you could trust me with your information?
4. Why did you not feel comfortable answering the questions you left blank?
5. Can any of this information be found on your social media pages publicly?