Factors Enabling Fraud: A Study of Social Engineering and Identity Theft

By

Brendan S. McDermott

A Master's Paper Submitted to the Faculty of the

DEPARTMENT OF MANAGEMENT INFORMATION SYSTEMS

ELLER COLLEGE OF MANAGEMENT

In Partial Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

In the Graduate College

THE UNIVERSITY OF ARIZONA

2016

STATEMENT BY AUTHOR

This thesis has been submitted in partial fulfillment of requirements for an advanced degree at the University of Arizona.

Brief quotations from this thesis are allowable without special permission, provided that an accurate acknowledgement of the source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: Brendan S. McDermott

APPROVAL BY MASTERS PAPER ADVISOR

This thesis has been approved on the date shown below:

_____ 05/06/2016

Dr. Mark Patton Date

Management Information Systems

ACKNOWLEDGEMENTS

I would like to thank my research partner, Ian Kaufer, and my advisors, Dr. Jesse Bockstedt and Dr. Matthew Hashim for their creativity, perseverance, and positivity throughout the course of this project. I give thanks to the SFS administrative team, Cathy Larson, Dr. Mark Patton, and Dr. Hsinchun Chen, for their support and guidance over the past two years. I would also like to express my gratitude for all the students who assisted us with the data collection as confederates: Cyrus Afarin, Calvin Barreras, Vincent Ercolani, Tiffany Feller, Ashley Ireson, AJ Jicha, Dominic Kaufer, and Jasper Puracan. Finally, I would like to thank my wife Joan for being by my side from the very beginning of this process.

This material is based upon work supported by the National Science Foundation under Grants No. DUE-1303362 and No. SES-1314631.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

In this paper we investigate a number of factors that make people vulnerable to social engineering and identity theft in particular. We do this by conducting a behavioral field experiment on the campus of the University of Arizona in Tucson, Arizona. Between May and December 2015, a group of eight confederates engaged over 600 potential subjects and collected a wealth of personally identifiable information.

1 INTRODUCTION

Information security breach reports often focus on the technological failures that enabled the attack; the malware, the patches, and the high-powered password crackers, to name a few. Yet, there is usually a less technology-oriented weakness in the defenses of breached companies, a weakness that cannot be merely patched over a long weekend. It is the human element of organizations.

When a technician leaves a remote login password written down and unprotected, when a customer service agent fails to verify the identity of someone claiming to need an address and phone number, or when a front-office worker accepts an unapproved USB from someone who appears to be a rushed job-seeker trying to print out a resume, these vectors are equally as fallible and perhaps more dangerous than standard technological defenses such as firewalls and two-factor authentication.

In information security parlance, exploiting the weaknesses in a human defense is known as Social Engineering. Although one could argue that the arts of deception are older than language itself, the age of the Internet and the rise of cybercrime provide a new context to these age-old techniques. Given the incredible wealth of information now stored in companies' databases, an advanced attack will often include some aspect of Social Engineering in a layered approach that includes a reconnaissance and delivery phase, such as the *Intrusion Kill Chain* (Hutchins et al. 2010).

In understanding how breaches occur and how to prevent them, it is fundamental to have a grasp of the factors involved in Social Engineering techniques. Many tales exist of charismatic confidence artists whose talents for manipulation allow them access to the most restricted of environments and there is much research into the cognitive biases that we humans possess in spite of our best efforts, but there has not been a thorough body of research developed around specifically the factors of reward and context to understand exactly why some people choose to give away precious information about themselves.

This study examines factors preceding Social Engineering vulnerabilities, namely fraud and identity theft, and does so in the context of behavioral economics.

2 BACKGROUND

2.1 Background / Literature Review / Previous Work

Stories and studies of deception, fraud, and identity theft abound, but not all of them relate directly to data theft in the sense of social engineering. This section will provide a topical overview of relevant stories in current events, a survey of popular literature and anecdotes of socially deceptive

hackers, an examination of academic explorations into social engineering, and illuminate some of the gaps remaining in the body of knowledge.

2.1.1 Popular Literature and Anecdotes

No discussion of social engineering would be complete without at least one reference to Kevin Mitnick, author of *The Art of Deception* (Mitnick & Simon, 2011) and often referred to as the "World's Most Famous Hacker". Mitnick's books are a collection of anecdotes of his life as a hacker, often conning hapless employees over the phone to gain access to their companies' data.

Mitnick provided the foreword on author and security professional Johnny Long's book *No Tech Hacking* (Long 2011). This book exists within a large body of instructional guidebooks about social engineering, explaining to professionals and amateurs alike the techniques of the trade.

In a similar vein, Chris Hadnagy, author of *Social Engineering: The Art of Human Hacking* (Hadnagy, 2010) and creator of the first social engineering framework, offers an instructional guide and includes terminology such as *pretexting, micro-expressions,* and *human buffer overflow.* Hadnagy's approach is based on the research of Dr. Paul Eckman, whose vast body of psychological research includes studies of deception, gestures, and facial expressions.

Although these types of books can offer some value in the form of professional education or entertainment, they are often told from the perspective of a skilled manipulator who has been honing their craft since their early teenage years. As you read their stories, it's easy to think that, sure, their victims might be foolish, but they are dealing with highly adept hackers, so the odds are against them. There is no sense of randomization or controlling for factors at all.

Amateur attempts at social engineering produce their own body of work, such as the DEF CON Social Engineer Capture the Flag contest, organized by Hadnagy and held in Las Vegas, NV each year (Jackson, 2014), in which contestants attempt to glean information over the phone while a conference of security enthusiasts looks on. The Robin Sage experiment (Ryan and Mauch, 2010) used a false LinkedIn profile of an attractive woman with the title of "Cyber Threat Analyst" and tricked hundreds of trained security professionals into providing information that breached the operational security standards of their employers.

2.1.2 News Reports

Information security attacks involving some element of social engineering are a nearly constant presence in the news. A notable breach took place in October 2015 when a hacker posed as a Verizon worker (by fabricating an employee ID) to trick a real Verizon employee into revealing CIA Director John Brennan's personally identifiable information (Zetter 2015). The hacker then used four digits of a bankcard and other information gleaned from Verizon to reset Brennan's AOL account password and gain access to it. The AOL account contained SF-86 forms (government security application forms with an incredible amount of data) and other sensitive personal information, including spreadsheets with the social security numbers of US intelligence officers.

In January 2016, A security savvy technician and heavy AWS user fell victim to a social engineering attack (Springer 2016) when WHOIS domain registration information about him was used to gather a zip code and email address, after which an online Amazon Customer Service agent was contacted via text chat. The attacker was given the real address and phone number of the target by

the Customer Service agent and then moved on to acquiring new copies of the target's credit cards. The target became aware of the situation, requested a new card and changed his account information, but the attacker attempted numerous times online and by phone to get access.

In both of the above examples, the attackers misrepresented themselves and deceived an employee to gain personally identifiable information without proper validation. An informal flash poll of 633 security professionals by *Information Week Dark Reading* (Cohodas 2014) ranked the most dangerous social engineering threats as: 56% lack of employee awareness; 21% phishing; 12% criminals; 6% other; and 5% *vishing* (VoIP phishing). This concern for employee awareness points to a deficit in training and appreciation for the dangers of social engineering and the impact it can have on the safety of citizens and customers.

2.1.3 Academic Literature

The ethics and proper design of phishing experiments have been under debate for a number of years. Finn and Jakobsson (2007) emphasize the importance of attempts to quantify vulnerabilities in order to understand where to focus preventative measures. Jagatic et al. (2007) performed a phishing experiment to harvest data on college students using social media data to manipulate the *context* of the attack learned that younger students are more vulnerable to phishing attacks and generated strong reactions including anger and denial. Griffith and Jakobson derived Mother's maiden names of over 4.1 million Texans in 2005, highlighting the weakness of this means of verification, although it is still commonly used.

Dimkov et al. (2010) performed a combination social engineering / pen testing experiment in the Netherlands in which master's students used any means at their disposal to gain possession of

eleven laptops without being caught by university security. A group of researchers from NYU-Poly studied certain psychological factors that would render an individual susceptible to spear-phishing (Halevi et al., 2015) by first providing a survey to determine certain characteristics of employees and then following up with a phishing email to see if they would respond to it. Many phishing experiments follow a similar model, examining for some factor while using email or false websites as the means of deception (Downs et al. 2007, Sheng et al. 2010, Hong et al. 2013).

Deception research in general has been well established in the field of psychology since the late 1800s (Corrigan 2013), including Milgram's landmark experiment on obedience in the mid-20th century (Milgram, 1963). The movement of certain economists into experimental work caused other economists to argue a ban on deception research, while it is still considered a useful tool for social scientists (Cook and Yamagishi, 2008). Economists and social scientists, agree, however, that when deception is pragmatic to understand the effects of a treatment, then it is the responsibility of the IRB to decide where the lines must be drawn ethically (Hertwig and Ortmann, 2008). In another 2008 paper, Hertwig and Ortmann conduct a survey of purported deception experiments and determine that there is not universal agreement on the meaning of the word "deception" as it applies to research methodology. An assertion is made that withholding information does not necessarily constitute deception (Hey, 1998).

2.2 Research Gaps

Although studies in deception have a long history in experimental social research, the recent interest in phishing and social engineering brings deception into the realm of technical professionals whose skill sets also include, for example, scanning and exploiting computer

networks and devices. The Internet allows criminals from around the world to trade in identities and PII in a manner inconceivable prior to the modern age, using this stolen data to its maximum economic benefit. This confluence of factors creates an opportunity for security researchers to examine the application of social techniques to risk appetites in the information security context. Workman (2008) conducted a social engineering field study in a large organization, using a combination of email attachments, web pages, and pretexting telephone calls from trained confederates to solicit confidential information, but did not engage their targets face-to-face.

3 EXPERIMENT AND METHODOLOGY

3.1 Introduction

In order to capture the data needed to understand particular weaknesses to social engineering, we designed a field experiment to gather Personally Identifiable Information (PII) from participants. To accomplish this required some degree of creativity, since following the usual conventions of lab experiments would not necessarily provide the quality of data that we were looking for, i.e., telling study participants up front that they were about to engage in an experiment involving deception would have introduced a number of confounding factors. Instead, we opted to conduct our data collection in the field, under the guise of a survey, with the offer to enter a raffle for free.

To understand the motivations of those who provide the information we were seeking, we chose to control for factors of reward (high reward / low reward) and situational context (profit / non-profit). Context variables are a way to differentiate between altruistic (charity) and utilitarian (marketing firm), while the two levels of reward distinguish between levels of utility for the participant, where a higher reward means more utility.

The premise of examining altruistic motivations has its foundation in sociology, as the urge to help others is a foundational element of social solidarity (Jeffries, 2014). Hence we thought that participants would be most likely to respond to the charity context. We also believed that participants would be most likely to respond to a higher reward (Von Neumann & Morgenstern, 2007), since the utility of the iPad mini is thought to be higher than the utility of a pizza, and therefore would be more willing to provide information in this situation. It follows that, based on the two previous beliefs, we also thought that the category with both the altruistic context and the higher reward would net the most personal information overall.

Study participants would be chosen at random on the campus of the University of Arizona and confederates would ask them if they wanted to enter a raffle, if so, then they could fill out the form. After completing the form, they would be asked to sit down with one of the researchers who would debrief them and ask the study participants to sign the consent form.

This final part caught the attention of the Institutional Review Board (IRB) and elevated our research application out of the department. It had not occurred to my research partner and me that our experiment design might be controversial due to its apparently deceptive nature. Our advisors were required to take additional steps to ensure that our methodology met the ethical standards of the IRB and the Department of Management Information Systems.

3.2 Field Collection Methodology

We used a two-by-two factorial design with two independent variables (context and reward) and two levels to each variable (charity context vs. commercial context, high reward vs. low reward). This design allowed us to study the interaction of both the independent variables and the levels within them and to later perform an analysis between each of the four categories: High Reward and Charity Context, High Reward and Commercial Context; Low Reward and Charity Context, Low Reward and Commercial Context.

Our approach began with defining the factors relevant to the experiment, high/low reward, and profit/ nonprofit context. To address the high or low reward component, we chose to offer a raffle for either an iPad mini (high reward) or a gift certificate for a pizza dinner at a local pizza restaurant (low reward). We assumed the value of the iPad mini to be around $400 and the value of the pizza dinner to be $50.

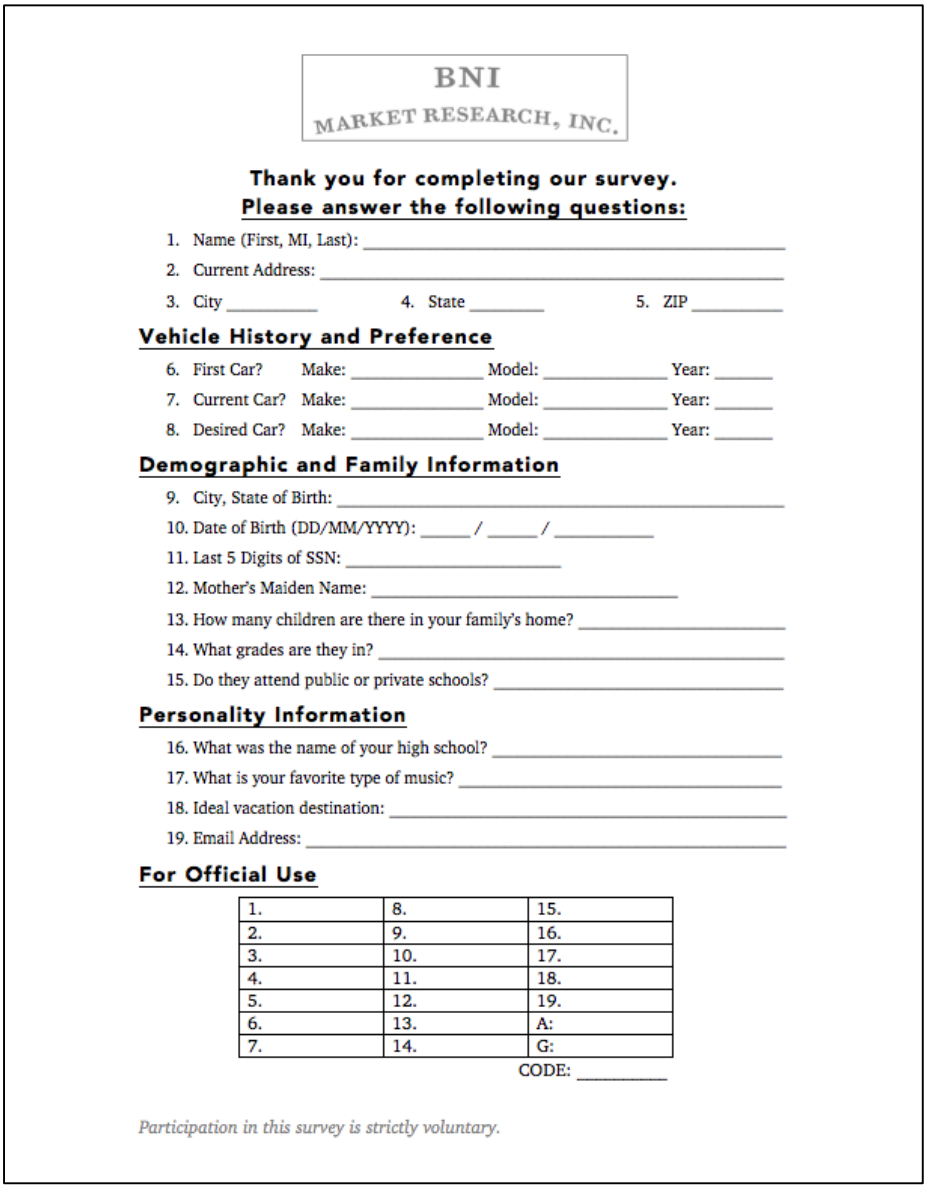
For the profit/nonprofit context, we chose to tell the participants that the information for the raffle was either going to be used for market research (BNI Market Research, a fictional company) or for a local charity (BFK, a fictional nonprofit organization).

	Profit Org	Nonprofit Org
Low Reward		
High Reward		

Table 1. Experimental Factor Matrix

For each category, we aimed to collect 30 data points, for a total of 120 subjects. This would allow us to perform a proper statistical analysis comparing the factors to one another.

The data we collected included obvious PII such as the last five digits of the social security number (SSN), mother's maiden name, date of birth, as well as some seemingly innocuous information such as name of high school and favorite type of music. A full list of questions and an example of the survey can be found in figure 1 below.



BNI

MARKET RESEARCH, INC.

Thank you for completing our survey.
Please answer the following questions:

1. Name (First, MI, Last): _____
2. Current Address: _____
3. City _____ 4. State _____ 5. ZIP _____

Vehicle History and Preference

6. First Car? Make: _____ Model: _____ Year: _____
7. Current Car? Make: _____ Model: _____ Year: _____
8. Desired Car? Make: _____ Model: _____ Year: _____

Demographic and Family Information

9. City, State of Birth: _____
10. Date of Birth (DD/MM/YYYY): _____ / _____ / _____
11. Last 5 Digits of SSN: _____
12. Mother's Maiden Name: _____
13. How many children are there in your family's home? _____
14. What grades are they in? _____
15. Do they attend public or private schools? _____

Personality Information

16. What was the name of your high school? _____
17. What is your favorite type of music? _____
18. Ideal vacation destination: _____
19. Email Address: _____

For Official Use

1.	8.	15.
2.	9.	16.
3.	10.	17.
4.	11.	18.
5.	12.	19.
6.	13.	A:
7.	14.	G:

CODE: _____

Participation in this survey is strictly voluntary.

Figure 1. Survey Example

3.3 Process

In order to run a successful field study and maintain our ethical standards, we needed to very carefully consider each stage of the data collection. We were careful to make clear after the survey was complete that the raffle was in fact real and that they had participated in an experiment approved by the university. One of us researchers would mark down whether or not the subject

completed the question (1-19) on the bottom of the perforated survey sheet, separate the bottom from the top, and shred the original information on site. There were a number of stages in the field experiment, from preparing the confederates to distributing the rewards.

3.3.1 Preparing the Confederates

We chose six of the confederates from a pool of other security researcher students in the Masters of Science in MIS program. Two confederates were undergraduate students who received extra credit in one of their courses for participating in the research. Each confederate was provided with a lanyard that had their name and the name of the fictitious organization printed on them (*Figure 2*).

Figure 2. Lanyards for Confederates

We provided the confederates with a script (*Appendix B*), though they were free to improvise slightly, with approval from the researchers. They were instructed to ask every third person passing by so as to avoid any individual preferences. Their clothes were informal, since this is the style of typical survey solicitors that engage passersby on campus. Dates and times for each collection period are displayed in *Appendix A.*

3.3.2 Engaging the Survey Participants

Each collection period took place outside of the Student Union Memorial Center (SUMC) on the campus of the University of Arizona. This is a well-trafficked area that contains the main bookstore, two coffee shops, a food court, and a lecture hall, among many other features, and it is a popular thoroughfare for students going to and from class. We typically collected data in the afternoon, between the hours of 12:00pm and 5:00pm, depending on the availability of the confederates.

The confederate would approach a subject and say, for example, "Excuse me, would you like to enter a raffle to win a free iPad? It's for market research."

Other conditions required a tailored approach based on the factors involved:
"Excuse me, would you like to enter a raffle to win a free iPad? It's for charity."
"Excuse me, would you like to enter a raffle to win a free pizza? It's for market research."
"Excuse me, would you like to enter a raffle to win a free pizza? It's for charity."

3.3.3 Collecting the Data

If the subject declined, then the confederate would record the time of the encounter as well as the gender and approximate age of the approached subject.

If the subject accepted, then the confederate would provide them with a pen and the clipboard containing the survey. Subjects were free to take all the time they needed to complete the survey, but it usually took no more than five to ten minutes.

3.3.4 Debriefing the Participants

Once the survey was completed, the confederate would ask the subject to sit down at a table and speak to their supervisor, who was actually one of the researchers. At this point, the confederate would return to engaging new subjects and the debriefing would begin.

The debriefing itself included a script that the researcher would read (*Appendix C*), the real raffle form for the subject to complete, and an optional consent form for the subject. At this point, the subject could choose not to consent, and we would destroy their data. Five subjects did in fact take this option. Responses from survey participants will be discussed in the qualitative analysis section.

3.3.5 Destroying the Original Information

At the point that the debriefing began, when the participant sat down, as one researcher started to explain the experiment, the other researcher would take the survey over to a table with the shredder (out of view of the confederates and the main thoroughfare). Here the researcher would mark off whether or not the participant answered the question, and record the time of the transaction, the gender, and age of the participant (based on the birth date provided or an approximation) on the lower portion of the survey sheet.

Once this was complete, the lower portion would be separated from the upper portion via the perforation, and the upper portion would be immediately shredded on site. This took place in front of the participants so that it would be very clear to them that their actual PII was being destroyed.

No one but the researchers was allowed access to either the completed surveys or the shredded papers. The shredded papers were ultimately destroyed in a secure disposal bin in the Department of MIS. No PII was saved after the debriefing.

3.3.6 Storing the Data

Each lower portion of the survey contained an anonymous unique identifier such as "D002" to ensure that each record was unique when entered into the final dataset. The researchers used a collaborative spreadsheet application to store data that included the unique ID, the date and time of the survey, the participant's gender and age, and whether or not the participant answered the questions. The researchers also stored data on rejections as recorded by the confederates, which included date and time, gender, and approximate age.

In a separate dataset, the researchers recorded the names and email addresses of participants who wished to enter one of the raffles. This information did not contain the unique identifier that was used for the research dataset, so there was no way to link the two together once the original surveys were destroyed.

3.3.7 Distributing the Rewards

After 118 surveys were collected, the researchers used a random selection function to determine the winners of the raffles based on the emails that they provided. Prizes were awarded in compliance with departmental procedures that include having the subjects sign a form including their name and address.

Given the relatively small number of entrants for each raffle (about 60), the odds of winning were substantially greater than most commonly held raffles or sweepstakes. Participants were not aware of this at the time of completing the survey, however.

3.4 Qualitative Methodology

The field collection methodology resulted in a rich data set, with 118 surveys completed and most of them providing valuable PII, including 115 cities and states of birth, 108 dates of birth, 85 mother's maiden names, and the last five digits of 34 SSNs. The entire experience, including reactions, quotes, and impressions, however, could not be captured with check marks corresponding to whether or not the subjects filled out a question in the survey. To capture and codify these additional experiences, we decided to include a qualitative approach as well.

In order to meet these ends, we collected a combination of field notes by the researchers and interviews with the confederates who actively engaged the participants. For my part, I kept notes on the times of each of the "blocks" of context/reward, general notes on the environment of each day (e.g., temperature and sky condition), personal observations, quotes that I overheard or were relayed to me, and stories in general of different reactions from participants.

For the interviews, we chose to use an unstructured format and a positivist approach, following guidelines recommended in *Research Methods in Anthropology* (Bernard, 2011). Although this is not an anthropological research project *per se*, a significant aspect of social engineering involves the culture in which it occurs, hence the "social" element. Therefore, the techniques of studying

cultural interactions from other disciplines are relevant to understanding how and why people are willing to part with their valuable personal data.

3.4.1 Overview

We chose to do interviews with the confederates in order to capture their first-hand experiences dealing with subjects in the field. From my own observations, I noticed that there were certain patterns that emerged from subjects engaging with the confederates and I wanted to follow up on them to see if I could verify the patterns that I noticed by speaking with the confederates who were actually face-to-face with the subjects who provided the PII in the four different scenarios.

The unstructured interviews consisted of open-ended questions based on an interview guide and script (*Appendix D*). The guide and script provide enough of a foundation that the questions remain focused on the most important details (i.e., "What sort of reactions did you observe while collecting the surveys?"), but leave enough room for probing questions to provide more depth. Since most of the interview subjects were my colleagues, it was unnecessary to make the interviews excessively formal.

3.4.2 Location

Interviews were held on the campus of the University of Arizona. All eight of them were conducted in the MicroAge Lab at the Eller College of Management, where the confederates were available during the day. The most important factors for the location were that it had some degree of privacy, a power outlet, and a minimal amount of background noise.

3.4.3 Technique

Primary audio recordings were taken using basic audio recording software with a high-quality microphone. Secondary recordings were made using a handheld recording device. Notes were taken during the interview and quotes were transcribed directly from the interview subjects.

3.4.4 Documentation

Coding of the field notes and interview text were conducted in accordance with guidelines suggested in *Basic Interviewing Skills* (Gorden, 1992). Coding text can be used to create an index of shorthand that can then be used to aggregate common themes and provide for a more rigorous analysis of qualitative data.

3.4.5 Storage

Audio and text files were stored locally (laptop hard drive), on an external hard drive, and in a cloud-based folder available to the other researchers.

3.5 Results

The following section will provide an analysis of the data we collected from both the subjects in the field, from my own notes during the execution of the experiment, and from interviews with the confederates after completion of the fieldwork. For a detailed statistical and quantitative analysis, please refer to my research partner's paper, *Human Exploits in Cybersecurity: A Social Engineering Study* (Kaufer, 2016).

3.5.1 Quantitative Analysis

The fieldwork efforts resulted in 118 surveys and 540 rejections, for a total of 658 total responses and a 17.9% response rate.

3.5.1a Total Responses by Factor

Our target number for each category was 30 responses. As we initially expected, the iPad and Charity group hit the target number first. By the time our collection schedule had run its course, we had gathered the following numbers.

	CONTEXT		
REWARD	**Commercial**	**Charity**	**Total**
Pizza	27	29	56
iPad	26	36	62
Total	53	65	118

Figure 3. Total Responses by Factor

3.5.1b Total Responses to Social Engineering Questions

Of the 19 questions on the survey, we chose five of them to represent the most significant social engineering questions.

- Name
- Date of Birth
- City and State of Birth
- Mother's Maiden Name
- Last five digits of SSN

To our surprise, 34 participants willingly provided part of their SSN, and more than three-quarters of participants provided the other social engineering information. 27.1% of subjects who completed the survey provided all five PII details.

QUESTION	NO. OF RESPONSES	% OF TOTAL
Name	117	99.2%
City, State of Birth	115	97.5%
Date of Birth	108	91.5%
Mother's Maiden Name	85	72.0%
Last 5 of SSN	34	28.8%
All of the Above	**32**	**27.1%**

Figure 4. Responses to Social Engineering Questions

3.5.1c PII Provided by Factor

Somewhat to our surprise, the pizza dinner proved to be much more tempting than we had initially expected, with 35.7% of respondents for the pizza reward providing all five PII details compared to 19.4% for the iPad. The commercial and charity groups were very close, within 2.1% of each other.

Our working theories about why this occurred revolve around two potential factors. One, it is possible that some number of people who filled out the survey for the pizza assumed that they might receive the pizza dinner right there after completing the survey, even though we never led them to believe this. There's a sense of immediacy about food that can be overwhelming, especially for a student population. Two, due to varying attitudes about the Apple brand and the necessity of a tablet, it may have been perceived as having the same value to everyone, even though it is worth about $400.

		CONTEXT		
REWARD		Commercial	Charity	Total
	Pizza	40.7%	31.0%	35.7%
	iPad	15.4%	22.2%	19.4%
	Total	28.3%	26.2%	27.1%

Figure 5. Percentage of Responses by Category

3.5.1d Confederate Response Rates

A factor that we needed to take into consideration when building the regression model was the individual response rate of each confederate. No one that we used was a professional solicitor, but certain confederates (Calvin and Ashley) were more confident and more capable than others (Tiffany and Vincent). This is a concern when we look at some of the "how-to" guides on social engineering written by Mitnick and Hadnagy. They are considered the very best at what they do and so their talents give them an outsized advantage and may skew any data that they could collect. Regardless, our confederates had response rates between 8.5% and 27.3%, with an average of 17.9%.

CONFEDERATE	SURVEY COUNT	REJECTION COUNT	TOTAL COUNT	SUCCESS RATE
Calvin	33	88	121	27.3%
Dominic	11	50	61	18.0%
Ashley	39	180	219	17.8%
AJ	13	61	74	17.6%
Cyrus	6	30	36	16.7%
Tiffany	5	35	40	12.5%
Jasper	7	53	60	11.7%
Vincent	4	43	47	8.5%
Total	118	540	658	
Average	14.75	67.5	82.25	17.9%

Figure 6. Counts and Response Rates by Confederate

3.5.1e Overall Responses by Gender

Figure 7 shows the number of responses to the survey separated by gender, starting with the total number of records on top and descending from that. Overall, responses from females appear to be relatively the same as males, at least before controlling for other factors. It is either a coincidence or a result of our random sampling efforts in the field that we received about 60 responses overall from each gender (60 female and 58 male).

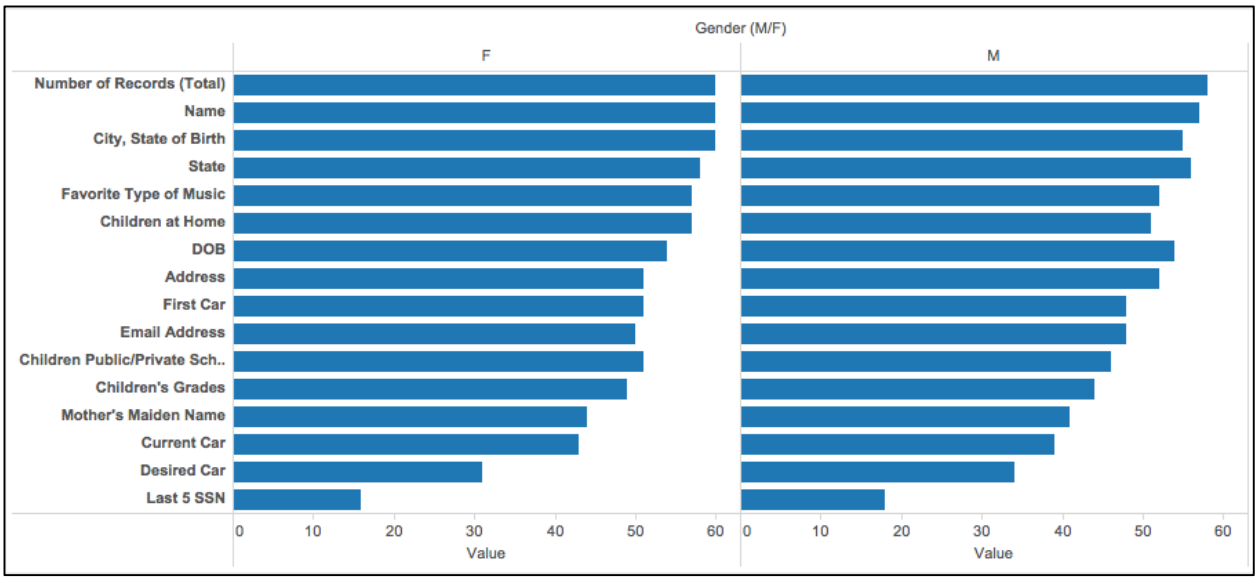


Figure 7. Total Responses by Gender

3.5.2 Qualitative Analysis

This section will first provide an analysis of observations from my field notes, to be followed by interview results with the confederates and my research partner, Ian Kaufer, who conducted 106 out of 118 debriefings.

3.5.2a Field Notes Overview

On the first day of data collection, May 13th, 2015, I did both the data processing, shredding, and debriefs all at once, with two confederates approaching the participants. The demanding pace of this setup did not allow for much in the way of pleasantries with survey participants who had just realized what they had done, i.e., given me more information than they should have.

The instantaneous switch from "You could win a raffle!" to "This is an experiment..." provoked shocking emotional reactions from about five respondents. One respondent, whose data was not included in the quantitative analysis since this person decided to withdraw consent, when I informed them that they had participated in an experiment, their face turned sour with shame and disappointment. My heart sank as I observed them recoil with the realization that they had made an error by exchanging their PII for a chance at some material good. This would become a theme as the experiment progressed, and I have chosen to categorize the members of this group as *angry refusals.* Although this group did not usually provide surveys and therefore were not part of the 118 data points, Ian and I agreed that they represented two per session over the course of ten sessions, for a total of 20, meaning 20/138 or 14% of respondents.

On the other hand, I found myself astonished at the apparent thoughtlessness of certain participants as they blithely completed all of the information on the survey form, and when told that they had engaged in an experiment, merely shrugged and continued to fill out the consent and actual raffle forms. I chose to categorize this group as *blithe participants*, at the opposite extreme from the *angry refusals*. This group provided all of the five social engineering data points, signed the consent form, and continued about their merry day. Based on our analysis, this group represented 34/138 individuals or 25% of all survey participants.

Most responses fell somewhere in between. Based on my initial impressions from engaging with survey respondents, people were willing to provide some of the social engineering data, but were surprised when they discovered that they were taking part in an experiment. Some were interested in our work and some were not, but this group provided city and state of birth, date of birth, mother's maiden name, signed the consent form, and provided their email addresses for the raffle.

I have labeled this group the *contented center*. They represented 51/138 individuals or 37% of all participants.

There is another, shrewder group, that I have labeled the *security savvy.* This group either tended to ask a lot of critical questions about the survey before completing it, or in some cases, willingly admitted to providing false information for the purposes of entering the raffle. In the event that they completed the survey, these types typically wanted to engage in a little more conversation during the debriefing. It's perhaps encouraging that 33/138 individuals or 24% of respondents fit this description, and did not provide either the last five digits of their SSN or their mother's maiden names. It would be interesting, however, to ask this particular group why 30 of them chose to provide their city and state of birth and 23 of them chose to provide their date of birth.

Group Name	Characteristics	Proportion
Angry Refusals	Confrontational, Disappointed, Frustrated	14%
Blithe Participants	Oblivious, Unconcerned, Naïve	25%
Contented Center	Neutral, Unfazed, Accepting	37%
Security Savvy	Alert, Curious, Suspicious	24%

Table 2. Group Categories of Respondents

3.5.2b Interview Results

In the interest of understanding more about the interactions of the confederates and the debriefing researcher with the subjects of the experiment, we conducted interviews with each of them seeking to capture their individual perspectives. Overall, the confederates had the experience one might expect from any type of job soliciting the public: a lot of people wearing headphones, a lot of

rejection, and a lot of being ignored. As our collection time took place in the afternoon between noon and five p.m., a number of students would be in a hurry to either get to class or get to whatever social event they were heading to.

For our confederate Calvin, who had the highest success ratio, of 27%, he thought that the suggestion of the prize most often caught people's attention and he thought that the context did not make a difference when getting people to respond. He said that after the debriefing, there were some subjects who came up to him, shaking their heads in disappointment that they had given up whatever information they had provided and some said, "I knew something was going on." This last statement leads one to question what exactly compelled these individuals to continue to provide PII even if they felt that something fishy was happening.

Our confederate Ashley, who received the highest number of responses overall, had a similar experience, and was left with the impression that people were more interested in getting something for free rather than engaging in the context of either the charity or the market research. She brings up another issue that we had not expected, but had become a theme: college students appeared to be more interested in the pizza than the iPad. Ashley and many of the confederates noted that many students would claim that they already had an iPad or were not interested in it in general.

The negative responses that confederates experienced typically occurred following the debriefing, when a subject would give them a sort of dirty look, as if to say, "How could you do this?" or during the questionnaire, when they realized what types of questions were on it. The following excerpt describes a subject reacting negatively to the types of questions on the survey and expressing their views to our confederate Vincent.

The one that I really remember that did respond to me was the one older gentleman who responded and he got halfway through the thing and said, "I don't want to do this anymore. I don't like the idea of this," and grabbed his paper and started to walk away and I directed him to you guys. And I'm not sure what he discussed with you afterwards, but he was like, as soon as we asked him for five digits of his social security and some of the other things he's like, as soon as he got past the cars [questions on the form] he's like, "I'll put the car information, but after that..." he's like, "you guys are asking too personal, that's it, I'm done." I think I had two people that did that, but I remember him the best.

Q: So he started filling it out because he was interested in, whatever it was, the iPad, the Pizza... do you remember what it was?

It was probably the pizza, and I don't even know if he was so interested in the pizza or more interested in just, you know, giving to the research, because it was the research one [Books For Kids] I don't think it was the marketing one. I think it was the research for the Books For Kids. So he was interested in giving to that, the information. But as soon as it got to be personal information he's like, "I don't care what kind of research you're doing, I'm not giving you, giving you this stuff" and, you know, he was completely done. He was like, "That's it, gimme the paper. I'm not giving you anything. I want to be finished!" [laughter]

The confederates' stories confirm that reactions like the one described above were rare, but did occur on occasion. Most of the subjects did not show any strong emotions upon completing the survey, but some reacted strongly during the debriefing with Ian.

> *There was also another instance where a guy essentially gave me a... I don't know if "death glare" is a clinical term, but he was very angry in a very quiet and passive-aggressive way. He didn't seem to comprehend why we were doing this and so he just stared at me while I was explaining the debriefing. After I completed the debriefing, his one word was, "Okay...?". I don't remember if he gave up his information, I'm pretty sure he did not, but he did want the raffle.*
>
> *Q: When did that happen?*
>
> *It was within the first five seconds [of the debrief], when, I'm talking to him, most people are nodding their heads or at least interrupt with a question, and he made a very... mean-looking face... He said very few words. He didn't question the debriefing, he didn't question our experiment -- He was just angry, I suppose.*

These examples were certainly the most extreme that we experienced. Thankfully, in the spirit of our research, we received positive responses as well, from people who were happy to have learned a lesson without anything particularly bad happening to them. Our confederate Jasper recounts this story:

This wasn't in the moment, but, probably like an hour later [a girl who completed a survey] sends me a message and says, "You know, that kind of taught me something, that I should probably be more careful about giving out my information, even if it's someone I know."

And that wasn't in the interaction at the table outside, but, that still, I believe is a pretty positive response to it is, "I realized I had messed up and made a mistake, but it taught me something and it was valuable because it was a situation where there wasn't any risk attached."

We found these types of responses encouraging, of course, because we would like to see more people understanding the value of their personal information. When we started with the design of the experiment, we understood that we could potentially prompt some very negative responses, but that the overall positive outcome would be worth it.

These quotes offer a number of lessons to inform future social engineering studies. They suggest that a follow up survey with participants who provided their email addresses would be exceptionally useful in capturing some of the qualitative feedback from subjects who would perhaps like to offer their own perspective on the experience. Also, it would be a good idea to have some additional training for the confederates about how to address a disgruntled or upset participant in a systematic way. It may also be useful to allow these angered individuals to express themselves, perhaps anonymously, via a web form, so that we can capture their perspective without requiring their email address.

Regarding how these quotes relate to the factors of the experiment, I believe that, especially in Vincent's case, they provide some evidence that people are willing to go to certain lengths to help

out what they perceive to be a good cause. This raises other questions about why people choose not to verify organizations that claim to be charitable, but in presenting the results of this research, I have been told stories of other lengths to which my colleagues have gone in the interest of helping out "a good cause", even when the nature of the cause seemed ambiguous. The man in Vincent's story wanted to complete the survey because he wanted to support the charity, an altruistic impulse, but changed his mind when he discovered that supporting this cause would require him to put himself potentially at risk of identity theft.

It is interesting to note that the interviews do not suggest that the confederates had any suspicions that gender-matched subjects would provide more information or that there was, in fact, a link between the charity and high reward groups. The experience of the confederates focused mostly on whether or not subjects were responding at all (response rate) and not so much on the details of the information that they were providing. Once the surveys were completed, the metadata was recorded and the original data shredded before any inferences of this sort could be made in the field.

3.6 Discussion

This research is only the beginning of understanding the reasons why people provide their PII for the promise of a reward, large or small. It would be ideal in this case to follow up with a survey and perhaps see if similar results are produced with a larger data set. Now that information security is such a topic of great interest, it's possible that researchers from other disciplines will begin to examine some of the human factors that lead to such large data breaches. Hopefully, our work can provide some insight and perhaps a useful methodology to continue these studies. Although there are many limitations to working in the field in terms of controlling variables, it is the truest way to understand how people will actually react given these types of situations.

We learned that a high reward and a charitable context in combination is a favorable scenario to collect PII from an individual, but we were surprised that we collected so much under any circumstances. We also determined that gender-matched confederates and subjects were more likely to gather personal information, regardless of the context. Over 27% of respondents, when provided with either scenario, were willing to provide enough information to allow their identities to be stolen. These results raise a number of questions about how identity verification should be handled altogether, if one out of four people will happily divulge their most unique personal data for a chance to win a prize.

Most subjects had a neutral response to learning that they had been manipulated. A vocal few had an overtly negative response, but these did not end up in the dataset, so the qualitative aspect was useful to capture these experiences. We know that at least one student felt grateful that they had been duped in an experimental context and that they should think twice about what they put on

paper. Other participants were simply curious about how experimental research is conducted and were happy to have the opportunity to engage with actual fieldwork, even at the expense of essentially breaching their own security.

Future analysis may involve focusing purely on a financial reward instead of a "prize", since the perceived value of the prize may differ. For example, offering a $50 and $400 reward instead of dinner or iPad may provide a clearer contrast between the factors. Collecting from a more diverse group of subjects, with different ages, professions, and education levels might provide a richer body of data. There were perhaps ten non-college aged potential participants who, after reading some of the questions, refused to participate in the raffle, even if they had been initially interested.

To build upon this study, it would be helpful to engage a more thorough qualitative approach from the beginning. This aspect was not something that we had initially considered, so the confederate interviews could only take place months after the events had taken place. A more homogenous group of confederates would also improve upon the execution. We were grateful to have the master's students who helped us, but the response rate ranged from 9% to 27%... ideally it would be more even. If we used, say, the same two confederates, had them dress exactly the same each time, and go into the field at the same time each time would reduce some of the influential factors.

A follow up survey collecting attitudes about the experience from the perspective of the subjects might help us learn something about the effectiveness of this technique as a training method. We don't know if any of the people who took the survey changed their behavior or found it to be a better or worse learning tool than other attempts to teach about personal information security. We don't know if they had ever had training at all in information security, but we know from the

debriefings that many subjects were not aware of the practices of social engineering. Since we did have such a young group as a population, it's worth considering the effect this may have on how employers train new hires or how colleges might approach introducing information security practices into their freshman orientations.

4 CONCLUSION

In this experiment, we designed an ethical way to test how much PII people would be willing to provide. We provided a context of either a charity or a market research firm, and provided a chance to win a free iPad mini or a pizza dinner. Eight confederates stood outside the student union at the University of Arizona and collected information from 118 survey respondents. 27% of these respondents provided their name, date of birth, mother's maiden name, city and state of birth, and the last five digits of their social security number. 72% provided all of the above, but not the SSN. The combination of the charity and the iPad mini garnered the most PII (36 responses), but the pizza category on its own turned out to be the more successful reward (35.7% success rate). Participants were two times as likely to provide these five PII items to a member of their same gender. Our design is easily replicated and, if executed correctly, upholds the ethical standards expected of professional research. All of the original data has been destroyed in accordance with IRB guidelines. We hope that future studies will be able to build upon the methodology that we have created here to understand the economic and security implications of personal identity theft and fraud.

5 REFERENCES

Bernard, H. R. (2011). Research methods in anthropology: Qualitative and quantitative approaches. Rowman Altamira.

Cohodas, M. (October 2, 2014). *Poll: Employees Clueless About Social Engineering.* InformationWeek Dark Reading. Retrieved from: http://www.darkreading.com/perimeter/poll-employees-clueless-about-social-engineering-/a/d-id/1316280

Cook, K. S., & Yamagishi, T. (2008). A defense of deception on scientific grounds. Social Psychology Quarterly, 71(3), 215-221.

Gorden, R. (1992). Basic Interviewing Skills. Itasca, IL: F. E. Peacock.

Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons.

Hertwig, R., & Ortmann, A. (2008). Deception in social psychological experiments: Two misconceptions and a research agenda. Social Psychology Quarterly, 71(3), 222-227.

Hey, J. D. (1998). Experimental economics and deception: A comment. Journal of Economic Psychology, 19(3), 397-401.

Hutchins, E.M., Cloppert, M.J., Amin, R.M. (2010) *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* Lockheed Martin Corporation Whitepaper. Retrieved from: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Jackson Higgins, K. (2014). *Social Engineering Grows Up.* InformationWeek Dark Reading. Retrieved from: http://www.darkreading.com/informationweek-home/social-engineering-grows-up/d/d-id/1204252

Jakobsson, M., Finn, P., & Johnson, N. (2008). Why and how to perform fraud experiments. *Security & Privacy, IEEE*, *6*(2), 66-68.

Jakobsson, M., Finn, P., & Johnson, N. (2008). Why and how to perform fraud experiments. *Security & Privacy, IEEE*, *6*(2), 66-68.

Jeffries, V. (2014). The Palgrave handbook of altruism, morality, and social solidarity: formulating a field of study. Palgrave Macmillan.

Kaufer, I. (2016). Human Exploits in Cybersecurity: A Social Engineering Study. *University of Arizona Master's Report.*

Long, J. (2011). No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress.

Milgram, S. (1963). Behavioral study of obedience. The Journal of abnormal and social psychology, 67(4), 371.

Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. John Wiley & Sons.

Ryan, T., & Mauch, G. (2010, July). Getting in bed with Robin Sage. In *Black Hat Conference*.

Springer, E. (January 25, 2016). *How Amazon customer service was the weak link that spilled my data.* Ars Technica. Retrieved from: http://arstechnica.com/security/2016/01/how-amazon-customer-service-was-the-weak-link-that-spilled-my-data/

Von Neumann, J., & Morgenstern, O. (2007). *Theory of games and economic behavior*. Princeton university press.

Zetter, K. (October 19, 2015). *Teen Who Hacked CIA Director's Email Tells How He Did It.* WIRED. Retrieved from: http://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/

APPENDIX A

Field Collection Dates and Times

Date	Times	Confederate(s)	Researcher(s)
5/12/2015	2:00pm - 4:00pm	Jasper and Tiffany	Brendan
9/2/2015	3:30pm - 5:30pm	Dominic	Brendan and Ian
9/16/2015	2:00pm – 4:00pm	Ashley	Ian
9/18/2015	11:30am – 1:30pm	Calvin	Ian
10/7/2015	2:00pm - 4:00pm	Ashley	Brendan and Ian
10/30/2015	1:30pm - 3:00pm	Cyrus and Ashley	Brendan and Ian
10/30/2015	3:00pm - 4:30pm	Vincent and Calvin	Brendan and Ian
12/2/2015	2:00pm - 4:00pm	Calvin	Brendan and Ian
12/2/2015	2:00pm - 4:00pm	Ashley	Brendan and Ian
12/15/2015	12:45pm - 2:30pm	AJ	Brendan and Ian

APPENDIX B

Script for Confederates

"Excuse me sir/ma'am, would you like to do a survey for a chance to win a (free iPad mini / free pizza dinner)? I am working with the (Books For Kids / BNI Market Research) organization and we are doing this because..."

1. Books for Kids
"Collecting data helps us to compare the needs of demographic groups in the US Southwest. It's for a good cause."

2. BNI Market Research
"Collecting data helps us to understand the needs of various local market segments and how they might respond to certain products."

[If they accept] "Thanks, here is the survey and a pen."

[If they decline] "That's okay, you can still enter the raffle if you would like by completing a raffle form." [Provides actual raffle form.]

APPENDIX C

Debrief Script

Thank you for participating in this research. Please allow me to explain the context of the survey. It was actually conducted as part of a University of Arizona study on persuasion and human behavior. We will destroy any information that you have provided to us today.

[*The confederate will make note of which questions were answered on a perforated section of the same document, and either return the survey to the subject or destroy it on site.*]

Your information is truly helpful in understanding the factors related to why individuals choose or refuse to provide personal information. The raffle is real and we will contact you if you are the winner. We will not sell or distribute your email address to anyone. Have a great day.

*** If the subject does not engage, they can still take the survey.
Script: If you don't want to take the survey, you can still enter the raffle by providing you email address on a raffle form.

[*Hands the subject the actual raffle form.*]

APPENDIX D

Interview Guide

Brendan McDermott
University of Arizona

Social Engineering Qualitative Study Interview Questions

1. How would you describe the types of people who participated in the survey? What particular categories come to mind?
2. What particular interactions with participants during the survey that stand out to your mind? Why?
3. What differences did you notice in reactions and responses between the different contexts and rewards?
4. What did you find surprising about the general interactions that you had with people?
5. What would you say was the most positive response that you received?
6. What would you say was the most negative response that you received?
7. Tell me about your opinion on the ethics of this experiment and that of deception research in general.