2018-06-01

Training Security Professionals in Social Engineering with OSINT and Sieve

Jared James Meyers
Brigham Young University

Training Security Professionals in Social Engineering with OSINT and SiEVE

Jared James Meyers

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Derek L. Hansen, Chair
Dale C. Rowe
Justin S. Giboney

School of Technology

Brigham Young University

ABSTRACT

Training Security Professionals in Social Engineering with OSINT and SiEVE

Jared James Meyers
School of Technology, BYU
Master of Science

This research attempts to create a novel process, Social Engineering Vulnerability Evaluation, SiEVE, to use open source data and open source intelligence (OSINT) to perform efficient and effectiveness spear phishing attacks. It is designed for use by “red teams” and students learning to conduct a penetration test of an organization, using the vector of their workforce. The SiEVE process includes the stages of identifying targets, profiling the targets, and creating spear phishing attacks for the targets. The contributions of this research include the following: (1) The SiEVE process itself was developed using an iterative process to identify and fix initial shortcomings; (2) Each stage of the final version of the SiEVE process was evaluated in an experiment that compared performance of students using SiEVE against performance of those not using SiEVE in order to test effectiveness of the SiEVE process in a learning environment; Specifically, the study showed that those using the SiEVE process (a) did not identify more targets, (b) did identify more information about targets, and (c) did lead to more effective spear phishing attacks. The findings, limitations, and future work are discussed in order to provide next steps in developing formalized processes for red teams and students learning penetration testing.

Keywords: social engineering, open source intelligence, ethics, IEEE, ACM, red team, cyber kill chain, cyber security

ACKNOWLEDGEMENTS

Many people helped to get me to where I am now. I would say that all those in my life supported me and knew that I can do whatever I set my mind too. This all started with a mentor asking me what I wanted to do with my life. I was back in school after a long break, and I thought chemistry was my calling. Quickly, I changed it to accounting and then to Information Systems. During this time, many people suggested I do that which I enjoy doing. That is what helped me decide to do a Masters. I came to love cyber security, especially social engineering. My chair and advisors have been fundamental in building me up and helping me perform this study.

My family and friends have always stood behind me, beckoning me to be better and to do more with my life. Nothing would have gotten done if not for their constant words of encouragement and questions that challenged and pushed me to learn. They are equally attributed to this study.

Finally, to Brigham Young University which desired that I push forward and complete my studies. To the many instructors, professors, and mentors, thank you for all your hard work in getting me out of bed to complete the many assignments and challenges you gave me to challenge me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Social Engineering and Red Teams

Cybersecurity “red teams,” or “ethical hackers,” are hired by organizations to attempt breaking into systems to evaluate security vulnerabilities through penetration tests, or a network ecosystem evaluation. These vulnerabilities could be based on a wide variety of security soft points, or specific vulnerable processes and systems. These can include open network systems, improperly trained employees, and even incorrect physical security practices. It becomes the job of an organization to harden, or increase security of, these potential failure points based on the information gathered by the red team after their penetration test. The scope of a penetration test is defined early on in this process and is signed by the organization and the red team. The scope document verifies the work the red team is allowed to do, and protects them from recourse from the company if an individual becomes alienated due to the Social Engineering processes followed by the red team (Debrosse, Debrosse, & Harley, n.d.).

Current trends in the use of social engineering have almost exponentially increased per year and continue to grow at similar rates (APWG, 2017). This issue is further compounded because a social engineering attack is usually coupled with another piece of malicious code, like ransomware or malware (Neely, 2017). Because of this trend in black hat attacks, or malicious attacks, red teams are more often tasked to use social engineering attacks to assess social engineering security vulnerabilities. This need requires an effective and efficient process for red teams to use in order to find targets within the hiring organization, create custom specific attacks, and launch the attacks in an ethically sound manner. However, such a process has not yet been developed or tested. Before the red teams can protect their organizations, these red teams need to be trained in recognizing these attacks by understanding the best practices that black hat teams are utilizing by exposing themselves to the tools and attacks available.

1.2 Open Source Intelligence

Many tools are available currently to create social engineering attacks. The most efficient tools are those that are free and available to all individuals participating in these attacks (red teams, black hats, etc.). Open Source Intelligence (OSINT) is a commonly-used method in the Cyber Security industry within the reconnaissance phase of the cyber kill chain(“Cyber Kill Chain® · Lockheed Martin,” n.d.). It is defined as a tool that involves collection, analysis, and use of data from open sources for intelligence purposes (Koops, Hoepman, & Leenes, 2013).

Figure 1-1 is a depiction of the Cyber Kill Chain and depicts the first 3 stages of what we will be covering in this research. OSINT has been used in the past as a tool to track and catch criminals, monitor movement of individuals, and even to create population overviews based on public postings but is now also being used as a data gathering tool by organizations to profile new customers or their own employees to understand them better. This process can be leveraged and used by red teams to protect their organizations, or by malicious users to compromise their targets. The problem is that organizations have differing levels of risk to Social Engineering due to publicly available information that their employees willingly or unwillingly share. OSINT, if used effectively, has the potential to compromise internal personnel networks by allowing red teams and black hats access to personal data on those that may be potential targets. Since OSINT helps with gathering pertinent target data, a spear phishing attack created with OSINT should have more effective results.

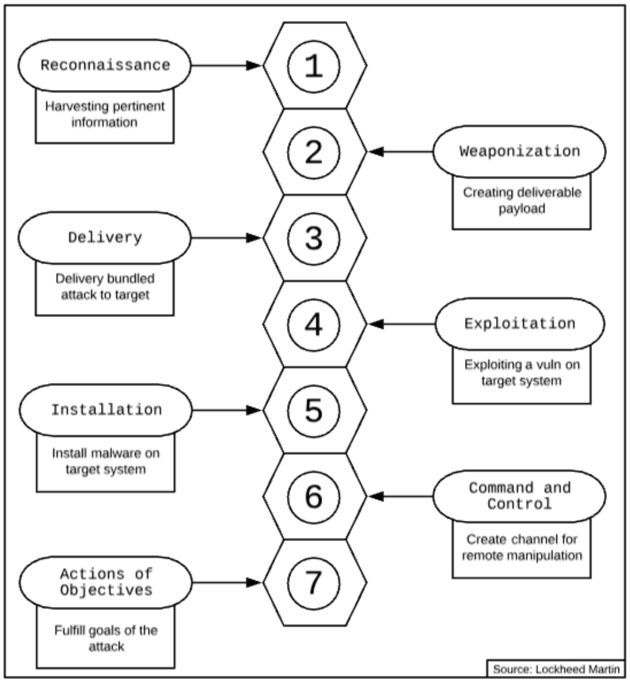

Reconnaissance
Harvesting pertinent information
1
2
Weaponization
Creating deliverable payload
Delivery
Delivery bundled attack to target
3
4
Exploitation
Exploiting a vuln on target system
Installation
Install malware on target system
5
6
Command and Control
Create channel for remote manipulation
Actions of Objectives
Fulfill goals of the attack
7
Source: Lockheed Martin

Figure 1-1 Lockheed Martin's Cyber Kill Chain

1.3 SiEVE Process

The SiEVE process, Social Engineering Vulnerability Evaluation, is a novel process that is a step by step process based on the framework in the cyber kill chain reconnaissance step. This process was created by the researchers and has been iteratively developed to perform this task. The purpose of the SiEVE process is to give a red team a defined process that increases the efficiency and effectiveness of a social engineering campaign during a penetration test. The idea behind creating a defined process is to allow quick enumeration of targets, or individuals at the organization, and quick discovery of useful information for creating directed spear phishing attacks. This process was tested in a Pilot Study by the researchers of this thesis and shown to be effective in doing the following: decrease the amount of time needed to enumerate targets, gather information for those targets, and increase the amount of gathered information. We intend to take these preliminary results and expound upon them herein to show that it can also be applied to the next two steps in the cyber kill chain by increasing the test population and controlling for more variables.

The study of the SiEVE process was performed with a between subject experiment design with two conditions "With SiEVE" or participants that have the process, and "Without SiEVE" or participants that do not have the process. These two conditions are the independent variables while the data being generated through the experiment are dependent variables. This will allow a full understanding of the data sets and simpler interpretation of the results.

1.4 Research Objectives, Questions and Hypothesis

1.4.1 Research Objective

Develop the SiEVE process for identifying personal information that can be used in spear phishing attacks. This will be iteratively developed and tested based on the feedback of security professionals and security students. The goal is to produce an efficient and effective process to identify targets, perform virtual reconnaissance on those targets, and create customized spear phishing attacks using OSINT techniques.

1.4.2 Research Question

Does the SiEVE process improve efficiency (time to perform reconnaissance and attack) and effectiveness (ability to identify key individuals and personal information about them) for cybersecurity students with security knowledge, but minimal training?

1.4.3 Research Hypotheses

Hypothesis 1: Students using the SiEVE process will generate more targets in a given timeframe than students not using the SiEVE process.

Hypothesis 2: Students using the SiEVE process will collect more personal information about targets in a given timeframe than students not using the SiEVE process.

Hypothesis 3: Students using the SiEVE process will create more effective spear phishing attacks in a given timeframe than students not using the SiEVE process.

2 REVIEW OF THE LITERATURE

2.1 Introduction to the Literature Review

This literary review will cover the network infrastructure within an organization and we need to first understand what tools and research there is when it comes to Social Engineering and Open Source Intelligence. First, we need to look at what data there is currently for the growing trend of social engineering as a black hat attack vector. Next, definitions will be given on how to interpret the various items we will discuss in this research. Finally, the general reaction within an organization after a red team runs a penetration test will be evaluated. This will allow for proper context as the data is explained.

2.2 Social Engineering as an Attack Vector

In a report created by Wombat Security Technologies, it is clear that the threat of social engineering attacks is a high risk (Wombat Security Technologies, 2016). They report that 76% say they were victims of phishing attacks from a data set of 500+ employees. So, from a global collection of professionals across 16 industries, there were hundreds of active social engineering breaches. This is further backed by 51% stating that attacks are increasing at their companies. This trend is increasing as attacks are more complex and use less resources (Abraham & Chengalur-Smith, 2010). The report states that the black hats can do this because there is more data available without proper security and protection in place. While the report states that rates of phishing are down, effective phishing, or phishing attacks that compromise an end user, are about the same. Also, other reports for 2017, show that attacks are becoming more frequent and more sites being created for phishing which are now hosted using HTTPS (APWG, 2017). This means that black hats are getting more effective at creating directed attacks at individuals and breaching their privacy. There is a need for red teams to assess the effectiveness of black hat attacks by understanding and implementing their own attacks before there is data loss which can lead to even more serious system and network breaches.

More research compounds the issue of social engineering by also stating that it is increasing, and extrapolates that attacks are becoming more sophisticated and more automated (Neely, 2017). In the InfoSec Reading Room article by the SANS Institute about the 2017 Threat Landscape, it is made clear that the largest threat to an organization is from social engineering. The responders in the survey sent out by the SANS Institute had 74% stating that clicking an embedded email link was one of the top threats facing their organization. 48% stated that a web download link was a top threat as well. This means that a large majority of threats included direct user intervention which required an end user, or target, to perform an action they would not normally perform. This is further compounded that 40% of responders labelled spear phishing and whaling as the top threat with significant impact for their organization. The survey results go on to address that the second most impactful threat would be various ransomware malware that is almost always coupled with social engineering as an attack vector. There is clearly a need for an organization to take steps to mitigate these threats as they continue to compromise and plague the industry.

2.3 Defining Terms

The research question states that the SiEVE process was created to increase efficiency and effectiveness of spear phishing in a security environment. Efficiency in a penetration test is paramount as many other security vulnerabilities need to be evaluated, not just the vulnerability towards Social Engineering. This means that a penetration test must have fast moving evaluator processes to fully evaluate an organization's ecosystem. For this research, efficiency will directly correlate to the time it takes to complete the task, or how many tasks can be completed in a given timeframe. Effectiveness in a penetration test is the success rate of running the processes. This means that when an attack is sent, the returning results of compromise compared with the lack of results dictate the overall effectiveness. In other words, effectiveness is how many exploited vulnerabilities appear during a process driven, efficient penetration test compared to a non-process driven, inefficient penetration test. It is measured differently for each step in the SiEVE process, as explained later. For example, effectiveness may be measured by the number of targets identified, the amount of information gathered about targets, or the success of a spear phishing attack on tricking a target.

There are two overarching styles of social engineering: Person-Person and Person-Person via media (Ivaturi & Janczewski, 2011). Person-Person attacks require the attacker and the target to be in the same room. An example of this kind of attack is piggybacking, where the attacker follows the target through a door or checkpoint under the pretense that the attacker is with the target. Even if it is not explicitly stated in a corporate policy, it is considered piggybacking and is a social engineering attack. Another example of a Person-Person attack is Pretexting or mimicking. In simple terms, the attacker pretends or impersonates a figure of authority to gain access to sensitive information or to a sensitive area. This does not necessarily need to be done in person but is categorized by a physical interaction with the target, or target organization. This is a high risk, high reward attack as it requires the attacker to leave the relative protection of a network and place themselves physically within an organization. This is usually only done if there is confidence of success in the attack or if there is no network to breach remotely.

Person-Person via Media attacks are the attacks generally associated with social engineering in the cybersecurity industry. These attacks can be as general as a phishing email, or as calculated and crafted as a Cross Site Request Forgery attack. The latter is when the attacker tricks the target's web browser into performing undesired actions in the target's name (Ivaturi & Janczewski, 2011). This could be done to execute malicious code on the victim's computer which could lead to further risky operations like the download and execution of ransomware, or software that takes the host computer hostage for money. The types of attacks that this research, and subsequently the SiEVE process, will focus on are phishing and spear phishing. Phishing is simply asking for credentials and personal information from an authoritative platform that tricks the target into thinking the attacker is somebody more trustworthy. This is the Person-Person via Media version of Pretexting and has become the most used Person-Person via Media attacks (Lee, Choi, & Kim, 2007). Spear phishing is like phishing, but is taken further and is usually backed by reconnaissance. This means that the spear phishing attack is used to attack one specific target and is tailored to that person. Usually, a spear phishing attack is created and targeted towards high priority targets; individuals of interest that have elevated rights or roles within an organization (Krombholz, Hobel, Huber, & Weippl, 2015).

Open Source Intelligence is a common way of handling information as more and more data is available for consumption. Originally used by government organizations and law enforcement, OSINT is now being leveraged as a tool to recon targets within the Cybersecurity industry (Tabatabaei & Wells, 2016). Because of the rise of social media and the cheapness of large, long-lasting storage, data is much easier to keep and search through allowing for all individuals with a little bit of training to search for sensitive information on a specific person. Frameworks have been created to track and log data trails on criminals, but what would happen if that is flipped? Criminals, black hats, can easily locate high priority targets and large amounts of publicly available information before committing to an illegal act. Since OSINT in the sense of social engineering is all open source and public, the data gathered is legal and available. It is not necessarily the fact that it is publicly available that makes it valuable or dangerous, but the amount of scrutiny it has gained (Mercado, 2008). The example Mercado points to is that military documents sometimes attach 3rd-party photographs like magazine clippings that depict military vessels. To the magazine reader, it is an interesting picture of a military vessel, but to an intelligence officer, it is verification of the enemy's power or even location data of that specific vessel. An example for a black hat would be a selfie, or picture of one's person, on a Social Media site. To the friends of the target, it is a memory of something enjoyable, but to the black hat, it could be verification that the target is not currently home or the photo has a geotag showing exactly where the target currently is located allowing for unrestricted access to an account, or a physical location. The use of OSINT within the realm of social engineering is untapped and not well documented as most literature talks about using OSINT from a militaristic sense when it is just as useful during the first step of the Cyber Kill Chain (Ansari, Akhlaq, & Rauf, 2013).

Even though a red team has the duty to defend the organization's critical information and systems, it is up to other individuals to classify and protect the organization's data. That individual is the Data Steward who performs proper Data Governance (Thomas, 2013). The steward works within the organization to classify the data they store to define the data distribution policies and protect sensitive information. Not only are these policies used to protect customer information, but also employee information. This is done by creating organization wide standards that all employees must follow in all aspects of daily business practices. When it comes to what a black hat wants for a phishing attack, the data classifications and policies created by a data steward do not have any bearing on what is necessary for a successful phishing attack. Since a red team will be tasked with protecting data they collect during their engagements just like the data steward, a new data classification will need to be created to give a value to information gathered by using OSINT. Since no literature covers this type of Data Governance, this will need to be done in the future.

2.4 Managing Organizational Reactions

Early studies have shown that the response to these simulated red hat attacks are negative and are due to poor employee training regarding social engineering (Jagatic, Johnson, Jakobsson, & Menczer, 2007). This means that there is a need for proper training and coordination between red teams and the hiring organization. To do this, many large corporations are hiring full-time security teams that handle their day-to-day network security. If they are unable to handle a breach, then they hire a 3rd-party contracted red team to assist the organization. This requires cooperation between three separate entities and trust that a 3rd-party has access to potentially sensitive employee and customer information. Since there currently is a negative reception to most red team security tests (Jagatic et al., 2007), there is a great need for better processes and controls to create a stable relationship between the two entities before a 3rd-party is hired into the organization. This needs to be done before the red teams perform a penetration test within an organization especially if Social Engineering is within scope as it is the attack vector with the most negative potential within an organization.

2.5 Intended Behavior

During the research, we intend to change the behavior of the targets as we attempt to explain them as a vulnerability. BJ Fogg has a well-defined series of behaviors that work with social engineering (Fogg, 2010). In his “15 Behavioral Patterns” there are two that fit the goal of a red hat or black hat. They are GreenDot and BlueDot behavioral patterns. In a GreenDot pattern, the end user (in our case, the target) performs a new behavior one time. This behavior is considered a new, or unfamiliar behavior, like opening a link within an email, downloading an unknown attachment, or replying to the sender of an email that the target does not know. A BlueDot behavior is like GreenDot, but instead performs a familiar behavior one time. It is the goal of a phishing attack to gain the trust of the target and immediately leverage that trust to change their behavior once. This allows for the red hat or black hat to compromise the target and retrieve the desired outcome. In each of the 15 behavioral patterns, there is a cue, or trigger, that the target sees that leads to the intended behavior. For a spear phishing attack, this could be a hobby, individual that the target knows, etc. that convinces the target to trust the attack and perform an action. This requires a tailored process of information gathering on the part of the red team to find the cue during the reconnaissance, leverage the cue by creating a spear phishing attack, and gaining the trust of the target in the process.

2.6 Processes and Checklists

It is well documented in many industries that having a meticulous, yet simple, set of steps can increase the effectiveness of an organization without drastic cost or risk. In the book

Checklist Manifesto, it states that with any complex task there are two possible outcomes of error: those of ignorance, in which the operator lacks the information necessary to perform a task properly; and those of ineptitude, in which information, although accessible, is not properly used, leading to faulty or incomplete execution (Gawande, 2010). Gawande also references Peter Provonost’s checklist for intensive care units on how to insert catheters properly. Using the simple, step-by-step process, infections for patients were observed to drop from 2.7 per 1000 patients to zero after three months. This illustrates that having a specified process, even though the operators are professionals, decreased the rate of infections and proved effective (Provonost, 2001).

3 METHODOLOGY

3.1 The SiEVE Process

The SiEVE process, Social Engineering Vulnerability Evaluation, will be developed using an iterative process wherein feedback from experts and pilot tests with students will inform future iterations. Specifically, an early version of the process was created and tested with a class of Brigham Young University (BYU) Information Technology (IT) students. The experience also provided practical feedback on how to improve the SiEVE process. During the thesis, improvements to the process, including addressing issues raised in the pilot test and adding instructions on creating spear phishing emails have been added to increase the efficacy of the process.

3.1.1 The Pilot Study

The pilot study of the first version of the SiEVE process was conducted in Winter 2017 with students from an IT 466: Information Assurance course here at BYU. Class students were randomly assigned into two equal groups. Both groups were given a series of questions asking them to identify members of the Network Security Team for BYU's Office of Information Technology and perform reconnaissance on them. Additionally, one of the groups was given the same set of questions with an accompanying set of SiEVE steps. The "with SiEVE" group was 18 students and the "without SiEVE" group was 19 students. Both groups were given the same primer on spear phishing and what types of information were useful to successfully phish a high priority target. This primer was given before splitting the groups, so all participants received the same briefing before the pilot study.

Each group performed the tasks separately and started at the same time. The amount of time to completion was measured and evaluated with other indicators, such as finding specific answers to questions like “What username does a specific user use?” and “What Social Media accounts can you find for that person?” These answers were then quantified and measured against both groups. The results of this pilot are shown in Table 3-1 and Table 3-2. Focusing on the difference between the aggregated results at the bottom of the tables compared between the independent variables (With SiEVE and Without SiEVE groups) can help with drawing conclusions.

The questions both groups were asked are as follows:

- What is your First and Last Name?
- What is your level of knowledge on Social Engineering? (1 being Very Low and 10 being an Expert)
- What is the Full Name of the IT department at BYU?
- Who is the current Chief Information Officer?
- Who is the Information Security Officer?
- Name 3 members of the BYU OIT Security Team.
- What is my title at BYU (As in myself, Jared Meyers)?
- What is my Username, or a handle that I use?

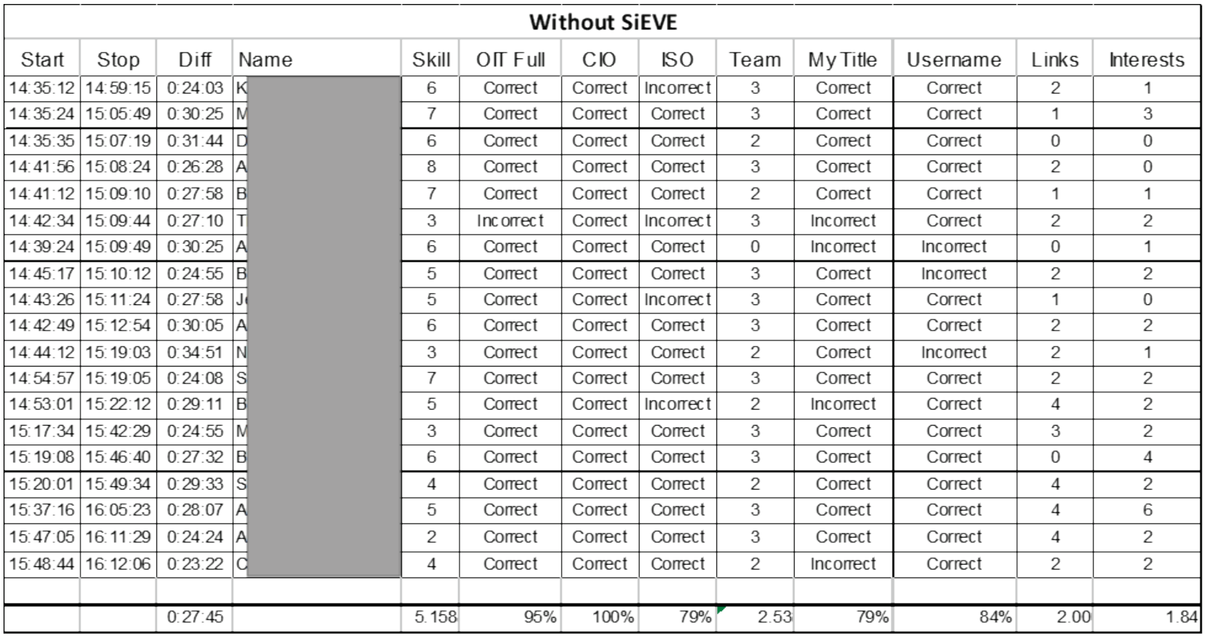
- What are the links to my Social Media?
- What are some of my hobbies and Interests?

Looking at the results from the Pilot Study, having a set series of steps and guidelines increases the amount of useful information gathered and reduces time to obtain the same information. In all metrics, except for enumerating the CIO, the With SiEVE group outperformed the Without SiEVE group. This theory that having a set process providing "better" results is not only backed by the pilot, but is also used in other domains.

3.1.2 The Current SiEVE Process

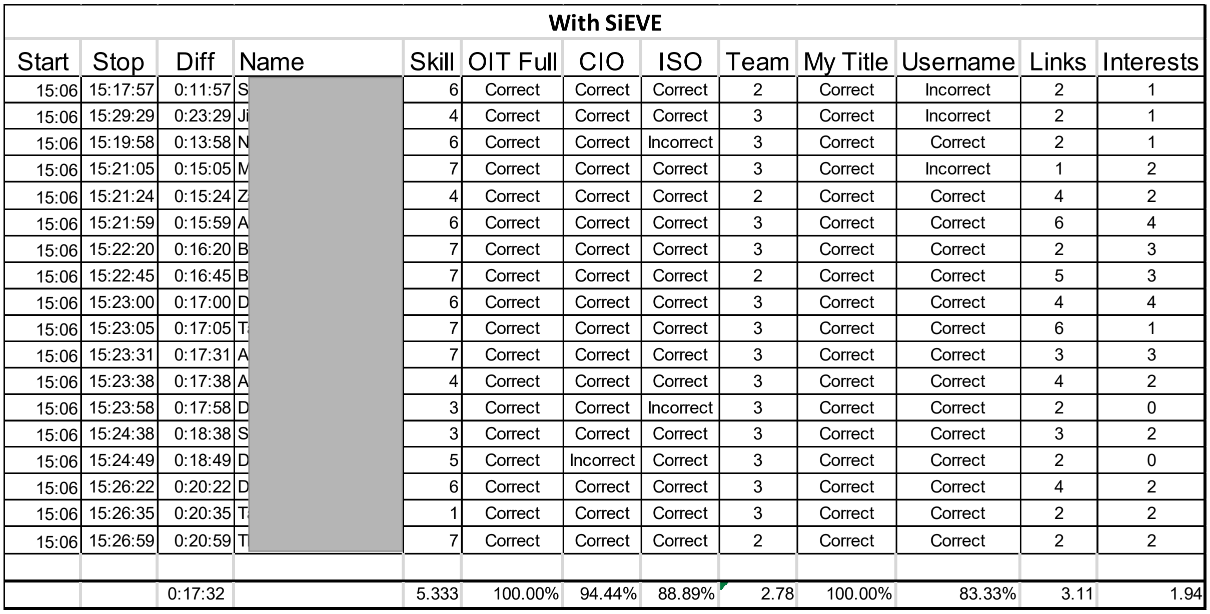
The following information is what is given in the non-Organization specific version of the SiEVE process. The full process with examples from BYU will be included as Appendix A. Both documents were given to the participants, but this version below was used during the study.

Table 3-1 Table 3-1: Participants Who Were a Part of the Pilot Who Did Not Use SiEVE



Without SiEVE												
Start	Stop	Diff	Name	Skill	OIT Full	CIO	ISO	Team	My Title	Username	Links	Interests
14:35:12	14:59:15	0:24:03	K[redacted]	6	Correct	Correct	Incorrect	3	Correct	Correct	2	1
14:35:24	15:05:49	0:30:25	M[redacted]	7	Correct	Correct	Correct	3	Correct	Correct	1	3
14:35:35	15:07:19	0:31:44	D[redacted]	6	Correct	Correct	Correct	2	Correct	Correct	0	0
14:41:56	15:08:24	0:26:28	A[redacted]	8	Correct	Correct	Correct	3	Correct	Correct	2	0
14:41:12	15:09:10	0:27:58	B[redacted]	7	Correct	Correct	Correct	2	Correct	Correct	1	1
14:42:34	15:09:44	0:27:10	T[redacted]	3	Incorrect	Correct	Incorrect	3	Incorrect	Correct	2	2
14:39:24	15:09:49	0:30:25	A[redacted]	6	Correct	Correct	Correct	0	Incorrect	Incorrect	0	1
14:45:17	15:10:12	0:24:55	B[redacted]	5	Correct	Correct	Correct	3	Correct	Incorrect	2	2
14:43:26	15:11:24	0:27:58	J[redacted]	5	Correct	Correct	Incorrect	3	Correct	Correct	1	0
14:42:49	15:12:54	0:30:05	A[redacted]	6	Correct	Correct	Correct	3	Correct	Correct	2	2
14:44:12	15:19:03	0:34:51	N[redacted]	3	Correct	Correct	Correct	2	Correct	Incorrect	2	1
14:54:57	15:19:05	0:24:08	S[redacted]	7	Correct	Correct	Correct	3	Correct	Correct	2	2
14:53:01	15:22:12	0:29:11	B[redacted]	5	Correct	Correct	Incorrect	2	Incorrect	Correct	4	2
15:17:34	15:42:29	0:24:55	M[redacted]	3	Correct	Correct	Correct	3	Correct	Correct	3	2
15:19:08	15:46:40	0:27:32	B[redacted]	6	Correct	Correct	Correct	3	Correct	Correct	0	4
15:20:01	15:49:34	0:29:33	S[redacted]	4	Correct	Correct	Correct	2	Correct	Correct	4	2
15:37:16	16:05:23	0:28:07	A[redacted]	5	Correct	Correct	Correct	3	Correct	Correct	4	6
15:47:05	16:11:29	0:24:24	A[redacted]	2	Correct	Correct	Correct	3	Correct	Correct	4	2
15:48:44	16:12:06	0:23:22	C[redacted]	4	Correct	Correct	Correct	2	Incorrect	Correct	2	2
		0:27:45		5.158	95%	100%	79%	2.53	79%	84%	2.00	1.84

Table 3-2 Participants Who Were a Part of the Pilot Study Who Used SiEVE



With SiEVE												
Start	Stop	Diff	Name	Skill	OIT Full	CIO	ISO	Team	My Title	Username	Links	Interests
15:06	15:17:57	0:11:57	[redacted]	6	Correct	Correct	Correct	2	Correct	Incorrect	2	1
15:06	15:29:29	0:23:29	[redacted]	4	Correct	Correct	Correct	3	Correct	Incorrect	2	1
15:06	15:19:58	0:13:58	[redacted]	6	Correct	Correct	Incorrect	3	Correct	Correct	2	1
15:06	15:21:05	0:15:05	[redacted]	7	Correct	Correct	Correct	3	Correct	Incorrect	1	2
15:06	15:21:24	0:15:24	[redacted]	4	Correct	Correct	Correct	2	Correct	Correct	4	2
15:06	15:21:59	0:15:59	[redacted]	6	Correct	Correct	Correct	3	Correct	Correct	6	4
15:06	15:22:20	0:16:20	[redacted]	7	Correct	Correct	Correct	3	Correct	Correct	2	3
15:06	15:22:45	0:16:45	[redacted]	7	Correct	Correct	Correct	2	Correct	Correct	5	3
15:06	15:23:00	0:17:00	[redacted]	6	Correct	Correct	Correct	3	Correct	Correct	4	4
15:06	15:23:05	0:17:05	[redacted]	7	Correct	Correct	Correct	3	Correct	Correct	6	1
15:06	15:23:31	0:17:31	[redacted]	7	Correct	Correct	Correct	3	Correct	Correct	3	3
15:06	15:23:38	0:17:38	[redacted]	4	Correct	Correct	Correct	3	Correct	Correct	4	2
15:06	15:23:58	0:17:58	[redacted]	3	Correct	Correct	Incorrect	3	Correct	Correct	2	0
15:06	15:24:38	0:18:38	[redacted]	3	Correct	Correct	Correct	3	Correct	Correct	3	2
15:06	15:24:49	0:18:49	[redacted]	5	Correct	Incorrect	Correct	3	Correct	Correct	2	0
15:06	15:26:22	0:20:22	[redacted]	6	Correct	Correct	Correct	3	Correct	Correct	4	2
15:06	15:26:35	0:20:35	[redacted]	1	Correct	Correct	Correct	3	Correct	Correct	2	2
15:06	15:26:59	0:20:59	[redacted]	7	Correct	Correct	Correct	2	Correct	Correct	2	2
		0:17:32		5.333	100.00%	94.44%	88.89%	2.78	100.00%	83.33%	3.11	1.94

3.1.2.1 Introduction

The SiEVE process (Social Engineering Vulnerability Evaluation) is a set of steps designed to help security teams create and evaluate general and spear phishing attacks. The process will help you identify targets, perform reconnaissance on them, and craft custom phishing attacks.

3.1.2.2 Sidebar: Definitions

- SiEVE Process – a process that helps security teams (e.g., red teams) create and evaluate phishing attacks as part of a penetration test
- Target – the person of interest who will be attacked
- Reconnaissance – gathering information about an organization or target
- General Phishing (or just Phishing) – the deceptive practice of sending a message (e.g., email) designed to induce targets to unknowingly reveal personal information such as login credentials
- Spear Phishing – a phishing attack where the message has been tailored to a specific target based on information gathered during reconnaissance

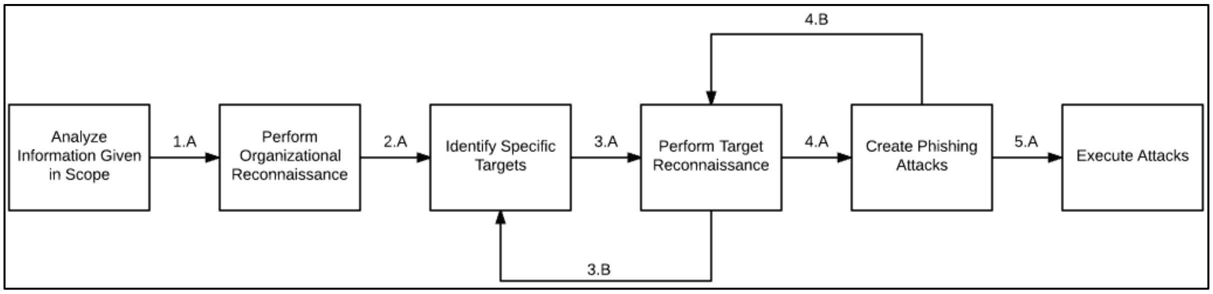

4.B
Analyze Information Given in Scope
1.A
Perform Organizational Reconnaissance
2.A
Identify Specific Targets
3.A
Perform Target Reconnaissance
4.A
Create Phishing Attacks
5.A
Execute Attacks
3.B

Figure 3-1 Flow Chart for SiEVE Process

3.1.2.3 Analyze Information Given in Scope

Review the base information that the organization has given you for the penetration test. This should include the organization name(s) and information about what is in and out of scope.

1. List all names for the organization.
2. List specific credentials (i.e., access rights) to look for that may be owned by targets within the organization.

3.1.2.4 Perform Organizational Reconnaissance

If the organization has multiple departments or groups, list each one within the organization. Note that finding the specific groups (or teams) is much harder than specific departments as a department is usually more structured. This step is focusing resources on an organization's structure to list out the possible departments of interest. Doing this allows for a security team to remove unimportant departments and give value to each department.

1. List as many departments within an organization as possible.
2. Rank each department from most important to least.
3. For each department, find one high profile target as a baseline.

3.1.2.5 Identify Specific Targets

Attempt to add subordinates to the list using simple search queries. We are increasing the attack surface of our penetration test by including as many individuals as possible. Remember that the best targets have access to more information.

1. Google the current target list and find other similar employees.
2. When completing the current target list, complete step 1 for any newly added targets.
3. Remove any targets that do not fit into the scope of the penetration test.
4. After all simple searches are complete (i.e. no more results), switch to publicly available data on high profile websites.
    a. Facebook
    b. LinkedIn
    c. Twitter
    d. Organization Specific Websites
    e. etc.

3.1.2.6 Perform Target Reconnaissance

Take each target found in 3.A and do information searches on each one. The goal is to find relevant information on the target, such as their hobbies or interests. Any information could work for this step, but the more details found, the better your attack can be later. Since you could have a long list of targets, find 2 to 3 details about a target and move on. Take note of individuals that have a lot of public data as they are usually more willing to give out their information.

1. Perform simple Google searches using the targets name with and without their title. A site like this one (https://www.social-searcher.com/google-social-search/) could aid in speed of searches.
2. Using any positive results from Step 1, delve into any social media hits (i.e. Facebook, Twitter, LinkedIn, Instagram, etc.).
3. Make note of any prolific user and their username and save for a later step.
4. Save any information you find on each target.

3.1.2.7 Create Attacks

Taking all the information found in previous steps, we are now ready to create spear phishing attacks. This step will vary greatly for each penetration test as each target list will vary in size and available information.

1. Select a base target to spear phish
2. Pick the simplest piece of information as the bait
3. Prepare the attack and set aside
4. Repeat steps for as many targets as you have time for in this penetration test

3.2 Summative Evaluation

A summative evaluation of the SiEVE process was conducted. Specifically, it was tested by two groups who received the same primer information of how the study will take place and then were given separate instruction where one group receives the SiEVE process and one does not. They will be referred to as the “With SiEVE” and the “Without SiEVE” groups. Students from “IT 366: Information Assurance and Security” (Winter, 2018) will be assigned based on their course section into the two groups. The Tuesday lab group of students were assigned into the Without SiEVE group and the Thursday section were assigned into the With SiEVE group. We anticipated that each group will have at least 25+ students, which gave a sufficient sample size. Each phase of the SiEVE process (identifying targets, profiling targets, crafting spear phishing email) will be evaluated separately in this methodology.

Before any work was completed by the student participants, the participants signed a consent form which will include approval to use their data. The consent form will be in Appendix B. The students were also told that they would be graded strictly on completion, and not on data gathered as this exercise was part of the course. However, they were told to do their best in completing the task and observations indicated that students took it seriously and stayed on task.

3.3 Identifying Targets

The first task that both groups will complete is enumerating a list of employees here at BYU. They can include names of employees at other organizations only if they have a direct contact with an active BYU employee. For example, if a BYU professor has a contact with a professor at another school, then they could be included in this enumeration process. This is considered a one-hop connection. Also, students were not allowed to login or use any of their personal accounts to identify targets. If any of the information was gathered contrary to what the participants were asked to do, then the researcher will filter out the data and be removed.

Each group had thirty-minutes to complete this task in order to keep the time frame consistent. The With SiEVE group was given an additional five minutes prior to this thirty-minutes to read the SiEVE process document. Students input the information they found in a spreadsheet to track their progress. The key dependent variable for this task is the number of targets identified. The difference between the With SiEVE and Without SiEVE groups was evaluated based on the average number of targets named by each student within the spreadsheet.

3.4 Profiling Targets

The second task, which was performed after a short break from task one, had both groups working with the list they created in the prior task discussed in 3.3 Identifying Targets. During this section they used open source intelligence to find as much information about each enumerated target. They were briefed that they may not log in to any site and had to use only information and sources that they discovered publicly, exactly in the same way as part 1. The With SiEVE group used the SiEVE process documentation during this task as well.

This task was timed for thirty minutes to ensure a consistent data collection between both groups. The information gathered on these targets was similar to that asked for in the Pilot Study. The data that was gathered included but was not limited to the following:

- Full Name, including pseudonyms and nicknames
- Current place of residence, or city/zip code if specific address is unavailable
- Email Addresses
- Phone numbers
- Social Media accounts, like Facebook or LinkedIn
- Personal Blog or website
- Hobbies and Interests
- Children or close relatives
- Birthday and other personally identifying data (e.g., employee number, netid)

The SiEVE process outlined websites and techniques useful in gathering this data. This process is documented in section 3.1.2.5. Some of this information is primarily useful to gather other information such as accounts, personal information, and hobbies.

3.5 Crafting Spear Phishing Emails

The third task will have both groups (With SiEVE and Without SiEVE) using information provided by the researchers gathered using the SiEVE process on specific targets with consent from the targets. These targets were from three distinct demographics with elevated credentials or important access. The three groups with the target names redacted are as follows:

- Security Professionals
    - Security Professional 1 (SP1) – Senior Security Architect
    - Security Professional 2 (SP2) – Access Manager Security Analyst
- Professors
    - Professor 1 (P1) – Adjunct Professor for the Vietnamese Language
    - Professor 2 (P2) – Distinguished Professor of Virology and Immunology
- Student Employees
    - Student Employee 1 (SE1) – Laboratory Industrial Hygienist
    - Student Employee 2 (SE2) – Risk Management Industrial Hygienist

A list of the participants was split into their groups (With SiEVE or Without SiEVE) where they were randomized and then assigned to three targets, one from each group. This means that about 20 attacks were created for each target. These attacks were then randomized and relabeled so that the targets did not see the author's name. In this case, the attacks were labelled after the letters in the NATO phonetic alphabet and given in bulk to the targets. The targets then placed each attack by its corresponding letter in order from “most likely to get me to click on a link, open an attachment, or respond” to its least likely equivalent then state which of the attacks would compromise them. So, if target P1 has the lineup of “Alpha, Bravo, Charlie, Echo” and stated that only “Alpha and Bravo” were attacks that would compromise them, then they would state that “Charlie” is their threshold of trust. The top 5 rated attacks for each target will be included in Appendix C.

3.6 Data Analysis

After the student participants completed the reconnaissance and attack creation processes, their data was collected in aggregate to obfuscate the individuals. The data was aggregated and secured according to the consent given by the student participants. This means that every data set was labelled with a letter and number instead of the participant’s name. The data points that were collected were listed by steps in the process along with their associated acronyms: Identifying Targets, Profiling Targets, and Crafting Spear Phishing Emails.

- Identifying Targets
    - Targets Enumerated – T
- Profiling Targets
    - Targets with Information Gathered – TwI
    - Sum of Information Gathered – SoI
    - Targets with Personally Identifiable Information (PII) Gathered – TwP
    - Sum of PII Gathered – SoP
    - Targets with Accounts Gathered – TwA

    - Sum of Accounts Gathered – SoA
    - Information per Target – IT
- Crafting Spear Phishing Emails
    - Overall Rating of Attacks Separated by Group – OR

These data points were collected and used to prove the effectiveness and efficiency of the SiEVE process. For each data point, there was a specific process to calculate the numbers. Targets Enumerated was a count of names in the first column with duplicate names ignored. Targets with Information was Targets Enumerated with any potentially useful piece of information listed. Sum of Information Gathered is the sum of all pieces of information. So, if one target had four piece of information, then Targets with Information would be incremented by one and Sum of Information Gathered would be incremented by four.

Targets with Personally Identifiable Information Gathered was a count of Targets Enumerated with PII given. PII, for the sake of the data is defined as personal emails, phone numbers, and information like birthdays. Sum of PII Gathered is the sum of all pieces of PII gathered. Targets with Accounts Gathered was the count of Targets Enumerated with Accounts found. Accounts would include social media and other enterprise information, but not including email addresses. Sum of Accounts Gathered was the sum of all Accounts discovered. Information per Target was just the Sum of Information Gathered divided by Targets Enumerated.

The data was then processed using logarithmic transforms if the data was skewed and t-Tests to show if the differences between group's averages were significant.

4 FINDINGS

4.1 Introduction to Findings

As stated in the Research Objective, the goal was to develop the SiEVE process to help security professionals become more effective and efficient in creating social engineering attacks for red team penetration tests. To show the efficacy of the experiments, the data set acquired is shown in aggregate in Table 4-1 for the Without SiEVE group and Table 4-2 for the With SiEVE group. The specific data points of importance are highlighted to show the statistically significant differences in performance between the two groups.

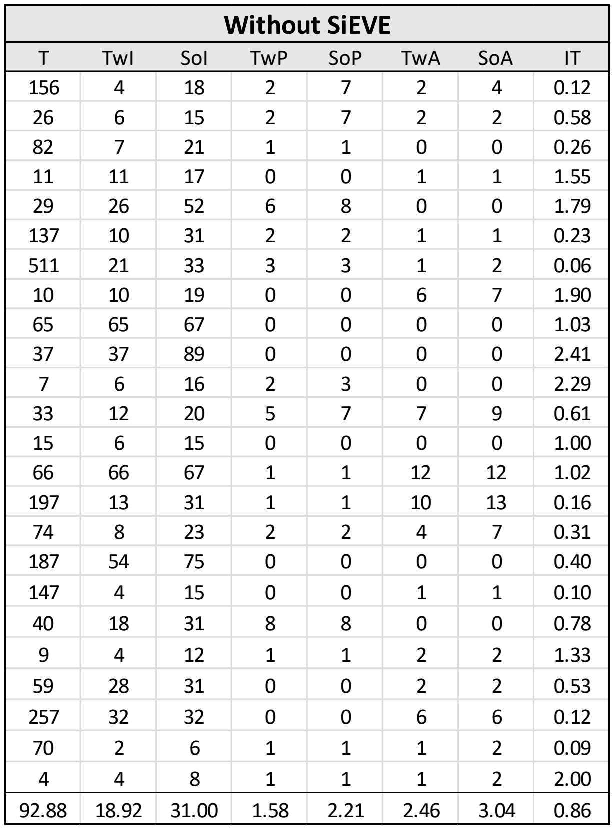
Efficiency and Effectiveness are inter-related, since spending a longer time may lead to more effectiveness. To control for this effect, the time that students had to work on each stage of the SiEVE process was held constant for each group. A reasonable time was chosen based on the Pilot Study, where students were allowed to spend as much time as they wanted. Having a constrained amount of time is also consistent with how live penetration tests are conducted.

To understand the effectiveness of the SiEVE process, a number of metrics were used to compare the number of targets identified, the amount of information gathered about targets, and the likelihood of a target clicking on a spear phishing attack (as described in Chapter 3, Section 3.5).

4.2 Summary of the Findings

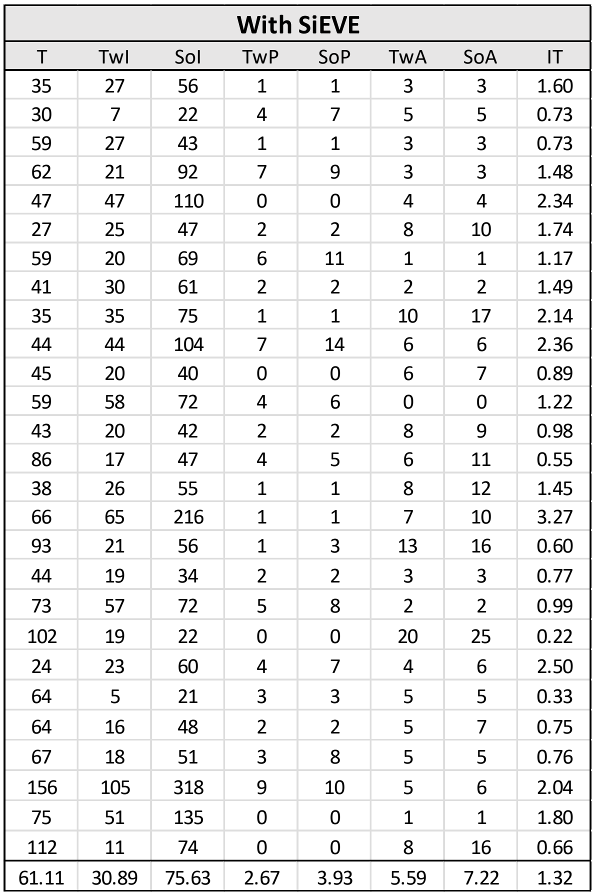
A cursory glance at the aggregated data shows a distinct difference between the With SiEVE (Table 4-2) and Without SiEVE (Table 4-1) groups. While the Targets Acquired (T) numbers were higher for the Without SiEVE group, they were not statistically significantly different. All metrics related to the amount of information gathered were higher for the With SiEVE group and these differences were statistically significant as described below.

Table 4-1 Aggregated Data From the Without and With SiEVE Groups



Without SiEVE							
T	TwI	SoI	TwP	SoP	TwA	SoA	IT
156	4	18	2	7	2	4	0.12
26	6	15	2	7	2	2	0.58
82	7	21	1	1	0	0	0.26
11	11	17	0	0	1	1	1.55
29	26	52	6	8	0	0	1.79
137	10	31	2	2	1	1	0.23
511	21	33	3	3	1	2	0.06
10	10	19	0	0	6	7	1.90
65	65	67	0	0	0	0	1.03
37	37	89	0	0	0	0	2.41
7	6	16	2	3	0	0	2.29
33	12	20	5	7	7	9	0.61
15	6	15	0	0	0	0	1.00
66	66	67	1	1	12	12	1.02
197	13	31	1	1	10	13	0.16
74	8	23	2	2	4	7	0.31
187	54	75	0	0	0	0	0.40
147	4	15	0	0	1	1	0.10
40	18	31	8	8	0	0	0.78
9	4	12	1	1	2	2	1.33
59	28	31	0	0	2	2	0.53
257	32	32	0	0	6	6	0.12
70	2	6	1	1	1	2	0.09
4	4	8	1	1	1	2	2.00
92.88	18.92	31.00	1.58	2.21	2.46	3.04	0.86

Table 4-2 Aggregated Data From Both the With and Without



With SiEVE							
T	TwI	SoI	TwP	SoP	TwA	SoA	IT
35	27	56	1	1	3	3	1.60
30	7	22	4	7	5	5	0.73
59	27	43	1	1	3	3	0.73
62	21	92	7	9	3	3	1.48
47	47	110	0	0	4	4	2.34
27	25	47	2	2	8	10	1.74
59	20	69	6	11	1	1	1.17
41	30	61	2	2	2	2	1.49
35	35	75	1	1	10	17	2.14
44	44	104	7	14	6	6	2.36
45	20	40	0	0	6	7	0.89
59	58	72	4	6	0	0	1.22
43	20	42	2	2	8	9	0.98
86	17	47	4	5	6	11	0.55
38	26	55	1	1	8	12	1.45
66	65	216	1	1	7	10	3.27
93	21	56	1	3	13	16	0.60
44	19	34	2	2	3	3	0.77
73	57	72	5	8	2	2	0.99
102	19	22	0	0	20	25	0.22
24	23	60	4	7	4	6	2.50
64	5	21	3	3	5	5	0.33
64	16	48	2	2	5	7	0.75
67	18	51	3	8	5	5	0.76
156	105	318	9	10	5	6	2.04
75	51	135	0	0	1	1	1.80
112	11	74	0	0	8	16	0.66
61.11	30.89	75.63	2.67	3.93	5.59	7.22	1.32

4.3 Targets Acquired Effectiveness

The higher number of Targets acquired in the Without SiEVE group (92.88) compared to the With SiEVE group (61.11) was unexpected. This is the only case where the With SiEVE has a lower aggregation than the Without SiEVE group. It is interesting to note, however, the outliers and standard deviation (SD) of both groups as shown in Figure 4-1. The SD of the Without SiEVE group is 113.05 and the SD of the With SiEVE group is 29.42 which denotes the large discrepancy in responses for the Without SiEVE group. Even removing the large outlier from the Without SiEVE aggregate data (the count of 511 targets enumerated) the SD is still 71.21.

A t-Test was performed for the dataset of Targets Enumerated (T) with a 95% level of confidence. The data went through a logarithmic transform to reduce the non-normalized data from being too skewed for the test to work properly. The graph (Figure 4-1) shows that there may be a difference in targets enumerated, but performing the t-Test assuming unequal variances (Table 4-3), we see that the results were not significant. Also, note that the degrees of freedom are fractional as a result of using the Welch-Satterthwaite equation of calculating effective degrees of freedom due to unequal variances (Satterthwaite, 1946).

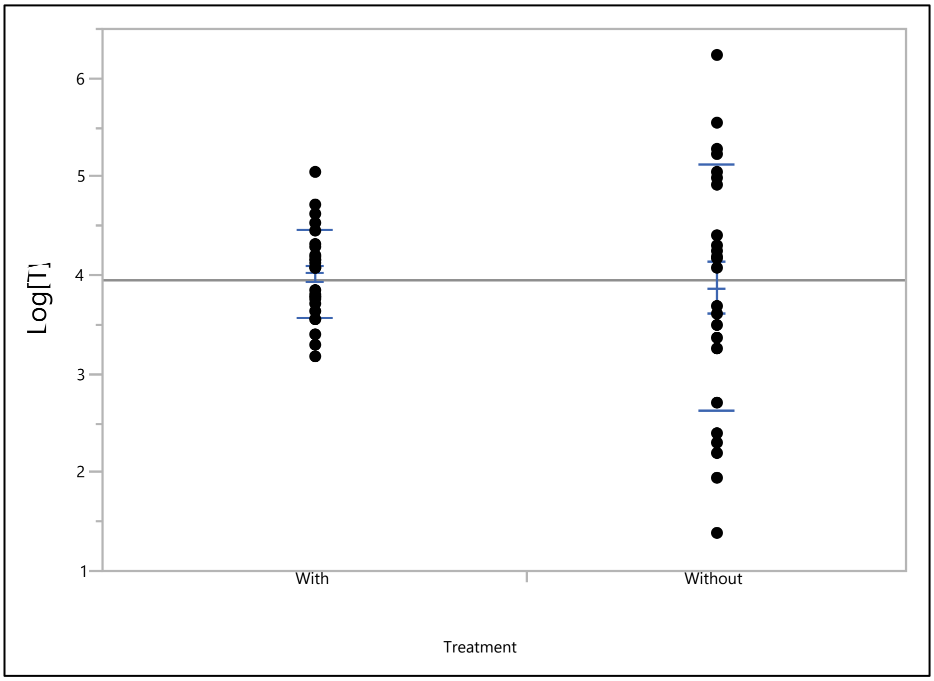
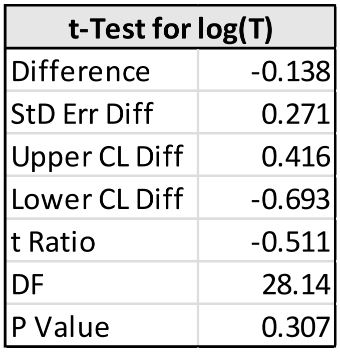


Figure 4-1 Logarithmic Transform of Targets Enumerated

As a result, we do not have any evidence to conclude that the SiEVE helped students enumerate more or less targets. It is interesting to note the large variation in spread between the two groups. It is possible that using SiEVE increased the targets enumerated for individuals who would have done worse, but also reduced the number of targets for those who would have done better. With this data, we have shown that Hypothesis 1 has not been proven or disproven as its results are insignificant. Another study with a larger population would need to be performed to prove Hypothesis 1.

Table 4-3 t-Test for Log(T) to Show non-Significance

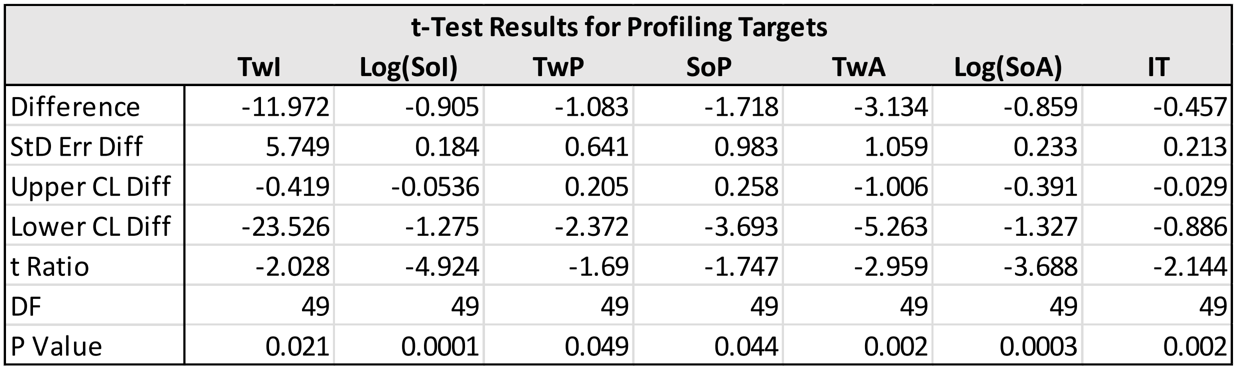


t-Test for log(T)	
Difference	-0.138
StD Err Diff	0.271
Upper CL Diff	0.416
Lower CL Diff	-0.693
t Ratio	-0.511
DF	28.14
P Value	0.307

4.4 Profiling Target Effectiveness

Multiple t-Tests with a 95% confidence level were performed on the data gathered during the Profiling Targets part of the study. Since there are many data points to cover, the data has been aggregated here and the full data generated for 3.4 Profiling targets will be in Appendix C. From the table (Table 4-4), we can see that each data set (Targets with Information Gathered, Sum of Information Gathered, Targets with Personally Identifiable Information (PII) Gathered, Sum of PII Gathered, Targets with Accounts Gathered, Sum of Accounts Gathered, and Information per Target) showed significance when the independent variables (With and Without SiEVE) are measured. All data points gathered are significant which supports the 2nd hypothesis as it states that using the SiEVE process increases the amount of personal information being enumerated (i.e. accounts and PII).

Table 4-4 t-Tests for All Data Sets in 3.4 Profiling Targets

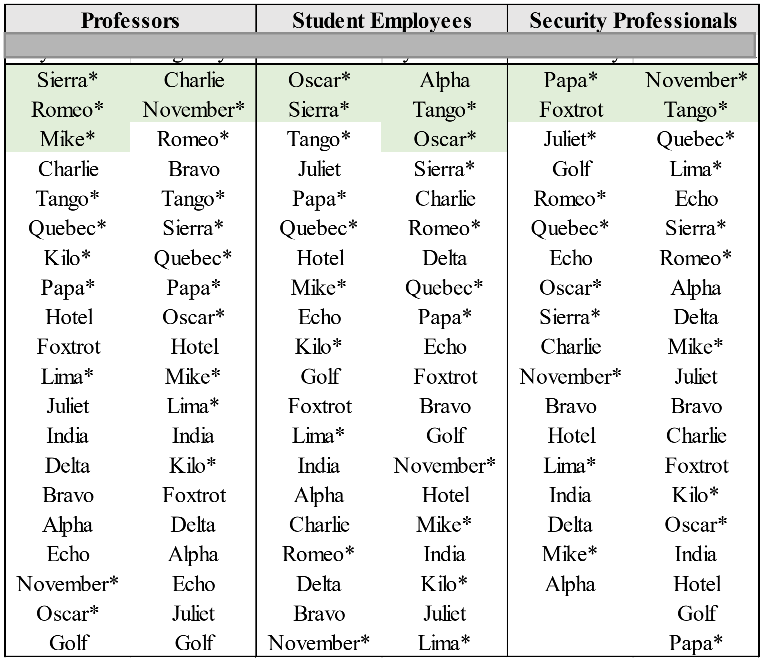


t-Test Results for Profiling Targets	TwI	Log(SoI)	TwP	SoP	TwA	Log(SoA)	IT
Difference	-11.972	-0.905	-1.083	-1.718	-3.134	-0.859	-0.457
StD Err Diff	5.749	0.184	0.641	0.983	1.059	0.233	0.213
Upper CL Diff	-0.419	-0.0536	0.205	0.258	-1.006	-0.391	-0.029
Lower CL Diff	-23.526	-1.275	-2.372	-3.693	-5.263	-1.327	-0.886
t Ratio	-2.028	-4.924	-1.69	-1.747	-2.959	-3.688	-2.144
DF	49	49	49	49	49	49	49
P Value	0.021	0.0001	0.049	0.044	0.002	0.0003	0.002

4.5 Spear Phishing Attack Effectiveness

Looking through the rankings in Table 4-5, we see a clear distinction between the With SiEVE and Without SiEVE groups effectiveness when it comes to creating spear phishing attacks. Note that those with a * are from the With SiEVE group.

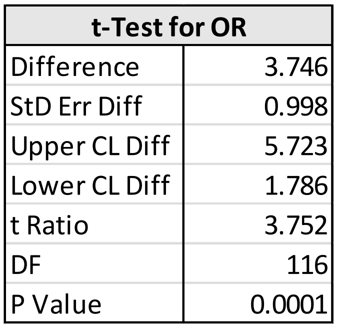
Table 4-5 Aggregated Data from Both the With and Without SiEVE Groups for 3.5



Professors		Student Employees		Security Professionals	
Sierra*	Charlie	Oscar*	Alpha	Papa*	November*
Romeo*	November*	Sierra*	Tango*	Foxtrot	Tango*
Mike*	Romeo*	Tango*	Oscar*	Juliet*	Quebec*
Charlie	Bravo	Juliet	Sierra*	Golf	Lima*
Tango*	Tango*	Papa*	Charlie	Romeo*	Echo
Quebec*	Sierra*	Quebec*	Romeo*	Quebec*	Sierra*
Kilo*	Quebec*	Hotel	Delta	Echo	Romeo*
Papa*	Papa*	Mike*	Quebec*	Oscar*	Alpha
Hotel	Oscar*	Echo	Papa*	Sierra*	Delta
Foxtrot	Hotel	Kilo*	Echo	Charlie	Mike*
Lima*	Mike*	Golf	Foxtrot	November*	Juliet
Juliet	Lima*	Foxtrot	Bravo	Bravo	Bravo
India	India	Lima*	Golf	Hotel	Charlie
Delta	Kilo*	India	November*	Lima*	Foxtrot
Bravo	Foxtrot	Alpha	Hotel	India	Kilo*
Alpha	Delta	Charlie	Mike*	Delta	Oscar*
Echo	Alpha	Romeo*	India	Mike*	India
November*	Echo	Delta	Kilo*	Alpha	Hotel
Oscar*	Juliet	Bravo	Juliet		Golf
Golf	Golf	November*	Lima*		Papa*

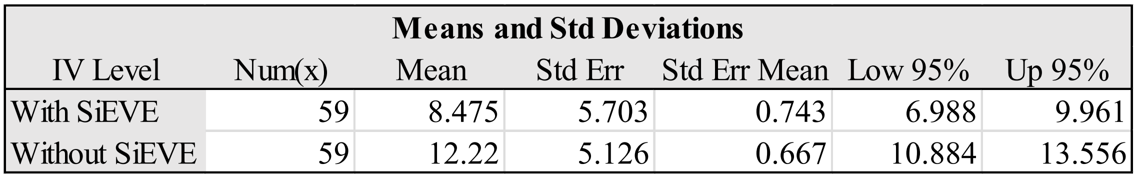
The cells that are in green are attacks above the Trust Threshold, indicating that the person self-reports that they would have fallen for the message and had their trust exploited by performing a new behavior (Fogg, 2010). A t-Test was performed on the Overall Ranking (OR) of the results from Crafting Spear Phishing Attacks. The following data, including the means and standard deviations, are seen in Table 4-6 and 4-7. The most apparent thing from the data in Table 4-6 is the P Value showing significance for the With SiEVE outperforming Without SiEVE for Crafting Spear Phishing Attacks. Looking at Table 4-7, we can see on average the attacks created Without SiEVE are placed at rank 12 and With SiEVE are placed at rank 8. Thus, using a specific process, like SiEVE, contributes to the success of a spear phishing attack and supports the 3rd hypothesis

Table 4-6 t-Test for OR Showing Significance



t-Test for OR	
Difference	3.746
StD Err Diff	0.998
Upper CL Diff	5.723
Lower CL Diff	1.786
t Ratio	3.752
DF	116
P Value	0.0001

Table 4-7 Various Important Numbers for Spear Phishing Attack Results



Means and Std Deviations						
IV Level	Num(x)	Mean	Std Err	Std Err Mean	Low 95%	Up 95%
With SiEVE	59	8.475	5.703	0.743	6.988	9.961
Without SiEVE	59	12.22	5.126	0.667	10.884	13.556

4.6 Observations from the Study

During the study, notes were taken while the student participants were performing the experiments. Some of the highlights from the various sections of the study will be given here as they show more insight into the performance of the SiEVE process being taught to security professionals in training.

4.6.1 Observations from Identifying Targets

While both groups were given the same briefing before the first part, the groups had differing reactions to the study. When the Without SiEVE group began the task, it was clear that there was a general lack of direction among the participants. Many were aimlessly googling about BYU employees and searching public forums for potential targets. This is also seen in the range and standard deviation. 4 targets were enumerated by the lowest of the range and 511 by the highest showing that there is a wide discrepancy in what to do, as in there was no focus in completing their task. The With SiEVE group was observed to immediately read the SiEVE process (as given in Appendix A) and then started using OSINT to enumerate targets. The result of this focus is seen in the range and standard deviation of the enumerated targets. At the end of the allotted thirty minutes it was clear that a couple participants in the Without SiEVE group had stopped enumerating targets as they had no more places to look.

4.6.2 Observations from Profiling Targets

The second part of the study began about ten to fifteen minutes after the first part. This was a small break for the student participants to give them some time to recover. The same things were said by the researcher before both groups began again. Like the first part of the study, the same observations were made during the second. The participants in the Without

SiEVE study did not have a sense of direction which was made clear in questions they asked the researcher. All the questions were about what to look for, what specifics would be needed for crafting a spear phishing attack. With the data shown in section 4, it is clear that with more focus and a tested process, there would be less questions and more efficiency by those performing reconnaissance.

4.6.3 Observations from Crafting Spear Phishing Emails

When the student participants were given the information found during the target information session, they could ask any questions about what was found on the six individuals. The only questions asked were asked by those in the With SiEVE group. The questions that were about how to make successful spear phishing attacks were answered with counsel to read the SiEVE process section on creating an attack. Questions about the targets were answered with specifics about what was found on each of the targets.

When asked, the six targets said similar things about which spear phishing attacks were most effective. They all said the same thing regarding the experiment that the knowledge of the attacks being spear phishing attacks allowed them to focus more on the content of the attack and less about the malicious nature of the attack. Clearly from what was stated by the targets, the attacks that specifically targeted their place of employment were often ignored and placed lower on their rankings. They said this was the case because they knew more about their job to see a discrepancy between an actual work email and a crafted spear phishing attack with one target stating “that an official looking e-mail” contained mistakes in vernacular or more glaring grammatical errors. The attacks that were more often rated higher contained the interests or hobbies of the targets, or information gathered during reconnaissance. While the SiEVE documentations did not explicitly state how to create attacks, it did talk about what works when creating a phishing attack. The BYU specific SiEVE process did contain some simple examples for creating spear phishing attacks and is included in Appendix A.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Impact of this Research

As stated in the research objective (1.4.1) the purpose of this study was to iteratively develop the SiEVE (Social Engineering Vulnerability Evaluation) to answer the research question of how to improve effectiveness (ability to identify key individuals and personal information about them) and efficiency (time to perform reconnaissance and attack) during the first 3 steps of the process outlined by Lockheed Martin's Cyber Kill Chain ("Cyber Kill Chain® · Lockheed Martin," n.d.). A comprehensive literary review was created to observe the processes and ideas currently in the industry and evaluate what is needed for red teams to perform a successful social engineering penetration test. Student participants were leveraged to perform a large-scale test of the SiEVE process by splitting them into a With SiEVE and Without SiEVE group separated into three thirty-minute sections. The data generated from these participants was aggregated for comparing the two groups. It is evident that using a simple process like SiEVE during the social engineering phase of a penetration test would yield more effective and efficient results compared to having no dedicated process.

Since the participants were from a wide variety of skill levels, we can state that the SiEVE process helps with training new security professionals on how to create efficient and effective spear phishing attacks. The SiEVE process does this by taking the concept of consistency and gives it a structure that allows for a security professional in training to create quick and correct results. The targets involved in the study identified the effectiveness of the crafted spear phishing attacks using SiEVE as more likely to gain and exploit their trust by getting them to click, download, or respond. The process can actively be used by a red team during their engagements as it has been proven to give results and increase the potential for a breach in protocol on behalf of an organization through an enumerated target (Tabatabaei & Wells, 2016).

5.2 Suggestions for Continued Research and Development

While not perfect, the SiEVE process has been shown to increase quality of results (in 2 of the 3 phases) and further iterative versions can be created to increase these metrics. This also allows for specialized use of this process for the use against the different industries that require security audits in the form of a penetration test. As the process is adapted to different circumstances, the information gained from that can be used to iteratively develop the process like how it was developed between the Pilot Study and this study.

Seeing that only two of the three hypotheses were found to be true, another study could be conducted to improve and evaluate an updated Targets Enumerated section of the SiEVE process. For example, techniques used by the outliers who gathered hundreds of targets could be introduced more explicitly in the SiEVE process. Additionally, the process may be modified to have those conducting SiEVE focus on targets that would be more useful in completing a penetration test (e.g., those with more elevated privileges). An additional study that measured the effectiveness of the updated process would be needed.

If we did another iteration of this study, there are a couple changes that should be done to achieve better results. The larger the sample size that performs the process, the more insights can be drawn from the data and the more confidence we can have in the results. Since this study used participants with security knowledge, but a lack of red team experience, having a study with either non-knowledgeable participants or fully trained security professionals would be beneficial to assess SiEVE's applicability to other potential users. SiEVE is simple in its design and gives a structure to the process, so having a training version, or a professional version could change the overall results of a penetration test. It would be more tailored to the needs of the individual that uses the process. The simplicity of the SiEVE process is also an advantage as it can be performed on both sides of the security spectrum with positive results.

With the possibility of many permutations of this study, scope must be tempered so that the study would augment the current SiEVE process to make it better. Also, with more iterations, more complex and inclusive "cheat sheets" could be created along with automation. There are many possibilities as the SiEVE process moves forward after this study. However, these findings suggest the importance and promising nature of creating formalized processes for social engineering activities, such as spear phishing.

REFERENCES

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183–196. https://doi.org/10.1016/j.techsoc.2010.07.001

Ansari, F., Akhlaq, M., & Rauf, A. (2013). Social networks and web security: Implications on open source intelligence. In *2013 2nd National Conference on Information Assurance (NCIA)* (pp. 79–82). IEEE. https://doi.org/10.1109/NCIA.2013.6725328

APWG. (2017). *Phishing Activity Trends Report Q4 2017*. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf

Cyber Kill Chain® · Lockheed Martin. (n.d.). Retrieved October 2, 2017, from http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

Debrosse, H., Debrosse, J., & Harley, D. (n.d.). MALICE THROUGH THE LOOKING GLASS MALICE THROUGH THE LOOKING GLASS: BEHAVIOUR ANALYSIS FOR THE NEXT DECADE. Retrieved from https://www.welivesecurity.com/media_files/white-papers/Harley-Debrosse-VB2009.pdf

Fogg, B. (2010). BJ Fogg's Behavior Grid. Retrieved February 15, 2017, from http://www.behaviorgrid.org/

Gawande, A. (2010). *The Checklist Manifesto*. New York: Metropolitan Books. Retrieved from https://avrl.catalogue.library.ns.ca/Record/887023/Cite

Ivaturi, K., & Janczewski, L. (2011). Association for Information Systems AIS Electronic Library (AISeL) A Taxonomy for Social Engineering attacks A Taxonomy for Social Engineering attacks. *AIS Electronic Library*. Retrieved from http://aisel.aisnet.org/confirm2011

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social Phishing. *COMMUNICATIONS OF THE ACM*, *50*(10), 7.

Koops, B.-J., Hoepman, J.-H., & Leenes, R. (2013). Open-source intelligence and privacy by design. *Computer Law & Security Review*, *29*(6), 676–688. https://doi.org/10.1016/J.CLSR.2013.09.005

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

Lee, D. H., Choi, K. H., & Kim, K. J. (2007). LNCS 4706 - Intelligence Report and the Analysis Against the Phishing Attack Which Uses a Social Engineering Technique. *LNCS Part II*, *4706*, 185–194.

Mercado, S. (2008). Sailing the Sea of OSINT in the Information Age — Central Intelligence Agency. Retrieved October 2, 2017, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html

Neely, L. (2017). A SANS Survey 2017 Threat Landscape Survey: Users on the Front Line. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

Provonost, P. (2001). Peter Provonost Checklist Protocol. Retrieved from http://laparoscopy.blogs.com/outcome/ItsTheOutcomeDocs/Peter Pronovost Protocol.pdf

Satterthwaite, F. E. (1946). An Approximate Distribution of Estimates of Variance Components. *Biometrics Bulletin*, *2*(6), 110. https://doi.org/10.2307/3002019

Tabatabaei, F., & Wells, D. (2016). OSINT in the Context of Cyber-Security (pp. 213–231). Springer, Cham. https://doi.org/10.1007/978-3-319-47671-1_14

Thomas, G. (2013). The The DGI Data Governance DGI Data Governance Framework Framework Management Data Governance Components of the DGI Data Governance Framework. Retrieved from http://www.datagovernance.com/wp-content/uploads/2014/11/dgi_framework.pdf

Wombat Security Technologies. (2016). *State of the Phish*. Retrieved from https://info.wombatsecurity.com/state-of-the-phish

APPENDICES

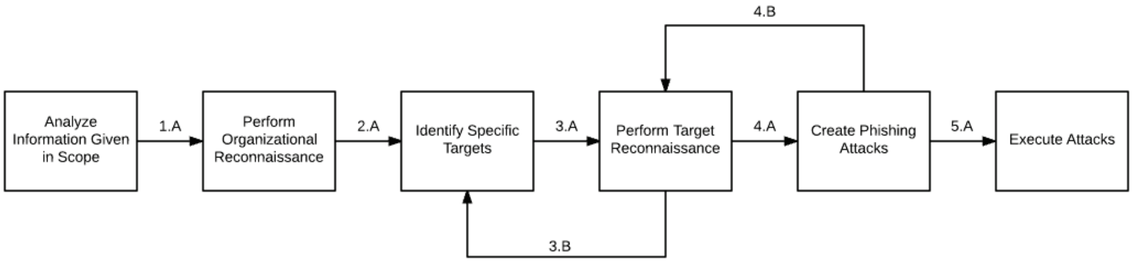
Appendix A. SiEVE Process – Full BYU Version – Not Used in Study

Introduction

The SiEVE process (Social Engineering Vulnerability Evaluation) is a set of steps designed to help security teams create and evaluate general and spear phishing attacks. The process will help you identify targets, perform reconnaissance on them, and craft custom phishing attacks.

Sidebar: Definitions

- SiEVE Process – a process that helps security teams (e.g., red teams) create and evaluate phishing attacks as part of a penetration test
- Target – the person of interest who will be attacked
- Reconnaissance – gathering information about an organization or target
- General Phishing (or just Phishing) – the deceptive practice of sending a message (e.g., email) designed to induce targets to unknowingly reveal personal information such as login credentials
- Spear Phishing – a phishing attack where the message has been tailored to a specific target based on information gathered during reconnaissance


Analyze Information Given in Scope
1.A
Perform Organizational Reconnaissance
2.A
Identify Specific Targets
3.A
Perform Target Reconnaissance
4.A
Create Phishing Attacks
5.A
Execute Attacks
4.B
3.B

Process

This process will have examples based off the idea that the Brigham Young University Office of Information Technology (referred here as OIT) is the target of the penetration test. Since OIT is a specific department, all given steps will refer to OIT as the organization.

Analyze Information Given in Scope – 1.A

Review the base information that the organization has given you for the penetration test. This should include the organization name(s) and information about what is in and out of scope. Note that everything in this process will be covered even if it is not within your own scope, or boundary.

3. List all names for the organization.
4. List specific credentials (i.e., access rights) to look for that may be owned by targets within the organization.

Example

1. OIT could be referred to as the IT Building, or ITB, per the BYU floorplan and map. Other organizations could have many official names colloquial, or non-standard names.
2. This is usually dependent on the nature of the penetration test. Some examples include access rights that allow for (a) enhanced directory information such as name, birthdate, or ID numbers, (b) financial records, (c) official records or documentation such as transcripts, (d) access to computing infrastructure such as servers or databases where data is stored. At OIT, this would be mostly anyone as any individual with an account has access to the directory.

Perform Organizational Reconnaissance – 2.A

If the organization has multiple departments or groups, list each one within the organization. Note that finding the specific groups is much harder than specific departments as a department is usually more structured. This step is focusing resources on an organization's structure to list out the possible departments of interest. Doing this allows for a security team to remove unimportant departments and give value to each department.

1. List as many departments within an organization as possible.
2. Rank each department from most important to least.
3. For each department, find one high profile target as a baseline.

Example

1. Since OIT is a department, then we are will list groups. This is where some basic reconnaissance happens. Googling BYU OIT shows us the main page for OIT at it.byu.edu. Going to the "Contact Us" section, we can list 2 groups that could be useful, BYU IT Support and OIT Reception. In the tab section of the "Contact Us" page, we see that OIT uses a CSR system of representatives for BYU. Most

definitions for this acronym are “Customer Support Representative,” but if you Google “csr byu” we find that it stands for “Computer Support Representative”.

2. We would rank CSR Group first as this would be the best group to pivot, or move into, other systems at BYU. Also, since they are representing OIT, they would have elevated rights. Second in the ranking would be BYU IT Support as they have access to some form of OIT reporting and information. Last would be OIT Reception, as they may only have access to records of employees at OIT.
3. For CSR Group, one of the first found links when searching “csr byu” we find the Chemistry Department’s CSR listed in their directory. Googling BYU Directory, we find a public listing of high profile targets at unicomm.byu.edu. Notable targets include the OIT Support Services Managing Director and the Customer Service and Support Director. This directory has many other potential high profile targets to pivot off and gives applicable employee titles to search later in the process.

Identify Specific Targets 3.A

Attempt to add subordinates to the list using simple search queries. We are increasing the attack surface of our penetration test by including as many individuals as possible. Remember that the best targets have access to more information (see 1.A.2).

5. Google the current target list and find other similar employees.
6. When completed the current target list, complete step 3.A.1 for any newly added targets.
7. Remove any targets that do not fit into the scope of the penetration test.
8. After all simple searches are complete (i.e. no more results), switch to publicly available data on high profile websites.
    a. Facebook
    b. LinkedIn
    c. Twitter
    d. Organization Specific Websites
    e. ETC.

Example

1. Googling the employee names will easily find 3 public Facebook profiles and LinkedIn profiles. Save these for later, but use the employee title and check for any internal public directories. Make sure to do searches with, and without the organization name. Googling the OIT Support Services Managing Director with BYU as a search term results in a blog from 2009 that include more names to add to the list.
2. Any targets discovered in step 1 can now be subjected to the same step. Basically, we are drilling down into the organization through the top-level target’s associations.
3. Since we are looking for anybody with elevated credentials or access to sensitive logs, all the gathered targets that work at OIT fit into the scope of the penetration test.

Any target that does not work at OIT will need to be removed to satisfy scope and useless information.

4. Taking the current target list and searching the listed websites is simple.
    a. The best one stop for this data is here. Simply find the target's public Facebook page and enter everything after facebook.com/ up till a "?" if there is one. For example, my Facebook is https://www.facebook.com/cmndrbunbun so I would input "cmndrbunbun" to receive the user number that Facebook uses. For this step, focus on any option that would find more targets.
    b. Again, we are searching for connection to our current target list. Start with the base list (i.e. the "high profile" targets) and attempt to find more individuals to add to list. This is more effective if you use a certified "dummy" account as LinkedIn requires you to have some form of significance. The best place to start is the "People Also Viewed" sidebar. These are individuals that are within their sphere of influence at the organization.
    c. Like the LinkedIn search by just googling the target's name with twitter after it. Also, much easier with a "dummy" account. You can easily look through the "followers" and recommended section of their account to find more targets.
    d. Some organizations have specific sites dedicated to their employees. These are usually public and give information on the employees. In the case of OIT, they have the it.byu.edu website with their directory pointing to the one we found earlier.
    e. Other places that could be useful, but more difficult include Slack, Instagram, Blogger, Flickr, Tumblr, etc. These are usually more difficult to find new individuals that the other sites. Also, in the case of Slack, it would require gaining access using other means of Social Engineering, like pretexting.

Perform Target Reconnaissance 4.A

Take each target found in 3.A and do information searches on each one. The goal is to find relevant information on the target, such as their hobbies or interests. Any information could work for this step, but the more details found, the better your attack can be later. Since you could have a long list of targets, find 2 to 3 details about a target and move on. Take note of individuals that have a lot of public data as they are usually more willing to give out their information.

5. Perform simple Google searches using the targets name with and without their title. A site like this one could aid in speed of searches.
6. Using any positive results from 4.A.1, delve into any social media hits (i.e. Facebook, Twitter, LinkedIn, Instagram, etc.).
7. Make note of any prolific user and their username and save for a later step.
8. Save any information you find on each target.

Example

1. Using my name, I would search for "Jared Meyers" in Google. Also from a previous step, I know that my username is sometimes "cmndrbunbun". Putting both together will find my twitter handle as the first hit. Farther down you will see my Facebook profile and Instagram account.
2. Looking through my twitter, you will easily find that I am a gaming and eSports enthusiast. Looking through both my Facebook and Instagram, will show that I like to hike and take pictures. Going to a site and search my name will yield similar results (i.e. LinkedIn usually uses a more professional username).
3. My social media presence would qualify as prolific as I am found in many locations with similar usernames.
4. With the basic information pulled from my accounts, attacks using eSports, Photography, and Outdoor Activities as "bait" will be more effective than a general phishing attack.

Create Attacks 5.A

Taking all the information found in previous steps, we are now ready to create spear phishing attacks. This step will vary greatly for each penetration test as each target list will vary in size and available information.

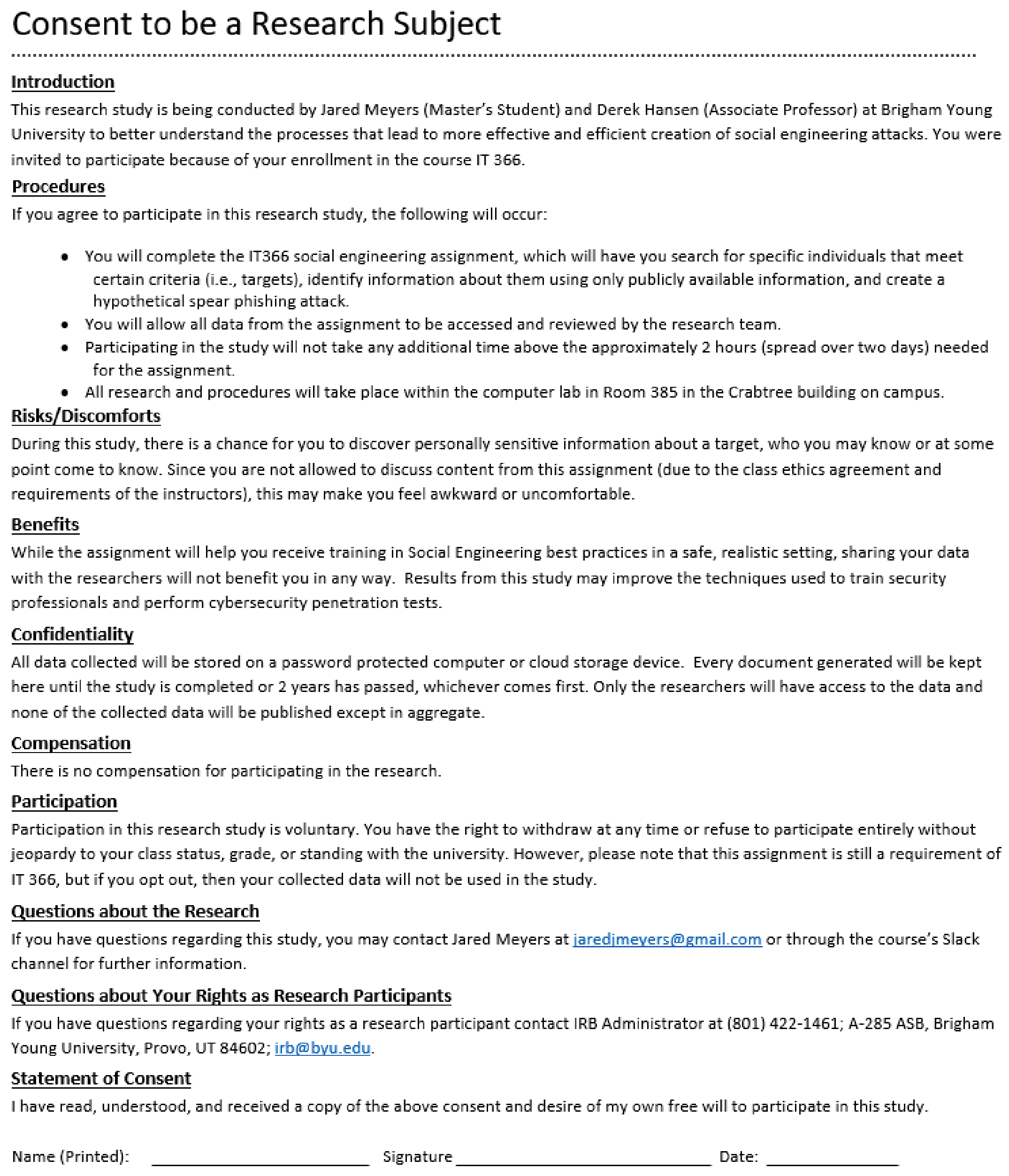
5. Select a base target to spear phish
6. Pick the simplest piece of information as the bait
7. Prepare the attack and set aside
8. Repeat steps for as many targets as you have time for in this penetration test

Example

1. Since we found a large set of information for my account in 4.A, it would be good to start with my account if you are attacking OIT. I have many interests that provide good bait for phishing attacks.
2. Looking through all my media and official accounts, it is clear from our research that eSports is a top hobby or interest of mine. This is where you can leverage your knowledge about a topic. If you (or the attack creator) do not know much about a specific topic and do not have the time to do adequate research, then move to another hobby. So, if I was the attack creator and I was a hobby photographer, then I would gravitate to creating an attack based on that.
3. There are multiple ways to create an effective spear phishing attack. The most common attack is to promise a reward if the target responds. This is a reward-based attack that preys upon the targets desire to have more and could be based on an invitation only event, a prize/raffle giveaway, or even monetary credit to a prolific website in that industry. So, if Photography is the bait, an email with the following

would be effective: winning a free vacation to a picturesque location, an entry-based giveaway of a new DSLR camera, a gift card for Amazon.com or Adorama.com.

Appendix B. Consent Form Given to Participants



Consent to be a Research Subject

Introduction

This research study is being conducted by Jared Meyers (Master's Student) and Derek Hansen (Associate Professor) at Brigham Young University to better understand the processes that lead to more effective and efficient creation of social engineering attacks. You were invited to participate because of your enrollment in the course IT 366.

Procedures

If you agree to participate in this research study, the following will occur:

- You will complete the IT366 social engineering assignment, which will have you search for specific individuals that meet certain criteria (i.e., targets), identify information about them using only publicly available information, and create a hypothetical spear phishing attack.
- You will allow all data from the assignment to be accessed and reviewed by the research team.
- Participating in the study will not take any additional time above the approximately 2 hours (spread over two days) needed for the assignment.
- All research and procedures will take place within the computer lab in Room 385 in the Crabtree building on campus.

Risks/Discomforts

During this study, there is a chance for you to discover personally sensitive information about a target, who you may know or at some point come to know. Since you are not allowed to discuss content from this assignment (due to the class ethics agreement and requirements of the instructors), this may make you feel awkward or uncomfortable.

Benefits

While the assignment will help you receive training in Social Engineering best practices in a safe, realistic setting, sharing your data with the researchers will not benefit you in any way. Results from this study may improve the techniques used to train security professionals and perform cybersecurity penetration tests.

Confidentiality

All data collected will be stored on a password protected computer or cloud storage device. Every document generated will be kept here until the study is completed or 2 years has passed, whichever comes first. Only the researchers will have access to the data and none of the collected data will be published except in aggregate.

Compensation

There is no compensation for participating in the research.

Participation

Participation in this research study is voluntary. You have the right to withdraw at any time or refuse to participate entirely without jeopardy to your class status, grade, or standing with the university. However, please note that this assignment is still a requirement of IT 366, but if you opt out, then your collected data will not be used in the study.

Questions about the Research

If you have questions regarding this study, you may contact Jared Meyers at jaredjmeyers@gmail.com or through the course's Slack channel for further information.

Questions about Your Rights as Research Participants

If you have questions regarding your rights as a research participant contact IRB Administrator at (801) 422-1461; A-285 ASB, Brigham Young University, Provo, UT 84602; irb@byu.edu.

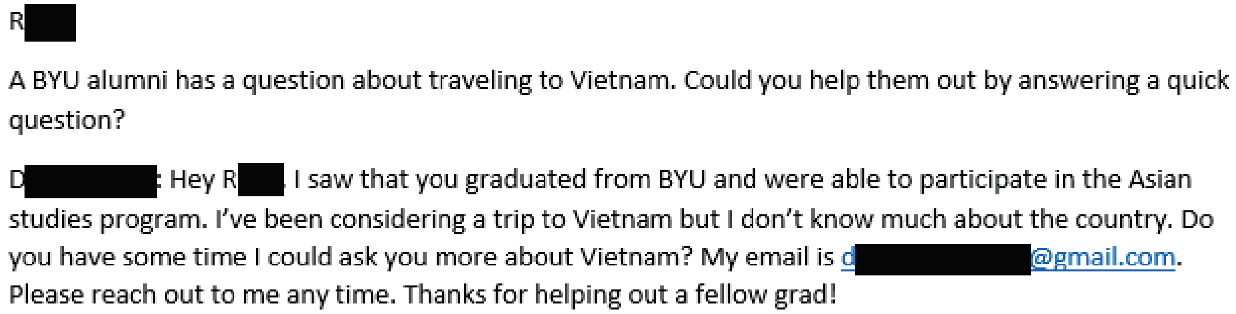
Statement of Consent

I have read, understood, and received a copy of the above consent and desire of my own free will to participate in this study.

Name (Printed): ________________________ Signature ____________________________ Date: _______________

Appendix C. Rank 1 Attacks

P1 Sierra Rank 1

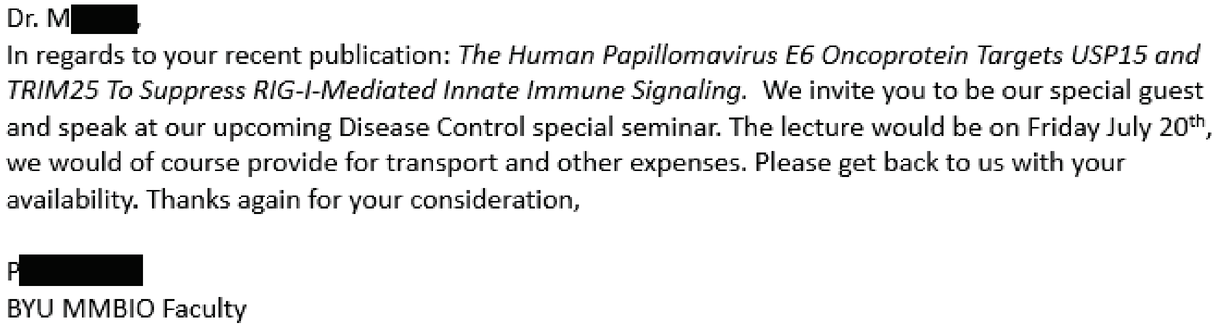


R[redacted]

A BYU alumni has a question about traveling to Vietnam. Could you help them out by answering a quick question?

D[redacted]: Hey R[redacted] I saw that you graduated from BYU and were able to participate in the Asian studies program. I've been considering a trip to Vietnam but I don't know much about the country. Do you have some time I could ask you more about Vietnam? My email is d[redacted]@gmail.com. Please reach out to me any time. Thanks for helping out a fellow grad!

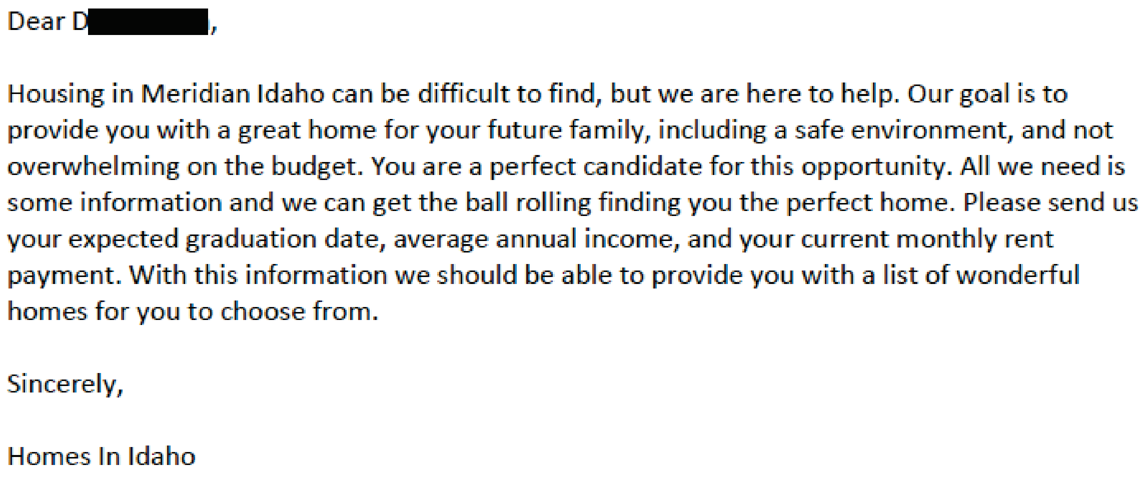
P2 Charlie Rank 1



Dr. M[redacted],
In regards to your recent publication: *The Human Papillomavirus E6 Oncoprotein Targets USP15 and TRIM25 To Suppress RIG-I-Mediated Innate Immune Signaling.* We invite you to be our special guest and speak at our upcoming Disease Control special seminar. The lecture would be on Friday July 20th, we would of course provide for transport and other expenses. Please get back to us with your availability. Thanks again for your consideration,

P[redacted]
BYU MMBIO Faculty

SE1 Oscar Rank 1



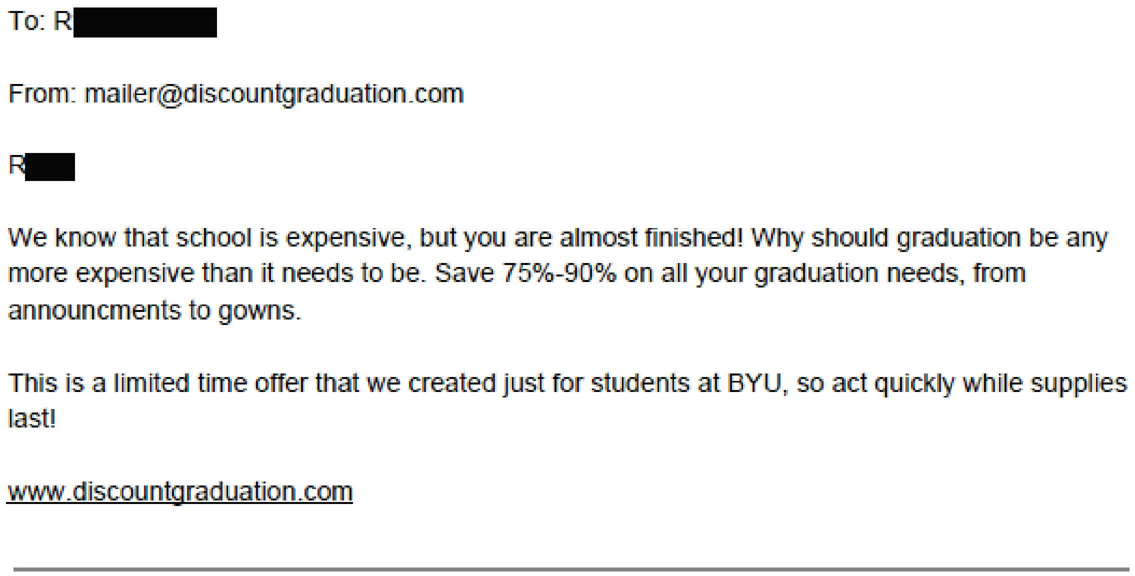
Dear D[redacted],

Housing in Meridian Idaho can be difficult to find, but we are here to help. Our goal is to provide you with a great home for your future family, including a safe environment, and not overwhelming on the budget. You are a perfect candidate for this opportunity. All we need is some information and we can get the ball rolling finding you the perfect home. Please send us your expected graduation date, average annual income, and your current monthly rent payment. With this information we should be able to provide you with a list of wonderful homes for you to choose from.

Sincerely,

Homes In Idaho

SE2 Alpha Rank 1



To: R[redacted]

From: mailer@discountgraduation.com

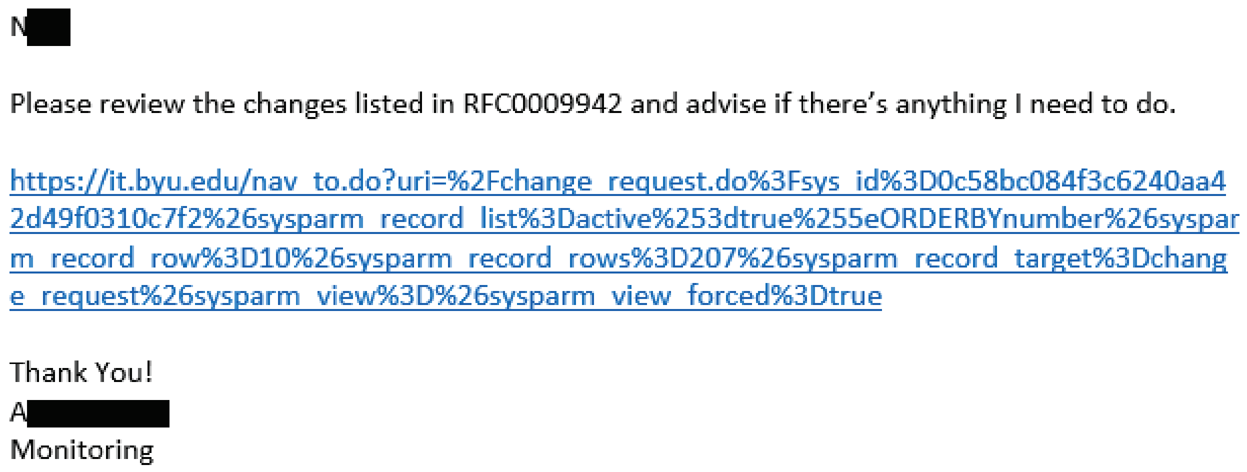
R[redacted]

We know that school is expensive, but you are almost finished! Why should graduation be any more expensive than it needs to be. Save 75%-90% on all your graduation needs, from announcments to gowns.

This is a limited time offer that we created just for students at BYU, so act quickly while supplies last!

www.discountgraduation.com

SP1 Papa Rank 1



N[redacted]

Please review the changes listed in RFC0009942 and advise if there’s anything I need to do.

https://it.byu.edu/nav_to.do?uri=%2Fchange_request.do%3Fsys_id%3D0c58bc084f3c6240aa42d49f0310c7f2%26sysparm_record_list%3Dactive%253dtrue%255eORDERBYnumber%26sysparm_record_row%3D10%26sysparm_record_rows%3D207%26sysparm_record_target%3Dchange_request%26sysparm_view%3D%26sysparm_view_forced%3Dtrue

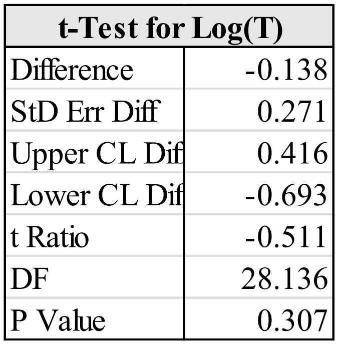
Thank You!
A[redacted]
Monitoring

SP2 November Rank 1

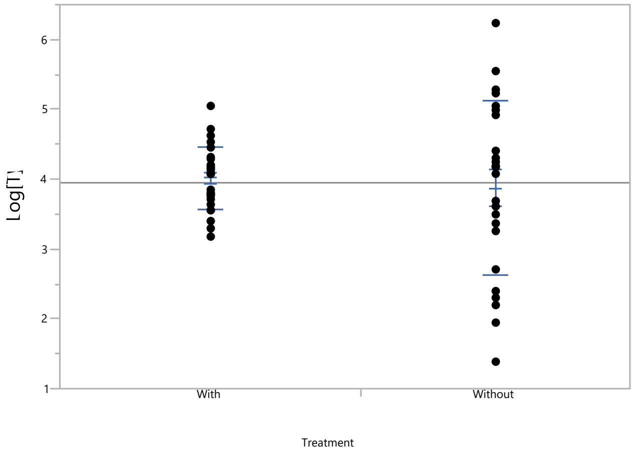
Not included due its personal nature.

Appendix D. Data Generated

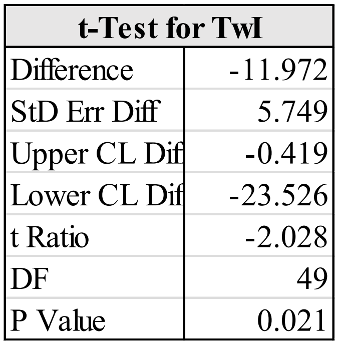
Identifying Targets Data -Targets Enumerated (Log(T))



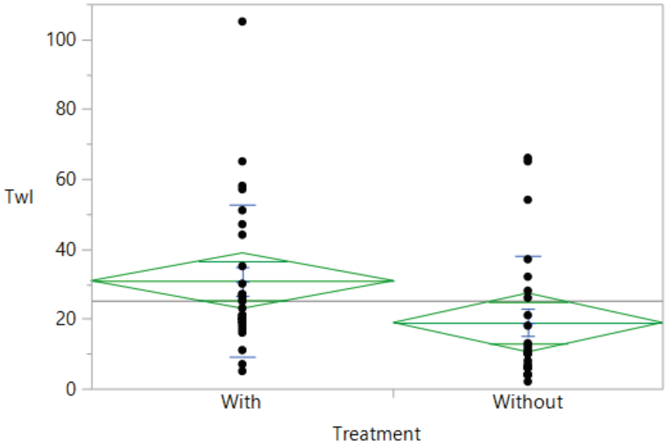
t-Test for Log(T)	
Difference	-0.138
StD Err Diff	0.271
Upper CL Dif	0.416
Lower CL Dif	-0.693
t Ratio	-0.511
DF	28.136
P Value	0.307



Profiling Targets – Targets with Information Gathered – TwI

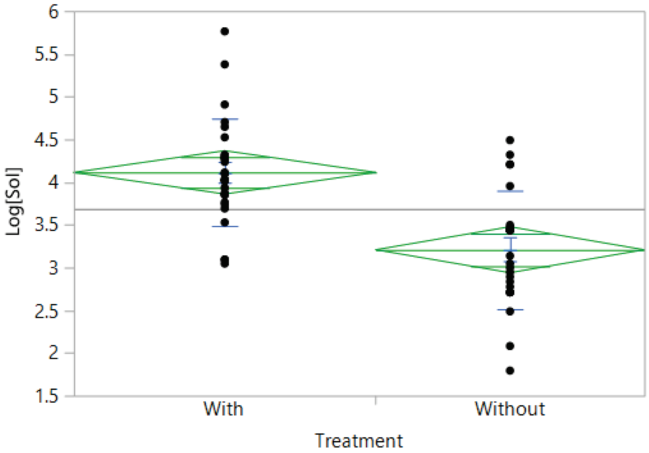


t-Test for TwI	
Difference	-11.972
StD Err Diff	5.749
Upper CL Dif	-0.419
Lower CL Dif	-23.526
t Ratio	-2.028
DF	49
P Value	0.021



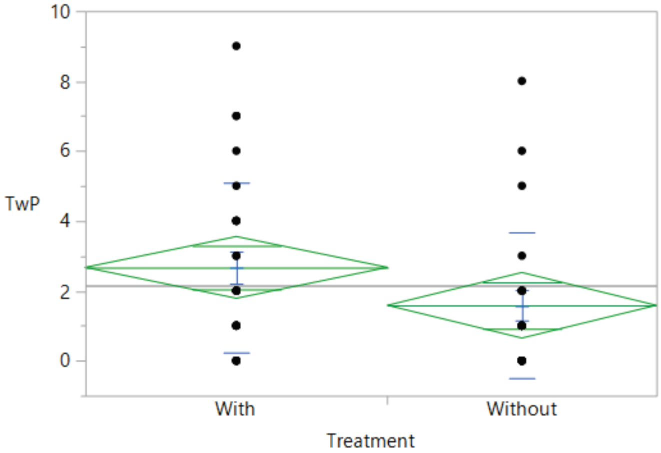
Profiling Targets – Sum of Information Gathered – SoI

t-Test for Log(SoI)	
Difference	-0.905
StD Err Diff	0.184
Upper CL Dif	-0.0536
Lower CL Dif	-1.275
t Ratio	-4.924
DF	49
P Value	0.0001



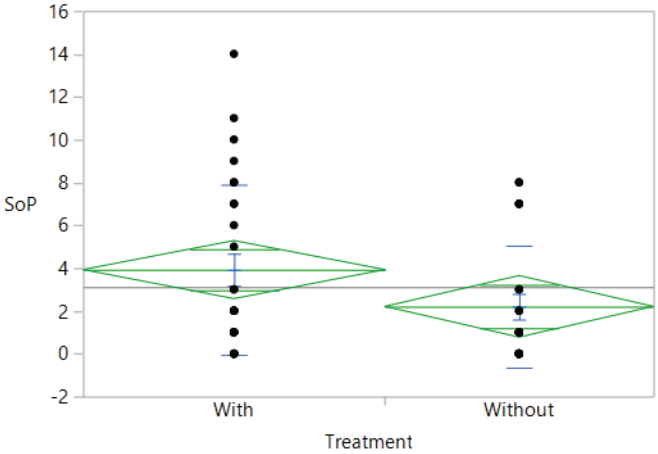
Profiling Targets – Targets with Personally Identifiable Information (PII) Gathered – TwP

t-Test for TwP	
Difference	-1.083
StD Err Diff	0.641
Upper CL Dif	0.205
Lower CL Dif	-2.372
t Ratio	-1.69
DF	49
P Value	0.049



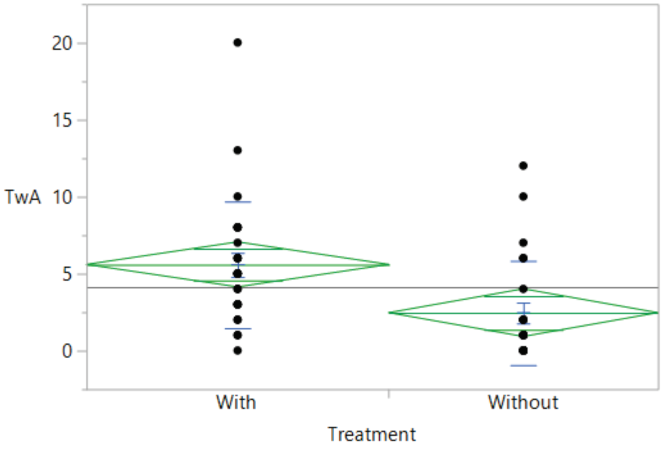
Profiling Targets – Sum of PII Gathered – SoP

t-Test for SoP	
Difference	-1.718
StD Err Diff	0.983
Upper CL Dif	0.258
Lower CL Dif	-3.693
t Ratio	-1.747
DF	49
P Value	0.044



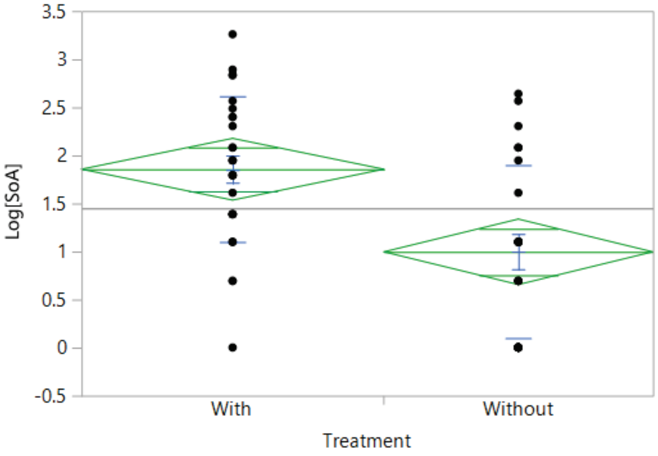
Profiling Targets – Targets with Accounts Found – TwA

t-Test for TWA	
Difference	-3.134
StD Err Diff	1.059
Upper CL Diff	-1.006
Lower CL Diff	-5.263
t Ratio	-2.959
DF	49
P Value	0.002



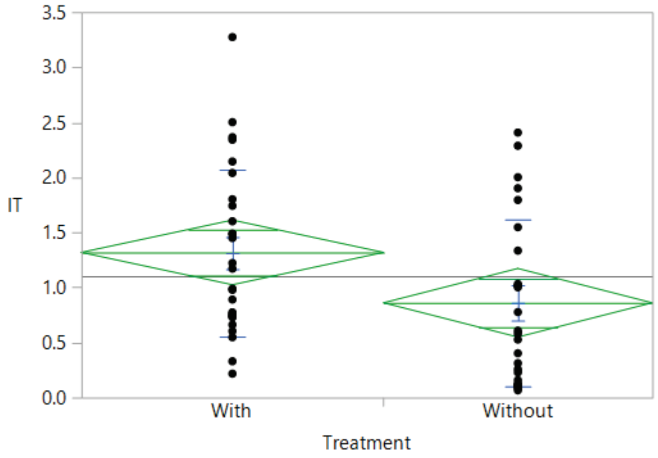
Profiling Targets – Sum of Accounts Gathered – SoA

t-Test for Log(SoA)	
Difference	-0.859
StD Err Diff	0.233
Upper CL Dif	-0.391
Lower CL Dif	-1.327
t Ratio	-3.688
DF	49
P Value	0.0003

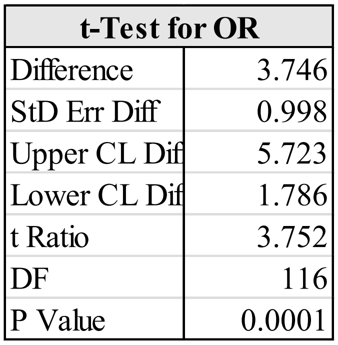


Profiling Targets – Information per Target – IT

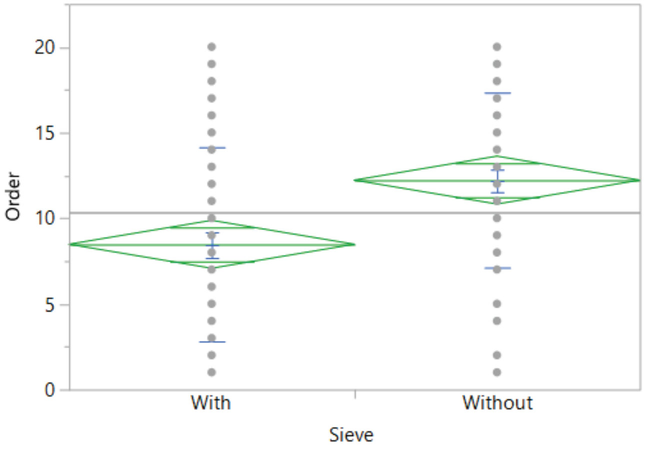
t-Test for IT	
Difference	-0.457
StD Err Diff	0.213
Upper CL Dif	-0.029
Lower CL Dif	-0.886
t Ratio	-2.144
DF	49
P Value	0.002



Crafting Spear Phishing Attacks – Overall Rank – OR



t-Test for OR	
Difference	3.746
StD Err Diff	0.998
Upper CL Dif	5.723
Lower CL Dif	1.786
t Ratio	3.752
DF	116
P Value	0.0001


Order
With
Without
Sieve