Training Future Cybersecurity Professionals in Spear Phishing using SiEVE

Jared James Meyers
School of Technology
Brigham Young Univ.
Provo, Utah, USA
jaredjmeyers@gmail.com

Derek L. Hansen
School of Technology
Brigham Young Univ.
Provo, Utah, USA
dlhansen@byu.edu

Justin S. Giboney
School of Technology
Brigham Young Univ.
Provo, Utah, USA
justin_giboney@byu.edu

Dale C. Rowe
School of Technology
Brigham Young Univ.
Provo, Utah, USA
dale_rowe@byu.edu

ABSTRACT

Most enterprise network attacks are the result of spear phishing, a highly personalized form of social engineering attack that is increasingly common. It is imperative that future cybersecurity professionals understand how to protect against such attacks, as well as how to effectively and efficiently perform such attacks during penetration testing. To help such education efforts, this paper introduces a process for creating spear phishing attacks called the Social Engineering Vulnerability Evaluation, or SiEVE for short. The step-by-step process relies solely on open source data and includes the steps of (1) identifying targets, (2) profiling targets, and (3) crafting spear phishing messages. SiEVE was evaluated as part of an experiment that compared performance of two groups of students in a 3rd year University Cybersecurity class: those with SiEVE (n=27) and those without SiEVE. (n=24). Findings show that those using the SiEVE process (a) did not identify more targets, though SiEVE students had significantly lower variance, (b) did identify more information about targets, and (c) did lead to more effective spear phishing attacks. The study illustrates the value of providing simple guidelines on improving performance of social engineering activities.

KEYWORDS

Social engineering; open source intelligence; red team; SiEVE, cybersecurity

ACM Reference format:

Jared Meyers, Derek Hansen, Justin Giboney, and Dale Rowe. 2018. Training Future Cybersecurity Professionals in Spear Phishing using SiEVE. In *The 19th Annual Conference on Information Technology Education (SIGITE '18), October 3–6, 2018, Fort Lauderdale, FL, USA*. ACM, NY, NY, USA, 6 pages. https://doi.org/10.1145/3241815.3241871

SIGITE '18, October 3–6, 2018, Fort Lauderdale, FL, USA

ACM ISBN 978-1-4503-5954-2/18/10...$15.00
DOI: https://doi.org/10.1145/3241815.3241871

1 INTRODUCTION

Social engineering attacks have become a major attack vector in recent years; accounting for billions of dollars in damages annually [1]. A common type of social engineering is spear phishing, which is the crafting of a fraudulent message (e.g., an email) that targets a specific individual as if from a trusted sender to induce the target to download malware or share personal information [2-3]. For over a decade, the number and quality of phishing and spear phishing attacks has increased dramatically [1,4-5] to the point where most of corporate attacks now begin with a spear phishing attack [6]. Recent reports indicate that 30% of phishing messages get opened by targeted users and 12% of users click on malicious attachments or links [7]. Spear phishing attacks have become highly personal, using data about the company, individuals, and projects to craft messages targeted at a handful of individuals with elevated privileges [8]. While most spear phishing campaigns last only for days, some use spear phishing for months as attackers gradually gain trust and develop a relationship before they perform an attack [8], often as part of an "advanced persistent threat" [9].

Exposing students and professionals to spear phishing attacks can help assess organizational risks and help train employees. Increasingly, companies that perform penetration tests are offering services to assess how vulnerable employees are to spear phishing attacks, and then helping train employees on how to not fall victim to them. For example, Wombat Security's ThreatSim® Phishing Simulations helps companies simulate attacks on employees and track who falls victim to them, as well as provide custom training for those who do fall victim [10]. While a handful of such services exist, there are few red team members who have been trained to craft spear phishing emails and the curriculum for that training is lacking. Furthermore, crafting such messages efficiently is important, since red teams have many vulnerabilities to assess.

This paper aims to help fill the gap by (a) developing a new process, called the Social Engineering Vulnerability Evaluation (SiEVE) process, designed to help novice red team members create spear phishing attacks, and (b) evaluating the effectiveness of the different stages of the process to illustrate the potential of step-by-step processes in improving efficacy in a time constrained context. Our evaluation provides promising results for this type of approach.

2 LITERATURE REVIEW

A wide variety of social engineering attacks have become commonplace in recent decades. These attacks that play out across different channels (e.g., email, voice, websites, social networks), are conducted by humans or software, and include different types including physical, technical, social, and socio-technical [9]. This paper is primarily focused on spear phishing attacks, a particularly common type of phishing attack wherein an attacker creates a personalized phishing attack aimed at a handful of targets with elevated privileges. It is clear from successful attacks that social media and Open Source Intelligence (OSINT) data is being used for reconnaissance [9,11]. For example, spear phishing emails often pose as an existing contact of the target, which has been shown to be 4.5 times more effective than sending them as an unknown individual [12]. Using only Facebook, researchers showed that personal data could be mined and used to create context-aware emails for 85% of Facebook users [13]. While researchers have demonstrated the use of automated tools to craft personalized messages (e.g., [14]), it is not clear that these are widely used for spear phishing attacks, which typically focus on only a handful of high-profile individuals in an organization who have elevated privileges [9]. Research has shown that users have a difficult time distinguishing between genuine and spear-phishing emails, particularly when the authority principles is used [15], that personality, gender, and age can affect how likely a user is to fall for a spear phishing attack [16-18], and that spear phishing is more effective than generic phishing attacks [12]. While a growing number of researchers are working on automatically identifying spear phishing attacks (e.g., [19-20]), this will not replace the need to train humans. User training via games and just-in-time education has helped significantly [21-22], but still requires the creation of realistic spear phishing attacks – the focus of this paper. Hand-crafting spear phishing attacks based on freely available content seems like the best way for red teams to reproduce the sophisticated types of attacks that are now common.

But how can red team members efficiently create spear phishing attacks that mirror those of potential attackers? Little evidence-based guidance is provided on how to do so. There are books designed to teach social engineering techniques including spear phishing (e.g., [23]), but research has yet to demonstrate the effectiveness of best practices that are shared. Furthermore, the techniques proposed are sometimes too high-level to be useful in practice or take an inordinate amount of time to learn about and implement. One promising approach is to provide a simple structured process, like a checklist, to help scaffold the experience and make sure best practices are considered or followed. Such checklists have resulted in dramatic reductions in cost and risk in a variety of industries, as outlined in the *Checklist Manifesto* [24]. For example, the book explains how using a step-by-step process checklist describing how to insert catheters properly led to a drop from 2.7 infections in 1,000 patients to 0 infections after 3 months. This paper takes a first stab at developing and testing a simple process (the SiEVE process) designed to help inexperienced cybersecurity students how to create spear phishing attacks.

3 RESEARCH QUESTIONS

The main objective of the research was to develop and evaluate the SiEVE process for identifying personal information that can be used in spear phishing attacks and evaluate its effectiveness. The process was developed using an iterative process that solicited input from experts and improvements based on a pilot test of the process that included 37 students and the final evaluation with 51 students. Section 5 presents the version of the SiEVE Process that was used in the final evaluated. The evaluation of the current version was designed to assess each key component of the SiEVE process separately and addresses the following high-level research question and specific hypotheses.

Research Question: Does the SiEVE process improve the effectiveness of cybersecurity students in gathering data for, and crafting spear phishing attacks within a specified time limit?

- Hypothesis 1: Students using SiEVE will generate more targets in a given timeframe than students not using SiEVE.
- Hypothesis 2: Students using SiEVE will collect more personal information about targets in a given timeframe than students not using SiEVE.
- Hypothesis 3: Students using SiEVE will create more effective spear phishing attacks in a given timeframe than students not using SiEVE.

4 METHODOLOGY

The SiEVE process was developed using the following iterative process. Existing research and professional resources were consulted to identify the key steps in development of spear phishing attacks, as well as specific tools that can be used. An initial version was drafted and iteratively improved based upon feedback from 2 professional penetration testers and one research scholar familiar with social engineering attacks. A pilot test of the beta version of the SiEVE process was performed as part of an experiment with Junior and Senior IT students taking a required Information Assurance and Security class in Fall 2017. The group was split into those who received the SiEVE process and those who did not receive the SiEVE process. During the pilot test, students could use as much time as they wanted on each of the different phases. The results were promising, showing that the SiEVE process helped to find more information on the provided targets. Feedback on the clarity and comprehensiveness of the SiEVE process was solicited from student and the final version of SiEVE was updated to reflect their suggestions. It was also used to choose reasonable timeframes for the summative evaluation, since we wanted to hold the amount of time constant for all participants.

To test the effectiveness of the final SiEVE version, we conducted a summative evaluation as part of a 2-condition experiment: with SiEVE and without SiEVE. The experiment was conducted during multiple Tuesday lab sessions (without SiEVE) and Thursday lab sessions (with SiEVE). Students were not

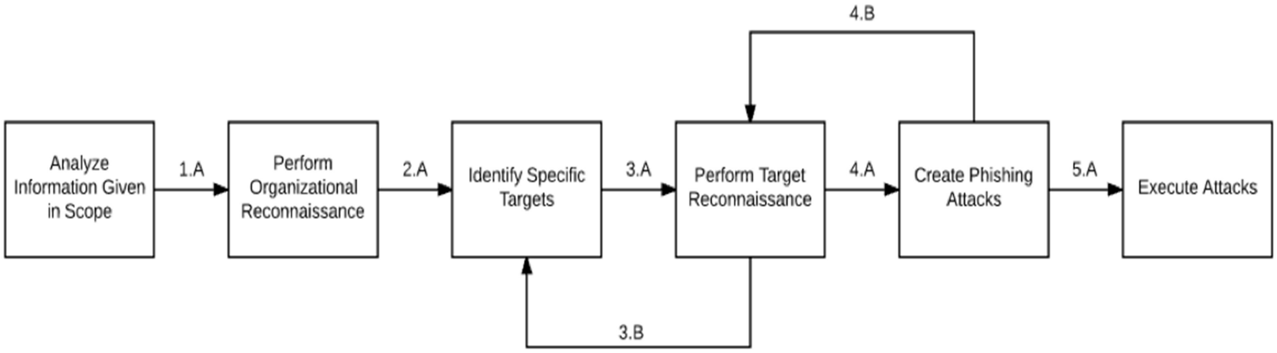
Analyze Information Given in Scope
1.A
Perform Organizational Reconnaissance
2.A
Identify Specific Targets
3.A
Perform Target Reconnaissance
4.A
Create Phishing Attacks
5.A
Execute Attacks
4.B
3.B

Figure 1. SiEVE Process Flow Diagram.

randomly assigned between the two sessions due to the logistical challenges that would raise. However, there was no apparent differences in students making up the two sections. The choice of which lab session was assigned the with SiEVE was random. Both groups were Junior and Senior students taking a required IT Information Assurance and Security course in Winter 2018. As part of class lectures, they had received the same instruction on social engineering and phishing attacks. All the students also filled out consent forms. The only difference was that the SiEVE group was given 5 minutes to review the SiEVE process and could use it throughout their assignments. It was made available in the form of a google doc. Observations showed that all students in the with-SiEVE condition read through the SiEVE document and referred to it throughout the assignments. The following sections explain the 3 assignments given students.

4.1 Identifying Targets

The first assignment was to identify as many Brigham Young University (BYU) employees as possible. They were not allowed to use their own credentials to login to university systems. Instead, they had to rely on open source data. Students each entered their data into a spreadsheet that was later used to tabulate the number of targets identified for each student. This number was the key dependent variable used for analysis. A strict timeframe of 30 minutes was used for both the with and without SiEVE conditions.

4.2 Profiling Targets

The second assignment was performed after a short break on the same day as the first assignment. The assignment was to identify as many pieces of personal information as possible about the targets they had identified in the first assignment. Specifically, they were asked to find information that could be useful in a spear-phishing attack, including Full Name, pseudonyms and nicknames; place of residence or city/zip code; email addresses; phone numbers; social media accounts; personal blogs or websites; hobbies and interests; children or close relative names; birthday and other Personally Identifying Information (PII) (e.g., employee number, usernames). As with the first task, they could not log into any sites to collect the data. Instead, they had to use publicly available information on the Internet. Each student entered the data they found and links to where they found it into a spreadsheet. We counted the sum of information gathered, sum of PII gathered, sum of accounts gathered (i.e., usernames and/or passwords), as well as the number of targets for each of these categories and the information per target. These all serve as dependent variables. This assignment was also timed and kept to 30 minutes for both groups.

4.3 Crafting Spear Phishing Emails

The third assignment was conducted on a different day than the first two assignments to reduce fatigue. The goal was to craft a spear phishing email attack designed to gain trust from a target. To standardize the information that was used to create the spear phishing attack, the same personal information about pre-identified targets was given to students. The first author gathered personal information using the SiEVE process on 6 different university employees with elevated privileges including: 2 security professionals (a Senior Security Architect and an Access Manager Security Analyst), 2 professors, and 2 student employees (Laboratory Industrial Hygienist and Risk Management Industrial Hygienist). Each student created a spear phishing email for only 3 assigned targets (one randomly assigned from each group). Students had 30 minutes and only used the provided information. The reason we used 6 targets, while only assigning 3 to students, was to reduce the load on the targets who were asked to assess the quality of the spear phishing emails as described below.

Each of the 6 targets was given a randomly ordered list of spear phishing emails that were directed toward them personally. In total, there were 20 or fewer per target, making this a manageable number. Note that these came from the with and without SiEVE groups, although the targets never knew which group they came from or that there were two groups. Targets were asked to order the emails from most likely to fall for to least likely to fall for. They also indicated a cutoff point where they believed all the ones ranked higher than said cutoff point would have undoubtedly deceived them. The average rank position was used as a dependent variable for statistical analysis. We also reported on the number of spear phishing messages that were above the cutoff for each group.

4.4 Data Analysis

Statistical analyses measure significant differences between the two conditions. Non-normally distributed data was transformed into normal data before conducting t-tests comparing the averages for the two groups. For example, a logarithmic transform was conducted on skewed data, such as the targets enumerated. In cases where there was a large difference in the variance between the two groups (i.e., Identifying Targets), a Welch's t-test was conducted. A 95% confidence interval was assumed for significance. Lab periods were observed by one author who took notes and observations that are used to supplement the statistical results.

5 THE SiEVE PROCESS

This section describes the SiEVE process that was provided to students. A generic version that is not university-specific was created, as well as a university-specific one that included examples from BYU. It was provided in the form of a google document.

An introduction states: "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." Definitions of target, reconnaissance, general phishing, and spear phishing are provided. Figure 1 is provided, followed by a brief description and when appropriate step-by-step instructions. For example, the Perform Target Reconnaissance step includes the following steps: 1. Perform simple Google searches using the target's 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.

6 FINDINGS

6.1 Identifying Target Results

In total, the without SiEVE (n=24) group found an average of 93 targets, while the with SiEVE group (n=27) found an average of only 61, though some significant outliers brought the without SiEVE group up (e.g., targets enumerated of 511 and 257). As shown in Figure 2, the distribution of results for the with SiEVE and without SiEVE groups were quite different. The results suggest that using the SiEVE process increased the minimum scores, though it may have also lowered some of the higher scores. This suggests there may be opportunities to improve the SiEVE instructions for this section by recommending strategies that were successful in the without SiEVE group. However, the fact that the SiEVE process increased the lowest performing student scores, suggests that it was helpful for at least some students. Due to the difference in variances between the groups, a Welch's t-test was conducted and no significant difference in the means was found (p=0.307; adjusted DF=28.14; Difference: -0.138). Thus, we reject Hypothesis 1, suggesting that the SiEVE process does not increase the number of targets enumerated.

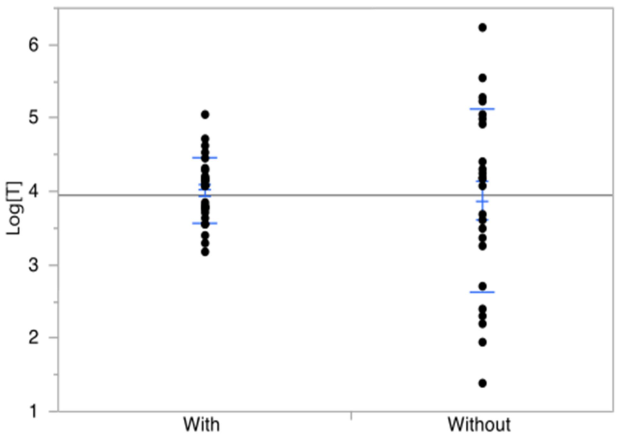

Figure 2. Box Plot of Log of Targets Enumerated for With SiEVE and Without SiEVE groups.

6.2 Profiling Target Results

Several dependent variables were used to measure the effectiveness of performing reconnaissance on targets. Table 1 shows the differences between the with and without SiEVE groups. *All* indicates the average number of all types of information pieces collected about targets by students. *PII* indicates the average number of Personally Identifying Information pieces collected per student. *Acc* indicates the average number of account-related information pieces collected per student. *Targets* indicates the number of targets with at least one piece of information gathered about them. Lastly, *All per Target* indicates the average number of pieces of information gathered per target. A t-test with degrees of freedom of 49 was performed for each dependent variable (or the log of the variables with a * shown in Table 1). In all cases, the difference was significantly better (at a 95% confidence level) for the with SiEVE group. Thus, we accept Hypothesis 2, indicating that those in the SiEVE group will perform better reconnaissance than those in the without SiEVE group.

Table 1. Profiling targets results

Metric	All*	PII	Acc*	Targets	All per Target
With SiEVE avg	75.6	3.9	7.2	30.9	1.3
W/O SiEVE avg	31.0	2.2	3.0	18.9	0.9
Difference	0.9	1.7	0.9	12.0	0.5
P Value	.0001	.044	.0003	.021	.002

6.3 Crafting Spear Phishing Email Results

As described earlier, each of the 6 targets ordered the spear phishing attacks targeted at them from most likely to least likely to influence them. An average rank was calculated for each condition, where a lower number indicates that the emails were more likely to trick the target into thinking they are real. The SiEVE condition had an avg. rank of 8.48, compared to the without SiEVE avg. of 12.22. A t-test found that these were significantly different (p=0.0001; DF=116; difference = 3.74). This confirmed Hypothesis 3, which indicated that the SiEVE group will create more effective spear phishing attacks than the without SiEVE group.

Targets also indicated which spear phishing attacks they would have fell for. While this is based on self-reported data, and thus likely to underreport the number they would fall for, comparisons of the two groups are still meaningful. Of the 14 emails that targets said would have tricked them, 11 (79%) were in the with SiEVE condition. This further confirms Hypothesis 3 by focusing on the spear phishing emails that are most likely to have an impact.

When the targets were asked about their ranking process, they indicated that messages related to the work environment were relatively easy to identify as fraudulent, since they often made references to things that did not make sense in the context of their work environment. The work-related messages often contained mistakes in work vernacular. Messages that were supposed to look like official messages were easy to identify, likely because they mirror many common phishing attacks. On the other hand, spear phishing attacks that were more often rated higher contained the interests or hobbies of the targets. The university specific examples provided as part of the SiEVE process mentioned hobbies (eSports; photography), which likely led to more students in that group using hobbies as opposed to work-related emails.

7 DISCUSSION AND CONCLUSTIONS

The purpose of this study was to iteratively develop and evaluate the SiEVE (Social Engineering Vulnerability Evaluation) process designed to help red team members create effective spear phishing attacks using only open source data. The process includes 3 key phases: identify targets, profile targets, and create the spear phishing attack. It is a simple step-by-step process that can be read and followed with no guidance and minimal time. The evaluation with university students in a required IT Cybersecurity class showed that the SiEVE process reduced the variability in the number of targets acquired (though it did not increase the total number of targets acquired); increased the amount of information, amount of personally identifiable information, amount of account-related information, and the amount of information per target; and increased the quality of spear phishing attacks. This was done in a time-pressure context, which is realistic for the use-case we imagine wherein resource constrained red teams perform. While there is still room for improvement (e.g., in how the SiEVE process recommends identifying targets), this first attempt to create a tool to help novice penetration testers perform effective spear phishing attacks has shown significant promise.

A key takeaway is that providing a simple step-by-step process can be extremely effective. This is not to say that finding and profiling targets or crafting effective spear phishing attacks is trivial. Rather, it suggests that adding a step-by-step process to students' existing abilities to search google and social media sites or understand and leverage social context through email messages is helpful. While this study helped show the viability of this approach, it did not delve deeply into the nuances of why the SiEVE process was so helpful. Future work will need to do so. Perhaps having a framework within which to work increases confidence in a students' ability to make progress since they aren't second-guessing themselves. Perhaps the resources and examples provided as part of SiEVE were unknown or not recalled in a timely manner by those who didn't use SiEVE. Or perhaps students floundered more without SiEVE because there were so many possible starting points.

One limitation of the study was that it focused solely on students. This is good, in that it demonstrates that SiEVE is useful in a teaching context. However, it is not clear how useful it would be to professional penetration testers who may already know best practices outlined in the SiEVE process. However, research on checklists in medical contexts [24] suggests that simply knowing something does not mean you will act upon it. This study was also limited in that it did not assess retention. We don't know if students who used the SiEVE process retain the information learned and could perform equally well without having it close by in the future. It is possible that the analogy of checklists may be useful to have even after internalizing it, though this is unproven as yet.

One novel aspect of this study that warrants further examination is the methodology used to assess the viability of spear phishing attacks. Clearly, studies that release spear phishing attacks in the wild and measure which one's work play a vital role in the literature (e.g., see [13,17]). However, even those studies are limited in some ways. For example, the number of spear phishing attacks that can reasonably be sent to a single person in a given timeframe is very limited. Our approach of having a small number of targets order approximately 20 messages has several possible advantages. Spear phishing attacks are highly personalized by nature and having a single person rank the efficacy of different attacks removes the variations between people. Additionally, the potential for ethical problems resulting from targets not giving consent ahead of time (which would ruin this type of study) is avoided by our method, since consent for others to perform reconnaissance and craft spear phishing messages is gathered ahead of time.

One possible concern is that targets will not identify the appropriate cutoff point at which they would "fall for" a spear phishing attack. Social desirability bias suggests that targets may underreport the number of messages that would fool them. But even if that is the case, ranked data is extremely useful in contexts such as the one used here to conduct experiments between multiple conditions. Our statistical results showing a high difference between the mean rank position of the with and without SiEVE groups is valid, irrespective of the cutoff point identified by the targets. There is a potential problem that treating ordinal data as continuous may not be appropriate. For example, targets may have ranking fatigue and discount the order of emails in the middle or bottom of the list. We tried to counter this through stressing the importance of all the rankings, but further research may be needed to validate the approach. Additionally, as we showed in this study, analysis can focus on different parts of the list, such as the area above a cutoff threshold or a research-defined value (e.g., the top 5 items).

While this study focused on creating and evaluating a simple step-by-step process for creating spear phishing attacks, the same approach could be used in several information technology and cybersecurity domains. One challenge we identified in creating the SiEVE process was in finding the right balance between providing a high-level structural overview (e.g., Figure 1) and providing specific details such as websites that are useful or examples that can be modified and used. Our approach was to include both, as efficiently as possible, given that we wanted a short process that was easy to follow for beginners. Our observations showed that students with the SiEVE seemed to jump right in, whereas those without SiEVE sometimes floundered at the start, not really knowing where to begin. We believe having the overall structure and lists of steps to perform helped those using SiEVE jump right in. Furthermore, as described in the findings, the examples provided for creating spear phishing attacks happened to use hobbies as opposed to work domains – something that turned out to be a key differentiator between the two groups and likely one of the main reasons the with SiEVE group outperformed the without SiEVE group. This shows the power of a good example, but also the potential problems of a bad example. The fact that this was not a planned characteristic of the example we chose suggests the importance of developing processes in an iterative fashion where insights such as this one can bubble up.

We hope that this work will help inspire additional work by educators and researchers that explores the power of systematic processes in supporting new red team members.

8 ACKNOWLEDGEMENTS

The authors would like to thank BYU's Department of Statistics for their aid in data analysis.

9 REFERENCES

[1] GreatHorn. *Spear Phishing Report.* Retrieved June 13, 2018 from https://www.greathorn.com/spear-phishing-report/

[2] Neely, L. 2017. *A SANS Survey 2017 Threat Landscape Survey: Users on the Front Line.* Retrieved June 12, 2019 from https://www.sans.org/reading-room/whitepapers /threats/2017-threat-landscape-survey-users-front-line-37910

[3] Hong, J.. 2012. The state of phishing attacks. *Commun. ACM 55*, 1 (January 2012), 74-81.

[4] Agari. Social Engineering, the #1 Cyber Security Threat. Retrieved June 13, 2018 from https://www.agari.com/social-engineering/

[5] Abraham, S., and Chengalur-Smith, I. 2010. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32* (3), 183–196.

[6] Symantec. 2018 Internet Security Threat Report. Retrieved June 13, 2018 from https://www.symantec.com/security-center/threat-report

[7] Verizon. 2018 Data Breach Investigations Report. Retrieved June 13, 2018 from https://www.verizonenterprise.com/verizon-insights-lab/dbir/

[8] Ironscales. How Modern Email Phishing Attacks Have Organizations on the Hook. Retrieved June 13, 2018 from https://ironscales.com/

[9] Krombholz, K, Hobel, H., Huber, M. and Weippl, E. 2015. Advanced social engineering attacks. *J. Inf. Secur. Appl.* 22, C (June 2015), 113-122.

[10] Wombat Security, a. Phishing Awareness Training Solution. [online] Wombatsecurity.com. Retrieved June 13, 2018 from https://www.wombatsecurity.com/phishing-awareness-training-lp

[11] Blond, S. L., Uritesc, A., Gilbert, C., Chua, Z. L., Saxena, P., and Kirda, E. A Look at Targeted Attacks through the Lense of an NGO. 2014. In *USENIX Security Symposium*, August 2014.

[12] Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. Social phishing. *Commun. ACM* 50, 10 (Oct. 2007), 94–100.

[13] Brown, G., Howe, T., Ihbe, M., Prakash, A., and Borders, K. 2008. Social networks and context-aware spam. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work* (CSCW '08). ACM, New York, NY, USA, 403-412.

[14] Huber, M., Mulazzani, M., Schrittwieser, S., and Weippl E. 2010. Cheap and automated socio-technical attacks based on social networking sites. In *Proceedings of the 3rd ACM workshop on Artificial intelligence and security* (AISec '10). ACM, New York, NY, USA, 61-64.

[15] Butavicius, M., Parsons, K., Pattinson, M. and McCormac, A. 2015. Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. DOI: https://arxiv.org/abs/1606.00887

[16] Halevi, T., Memon, N., and Nov, O. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015). Available at SSRN: https://ssrn.com/abstract=2544742

[17] Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., and Ebner, N. 2017. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). ACM, New York, NY, USA, 6412-6424.

[18] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and Downs, J. 2010. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '10). ACM, New York, NY, USA, 373-382.

[19] Laszka, A., Vorobeychik, Y., and Koutsoukos, X. 2015. In *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence* (AAAI-15). 958–964.

[20] Zhao, M., An, B., and Kiekintveld, C. 2016. In *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence* (AAAI-16). 658–664.

[21] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., and Hong, J. 2010. Teaching Johnny not to fall for phish. *ACM Trans. Internet Technol.* 10, 2, Article 7 (June 2010), 31 pages. DOI: http://dx.doi.org/10.1145/1754393.1754396

[22] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and Downs, J. 2010. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '10). ACM, New York, NY, USA, 373-382.

[23] Ozkaya. E. 2018. *Learn Social Engineering*, Packt Publishing.

[24] Atul Gawande. 2010. *The Checklist Manifesto: How To Get Things Right!*, New York: Metropolitan Books.