Higher Education Social Engineering Attack Scenario, Awareness & Training Model

Thai H Nguyen
nguyent62509@mail.sacredheart.edu

Sajal Bhatia
bhatias@sacredheart.edu

Jack Welch College of Business & Technology
School of Computer Science and Engineering
Sacred Heart University
5152 Park Ave.
Fairfield CT 06825

Abstract – In today's current information security ecosystem, hardware and software securities have made the professions of hackers and threat actors harder in achieving their goals. Hackers and threat actors are now increasingly using social engineering tactics in the face of increasing technical security technologies. Social engineering tactics utilizes psychological manipulation techniques to circumvent technical security systems. While every year there are vast leaps in technical security systems, one critical dynamic still needs a dire upgrade to their operating system. The human dynamic and our innate psychological processing algorithms need a new approach to mitigating and stopping social engineering attacks. Higher education institutions are prime target for social engineering engagement missions. Universities and colleges across the world house a great number of diverse faculties, students, alumni, and employees in their ecosystem. When taken into account the increasing number of inclusions of international individuals, it only increases the existing dynamic vulnerable landscape. The authors of this paper proposes utilizing social engineering awareness training with specialized crafted scenarios focused on real-world techniques geared toward a higher education environment to combat social engineering attacks. This paper will gather a pre-awareness survey of a sample student, faculty, and employee body to assess the level of awareness. The results will be compared to a post-awareness survey to assess the effectiveness of social engineering awareness and training.

Keywords

Information Security, Social Engineering, Social Engineering Attack Scenario, Social Engineering Awareness Model, Social Engineering Training Model, Social Engineering Ethics

1. INTRODUCTION

In the 21st century, information technology (IT) is ingrained into the fabric of every society in the majority of the world. There isn't an industry that IT is not utilized from Financial, Government, Healthcare, Education, Industrial, Hospitality, Entertainment, Transportation, Retail, Telecommunication, and more. Technology that we all use today is also the very same technology that is used against us to cause harm to ourselves and society, either physically, mentally, and/or financially. Information security (IS) is continually becoming an essential in-demand and on-demand service for all of society's industries. It is critical that society's industries protect data at-rest, in-transit, and in-use from internal and external threats. The need for more IS has created a steadfast emergent of hardware and software technologies to combat a

multitude of technical vulnerabilities and threats. It has made it harder for hackers and threat actors (the authors will refer to them as "attackers") to circumvent the technical security technologies but has not made it impossible.

Attackers are turning to social engineering (SE) tactics to circumvent the technical securities emplaced. SE is the deliberate act of manipulating an individual or group of individuals into giving access to confidential and unauthorized information voluntarily [1 – 13]. Research showed that an ontological definition of SE by Mouton et al. provided a more concrete definition of SE stating, "the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity" [2]. The techniques that attackers will use in a SE attack (SEA) are identified by Mitnick as, "research, developing rapport and trust, exploiting trust, and utilize information" [4].

The authors surveyed ethical concerns pertaining to SE penetration testing and research [9, 10, 11]. SE penetration testing and research are crucial in assessing and evaluating the weaknesses in an industry such as higher education (HE). Experimentation and live executions of SEA can yield significant results, but conducting such excursions raise ethical concerns. To gather unfettered and unbiased results from the experiments, deception is a critical factor in testing and research missions [9, 10, 11]. Attackers are not restrained by the ethical constraints that penetration testers and researchers are held to. The authors proposes that crafting specialized SEA scenarios based on real-world SE events can come close to those that attackers will utilize in their profession and satisfy ethical concerns.

To assess the current state of SE awareness training policies in HE institutions, the authors surveyed a number of HE institutions[1]. The findings showed that all provided information security awareness training to their students, faculty, and employees. The authors could not assess the actual content of the training material as they were only authorized to their appropriate institutions[1-6]. From the surface level information assembled, one institution provided about two 5 min general IS awareness videos[7] and another provided only a broad generalized IS awareness text-based information[8]. Although HE institutions are providing IS awareness training, the propriety nature and generalization of IS awareness is holding back the good it can provide to the educational community.

Due to these limitations, the authors proposes utilizing an open source approach in developing and providing specialized SEA scenarios based on Mouton et al. proposed, Social Engineering Attack Framework, which expands on Mitnick's "Social Engineering Cycle" [3, 4]. The proposed scenarios are based on real-world SE events, which will replicate actual prior SEAs and be able to satisfy ethical concerns. SEA scenarios will focus specifically on the threat landscape of HE institutions. By incorporating specialized SEA scenarios into SE Awareness and Training, technical and non-technical individuals will be able to spot SEAs. This will provide individuals within institutions a superior security awareness and be more vigilant against such types of SEAs [3].

2. BACKGROUND

[1] https://is.richmond.edu/infosec/securityawareness/training/index/html
[2] https:// cybersecurity.yale.edu/mss/yale-mss-12.1
[3] https://www.technology.pitt.edu/security/information-security-awareness-training
[4] https://it.arizona.edu/documentation/seecurity-awareness-training
[5] https://cuit.columbia.edu/ciso/security-training
[6] https://its.gse.harvard.edu/services/information-security/awareness-training
[7] https://informationsecurity.princeton.edu/training
[8] https://its.ucsc.edu/security/training/index.html

Social engineering (SE) is on the rise and higher education (HE) institutions are faced with an increasing vulnerable landscape. Every year there are massive migrations of local, national, and international high school graduates, transfer students, faculty and employees hires. All interfacing with HE institution systems, adding hundreds to thousands of dynamic vulnerabilities to their information technology and information security (IT/IS) ecosystem. These individuals need to adapt to the IT/IS systems to be able to conduct their duties as students, professors, and employees.

HE institutions are a prime target for attackers because of (1) the stockpiles of valuable information (VI) they collect and store. As well as (2) the openness and transparency of institutional public information provides enormous amounts of open source intelligence (OSINT) information. Information is a critical necessity involved in running a HE institution, which offer attackers a one stop shop for VI.

Table 1

Types of Valuable Information

Personal Identifiable Information (PII)	**Parental Personal Identifiable Information (PPII)**
Protected Health Information (PHI)	**Free Application for Federal Student Aid (FAFSA)**
Financial Information (FI)	**Employment Information (EI)**
Institutional Partnership Information (IPI)	**Intellectual Property / Academic Research**
3rd Party Vendor Information	**Payment Card Information (PCI)**

Table 2

Types of Open Source Intelligence

Full Name (First, Last, Middle)	**Job title & role**
Monitor/review social media accounts	**Monitor personal & institutional news feed**
Explore old version of websites	**Public directory (phone & email)**
Google map & satellite imagery	**Public photos (Flickr, Google Images, etc.)**

Table 2 illustrates the multiple public facing information that attackers can compile in their research to formulate a refined engagement mission against an individual or group of individuals at a HE institution.

Individuals at every level in HE institutions are mandated at one point to provide multiple data points in Table 1. Attackers will not need to initiate SE engagement missions into individual industries. Attackers merely need to conduct a single SE engagement mission on an unprepared HE institution and gain access to a treasure trove of VI. VI can be utilized in a follow up SEA into other industries. In a 2019 survey conducted by PurpleSec[9] from a number of sources[10] states:

SE Statistics:

- 98% cyber-attacks rely on social engineering.
- 63% of successful attacks come from internal sources, either control, errors, or fraud.
- 60% of IT professional citing recent hires as being at high risk.

[9] https://purplesec.us/resources/cyber-security-statistics/

[10] https://3th2q02cq5up44zpe81rwase-wpengine.netdna-ssl.com/wp-content/uploads/2020/02/2019-Cyber-Security-Statistics-Sources.pdf

- SE attempts spiked more than 500% from the Q1 to Q2 of 2018.

Education Industry Statistics:

- The education industry is ranked last in cybersecurity preparedness out of 17 major industries.
- 41% of HE cybersecurity incidents and breaches were caused by SEA.
- 455 cybersecurity incidents in the educational sector last year.
- Educational records can fetch up to $265 on the black market.
- 25% have experienced critical intellectual property theft.
- 79% universities have experienced damage to reputation.
- 77% also say a cyber breach has the potential to impact national security, due to the potentially sensitive nature of the information which could been compromised.
- In March 2018, over 300 universities worldwide suffered from a giant cyber-attack organized by nine Iranian hackers. According to official information, 31 terabytes of "valuable intellectual property and data" was exposed.

Armed with enough time, motivation and unchained ethical constraints, attackers will achieve their goals of infiltrating HE/IT infrastructure. HE institutions around the world have a lot to lose in the aftermath of a security breach.

Table 3
Types of Negative Impacts on HE Institutions

Financial Losses	**Loss of Trust**
Legal Action	**Drop in Retention Rate**
Reputation Damage	**Loss of Research Affiliations**

3. ETHICAL SOCIAL ENGINEERING APPROACH

For professional penetration testers and researchers conducting live social engineering attack (SEA) experimentations for the improvement of society, to attain accurate and unfettered results from their experimentations, penetration testers and researchers must engage in a high level of deception and manipulation [9, 10, 11]. By executing tactics that malicious social engineers will utilize in their own engagement missions against real-world targets, they are able to enlighten the organization(s) of the weaknesses in their environment. The individual or group of individuals conducting SEA experimentations must also abide by ethical guidelines to satisfy their respective ethical oversight committee such as their institutional review board [11].

According to Mouton et al. penetration testers and researchers must adhere to the 3 major normative ethics principles of virtue ethics, utilitarianism, and deontology, to be viewed as ethical [9]. If there are any deviation from the 3 principles then the individual or group of individuals are unethical in their actions. In the following, the authors emphasizes the distinctions between ethical and unethical in each principle [9].

3.1 Virtue Ethics

The actions of an individual in the context of virtue ethics is considered to be ethical or "virtuous" if the individual is adhering to a defined moral code or code of ethics[11]. If the actions taken by the individual deviates from the moral code or code of ethics then they are considered unethical. For penetration testers and researchers, Mouton et al. focuses on the Code of Ethics described by the IEEE & ACM as the guiding principles [9].

3.2 Utilitarianism

Utilitarianism, also known as consequentialism, considers an individual to be ethical if the individual's actions benefits society[12]. Otherwise, if the individual's actions do not benefit society it is considered unethical. Penetration testers and researchers conducting SEA are considered ethical if it provides beneficial outcomes to the greatest number of people. It disregards the consequences it has on the victim in which the SEA was directed toward [9].

3.3 Deontology

Deontological ethics defines what individual(s) should and should not do by the moral standards of society[13]. If such actions by the individual deviates into morally forbidden norms of society then it is considered unethical. According to Mouton et al., SEA needs to strictly adhere to the deontological rules of the world from the very beginning, regardless of the consequences [9].

There is no substitute to genuine live SEA, but conducting these experimentations require thorough and precise navigation to be within ethical standards. Malicious attackers are uninhibited by such ethical limitations. The authors recognizes the limitations that penetration testers and researchers face in conducting meaningful SEA experimentations. To bridge the unethical advantages of malicious attackers, the authors proposes using Mouton et al. proposed social engineering attack framework (SEAF) [3]. Penetration testers and researchers are able to step into the mindset of a malicious social engineers and plan full spectrum SEA engagements targeted at their specific environment. SEAF will allow penetration testers and researchers to create a multitude of ethical and unethical SEA scenarios. An additional benefit for penetration testers and researchers in utilizing SEAF is the ability to provide detailed execution procedures of their experiment to their respective ethical oversight committee for review.

4. SOCIAL ENGINEERING ATTACK FRAMEWORK

Mouton et al. proposed social engineering attack framework (SEAF) expanded upon their ontological SEA model defines 7 components [2] and 6 core phases [3]. SEAF provides a comprehensive outline of the processes that attackers utilize in conducting their social engineering attack (SEA). The authors recognizes the thoroughness of SEAF, and it is the basis to the authors' specialized crafted higher education (HE) social engineering (SE) scenarios. In the following the authors outlines the 7 components then 6 core phases of SEAF:

1. ***Communication***: Direct (includes Bidirectional & Unidirectional) & Indirect
2. ***Social Engineer***: Individual or Group of Individuals
3. ***Target***: Individual or Organization
4. ***Medium***: Method of Initiating Communication (Social Engineer to Target)

[11] https://plato.stanford.edu/entries/ethics-virtue/
[12] https://plato.stanford.edu/entries/consequentialism/
[13] https://plato.stanford.edu/entries/ethics-deontological/

5. ***Goal***: Financial Gain, Unauthorized Access, or Service Disruption
6. ***Compliance Principles***: Reasons why a Target complies with the Social Engineer's Request
7. ***Technique***: Method(s) a Social Engineer utilizes in achieving their Goal

The authors recognized that the medium component can be broken down into 2 types of defined methods, human-based and technology-based [8]. Workman's defined human-based and technology-based medium allows individuals and organizations to better recognize and categorize the medium in which social engineers are utilizing in their attack. The following are 6 core-phases of SEAF:

1. ***Attack Formulation***: Goal Identification & Target Identification
2. ***Information Gathering***: Identify Potential Sources, Gather Information from Sources & Assess Gathered Information
3. ***Preparation***: Combination and Analysis of Gathered Information & Development of an Attack Vector
4. ***Develop Relationship***: Establishment of Communication & Rapport Building
5. ***Exploit Relationship***: Priming the Target & Elicitation
6. ***Debrief***: Maintenance, Transition & Goal Satisfaction

Refined advancements Mouton et al. implemented to their ontological SEA model in creating their SEAF provides an important step forward for penetration testers and researchers. For penetration testers, it provides the individual or team of individuals a preliminary tool to utilize in formulating their authorized SEA mission. For researchers, the comprehensiveness of every phase and associated steps of the SEAF provides accurate repeatable results which can be utilized in verifying and comparing to other models, processes and frameworks within SE [3].

5. SOCIAL ENGINEERING ATTACK SCENARIOS

Utilizing Mouton et al. proposed Social Engineering Attack Framework, the authors developed 9 total higher education social engineering attack scenarios. Attack scenarios are separated into 3 Bidirectional Attacks, 3 Unidirectional Attacks, and 3 Indirect Attacks.

5.1 Higher Education Attack Scenarios

Please refer to the authors' open source GitLab repository to access specialized higher education social engineering attack scenarios [17].

6. SOCIAL ENGINEERING AWARENESS AND TRAINING

Current technical information security (IS) commodities have provided organizations across major industries greater capabilities in securing their information technology (IT) infrastructure. While every year there are incremental advances in IS products, they still fail to secure the human operators. It is due to the expansion of technical IS solutions have pressed attackers into conducting social engineering (SE) engagements against an individual(s) of an organization [12, 13, 14]. The authors theorizes that it is due to the lack of awareness and knowledge of SE tactics which is the main factor in increased social engineering attacks (SEA). Technical and non-technical individuals do not need to understand the weaknesses in an IT system. They need to be aware of the tactics used by attackers to circumvent the technical security systems.

If a person sees something suspicious they can report and stop the incident from escalating to compromised IT systems.

Individuals are an essential component to the IS landscape. Not only are individuals a part of the IS problem, but they are an integral part of the IS solution [12]. Organizations across the industries have implemented security awareness and training solutions to enhance their organizational human security. An example is The Department of Homeland Security's (DHS): National Cybersecurity Awareness Month[14] (NCSAM). NCSAM does a great job in providing annual guidance and awareness to industries and the general public for the month of October.

The authors proposes developing a High Education (HE) Awareness and Training Model similar to Mohammed et al. and Jansson et al. [13, 14] but improves upon their limitations. By incorporating specialized crafted social engineering attack (SEA) scenarios into awareness and training programs. It will greatly increase the level of preparedness in student, faculty, and employees when challenged with a SEA. In the following sections are the Higher Education Awareness and Training Models.

6.1 Higher Education Awareness Lifecycle Model

HE awareness model is tailored to 3 human domains (HD) in HE institutions. HD encompasses: (1) Students, (2) Faculty, and (3) Employees. Segmenting awareness education allows for effective absorption of the information [13]. Each HD combined together interface with varying ITs and hold varying levels of access privileges. Tailored awareness education provides each HD clarification to their defined responsibilities in their realm of influence. Method of distributing awareness materials will take the form of physical and electronic mediums. Figures 1 & 2 below detail the types of mediums:

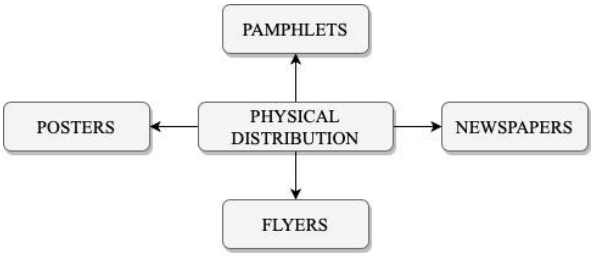

Figure 1: Physical Distribution Medium

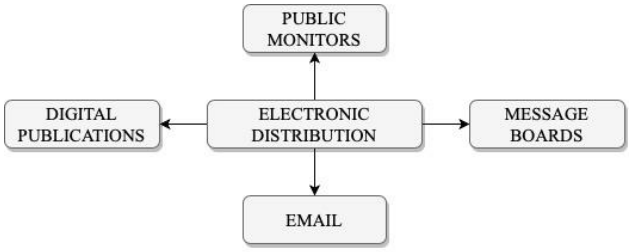

Figure 2: Physical Distribution Medium

The authors proposes a continuous rotating lifecycle approach to HE awareness education. This approach can also be classified as passive learning. Awareness information is distributed but does not mandate the HD to engage with it. The proposed lifecycle tailors specialized awareness information for each HD, utilizing each communication medium, and refreshes monthly and bi-weekly. Figure 3 below details the HE Awareness Lifecycle Model:

[14] https://www.cisa.gov/national-cyber-security-awareness-month

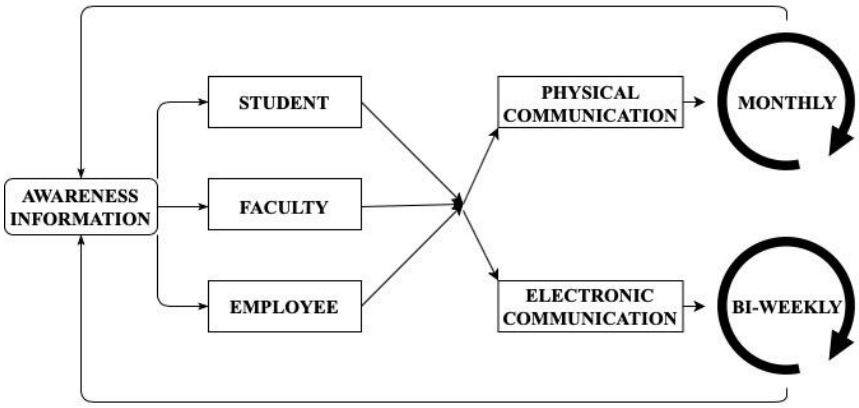

Figure 3: Higher Education Awareness Lifecycle Model

6.2 Higher Education Training Lifecycle Model

Similar to the proposed HE Awareness Lifecycle Model, HE Training Lifecycle Model proposes an active learning approach. The proposed model will mandate incoming or transfer, undergraduate or graduate students, new faculty, and employees to physically participate in an IS on-boarding program with an institutional directed IS professional. The on-boarding program will provide guidance and orient individuals to the higher education's specific IT ecosystem and IS policies. Throughout the individual's duration in the institution, electronic refresher training is required. Refresher training will be conducted in a tri-annual cycle. The proposed tri-annual timeline commences January, May, and September. Training will also include review of on-boarding concepts and up-to-date SE attacks. Figure 4 details the Higher Education Training Lifecycle Model:

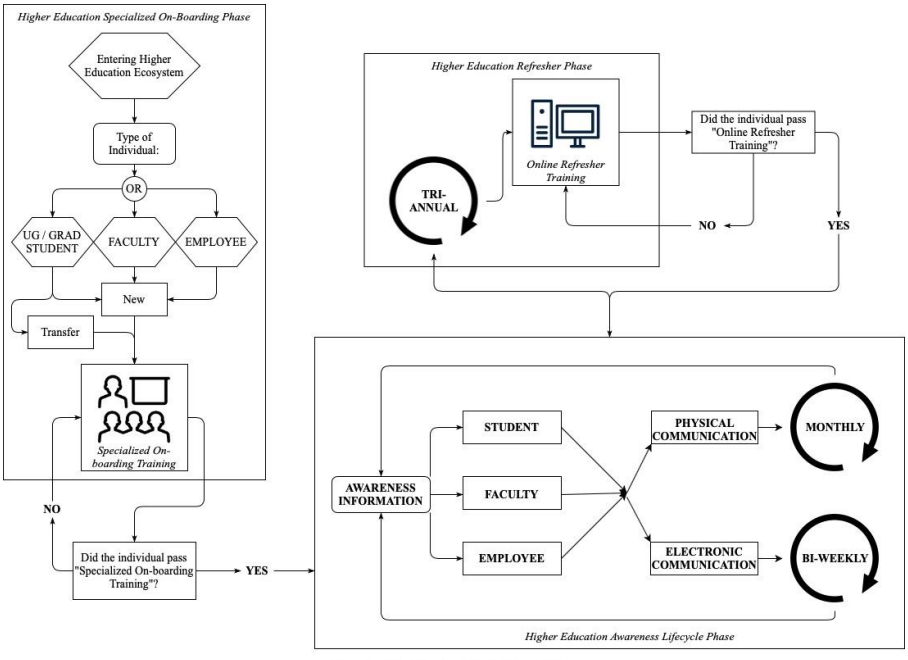

Figure 4: Higher Education Training Lifecycle Model

7. DICUSSION AND FUTURE WORK

The paper proposes 9 specialized social engineering attack (SEA) scenarios focusing on the higher education (HE) landscape. These attack scenarios provide a detailed mission plan for SEAs on higher education institutions. The social engineering attack framework (SEAF) allows penetration testers and researchers to step through each phase an attacker will take in conducting a SEA. This grants penetration testers, researchers, and ethical oversight committees another tool in fulfilling their professional obligations. For penetration testers and researchers, it allows them to engage in both ethical and unethical SEA planning and research. For ethical oversight committees it allows the committee body to review the work of penetration testers and researchers so that they are within ethical standards.

The authors theorizes the proposed HE social engineering awareness and training models will assist in securing the human dynamic. Through policies of continuous social engineering awareness and training, across every level of the human dynamic, HE institutions will be able to actively and passively educate an individual the moment they enter the institution's technology ecosystem until they leave. This affords HE institutions a comprehensive information security defensive formation alongside their physical security, hardware and software security technologies.

The authors realizes the necessity for quantifiable data on the effectiveness of proposed HE social engineering awareness and training. With the foundation of the specialized higher education social engineering attack scenarios created, the authors proposes a 3 phases methodology in gathering the data set. In the authors' future work, the first phase is collecting a baseline awareness of social engineering concepts and techniques by conducting a pre-awareness survey [15, 16]. In the second phase, implement the proposed higher education awareness lifecycle to initiate passive learning on existing individuals in the ecosystem. In parallel implement the higher education training lifecycle to initiate active learning on new individuals entering the ecosystem. In the third phase, conduct a post-awareness survey [15, 16] to gather quantifiable data on the effectiveness of the proposed awareness and training lifecycle model.

REFERENCES

[1] T. Thornburgh. Social Engineering: The "Dark Art", in Proceedings of the 1st Annual Conference on Information Security Curriculum Development, InfoSecCD Conference October 8, 2004, Kennesaw, GA, USA, 2005.

[2] F. Mouton, L. Leene, M. M. Malan and H. S. Venter. Towards an Ontological Model Defining the Social Engineering Domain, in: K.K. Kimppa et al. (Eds.): HCC11 2014, IFIP AICT 431, 2014, pp.266 – 279.

[3] F. Mouton, L. Leene, M.M. Malan and H.S. Venter. Social Engineering Attack Example, Templates and Scenarios, Computer & Security, Volume 59, 2016, pp.186-209. ISSN 0167-209. https://doi.org/10.1016/j.cose.2016.03.004.

[4] K. D. Mitnick, W. L. Simon. THE ART OF DECEPTION: Controlling the Human Element of Security, Wiley Publishing, Indianapolis, 2002.

[5] T. R. Peltier. Social Engineering: Concepts and Solutions, Information Systems Security; Nov 2006; 15, 5; ABI/INFORM Collection pg. 13.

[6] S. D. Applegate, Major. Social Engineering: Hacking the Wetware!, in Information Security Journal: A Global Perspective, 18:40-46, 2009, Taylor & Francis Group, LLC. ISSN: 1939-3555 print / 1939 – 3547 online. DOI: 10.1080/19393550802623214.

[7] R. Heartfield, G. Loukas and D. Gan. You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks, in IEEE Access, vol. 4, pp. 6910 – 6928, 2016.

[8] M. Workman, Ph.D. Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, 16:6, 315 – 331, 2007. DOI: 10.1080/10658980701788165

[9] F. Mouton, M.M. Malan, K.K. Kimppa and H.S. Venter. Necessity for Ethics in Social Engineering Research, Computer & Security, Volume 55, 2015, pp.114 – 127. https://doi.org/10.1016/j.cose.2015.09.001

[10] J. Pierce, A. Jones, and M. Warren. Penetration Testing Professional Ethics: a conceptual model and taxonomy, in Australasian Journal of Information Systems, 13(2). 2006. https://doi.org/10.3127/ajis.v13i2.52

[11] D.B. Resnik and P.R. Finn. Ethics and Phishing Experiments, Science & Engineering Ethics, 2018, 24:1241 – 1252. https://doi.org?10.1007/s11948-017-9952-9

[12] G. Rotvold. How to Create a Security Culture in Your Organization: A recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness programs, Information Management Journal, vol. 42, no. 6, Nov-Dec, 2008, ABI/INFORM Collection, pp 32+.

[13] S. Mohammed and E. Apeh. A model for social engineering awareness program for schools, 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), Chengdu, 2016, pp. 392 – 397.

[14] K. Jansson & R. von Solms. Phishing for phishing awareness, Behavior & Information Technology, 32:6, 584-593, 2013. DOI: 10.1080/0144929X.2011.632650

[15] R.M. Groves, F.J. Fowler Jr, M.P. Couper, J.M. Lepkowski, E. Singer and R. Tourangeau. Survey Methodology. John Wiley & Sons, 2011, pp.149 – 253.

[16] T.L. Jones, M.A. Baxter, V. Khanduja. A Quick Guide to Survey Research. The Annals of The Royal College of Surgeons of England. 2013, pp.5 – 7.

[17] T. Nguyen. https://gitlab.com/chuck_x_chuck/social-engineering-attack-scenarios/, (Accessed 03/14/2020).