# Toward an Effective SETA Program: An Action Research Approach

Humayun Zafar, Ph.D.
Kennesaw State University
hzafar@kennesaw.edu

Jason A. Williams, Ph.D.
Augusta University
jwilliams45@augusta.edu

Saurabh Gupta, Ph.D.
Kennesaw State University
sgupta7@kennesaw.edu

## Abstract

This study uses action research methods at a large US healthcare facility. Based on self-regulation theory, we created a new security education training and awareness (SETA) program that is focused on three threats: phishing, unauthorized use of cloud services, and password sharing. The new SETA program was shown to be more effective than the existing SETA program. Findings also indicate that the training was effective at helping users to identify and avoid all three threats to the environment. Future research directions based on this study are also discussed.

**Keywords:** healthcare, security, training, SETA, Action research

## 1. Introduction

It is widely accepted that organizations need to implement security training programs to counter potential threats in cyberspace. Yet, incidents of successful breaches continue to rise. Researchers have begun to question the effectiveness of training programs (Algarni, 2019). Some have even concluded that traditional one size fits all training programs are largely ineffective (Silic & Lowry, 2020). This may be since those approaches lack a systematic understanding of the nature of SETA programs, programs, the paths through which SETA impacts employees' security-related beliefs or behavioral intentions, and the conditions that might influence such a relationship. For example, almost all SETA programs in organizations are implemented for the purposed of ensuring adherence to compliance (Barlow et al., 2018).

There are, however, many threats to organizations. A one-size-fits-all-organizations approach to SETA has been tried and been found lacking, based on the proportion of user-caused cybersecurity breaches (Alshaikh, 2020). Instead, we focus our action research on developing SETA training customized to the business function of a healthcare organization. The training is further customized by our use of self-regulation theory. We help SETA trainees develop self-regulated skills that are context-dependent and thus more valuable than skills learned in generic SETA training.

We were tasked by a global leader in healthcare, hereafter referred to as Caregiver, to assist with efforts to strengthen their internal security protocols based on identified threats, in light of threats at a time when information technology is increasing in scope, scale, and importance to all areas of medicine. A critical element of this effort based on our research was training the disparate groups of professionals that must coordinate their efforts to provide best-of-care standards that are the hallmark of this organization. We hypothesize that users in each of our training programs will perform significantly better on post-tests than the control group for each audience of users.

## 2. Literature Review

Previous research in SETA has portrayed it as formal initiatives that aim to change employee behavior by introducing them to safe security practices (Dhillon et al., 2020; Yoo et al., 2018). Previous studies have also typically incorporated a pedagogical orientation as a primary means of improving user compliance with IS security policies. These include instructor led, video based, and game based approaches (Abawajy, 2014).

It has also been claimed that there is a need in IS to develop theory-based SETA program design and implementation (Karjalainen & Siponen, 2011; Puhakainen & Siponen, 2010). In our literature analysis, we found that the existing research scarcely focused on different approaches to designing the content and delivery methods of SETA.

Based on the philosophy of learning, the self-regulated learning approach is fundamentally different from the traditional behaviorist learning approaches (Rumjaun & Narod, 2020). Behaviorists apply the notion of objectivism as a learning theory, with a simple focus on "stimulus-response." Diverging from the objectivist's view of the existence of one single reality, the behaviorist model of learning asserts that there is a true and absolute knowledge existing in the world and that knowledge is transmittable to learners through a teacher's instruction. In other words, in a behaviorist learning environment, the SETA instructor sets a prescribed learning goal and identifies a series of required behaviors for performance.

URI: https://hdl.handle.net/10125/103036
978-0-9981331-6-4

By contrast, self-regulated skills, which are assumed to be context dependent, argue for triadic reciprocal determination based on Bandura's social cognitive theory (Bandura, 1986). Social cognitive theory focused on the individual, behavioral and environmental events which, while separate, influence each other. Emerging from social cognitive theory, self-regulation theory adds in learning that results from students' self-generated cognitions and behaviors that aid in learning (Schunk & Zimmerman, 2013). Covert self-regulation involves the learner monitoring and adjusting their cognitive and affective states, while environmental and behavioral elements focus on meta-cognitive learning and adjustments as needed in the specific context i.e., cybersecurity (Rosenthal & Zimmerman, 1978; Schunk & Zimmerman, 1998; Zimmerman, 1989, 2003). Our learning environment focuses on knowledge discovery, emphasizes knowledge construction, and supports meaningful learning through authentic tasks relating to real-world experiences.

Despite self-regulation's broad application in education, it has rarely been used in SETA training in organizations. The single SETA study we could find to have used it have employed quantitative methods (Ifinedo & Longe, 2019). The present research is among the first SETA research papers to design a SETA training program using self-regulation theory.

## 3. Action Research Approach

To fully actualize the use of self-regulatory theory in the context of SETA at Caregiver, we took an action research approach. Action research stands out as an ideal research method for validating and possibly refining a security training program (Checkland & Holwell, 1998). Owing to the principle of cyclical field intervention, action research allows theory refinement in practice, in addition to theory testing (Baskerville, 1999). Action research is also a clinical method, aimed at creating organizational change and solving practical problems through the research (Baskerville & Myers, 2004). As our aim was not only to validate and possibly refine the IS security policy compliance program in practice, but also to study how the program can be used to change employee behavior, action research seems the perfect method. This is supported by Walsham (2006), who regards action research as the ideal way to perform involved research, where the researcher has direct involvement in the change action in an organization. In following exemplars of action research in organizations, we followed the following four steps at Caregiver: problem identification, planning, delivery, and evaluation (Puhakainen & Siponen, 2010)

## 4. Caregiver Background and Participants

Caregiver is considered a leader in the healthcare arena and is based in the United States. It employs over 2,000 physicians and scientists, as well as over 40,000 staff. The employees are distributed across several campuses. Security education, training, and awareness is already embedded at the organization. However, Caregiver wanted to extend traditional information security training techniques to influence users' unconscious behavior. This reason along with the fact that Caregiver is a leader in healthcare makes it an appropriate site for our research.

Each advance in information technology that can be used for healthcare creates a potential problem for Caregiver from the perspective of information security. The IT department at the Caregiver used to centrally control security, but the new architecture is massively distributed where BYOD (bring your own device) has become standard operating procedure. This mismatch left Caregiver with inconsistency between the technology being used by the users and the security policies governing said use.

The challenges in providing training for Caregiver's personnel and associates are legion. We interviewed the head of the information security division at Caregiver (hereafter, the division head). According to him, clinical professionals, from physicians and nurses to technicians and adjunct staff, have little time for training, are not motivated to learn about information security, and have highly variable knowledge regarding information technology. Some of the other challenges according to the division head include the following:

1. Clinical professionals automatically prioritized patient care above information security.
2. Historically, healthcare has been a low priority for hackers due to a lack of standardized platforms that would make hacking profitable, though that is now changing (Algarni, 2019). Because of this, information security has been seen as an IT function as opposed to a globally shared responsibility.
3. Caregiver has an extensive network of contractors and external vendors, as well as medical staff distributed around the world, making training even more important while simultaneously making it more difficult to provide.
4. As a leading medical research organization and globally recognized leader in medical training, creation and sharing of information is paramount to progress.

Conversely, according to the division head, the need for information security in healthcare in general,

and information security training specifically, is increasing in urgency. According to the division head, federal regulations require adoption of standardized software platforms to exchange patient information that makes hacking healthcare providers inevitable.

## 5. Action Research at Caregiver

In order to test and refine a theory (Baskerville, 1999), the 9 month action research consisted of an action research cycle (see Figure 1). The research cycle at Caregiver involved identifying the problem, planning the training, delivering the training, and concurrently evaluating the results (Sein et al., 2011). This section elaborates each of the steps of the action research cycle specified in Figure 1, taken from Sein et al. (2011).

Caregiver asked us to come into their organization and observe their current cybersecurity problems. We identified the problems as a SETA delivery problem. That is, we identified improvements in the way the SETA program could be contextualized and allow users to self-regulate.

The researchers did not hold any position at Caregiver other than being cybersecurity consultants for the purposes of the action research. Participants in the action research from Caregiver were not paid to participate in our research other than their normal salaries from Caregiver. Participation was completely voluntary.

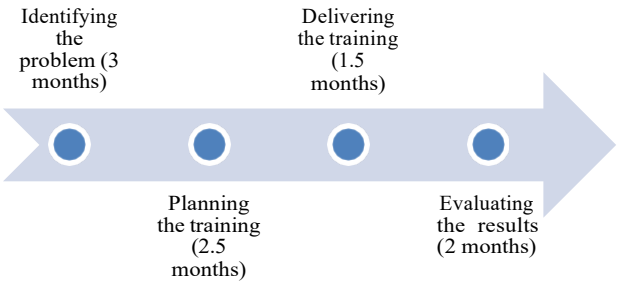


**Figure 1: Action Research Cycle**

### 5.1 Identifying the Problem

We worked closely with Caregiver's information security team to understand the organization's current approach to information security, including secure network access, encryption, password policies, and biometrics. We found that end-user training had to be customized to support Caregiver's security policies. According to the division head, the organization recognized that some of the main information security threats it faces include phishing, use of unauthorized and unencrypted cloud file sharing services, and unauthorized password sharing by users.

Previous literature in IS and complementary fields has commented on the importance of addressing these domains of information security (Crossler et al., 2013; Ferreira et al., 2013; Stanton et al., 2005; Takabi et al., 2010; Vishwanath et al., 2011; Wright & Marett, 2010; Zviran & Haga, 1999). We also used this as the basis for focusing on training that revolved around these three threats. This allowed us to create a training program that was built for a particular organization's threat profile.

We also worked with various units throughout the organization that received information security training to understand all of the contexts under which personnel engage in behavior that could lead to a data breach. This context helped us leverage students' prior knowledge to gain new knowledge (Schunk & Zimmerman, 2013). We shadowed representatives from each unit and performed interviews to better understand their behavior. We wanted to diagnose the behavior to determine risks posed by unconscious and conscious processes. Within each context, we coordinated with Caregiver's information security group to determine appropriate information security behavior.

### 5.2 Planning the Training

Training at the Caregiver already included focus on skill level, focusing on declarative knowledge steps that an individual should follow. As discussed, this was primarily focused on compliance, and did not result in significant improvement in outcomes. Consequently, our approach focused on training on higher levels of outcomes, including cognitive, affective, and meta-cognitive levels (Gupta et al., 2010).

Our approach focused on using self-regulation-based learning. This approach builds on the first two levels of vicarious and enactive learning approaches outlined by social cognitive theory (Gupta & Bostrom, 2013). Self-regulation theory adds the steps of self-control and self-regulation to social cognitive theory. The first step focuses on using knowledge on existing problems, while the later focuses on using knowledge for new problems.

To implement the training, individual and environment were separated by looking at the role of the individual (discussed later) and the cybersecurity context divided across phishing, cloud services training and password sharing. The behavioral component of the training was implemented by examining the four components of self-regulated study as outlined in Table 1. Table 1 specifies the level of self-regulated learning, the learning goal level it focused on and how it was implemented in this study. We divided the population into three groups: administrators (mostly managers),

medical professionals (included physicians, physician assistants etc.) and staff (appointment coordinators, billing specialists etc.). This allowed the content, scenarios, and discussions to be tailored more to each group's needs.

**Table 1. Self-Regulated theory components.**

| Self-regulation Learning Level | Learning Goal Level | Implementation in Training |
|---|---|---|
| Learning by vicarious modeling | Cognitive | Overview of the situation and demonstrations |
| Imitation level including social guidance | Cognitive | Simulated cybersecurity campaigns and with debrief sessions |
| Self-control i.e., successful application in context | Skill | Targeted phishing campaigns similar to what they had seen |
| Self-regulation i.e., adaptive use in changing conditions | Meta-cognitive | Targeted phishing campaigns dissimilar to what they had seen |

Details of each training topic, phishing, cloud services, and password sharing are described below.

**5.2.1 Phishing.** Training was divided into multiple sections. In the first section, there was an overview of phishing. The attendees were also provided with multiple demonstrations of phishing attacks and asked what they would do if faced with particular scenarios. We also trained attendees to actively report phishing emails even if there was a high probably of false positives.

**5.2.2 Cloud Services Training.** According to the information security division, Caregiver subscribes to a proprietary cloud service that encrypts data. However, the division head stated that only 20% of the employees use that service. Our interviews with users indicated the reasons for this low adoption rate were low ease of use and the relative intuitiveness of using alternatives to the enterprise-provided service. Other desirable features from competitors include compatibility on various mobile and desktop platforms, the speed at which data could be accessed, and overall lack of familiarity with Caregiver's cloud services. Unlike phishing, for this portion of our study we had access to aggregated data of each user group that was provided to us by Caregiver.

**5.2.3 Password sharing and general use.** According to Caregiver, a high portion (45%) of their employees at some point share their credentials to the hospital information system (HIS) with other employees. This percentage is especially high in areas where health decisions supersede all others (e.g., critical care unit and ER). All password sharing is prohibited by Caregiver's information security policies that are shared with all users. Based on our data gathering with users, some of the reasons given for sharing passwords in violation of policy included a new employee who did not have credentials for the system, an overall sense of trust in situations that required life or death decisions to be made, and a sense that nothing personal could be gained by having access to the HIS.

## 5.3 Delivering the Training

We chose a pilot group to roll out the custom training. Pilot group subjects were randomly selected from within each department at Caregiver to test the effectiveness of the training within specific contexts and help ensure overall success of the action research approach. Each attendee was randomly assigned to a treatment group (received self-regulation-based training) and a control group (did not receive self-regulation-based training). We also carried out pre- and post-tests for each group using a proprietary automated testing system. The tests dealt with phishing, use of unauthorized cloud services, and password sharing. Behavioral monitoring through technology is something that has not been extensively researched in IS (Crossler et al., 2013). However, the value of measuring actual behaviors instead of intentions has been noted in various studies (Anderson & Agarwal, 2010; Mahmood et al., 2010; Straub, 2009; Warkentin et al., 2012)

**5.3.1 Phishing.** Participants were then split into teams (medical, staff, and administrators) and provided a simulated phishing campaign, with the goal of attendees realizing that though they were not expected to be cybersecurity experts, each group had a particular role to play in defending the perimeter of their organization. The attendees were asked to identify an email and if it was an attempted phish or not, and what they felt were the consequences if the attack was successful. Attendees were also debriefed on impacts of breaches, the role of HIPAA, and their responsibilities in ensuring their systems were not compromised. We then reminded attendees that all employees will be sent campaigns and their responses will be recorded to ensure that Caregiver is prepared for cybersecurity threats. At the end of the training, all participants took a summary examination that assessed their knowledge of phishing.

We simulated two (one as a pre-test and the other as a post-test) targeted phishing campaigns based on an employee's classification. For example, a medical

professional received an email asking them to click on a link that would purportedly take them to a website that had a listing of speakers from a major medical conference. Members of staff received an email that referred them to a website they could use to register for an advanced training session that would be paid for by Caregiver. Finally, the administrators were sent an email that asked them to go to a website that talked about upcoming updates to HIPAA. In each case the phishing campaign system allowed us to not just monitor the number of people who clicked on links in emails but also trace it back to the user.

**5.3.2 Cloud Service Training.** The healthcare institution has partnered with a vendor for a customized cloud service solution for their data storage and sharing needs. Attendees were provided a brief introduction to the cloud and what it entails. We specifically distinguished between commercial cloud applications and the customized one that the Caregiver licensed for official use. The one licensed by Caregiver only allowed for two devices to use the same user account. So, if a user had a PC and a laptop, the user could not also connect a tablet or phone. This meant that a user had to de-register a device if he/she wanted to use a third one. The attendees were also shown how to log in to the service. Unfortunately, the vendor only offered a web interface for the cloud service. There were no native mobile applications that attendees could use. The attendees were also asked to enable multi-factor authentication. Finally, the attendees were asked to not use any other applications for collaboration or document sharing since it would not only be an internal policy violation but may also result in a Health Insurance Portability and Accountability Act (HIPAA) violation.

**5.3.3 Password sharing and general use.** Attendees were asked not to share their passwords, even if they felt comfortable with the person they were sharing the password with. The primary reason given was that it would not allow for a valid audit trail to be maintained in the event of a breach. Attendees were also told that once a password is shared with one person, there is no reason to believe it would be shared with an unethical person at some point.

Attendees were also asked to think about password hygiene. For example, use complex passwords, not use the same password across different systems, and to use a VPN when accessing Caregiver's systems remotely. Attendees were assessed about their general knowledge about password hygiene at the end.

The pre-test window covered three weeks. The post-test window was the same time frame. A total of 343 employees were a part of the pre- and post-tests. The initial number was 345, however 2 were unable to complete because they left Caregiver. Table 2 provides details of the participants of the study.

180 participants received threat-based training (treatment group), with the rest (163) relying solely on the basic training that Caregiver provides to all its employees every two years (control group). Table 3 shows the breakdown of employees based on treatment and control groups.

**Table 2: Study participants.**

| | Medical Professionals (MP) | Staff (ST) | Administrators (AD) |
|---|---|---|---|
| Male | 59 | 76 | 25 |
| Female | 47 | 125 | 11 |
| **Total** | **106** | **201** | **36** |

**Table 3: Group totals.**

| | MP | ST | AD |
|---|---|---|---|
| Treatment Group | 54 | 100 | 19 |
| Control Group | 52 | 101 | 17 |

## 5.4 Evaluating the Results

This research sought to improve the existing SETA training delivered at Caregiver by incorporating self-regulation theory into the SETA training. We hypothesized that our training would show significant improvements over the existing training in all three areas of training (phishing, password sharing, and cloud services) across all three user groups (medical professionals, staff, and administrators).

This setup produced a 3x3 experimental design. We tested the subject groups before and after each training to determine its effectiveness. We also tested a control group that received the traditional SETA training provided by Caregiver. All statistical tests were performed using SPSS 28.

Table 4 presents an overview of the treatment and control groups using chi-squared tests. The first value in each cell represents the total number of employees that we were able to capture instances of either phishing, password sharing and unauthorized cloud services usage. The second value represents the expected cell totals, which is followed by the chi-square statistic for each cell.

After comparing each threat instance's pre- and post-test scores against each group (treatment against control) we get the following chi-square statistics (see Table 5). All threat types for both medical professionals and staff showed significant improvements in their post-tests compared to their pre-tests. The sample size for administrators was too small to draw a statistical conclusion.

**Table 4: Pre and Post Test Results**

| | Threat | Pre-test | | | Post-test | | |
|---|---|---|---|---|---|---|---|
| | | **MP** | **ST** | **AD** | **MP** | **ST** | **AD** |
| **Treatment Group** | Phishing | 49<br>(42.37)<br>[1.04] | 64<br>(50.29)<br>[3.74] | 9<br>(7.58)<br>[0.26] | 21<br>(27.63)<br>[1.59] | 19<br>(32.71)<br>[5.75] | 4<br>(5.42)<br>[0.37] |
| | Password Sharing | 40<br>(31.96)<br>[2.02] | 53<br>(38.35)<br>[5.60] | 1<br>(0.53)<br>[0.42] | 18<br>(26.04)<br>[2.48] | 9<br>(23.65)<br>[9.07] | 0<br>(0.47)<br>[0.47] |
| | Cloud Services | 48<br>(40.45)<br>[1.41] | 78<br>(60.69)<br>[4.94] | 7<br>(5.79)<br>[0.25] | 23<br>(30.55)<br>[1.86] | 21<br>(38.31)<br>[7.82] | 2<br>(3.21)<br>[0.46] |
| **Control Group** | Phishing | 43<br>(49.63)<br>[0.89] | 59<br>(72.71)<br>[2.58] | 12<br>(13.42)<br>[0.15] | 39<br>(32.37)<br>[1.36] | 61<br>(47.29)<br>[3.97] | 11<br>(9.58)<br>[0.21] |
| | Password Sharing | 41<br>(49.04)<br>[1.32] | 67<br>(81.65)<br>[2.63] | 8<br>(8.47)<br>[0.03] | 48<br>(39.96)<br>[1.62] | 65<br>(50.35)<br>[4.26] | 8<br>(7.53)<br>[0.03] |
| | Cloud Services | 50<br>(57.55)<br>[0.99] | 82<br>(99.31)<br>[3.02] | 2<br>(3.21)<br>[0.46] | 51<br>(43.45)<br>[1.31] | 80<br>(62.69)<br>[4.78] | 3<br>(1.79)<br>[0.83] |
| MP = Medical Professional ST = Staff AD = Administrator<br>Number of Participants in this group<br>(expected total)<br>[Chi-square] | | | | | | | |

**Table 5: Chi-square statistics.**

| | MP | ST | AD |
|---|---|---|---|
| Phishing | 4.87* | 16.04* | 0.99 |
| Password Sharing | 7.44* | 21.56* | 0.94 |
| Cloud Services | 5.57* | 20.56* | 2.00 |
| * Significant at $p < 0.05$ | | | |

## 6. Discussion

Based on these results, we can see that threat focused training positively impacted medical professionals and staff in their adherence to information security policies and controls as they relate to phishing, password sharing, and unauthorized cloud service access at Caregiver.

Our training that included simulations with demonstrations, debrief sessions, and targeted attacks both similar and dissimilar to what the attendees had seen while doing their jobs at Caregiver activated several levels of self-regulation theory, including the cognitive, skills, and meta-cognitive levels. By developing training at all these levels, we were able to effectively train users from the medical professional and staff groups.

Six of our hypotheses were supported. We provided more effective SETA training to medical professionals and staff for phishing, password sharing, and cloud services. The remaining three hypotheses were unsupportable due to small sample sizes for the administrator trainings. Thus, we conclude that our SETA training, based on self-regulation theory, was more effective than the existing training at Caregiver.

We had an opportunity to discuss our results with executives at Caregiver. They provided us with unique perspectives that showed how far healthcare has come in reliance on technology. These perspectives are not only relevant to Caregiver, but to all healthcare organizations as well. Information technology has expanded geometrically at Caregiver over the past two decades with the advent of digital/electronic patient records (EMR and EHR), advanced imaging technologies (MRI, PET Scan, etc.), broadband networks (wiredand wireless), and device technologies (flat panel monitors, laptops, smartphones, and tablets). These advances have put tremendous pressure on IT departments that must develop networks and data storage to not only handle massive data files, but also to make the information readily and easily accessible to a wide range of authorized users across an ever-increasing range of devices. In addition, new communications technologies also continue apace with text, social

media, and thousands of apps fundamentally changing how patients and healthcare providers interact.

Based on our research at Caregiver we believe information gains value when it is relevant, reliable, accurate, timely, rich, fast, easy to access, easy to use, cheap, customizable, and secure. Unfortunately, the easier it is to access and use information, the more difficult it is to secure it. For example, the reflex to download a patient report at a local coffee shop's free Wi-Fi can easily override hours of information security education. This insight into behavior helps explain why such a high percentage of Caregiver's personnel clicked on a phishing email exploit even though they had all gone through security education, training, and awareness session once every two years.

These findings show that SETA trainings based on self-regulation theory were effective in this global large healthcare leader. Future work should be done to determine if similar SETA trainings based on self-regulation theory would be similarly effective in smaller healthcare settings or outside healthcare in segments such as finance, education, and commerce.

## 7. Conclusion

This research stemmed from an opportunity of the researchers to directly apply theory to practice by using an action research approach to apply self-regulation theory principles to SETA in a large healthcare setting. The findings show that the application was successful, and the users of the organization adhere more to security policy now than before the training. The successful application of self-regulation theory indicates that this approach holds merit for other SETA training implementations.

## References


Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

Algarni, A. (2019). A survey and classification of security and privacy research in smart healthcare systems. *IEEE Access*, *7*, 101879-101894.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & security*, *98*, 102003.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

Bandura, A. (1986). *Social foundations of thought and action : a social cognitive theory*. Prentice-Hall.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance [Article]. *Journal of the Association for Information Systems*, *19*(8), 689-715. https://doi.org/10.17705/1jais.00506

Baskerville, R., & Myers, M. D. (2004). Special issue on action research in information systems: Making IS research relevant to practice: Foreword. *MIS quarterly*, 329-335.

Baskerville, R. L. (1999). Investigating information systems with action research. *Communications of the Association for Information Systems*, *2*(1), 19.

Checkland, P., & Holwell, S. (1998). Action research: its nature and validity. *Systemic practice and action research*, *11*(1), 9-21.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101.

Dhillon, G., Abdul Talib, Y. Y., & Picoto, W. N. (2020). The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems*, *21*(1), 5.

Ferreira, A., Correia, R., Chadwick, D., Santos, H. M., Gomes, R., Reis, D., & Antunes, L. (2013). Password sharing and how to reduce it. In *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications* (pp. 22-42).

Gupta, S., & Bostrom, R. P. (2013). An Investigation of the Appropriation of Technology-Mediated Training Methods Incorporating Enactive and Collaborative Learning [Article]. *Information Systems Research*, *24*(2), 454-469. https://doi.org/10.1287/isre.1120.0433

Gupta, S., Bostrom, R. P., & Huber, M. (2010). End-user training methods: What we know, need to know. *SIGMIS Database for Advances in Information Systems*, *41*(4), 9-39. https://doi.org/10.1145/1899639.1899641

Ifinedo, P., & Longe, O. B. (2019, July 2019). Factors Influencing Nigerian Workers' Participation In Unhygienic Cyber Practices. The Nigerian Computer Society Annual Conference,

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 3.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. (2010). Moving toward black hat research in information systems security: an editorial introduction to the special issue. *MIS Quarterly*, *34*(3), 431-433.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study [Article]. *MIS Quarterly*, *34*(4), 767-A764.

Rosenthal, T. L., & Zimmerman, B. J. (1978). *Social learning and cognition*. Academic Press.

Rumjaun, A., & Narod, F. (2020). Social Learning Theory—Albert Bandura. In *Science education in theory and practice* (pp. 85-99). Springer.

Schunk, D. H., & Zimmerman, B. J. (1998). *Self-regulated learning from teaching to self-reflective practice*. Guilford Press.
Schunk, D. H., & Zimmerman, B. J. (2013). Self-regulation and learning.
Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS Quarterly*, 37-56.
Silic, M., & Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance [Article]. *Journal of Management Information Systems*, *37*(1), 129-161. https://doi.org/10.1080/07421222.2019.1705512
Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.
Straub, D. (2009). Black hat, white hat studies in information security. Keynote Presentation of the 1st IFIP 8.2 Security Conference, Cape Town, South Africa.
Takabi, H., Joshi, J. B., & Ahn, G.-J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), 24-31.
Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586.
Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320-330.
Warkentin, M., Straub, D., & Malimage, K. (2012). Measuring secure behavior: A research commentary. Annual Symposium on Information Assurance & Secure Knowledge Management, Albany, NY.
Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273-303.
Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107-118.
Zimmerman, B. J. (1989). A social cognitive view of self-regulated academic learning. *Journal of Educational Psychology*, *81*(3), 329-339.
Zimmerman, B. J. (2003). Motivating self-regulated problem solvers. In J. E. Davidson & R. J. Sternberg (Eds.), *The psychology of problem solving* (pp. 233-262). Cambridge University Press.
Zviran, M., & Haga, W. J. (1999). Password security: an empirical study. *Journal of Management Information Systems*, *15*(4), 161-185.