Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 1 Article 4

July 2023

How Effective are SETA Programs Anyway: Learning and Forgetting in Security Awareness Training

David Sikolia
Pittsburg State University, dsikolia@pittstate.edu

David Biros
Oklahoma State University, david.biros@okstate.edu

Tianjian Zhang
City University of Hong Kong, tj.zhang@cityu.edu.hk

How Effective are SETA Programs Anyway: Learning and Forgetting in Security Awareness Training

Abstract

Prevalent security threats caused by human errors necessitate security education, training, and awareness (SETA) programs in organizations. Despite strong theoretical foundations in behavioral cybersecurity, field evidence on the effectiveness of SETA programs in mitigating actual threats is scarce. Specifically, with a broad range of cybersecurity knowledge crammed into in a single SETA session, it is unclear how effective different types of knowledge are in mitigating human errors in a longitudinal setting. his study investigates how knowledge gained through SETA programs affects human errors in cybersecurity to fill the longitudinal void. In a baseline experiment, we establish that SETA programs reduce phishing susceptibility by 50%, whereas the training intensity does not affect the rate. In a follow-up experiment, we find that SETA programs can increase employees' cybersecurity knowledge by 12-17%, but the increment wears off within a month. Furthermore, technical-level knowledge decays faster than application-level knowledge. The longer "shelf-life" of application-level knowledge explains why training intensity makes no difference within a month. This study reveals a (relatively) more effective component of SETA programs and cast doubts on the overall effectiveness of SETA programs in the long run.

Keywords

SETA, Training, Learning, Forgetting Curve

How Effective are SETA Programs Anyway? Learning and Forgetting in Security Awareness Training

David Sikolia
Computer Information Systems
Pittsburg State University
Pittsburg, KS 66762, USA
dsikolia@pittstate.edu
ORCID:0000-0002-8894-9194

David Biros
Department of Management Science & Information Systems
Oklahoma State University
Stillwater, OK 74078, USA
david.biros@okstate.edu
ORCID: 0000-0002-4236-7914

Tianjian Zhang
Department of Information Systems
City University of Hong Kong
83 Tat Chee Ave, Kowloon Tong, Hong Kong
tj.zhang@cityu.edu.hk
ORCID: 0000-0003-1035-2838

***Abstract*— *Prevalent security threats caused by human errors necessitate security education, training, and awareness (SETA) programs in organizations. Despite strong theoretical foundations in behavioral cybersecurity, field evidence on the effectiveness of SETA programs in mitigating actual threats is scarce. Since memory decay will inevitably occur after absorbing a broad range of cybersecurity knowledge in a single session, the effectiveness of SETA programs in longer terms is unclear. This study investigates whether and how knowledge gained through SETA programs can mitigate human errors in a longitudinal setting. In a baseline experiment, we established that SETA programs reduce phishing susceptibility by 50%, whereas the training intensity does not affect the susceptibility rate. In a follow-up experiment, we found that SETA programs can increase users' cybersecurity knowledge by 12-17%, but the increment wears off within a month. Furthermore, technical-level knowledge decays faster than application-level knowledge. The longer "shelf-life" of application-level knowledge explains why training intensity makes no difference in the baseline experiment. This study reveals a (relatively) more effective component of SETA programs and casts doubts on the overall effectiveness of SETA programs in the long run.*

Keywords*—*SETA, Security Awareness, Security Education, Training, Phishing, Learning, Forgetting.

I. Introduction

A 2022 report by the Ponemon institute indicates that insider threats have increased in frequency and cost over the past two years. Moreover, 56% of incidents arose from insider negligence [1]. Cybersecurity threats may arise from inside or outside the organization. Perpetrators may be human or non-human. The motivations might be accidental or intentional. Regardless of the cybersecurity source, perpetrator, or motivations, the consequences are the same – denial of use, modification, destruction, or disclosure of information [2]. Although popular media highlights complex cybersecurity attacks involving viruses, worms, Trojans, rootkits, and distributed botnet attacks mounted by criminal gangs and sometimes foreign governments, the greatest threat is the insider threat, the trusted employee [3].

For this reason, security education, training, and awareness (SETA) programs have become more prevalent in organizations [4]. These programs intend to train employees who often lack the basic knowledge or awareness to adopt and use the correct cybersecurity measures. With companies devoting resources to training their employees about cybersecurity, it is crucial to understand how practical these training sessions are. Numerous prior studies have laid solid theoretical foundations for effective SETA programs [5]-[9], but few have examined the decrement of cybersecurity knowledge after a SETA intervention. One of these few studies found that SETA campaigns reduce vulnerability only in the short term, just two weeks [10].

To understand the effectiveness of SETA programs, we need to differentiate the different types of knowledge in a training session. IT knowledge is typically classified as 1) application-level knowledge for practical IT usage and 2) technical-level knowledge that goes beyond the simple usage of IT [11]. For cybersecurity, application-level knowledge may include standard procedures such as spotting phishing emails, whereas technical-level knowledge can include how to configure a network firewall. While SETA programs include both types of knowledge, their effectiveness in mitigating actual threats may differ. Against this backdrop, this study examines how knowledge acquired through SETA programs affects cyber risks due to human negligence.

II. Theoretical Development

A. Learning

Past studies have shown that SETA programs effectively deter intentional computer misuse [12]. Fear appeals and communications effectively ensure security policy compliance [13]. However, for unintentional human mistakes, it is possible that employees do not understand or have enough knowledge to identify a potential threat. For this reason, we examined the learning effect of SETA programs in building up employees' cybersecurity knowledge to mitigate unintentional human errors.

Training in organizational settings effectively increases trainees' knowledge level and improves organizations' productivity [11], [14]. In IT knowledge, learning and knowledge transfer are vital mechanisms for performance improvement in IT support [11]. Because cybersecurity management is a knowledge-intensive activity [15] and new threats are constantly emerging, SETA programs can potentially increase the knowledge level of employees.

A typical SETA program includes basic cybersecurity knowledge, such as how to spot phishing emails, when employees should use VPNs, and different types of computer

viruses. While these types of knowledge are rudimentary for IT personnel and security researchers, many non-IT employees are unfamiliar with cybersecurity [16]. For this reason, even a single training session can substantially increase employees' knowledge level in cybersecurity. With relatively low cybersecurity knowledge and the known effectiveness of training in corporate settings, we posit that SETA programs will increase employees' cybersecurity knowledge.

Hypothesis 1: After a SETA program, employees' cybersecurity knowledge will increase compared to the pre-training level.

Importantly, we need to understand the effectiveness of the cybersecurity knowledge acquired through SETA programs in mitigating cyber threats. Since phishing is the leading cause of data breaches and most SETA programs include segments on mitigating phishing, we focus on the effect of SETA programs in reducing successful phishing attacks. Prior literature has addressed various behavioral factors and phishing techniques that might affect the chance of employees falling for a phishing attack [17]-[19]. Since SETA programs specifically teach employees how to spot phishing emails, we contend that such knowledge acquired through those programs will decrease the susceptibility to phishing emails. For those who already know about phishing email identification, a training session may serve as a reminder to increase employees' vigilance in looking out for phishing emails.

Hypothesis 2: After a SETA program, employees' susceptibility to phishing attacks will decrease compared to the pre-training level.

B. Forgetting

While employees' cybersecurity knowledge can be boosted through SETA programs, its longevity is not guaranteed. Knowledge acquired through SETA programs may be forgotten over time. After a SETA session is completed, organizations typically consider the box is ticked and seldom look back. Without persistent organizational engagement, many non-IT professionals will quickly push cybersecurity to the back of their minds as they focus on their primary job duties. Any positive learning quickly wears off, and employees are essentially untrained after they forget about the new knowledge. Hence, decay in knowledge will likely negatively affect security policy compliance over the long run.

To model the knowledge decay, we utilize forgetting curves. The simplest form of the forgetting curve is a decreasing linear function of time, which best approximates forgetting in shorter periods. For extended periods, non-linear functions capture the de-acceleration in forgetting. Non-linear forgetting curves include the power function, hyperbola function, exponential function, logarithmic function, and combinations of the above [20]. Notably, the non-linear and convex structure suggests that the initial decline is sharper than the last decline.

The forgetting curve was first proposed by psychologist Hermann Ebbinghaus, who memorized a series of nonsense syllables and tested his memory at various periods ranging from 20 minutes to 31 days [21]. His experiment showed an exponential decay in memory; the most extended shelf-life for newly acquired knowledge is less than a month. Following Ebbinghaus's theory and empirical findings, we posit that the "shelf-life" of knowledge gained from security training sessions is up to one month.

Hypothesis 3: Knowledge acquired through a SETA program will be forgotten over a period measured in weeks.

SETA programs consist of a mixture of cybersecurity knowledge, ranging from practical tips on spot phishing emails to more technical concepts such as the classification of computer viruses. Given the wide range of knowledge, it is essential to identify potential heterogeneity in their "shelf lives" to understand how knowledge decay affects risk mitigation and devise meaningful measures to mitigate the knowledge loss over time. Ideally, such measures should aim to renew the "shelf-life" for knowledge pointed toward risk reduction.

As such, we follow [11] and classify cybersecurity knowledge into application and technical levels. Application-level knowledge is knowledge aimed at practical IT usage. Examples in the cybersecurity context include how to spot phishing emails, how to connect to a VPN, and whether passwords should be written down on a piece of paper. In contrast, technical-level knowledge goes beyond simple IT usage and includes conceptual topics such as classifications of computer viruses and hackers. As most non-IT professionals do not come from technical backgrounds, technical-level knowledge may be more difficult to retain for extended periods. On the other hand, everyday use of technology does not require a deep technical background, making application-level knowledge more retainable. Given the contrast, we posit that application-level knowledge will have a longer shelf-life than technical-level knowledge.

Hypothesis 4: Technical-level knowledge acquired through a SETA program will decrease faster than application-level knowledge.

III. METHODOLOGY

To empirically test the hypotheses, we conducted two experiments. Study 1 investigated the effectiveness of SETA programs in preventing simulated phishing attacks. The goal was to set a baseline for the effectiveness of SETA programs against phishing emails. Study 2 examined knowledge increment and decay following a SETA program. Together, the two studies addressed how knowledge accumulation and decay following a SETA program relate to mitigating phishing email attacks.

A. Study 1: Phishing following a SETA program

The objective of study 1 was to determine whether training can mitigate employee phishing attacks in the baseline experiment. The study occurred in a first-year class at a large university in the mid-western United States. College students are appropriate participants for this study because, like corporate employees, they face losses and other potential consequences if they succumb to phishing attacks. First-year college students are similar to new employees in that they are both new to their organization, and cybersecurity is not their main priority. Students tend to focus more on their coursework than cybersecurity, and employees mainly focus on their job performance. Like any other organization, universities

experience data breaches. College students, the main campus population, are frequent targets of phishing attacks [22].

The three sections of the class were naturally divided into one control and two treatment groups. Students from all three sections are comparable first-year students taking the same course. However, the three sessions occurred at different times during the day, which we acknowledge is a limitation. All three groups of participants received a pre-test on their ability to identify phishing emails. The results showed non-significant differences ($p<0.01$) statistically. After the pre-test, participants from the first treatment group ($n_1 = 239$) received a 5-minute training session once a week for the next four weeks. Since the study focuses on phishing susceptibility, the training focused on the part of the SETA program that directly addresses phishing email identification, where participants review various emails and determine whether they are phishing attacks. After the participant's determined the correct answers, brief explanations were displayed. Since theory predicts knowledge decrement following SETA programs, retraining may reinforce the learning outcome. Therefore, participants from the second treatment group ($n_2 = 203$) received more intense training - the same training twice a week during the same timeframe. In the meantime, participants from the control group ($n_0 = 147$) receive no SETA program training.

Participants received an artificial phishing email one week after the last training session (Appendix A). The email claimed an outstanding bursar account balance of $2143.56 and asked students to log in to view the statement via a non-school link that leads to a phishing site. The site used a URL that resembled the official school website, and the layout mimicked the official site. When the students "logged in" via the phishing site, it displayed a warning page showing that they have been phished and reminded them to avoid clicking on suspicious links. The system recorded their ID but not their password.

The results showed that 20% of participants in the control group succumbed to phishing attacks. The number dropped to 10% for treatment groups, suggesting the positive effect of the training. The difference is also statistically significant ($p<0.01$). However, there is no significant difference between the two treatment groups ($p>0.10$). The high susceptibility rate in both the control and the treatment groups is likely because the simulated phishing email is very similar to a regular bursar email (due to researchers' insider knowledge of the organization). Naturally, students are concerned over potential debt. A less authentic email may result in weaker overall susceptibility. Nevertheless, this baseline experiment establishes a significant outcome of SETA programs - cutting phishing susceptibility by half. This suggests a positive learning effect of SETA programs in mitigating actual threats, which confirms Hypothesis 2. The indifference to training intensity prompted us to investigate the learning and forgetting process of SETA programs more closely in the follow-up study.

B. Study 2: SETA knowledge accumulation and decay

Study 2 investigated knowledge accumulation and decay of SETA programs. Similar to study 1, the study was conducted in a first-year class (three sections) at the same mid-western university in the US. To examine the learning of different types of knowledge, participants were given a comprehensive SETA program similar to those conducted in an organizational setting. SETA quiz results measured cybersecurity knowledge levels. Each quiz had twenty questions, half evaluating technical-level knowledge and the other half measuring application-level knowledge. Appendix B presents all quiz questions.

All three groups were given a pre-test to assess the baseline knowledge level. We found no significant differences among the three groups ($p>0.10$), suggesting a similar knowledge level before the SETA program. A week after the pre-test, the course instructor conducted SETA program sessions for all three groups. Immediately after the training, participants took the first post-test. The pre-test and post-test 1 used the same quiz. We expected to observe the learning effect based on comparisons of the pre-test and post-test 1. After the training, we retested the participants' knowledge to examine the knowledge decay process. Questions in post-test 2 differed slightly from post-test 1 but were equally difficult and measured the same knowledge. Since repeated testing on the same subject would induce learning distortions, we tested participants from different groups at different points following the training. Depending on the group number, participants took the second post-test 15, 30, or 45 days after post-test 1. We chose 45 days to ensure the capture of the knowledge expiration, which is predicted to be around a month [21]. While the forgetting curve is continuous, we are constrained by the number of subgroups. Therefore, this design (Figure 1) takes three points from the forgetting curve.

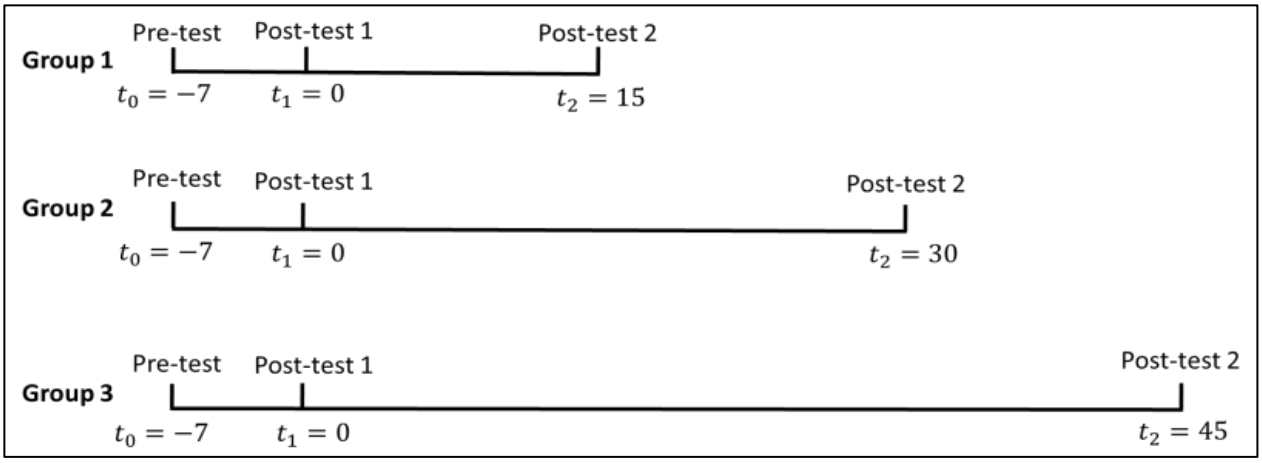

Fig. 1. Design for study 2

TABLE I. AVERAGE SCORES

	Pretest	Posttest 1	Posttest 2
Group 1	12.55	14.71	12.85
Group 2	12.50	14.11	12.78
Group 3	12.48	14.51	12.95

Participants' IDs paired the three test scores. Observations with one or more missing scores are dropped. We observed a sharp increase in scores from the pre-test to post-test 1. Across all three groups, the knowledge levels increased significantly ($p<0.01$). The average score increment is between 1.61 and 2.16 (Table 1), suggesting the magnitude of the knowledge accumulation is 12%-17%.

This result points to a significant learning effect of SETA programs, which confirms Hypothesis 1. To examine the knowledge decay, we first compared the scores from post-tests 1 and 2. The average score decrement ranges from 1.33 to 1.86. The decreases across all three groups are statistically significant ($p<0.01$). This confirms the knowledge decay following SETA programs. The knowledge increment and decay in all three groups are plotted in Figures 2, 3 & 4.

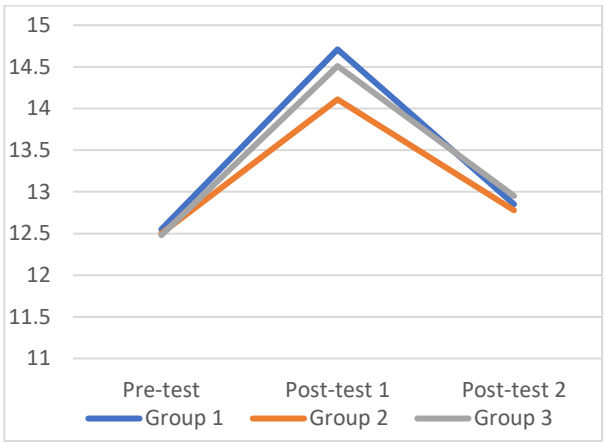

Fig. 2. Overall knowledge change

Fig. 3. Technical-level knowledge change

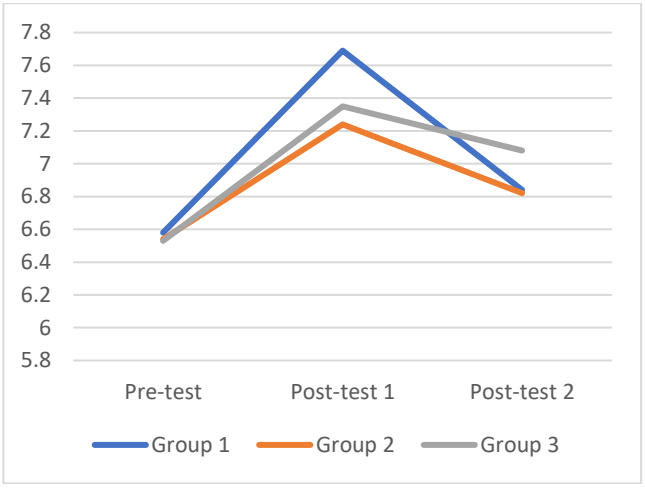

Fig. 4. Application-level knowledge change

A similar pattern of initial increase and eventual decrease can be observed for participants scoring 80% or higher right after the training (post-test 1), which means any positive learning effect soon wears off. While government regulations such as HIPAA and FISMA require employees in specific industries to be trained and reach a certain threshold, the knowledge decay pattern shown here suggests that such seemingly demanding regulations may eventually lose effect.

We compared the pre-test and post-test two scores to quantify the "shelf-life" of knowledge acquired through SETA programs (Table 2). Intuitively, the "expiration date" for a training program is when the post-test two scores are equal to the pre-test scores. If scores in post-test 2 are still higher than the pre-test scores, then the knowledge has not fully "expired." For the "shelf-life" of the overall knowledge, we observe that for group 1 (15-day), the post-test 2 score is still significantly higher than the pre-test score ($p<0.10$), suggesting that the knowledge level may further decline. For a longer interval (30-day), the post-test 2 scores for group 2 is not significantly different from the pre-test score, which means that the overall knowledge level has returned to the pre-training level within a month. Combining the results on groups 1 and 2, we can infer that the "shelf-life" of knowledge acquired through SETA programs is between 15 and 30 days, which supports hypothesis 3.

We included both types of knowledge for the training session to examine the decay of technical- and application-level knowledge. For the knowledge measurement, half of the quiz questions were designed to measure technical-level knowledge and the other half for application-level knowledge. The classification follows definitions from [11]. For technical-level knowledge, the post-test 2 score is statistically the same as the pre-test score for group 1 (similarly for groups 2&3, see Table II). This means the "shelf-life" of technical-level knowledge is within 15 days. For application-level

knowledge, the result for group 1 (15-day) shows that the post-test 2 score is still significantly higher than the pre-test score at 0.05 level (Table II). For group 2, the post-test 2 score is statistically the same as the pre-test score. Therefore, the "shelf life" for application-level knowledge is between 15 and 30 days. Since application-level knowledge has a longer "shelf-life" than technical-level knowledge, the latter has a faster decay rate, which supports hypothesis 4.

In Study 1, the training intensity did not affect phishing susceptibility (in a month). This somewhat puzzling finding can be explained by the "shelf-life" of application-level knowledge. Since identifying phishing emails relies on application-level knowledge, its longer "shelf-life" (15-30 days) suggests that the knowledge likely did not deteriorate to the point where retraining was necessary. As application-level knowledge has not yet worn off, retraining in Study 1 does not provide significant additional value in returning the knowledge to the desired level. Therefore, more intense training before the application-level knowledge significantly wears off does not further reduce susceptibility to phishing emails.

Overall, the two studies document the short-term effectiveness of SETA programs such as those required by some compliance laws, and cast doubts on their longer-term effectiveness and heterogeneity among different types of knowledge.

TABLE II. PAIRED T-TESTS FOR PRETEST AND POSTTEST 2

$H_0: y_0 = y_2$ $H_a: y_0 < y_2$	n	(Overall) Score Difference	p-value		
			Overall	Technical-level	Application-level
Group 1 (15-day)	122	0.30	0.0849	0.3881	0.0383
Group 2 (30-day)	112	0.28	0.1579	0.4805	0.1101
Group 3 (45-day)	74	0.47	0.0026	0.4044	0.0001

[a.] y_i $(i = 0,\ 2)$ stands for the test score at the pre-test or post-test 2.

IV. DISCUSSION

This research finds that SETA programs can reduce phishing susceptibility by 50% while increasing employees' knowledge level by 12% to 17%. However, the knowledge increment wears off within weeks, and technical-level knowledge decays faster than application-level knowledge. The findings suggest that SETA programs are practical tools to mitigate benign human errors in cybersecurity in the short run, but the longer-term effectiveness is not assured. Since some compliance laws require employees to be trained annually, this may not be an effective control.

Before discussing the literature contributions, we acknowledge this study's limitations. In testing the longer-term effectiveness of SETA programs, we only measured knowledge decay but did not examine phishing susceptibility longitudinally. This is mainly due to constraints at the experiment site. The phishing email in Study 1 generated significant pushback from the university's IT department, and we were subsequently banned from carrying out additional phishing experiments. Therefore, the planned simulated phishing attack after post-test 2 in Study 2 was dropped from the experiment. In addition to the phishing constraints, we are also constrained by the number of class sections. Fewer groups mean we can only take a few points from the continuous (and concave) forgetting curve. More groups of participants would depict a fuller picture of the knowledge decay process. Finally, while the use of student samples is not uncommon [19], [23], characteristics specific to students, such as better IT literacy, may limit the generalizability of our findings.

Despite the limitations, this paper makes several contributions to the literature. The behavioral information security literature has established rich theories on why SETA programs can facilitate security policy compliance and reduce IT misuse [5], [6]. This paper adds to this stream of literature by providing field evidence and documents the magnitude of SETA programs' effectiveness. The 50% reduction in phishing susceptibility suggests that SETA programs are indeed practical tools to mitigate human errors, just as theories in prior studies predicted. Significantly, the study adds to the behavioral information security literature by using theories on the forgetting curve and suggests that the longer-term effectiveness of SETA programs is in question. By differentiating application-level and technical-level knowledge, we establish that retraining aiming to mitigate knowledge decay should consider the knowledge type and heterogeneities in the "shelf-life" of different types of knowledge. Finally, the paper contributes to the literature on phishing attack mitigation. While prior literature has documented the relationship among email characteristics, psychological traits, and phishing email susceptibility [17], [24], this study suggests that SETA programs are valuable tools to help reduce phishing susceptibility for an average employee.

For practitioners, our findings suggest that training employees on cybersecurity knowledge is a worthy investment that can reduce human errors with respect to organizations' information security programs. With tangible financial costs associated with data breaches and ubiquitous human errors in information security, SETA programs can potentially spare companies from the financial damages due to severe data breaches caused by benign insiders. However, managers should be wary of the longer-term ineffectiveness of SETA programs. Since employees tend to forget what they learned rather quickly, it is essential to remind them of various potential attacks (e.g., remind employees of active phishing attacks), and possibly provide more training at shorter intervals. Furthermore, in reminding employees or conducting retraining, organizations can leverage the heterogeneity of different knowledge types to prolong the effectiveness of SETA programs.

REFERENCES

[1] Ponemon Institute, "2022 Ponemon Institute cost of insider threats: Global report," Ponemon Institute LLC, 2022.

[2] K. Loch, H. Carr and M. Warkentin, "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly, vol. 16, (2), pp. 173-186, 1992. . DOI: 10.2307/249574.

[3] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," Information & Management, vol. 51, (1), pp. 69-79,

2014. Available: https://dx.doi.org/10.1016/j.im.2013.10.001. DOI: 10.1016/j.im.2013.10.001.

[4] R. K. Nilsen et al, "A Developmental Study on Assessing the Cybersecurity Competency of Organizational Information System Users," Journal of Cybersecurity Education, Research and Practice, vol. 2, (2), 2017.

[5] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, vol. 20, (1), pp. 79-98, 2009. . DOI: 10.1287/isre.1070.0160.

[6] P. Puhakainen and M. Siponen, "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," MIS Quarterly, vol. 34, (4), pp. 757-778, 2010. . DOI: 10.2307/25750704.

[7] P. Menard, G. J. Bott and R. E. Crossler, "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," Journal of Management Information Systems, vol. 34, (4), pp. 1203-1230, 2017. . DOI: 10.1080/07421222.2017.1394083.

[8] G. D. Moody et al, "Toward a Unified Model of Information Security Policy Compliance," MIS Quarterly, vol. 42, (1), pp. 285-311, 2018. . DOI: 10.25300/MISQ/2018/13853.

[9] Y. Chen et al, "Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model," Information Systems Research, vol. 32, (3), pp. 1043-1065, 2021. . DOI: 10.1287/isre.2021.1014.

[10] J. H. Bullée et al, "Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention," -01, 2016.

[11] Y. Kim, R. Krishnan and L. Argote, "The Learning Curve of IT Knowledge Workers in a Computing Call Center," Information Systems Research, vol. 23, (3-part-2), pp. 887-902, 2012. . DOI: 10.1287/isre.1110.0401.

[12] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, vol. 20, (1), pp. 79-98, 2009. . DOI: 10.1287/isre.1070.0160.

[13] A. C. Johnston, M. Warkentin and M. Siponen, "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," MIS Quarterly, vol. 39, (1), pp. 113-134, 2015. . DOI: 10.25300/MISQ/2015/39.1.06.

[14] W. I. Zangwill and P. B. Kantor, "Toward a Theory of Continuous Improvement and the Learning Curve," Management Science, vol. 44, (7), pp. 910, 1998. . DOI: 10.1287/mnsc.44.7.910.

[15] P. Belsis, S. Kokolakis and E. Kiountouzis, "Information systems security from a knowledge management perspective," Information Management & Computer Security, vol. 13, (3), pp. 189-202, 2005. . DOI: 10.1108/09685220510602013.

[16] M. Evans et al, "Human behaviour as an aspect of cybersecurity assurance Human behaviour as an aspect of cybersecurity assurance"," Security and Communication Networks, vol. 9, (17), pp. 4667-4689, 2016. . DOI: 10.1002/sec.1657.

[17] A. Abbasi et al, "The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites," Information Systems Research, vol. 32, (2), pp. 410-436, 2021. . DOI: 10.1287/isre.2020.0973.

[18] J. Wang, Y. Li and H. R. Rao, "Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences," Information Systems Research, vol. 28, (2), pp. 378-396, 2017. . DOI: 10.1287/isre.2016.0680.

[19] R. T. Wright et al, "Research Note-Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," Information Systems Research, vol. 25, (2), pp. 385-400, 2014. . DOI: 10.1287/isre.2014.0522.

[20] D. C. Rubin and A. E. Wenzel, "One Hundred Years of Forgetting: A Quantitative Description of Retention," Psychological Review, vol. 103, (4), pp. 734-760, 1996. . DOI: 10.1037/0033-295X.103.4.734.

[21] H. Ebbinghaus, "Memory: a contribution to experimental psychology," Annals of Neurosciences, vol. 20, (4), pp. 155-156, 2013. . DOI: 10.5214/ans.0972.7531.200408.

[22] Barracuda Networks, "Spear phishing: Top threats and trends," Barracuda Networks .

[23] R. Chen, J. Gaia and H. R. Rao, "An examination of the effect of recent phishing encounters on phishing susceptibility," Decision Support Systems, vol. 133, pp. 113287, 2020. Available: . DOI: 10.1016/j.dss.2020.113287.

[24] A. Abbasi et al, "The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites," Information Systems Research, vol. 32, (2), pp. 410-436, 2021. Available: https://search.proquest.com/docview/2546647342. DOI: 10.1287/isre.2020.0973.

Appendix A. Simulated Phishing Email

From: [redacted] Bursar <bursar.[redacted]@gmail.com>
Date: Mon, May 8, 2017 at 11:49 PM
Subject: New billing statement issued
To: bursar[redacted]@gmail.com

A new [redacted] University monthly bursar statement has been issued. Payment Plan participants are sent installment payment due notifications in separate emails and this email is to inform you of the total monthly billing statement amount for information purposes only.

View the statement by logging at [redacted] and clicking on [redacted] Bursar Account under the Quick Links. Once logged in, you can view your account information, pay your bill, and set up an authorized user.

Payment in full is due no later than the 15th of the month unless you are enrolled in the payment plan. Past due accounts accrue a penalty at the rate of 1.5% monthly (19.56 APR) and incur enrollment and academic record holds.

A 2.75% convenience fee will be added to all credit card bursar account payments. Credit card payments may only be made online and can no longer be made at the Bursar Office. To avoid the convenience fee, you may consider several other options such as:

* Online by Web Check/ACH

* Mailing checks, cashier checks or money orders to:
[redacted]

* In person by check, money order, or cash at the Office of the Bursar, [redacted] Student Union. Hours 8 a.m.-5 p.m. Monday-Friday. After-hour payments can be placed in the secure depository slot adjacent to the Bursar Office Windows.

Paying with a Check: You authorize the University to clear your check electronically. Your checking account may be debited the next day your payment is received. Although it appears on your bank statement, your check will not be presented to your financial institution or returned to you. Please be aware payment by check constitutes acceptance of these terms unless noted on the check.

======== STATEMENT DETAILS ==========
Amount Due --- [$2143.65]
Due Date --- [5/15/17]
==========

Refund Information: It is the policy of the University to refund any credit on the account. To accept the federal Title IV authorization for financial aid disbursements to pay all current semester educational expenses and up to $200 prior year charges, you must do so prior to disbursement or complete the TIV Form available on our website.

The Electronic Direct Deposit Refund Program was developed to provide quicker access to refunds when bursar accounts have credit balances. If you have not done so already, complete the Direct Deposit Sign-Up electronically.

Appendix B.

Cybersecurity Quiz

1. Which of the choices below defines information security?
   A. A broad term encompassing the protection of information
   B. Protects information from accidental misuse
   C. Protects information from intentional misuse
   D. All of these are correct.

2. Which of the following types of viruses spread themselves, not just from file to file, but also from computer to computer?
   A. Polymorphic virus
   B. Worm
   C. Trojan-horse virus
   D. Backdoor programs

3. Which of the following is a cost of downtime in addition to lost revenue?
   A. Legal expenses
   B. Loss in financial performance
   C. Damage to reputation
   D. All of these are correct

4. Which of the choices below is a common Internet monitoring technology?
   A. Key logger
   B. Hardware key logger
   C. Cookie
   D. All of these are correct

5. It is acceptable to share your password with which of the following:
   A. Your immediate supervisor
   B. Your significant other
   C. Your coworkers
   D. No one

6. Access to a company intranet from off-site is accomplished by
   A. Going to the company site using a browser
   B. Using a VPN
   C. Logging in
   D. The company intranet cannot be accessed from off-site

7. If you have to have a password, id, and token/smart card to log onto the company site, what type of authentication is the company using?
   A. Single-factor authentication
   B. Two-factortor authentication
   C. Multi-factor authentication
   D. Encryption

8. You receive an email from the president of the company. It asks you to click on a link and log on. It might be an attempt at what type of identity theft?
   A. Phishing
   B. Pharming
   C. Pretexting
   D. Spoofing

9. You receive an email attachment from a customer that you were not expecting. Which of the following is the best way to handle it?
   A. Call the sender to verify they sent it
   B. Contact IT
   C. Just open it
   D. Mouse over the attachment to see what it is

10. You should expect that the company you work for will honor your privacy and not monitor your Internet use.
    A. True
    B. False

11. You work in an open office plan. You are logged into your computer. You have to go to another floor in the building to get a file. You can leave your computer logged in because everyone in the area is a co-worker.

A. True
B. False

12. Which of the following is *not* included as a common stipulation an organization would follow when creating an employee monitoring policy?
    A. Be as specific as possible stating when and what will be monitored
    B. Do not state the consequences of violating the policy
    C. Always enforce the policy the same for everyone
    D. Expressly communicate that the company reserves the right to monitor all employees

13. Which of the following definitions represents physical security?
    A. A problem that occurs when someone registers purposely misspelled variations of well-known domain names
    B. Tangible protection such as alarms, guards, fireproof doors, fences, and vaults
    C. Government attempts to control Internet traffic, thus preventing some material from being viewed by a country's citizens
    D. Choosing to deny permission to incoming emails

14. What outlines the corporate guidelines or principles governing employee online communications?
    A. Social media monitoring
    B. Social media manager
    C. Social media policy
    D. Information privacy manager
15. What is the process of monitoring and responding to what is being said about a company, individual, product, or brand?
    A. Social media monitoring
    B. Social media manager
    C. Social media policy
    D. Anti-spam policy

16. The first line of defense to protect the company's intellectual property is authentication and authorization.
    A. True
    B. False

17. Jensen is a senior developer for HackersRUs, a company that helps secure management information systems. Jensen's new task is to break into the computer system of one of HackersRUs's top clients to identify system vulnerabilities and plug the holes. What type of hacker is Jensen?
    A. Cracker
    B. White-hat hacker
    C. Script bunny
    D. Black-hat hacker

18. Angela works for an identity protection company that maintains large amounts of sensitive customer information such as usernames, passwords, personal information, and social security numbers. Angela and a coworker decide to use the sensitive information to open credit cards in a few of her customers' names. This is a classic example of which of the following security breaches?
    A. A social engineer
    B. An insider
    C. A spammer
    D. A dumpster diver

19. A typical acceptable use policy includes which of the following:
    A. Not using the service as part of violating any law
    B. Not attempting to break the security of any company network or user
    C. Not posting commercial messages to groups without prior permission
    D. All of the above are part of a typical policy

20. Who is responsible for the security of the company's information?
    A. IT
    B. Database management
    C. All employees
    D. The CIO