GAMIFICATION OF SECURITY AWARENESS TRAINING PROGRAMS: A LITERATURE REVIEW

by

Dawn C. Tatum

B.S., University of Central Florida, 1986
M.S., Southern Polytechnic State University, 2012

A Research Paper Submitted to the School of Computing Faculty of
Middle Georgia State University in
Partial Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2023

Gamification of security awareness training programs: a literature review

Dawn Tatum, *Middle Georgia State University, dawn.tatum1@mga.edu*

Abstract

Gamification is a term used to describe the art of taking a process or a task and making it into a game. Using games as a way to make mundane tasks or necessary lessons more fun is used in many aspects of life. Parents often use games to teach children tasks, and teachers use games to enforce learning, and much more. The gamification of Security Awareness Training Programs has been researched recently due to the rise of security breaches worldwide. Unfortunately, there have been very low participation rates in the methods tried over the years. This paper will highlight the different aspects of research that have been conducted in the areas of security awareness training, psychology for changing human behavior, and studies that have attempted to combine the two. The purpose of this literature review is to determine possible areas where more research should be pursued to gain increased security awareness and enhanced programs that may have a positive effect on security awareness behaviors and the persistence of those behaviors.

Keywords: security awareness training, gamification, human behavior modification, cybersecurity

Introduction

This research seeks to gauge further the interest in research on the topic of gamification, specifically for security education training and awareness (SETA) programs. The National Institute of Standards and Technology (NIST) defines awareness as “a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure” (CSRC Content Editor, 2023). It follows that security education and training awareness is focused on programs that target education for security and awareness for organizations. Gamification is defined by Gartner as “the use of game mechanics and experience design to digitally engage and motivate people to achieve their goals.” (*Definition of Gamification - Gartner Marketing Glossary*, 2019). Gartner also states there is a difference between gamification and video games. Gamification uses techniques to influence a person to achieve their goals. A review of a case study is conducted to introduce previous research in this field. Information is gathered from information security research regarding the delivery of these programs and the results they have produced regarding user participation and the efficacy of current programs. Based on the analysis research of gamification for security awareness training, an approach will be determined for the next research stage for measuring the gamification impacts on user participation.

With the increase of cybersecurity threats on the rise, user training in cybersecurity is even more critical (Cisco, 2021). Currently, the security awareness training is often a short video with a few questions at the end to “check the box” that training is complete.

Most information security professionals and educators recognize that the human element is the “weakest link” in our security chain. Individuals most often complete security awareness training because of obligation and not because of interest in increasing their knowledge or ability to reduce security threats. Malware and ransomware attacks are on the rise worldwide, with the majority of the forensic data pointing to the point of origin with a human error that could have been prevented (Cisco, 2021). With smartphones, augmented reality, streaming, and games becoming part of everyday life, we have become a more impatient society. We want things quickly, and our attention spans demand that information is presented quickly.

The purpose of this study is to examine previous research to determine whether there are gaps that merit further study in attempting to gamify security awareness training. Consistent with the study's purpose, this research will answer the following question.

RQ1: What unique gaps are identified in the previous research on the gamification of SETA programs that can be used to construct a new study on the gamification of SETA programs that may improve employee participation rates and lower an organization's security risk?

The findings of this study will reveal the gaps in the previous research regarding the gamification of security awareness training that may reveal a new study that can be developed that will improve the outcomes for SETA program participation and lead to lowering an organization's security risk.

This research is organized as follows. A review of the literature is presented, followed by a methodology that includes a description of the procedure and data analysis.

Literature review

Security awareness is necessary for all people throughout the world, as security incidents have risen exponentially over recent years. As we as a population continue to increase the amount of technology we encounter in our daily lives, we also increase our security risk. Companies such as Check Point and HP Labs state that the security strategies of corporate industries will never go back to pre-pandemic states (Scroxton, 2020). Companies realize that the pandemic stretched the risk exposure from the corporate data center to the employee home infrastructure; creating even more risk beyond the work laptop they are using to conduct remote work also including the added exposure of home networks that include IoT devices at their homes. The strategy for security awareness training has previously been focused on the infrastructure of the organization's environment, and now that has become quite muddled. While there has been a lot of research completed in the area of security awareness training and the gamification of security awareness training, the timing may be good to motivate individuals to participate in security awareness training and change their behavior due to heightened personal security risk they are faced with in this remote workplace environment (Loishyn, 2021). Loishyn's research shows statistical data that there has been an increase of 600% in cyberattacks since the pandemic began in 2020. With this type of rise in attacks, organizations are taking a different look at their cybersecurity strategies and mitigating risk in this new era.

Cybersecurity compliance focuses on mitigating or avoiding security risks by educating employees, putting physical and logical countermeasures in place to thwart attacks, and creating a sense of responsibility for employees to behave proactively in a responsible way to reduce security risk (Silic, 2020). Silic indicated in their 2020 research that Security Awareness Training and Education (SETA) programs are often the main line of defense in preparing employees to behave responsibly to mitigate risk. While SETA programs are evolving, they still need to evolve to a point where employee participation is higher, and the impact on employee behavior is greater. Employees often do not participate in training, even when mandatory, and the programs have a long history of failure as shown in Silic's 2020 research. An experiment by Ferguson (Ferguson, A.J., 2005) also shows that employees participating in SETA programs failed to be able to transfer the knowledge from the training program to effectively recognize a phishing attack sent in email.

Developing a strategy to get employees to pay heed to SETA programs by creating a security culture within the workplace is a key strategy. Most often, cyber attackers target an attack on an individual who is part of an organization (Fearn, 2021). To create a security culture within a company, Fearn suggested developing a program that is dynamic to existing employees, that is a part of the onboarding process for new employees and allocates time for employees to continually engage in the training as well as reward good behavior.

Research has also been conducted to test the learning outcomes of applying gamification to employee training. In one study, the results showed that employees who were "gamers" outside of work gained more knowledge through the game experience than "non-gamers" (those who did not play games outside of the workplace) did but were less satisfied with the experience (Baxter, 2016). Larson's research indicated that many corporations have adopted gamification to develop new training methods for their employees in many different topic areas. The research shows that many corporations have an obstacle to overcome with changing a legacy system and the fears that accompany adapting to a new methodology. With large companies adapting to using gamification strategies within their corporations and showing successful outcomes, more companies are likely to begin to develop their strategies.

Research for motivation on behavior change in the security field has been evolving but still not conclusive on what motivates users to change their behavior as it relates to security risk and those events that increase risk. Many researchers have explored using fear to encourage behavior change (Schuetz, 2020). There is the idea of abstract vs. concrete fear appeals, which can be used to affect the users' behavior. Abstract appeals are more subtle (e.g., "victims of spear-phishing attacks will get hacked") as opposed to concrete appeals being more direct (e.g., "victims of spear-phishing attacks will get hacked, lose their identity, their monetary valuables and may never recover"). While both appeals refer to the fear involved, there is also a difference in the efficacy if the appeal is directed at a user and their security and a user and their organizational security. Schuetz's research found that the earlier research claims that fear appeals were not effective were pre-mature. The concreteness of the messaging greatly increased the efficacy of the user behavior.

While investigating the research available on SETA programs and the gamification research available as well, there are many facets to the research that needs to be explored. The research examined explored not only specific research in SETA programs, gamification of training and marketing, the psychology of changing behaviors, and the gamification of SETA programs. There is support to show that the training efficacy rates do go up for traditional SETA programs when repeated with the audience in regular intervals (Gundu, T. et al., 2019). There is also research that indicates that gamification does not have a major impact on learning (Baxter, R., et al., 2016). The summary of results presented in 2019 by Gundu, T. et al. showed that in typical SETA programs, there is an annual training focused primarily on security awareness without a connection or study of related attitudes and behaviors. When the Gundu study was intentionally performed to study increasing the repetition of the SETA training programs and the connection they have with changing employees' attitudes and behaviors, there is a positive increase in the efficacy rates from 51% to 90%. There has been promising research completed on immersive VR training used for SETA programs, especially in the areas of social engineering and where ethics concerns come into play. The VR experience also gives the ability to engage multiple players in a real-world scenario without the real consequences of an actual breach. The idea of allowing the entire story to unfold for a user so that they can understand the ramifications of a simple wrong click-through in a phishing email or answering a probing question by a third party. These types of stories make a lasting impact and keep the user engaged. One particular research study introduced this idea using spatial, temporal, Spatio-temporal, and emotional, temporal dimensions to study the users as characters in the VR environment and how they became absorbed in the stories (Ulsamer, 2021). This is the most promising research I have found in the field that begins to create an immersive experience that the user is likely to want to engage in and also will have a lasting impact on their behavior.

In reviewing the literature and research from these types of studies, some gaps are still left to explore in many areas. The immersive storytelling feature of VR to impart the seriousness of the training is effective (Ulsamer, 2021). The VR experience itself needs to be researched further to explore ways of allowing for interactive characters with the users to test knowledge during the training, test if behavior changes through the game, and have a way to keep a game persistent to measure changes over time.

There is also the need for research regarding the idea of gamification, whether in digital or analog form. Much of the research found in gamification for SETA programs revolved around phishing email campaigns, small games that were one-time games that fell into the same trap of the "check the box" for employee training (. There is much research on gamification for other markets and the psychology of changing human behaviors, (Fogg, B. J. & Euchner, J., 2019), which may help to create the appropriate storylines that would allow for a multi-player persistent game that would allow users to complete different components of the game and be incentivized to complete different levels. Once developed, it would also be interesting to see if the security awareness personnel could be engaged as potential attackers in the game to make the training more of a dialogue and identify gaps not only in the common users but also those trained and employed as security professionals.

Methodology

The past research and literature will be examined in an integrative way to produce a metatheory for future research. Integrative literature reviews have contributed to the common body of knowledge in various domains in a positive way, especially in areas of new research (Torraco, R. J., 2016).

Torraco's research is highly respected in qualitative research literature reviews. Many such literature reviews have produced frameworks in areas of research for human resources and the social sciences. While literature reviews have often been discounted as substantial research in the past, the views of researchers have been changing in recent years due to the vast amount of research available. It is extremely helpful to researchers conducting case studies to incorporate literature reviews into their background research before embarking on a new study. Researchers can fine-tune the basis of their research and identify new areas that need to be covered in their research by examining the gaps identified by literature reviews.

The methodology used in this research will examine literature in various areas of cybersecurity research, gamification research, and the psychology of human behavior, specifically what can change human behavior.

Publications from books, journals, professional magazines, and scholarly articles were searched based on the words "gamification of security awareness programs", "gamification of security awareness and behavior modification,", and "gamification and behavior modification."

Literary reviews were excluded from the coding analysis and were used primarily as a basis for background information on the body of research available.

The research literature is examined in the following categories:

Results of studies of gamification and learning
Results of studies of attempts to gamify SETA programs
Results of studies of behavioral change research
Results of studies combining gamification of SETA and behavioral change goals research
Articles related to the need for better SETA programs

Articles are codified in an excel spreadsheet based on the category they belong to and analyzed according to several topics. Overlaps were examined, and gaps were identified by reviewing the results, limitations, and future research indicated by each article. The spreadsheet represents an organized table that builds an overall view of how gamification, security awareness training programs, and changes to human behavior have been studied separately and in combination. This research does not claim to examine all literature available. However, the intent is to examine research in the various categories listed previously to create a foundation for possible research in the future that encompasses gamification as it relates to security awareness training programs and the necessary conditions to promote the modification of behavior.

Results

To answer the research question posited**, "**What unique gaps are identified in the previous research on the gamification of SETA programs that can be used to construct a new study on the gamification of SETA programs that may improve employee participation rates and lower an organization's security risk?" a review of several categories of research are examined.

The research literature is examined in the following five categories:

Category I: Analysis of research articles related to gamification and learning

Reference	**Sample**	**Results**
Baxter, R. J. et al., (2016)	(n=856), 1 training	856 employees completed a survey; employees with gaming experience enjoyed gamified training more than those with no gaming experience. Unable to determine what factors led to positive reactions to training because of possible bias prior to training and survey results
Fatima, R. et al., (2019)	(n=63), 1 training	63 Participants were divided into groups to discuss and design a phishing attack. The game is analogue, thus not requiring previous digital gaming skills. The analogue approach also provided socialization. The team approach and interaction were presumed to create a better learning outcome and retention of knowledge gained through the training. Observations were made that the participants were engaged when understanding all the factors that makeup designing a phishing email attack.
Ferguson, A. J. (2005)	(n=512), 1 test email	Development of a suspicious email regarding an incorrect grade report was sent to 512 cadets (all had received a minimum of 4 hours of SETA training) with an embedded link to fix the incorrect grade report. The email was signed by an Army Colonel. Over 400 cadets (80%) clicked on the link even though they thought it was suspicious.

Category II. Analysis of research articles regarding gamification of SETA programs

Reference	Sample	Results
Scholl, M. (2018)	-	Development of analogue training scenarios to be completed by teams of employees. The psychology behind the learning exercises is that the team learning approach and tactical learning approach engage the learner to an extent that is more likely to increase retention and change behavior. In Addition to analogue training, digital training is also created as a supplement for individuals to increase retention beyond the team exercise.
Canham, M. et al., (2022)	1 (n=101), one month	Development of a phishing email campaign to select individuals interested in participating in a competitive-style gamified SETA program. Six different types of phishing emails were sent to the individuals participating in the study
Yerby, J. et al., (2014)	-	Development of digital game for teaching forensics investigations
Ulsamer, P. et al., (2021)	1(n=50), 2 weeks	Observation of using immersive VR storytelling to improve learning and retention of participants in contrast to traditional e-Learning. The test was conducted with 2 sets of participants, one with traditional e-learning and one with VR immersive storytelling. A test was given to explore the knowledge gained after participating in the learning exercise immediately after the test. The VR immersive learning group of participants scored higher. A week later the test was given again and the e-Learning participants scored lower than their first score on the test and the VR immersive learning group scored even higher on the second test, suggesting that not only did the VR immersive learning group retain the information but also expanded their knowledge on the subject.
Francia, I. G. et al., (2014)	-	Gartner predicted that 50% of corporate innovation would be "gamified" by 2015. In areas of healthcare well-being, customer loyalty and rewards, employee loyalty and rewards, and training would be gamified and part of day-to-day business activities. Scenarios were created and deployed for one fall semester term. The scenarios addressed: Password Protection, Phishing Scams, Spyware, ID Theft, Wireless Vulnerabilities, Anti-Virus Protections, Digital Forensics, and Critical Infrastructure Protection

Category III. Analysis of research articles related to behavioral change

Reference	Sample	Results
Fogg, B. J., & Euchner, J. (2019)	-	Fogg is a pioneer in persuasive technology and what he calls "captology" or Computers as Persuasive Technology. He discusses the fact that we as humans relate to computers as social actors as if they are alive in some way. He developed the framework called the Fogg Behavior Model: B=MAP. Behavior happens when three things come together at the same moment: Motivation (M), Ability (A), and a Prompt (P). He uses this framework to create the Behavior Grid, which maps out 15 ways behaviors can change. This leads to the Fogg Maxims. Fogg Maxim #1 is, Help people do what they already want to do. That is the pattern of every successful consumer elective product or service: it helps people do what they want to do. Instagram is an example. The founders realized that people wanted to share photos, so they made a really easy service that helps people share photos. If you have a product that already exists and you need to convince users to do something they don't already want to do, it can be difficult. So you have to align the behavior with an aspiration they already have. Fogg Maxim #2 is, to help people feel successful. These four words will get people to continue to use a product or service, sustain a habit, or get engaged. It is not to be successful but to feel successful. Behavior Design is all about figuring out the user side of the equation. If autistic people need to be persuaded to show up to work every day -- understand why they are not showing up to work every day and then understand what will motivate them to reach the goal. Gamifying everything is not always the answer. Look at the prompts, and if the prompts are there, then they are not effective. Either the task needs to be easier or the person needs to be more motivated. Make sure to understand what is making something easy or difficult, effective or ineffective. What is the cause of why it is not working the way it is now? Fogg developed a model called the Ability Chain which lets you look at what's making something hard to do and how to make it easier. If that doesn't work, look at motivation.
Rapp, A. (2019)	1 (n=48), each course, 24 participants for 40 hours over 8 weeks	Human-Centered Interaction (HCI) methodologies for designing courses to build prototypes for behavior change. Some used positive reinforcement and some used negative reinforcement, both of which required users to accept the module's prompts to continue. Others allowed users to engage casually to reach a point of self-awareness and voluntary behavior change.

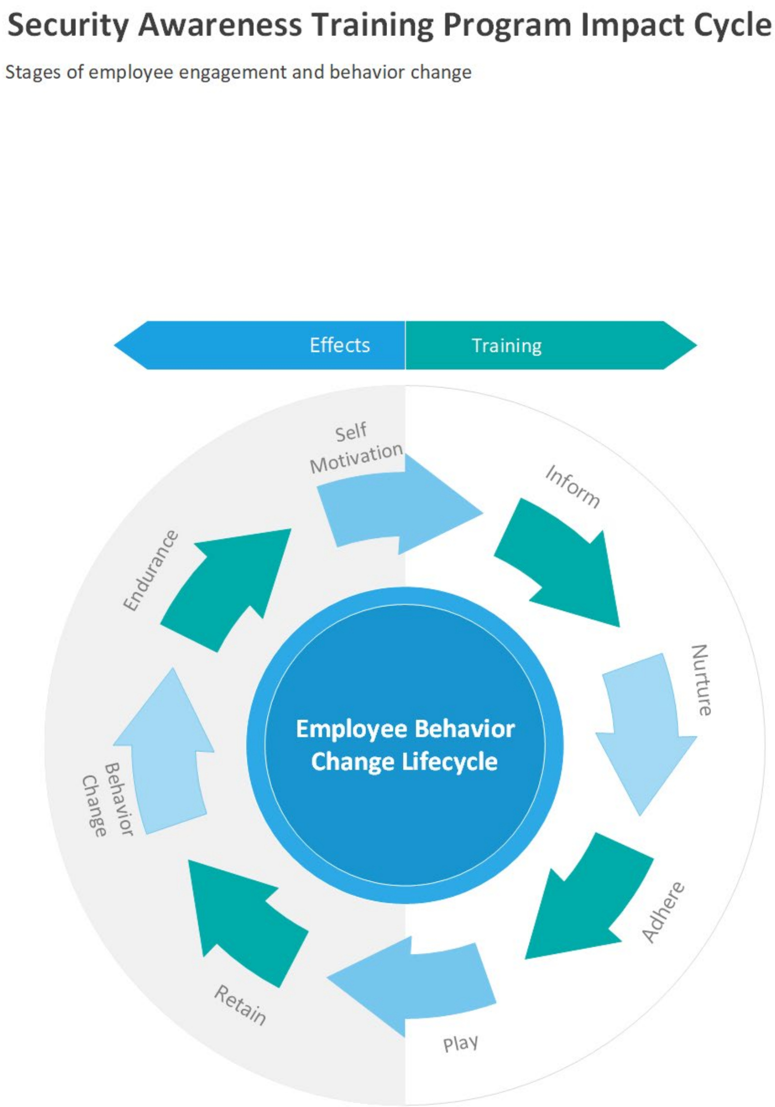
Category IV: Analysis of research articles related to the gamification of SETA and behavioral change goals

Reference	Sample	Results
DeCarlo, S. M. (2021)	1 (n=218), 5 months (2 months of pre-training security incidents, 1 month of training, 2 months of post-training security incidents)	The study was conducted to show evidence of using gamification training to improve the education and training of healthcare professionals in the use of sensitive data. The controlled experiment resulted in showing that gamification had a positive effect on the training of healthcare professionals and should be considered a viable option in the design of security awareness training programs for the healthcare industry
Meyer, C. (2017)	-	The article examines the five key elements in gamifying security awareness training to make it effective for employees. Providing these elements: 1) Autonomy: giving people choices 2) Mastery: giving people the opportunity to improve 3) Feedback: Let people know how they are doing, compared to their team, the organization, or as a whole to other organizations 4) Purpose: Let people know why this matters. In security, deconstruct a past attack - demonstrate the importance and the risks 5) Social: Things matter more to people when they do them together. Publishing a leadership or assigning points to a group or team, individual thank you notes posted on internal social media boards.

Category V. Analysis of research articles related to the need for better SETA programs

Reference	Sample	Results
Fearn, N. (2021)	-	Research on senior corporate executives and their perspectives on security awareness training programs. The article highlights that many executives are aware that most risk can be mitigated by educating their employees and changing risky behaviors. The majority of executives believe that positive reinforcement methods work best to change behavior.
Lugnet, J., & Ericson, Å. (2022)	-	Research on a different pedagogical approach to security awareness training using scenarios with non-binary approaches to solving the problems presented.

Through the analysis of this research, the following cycle of events (Figure 1) has revealed itself that naturally happens through a training program that can change human behavior:


Security Awareness Training Program Impact Cycle

Stages of employee engagement and behavior change

Figure 1. Security Awareness Training Impact Cycle

In the area of the studies of gamification and learning, there exist some gaps left to explore in many areas. The immersive storytelling feature of VR to impart the seriousness of the training is effective (Ulsamer, 2021), but the VR experience itself needs to be researched further to explore ways of allowing for interactive characters with the users to test knowledge during the training, test if behavior changes through the game and have a way to keep a game persistent to measure changes over time. Much of the research found in gamification for SETA programs revolved around phishing email campaigns, small games that were one-time games that fell into the same trap of the "check the box" for employee training. There is research on gamification for other markets (Rapp, A., 2019, Fogg, B. J., & Euchner, J., 2019) and the psychology of changing human behaviors, which may help to create the appropriate storylines that would allow for a multi-player persistent game that would allow users to complete different components of the game and be incentivized to complete different levels. Once developed, it would also be interesting to see if the security awareness personnel could be engaged as potential attackers in the game to make the training more of a dialogue and identify gaps not only in the common users but also those trained and employed as security professionals. West Point conducted a test as early as 2005 to see if gamifying security awareness for cadets would affect learning (Ferguson, A.J., 2005). The results of the experiment for cadets were astounding, with eighty percent of the cadets clicking on a link in a phishing email sent by an individual with authority within the institution.   An analog version of gamification was tested by Fatima, R. et al. in 2019 with a small group of students, and no real results were found regarding improvement of learning or retention due to participating in the game.

In 2019, Scholl, M. developed analog game scenarios related to security awareness training with attention to the details of the ethics and responsibilities of those who are made aware of security vulnerabilities and how each individual can help prevent security incidents from occurring. While these scenarios were not tested on a selected group of individuals, the work is very well thought out and includes enough information to deploy either with a digital equivalent or on its own.

The attempts to gamify SETA programs have had a long history of research, and the attempts have shown promise. Many companies have deployed third-party vendor solutions for systems to send out fake phishing emails as part of their SETA program. The solution is an attempt to attack at least one major component of the security awareness training that has been proven to cause a major security risk **(***The Human Factor 2021 Cybersecurity, Ransomware and Email Fraud in a Year That Changed the World Proofpoint.com REPORT*, n.d.). As cybersecurity continues to grow and risks continue to become a major problem, combatting risk by attempting to educate people and train them in companies, schools, and at home is the best way to thwart potential harm. The research shows that gamification, in analog and digital forms, seems to provide a way to improve the learning experience and the retention of the material. By providing these two aspects of learning, there is a connection to human behavior change. Understanding what motivates human behavior change is a larger research component, but there is hope that by taking the first steps to gamify SETA programs and study them on a long-term basis, insights into behavior change will become more visible. The relationship diagram in Figure 2 shows the interconnectedness between all the research and the necessity of incorporating these areas into a SETA program that has the potential to be extremely successful.

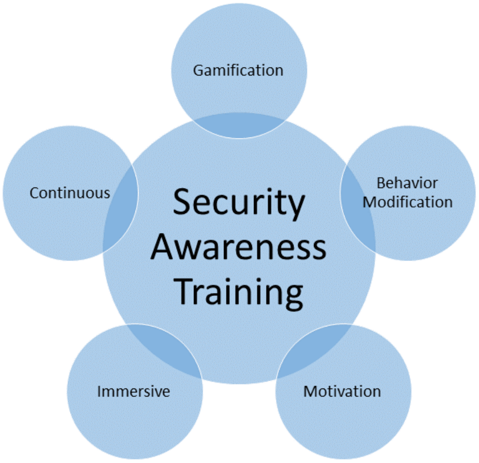


Figure 2. Relationship Diagram

This review of the research and case studies that have happened to date regarding the gamification of security awareness training programs and changing human behavior contributes to the scientific body of knowledge by providing a holistic view of the research available to use as a foundation for future research.

Conclusion

The review of research studies performed reveals some insights into why SETA programs are still ineffective. The insights regarding retention, lack of participation, and lack of motivation for users of SETA programs are all quite similar (De Carlo, S.M., 2021; Fearn, N., 2021). While many of the studies encouraged the development of parts of SETA programs such as a phishing email campaign to address a small portion of the security risks organizations face, there is still much to be done regarding the whole domain of security risk and SETA programs (Canham, M., Posey, C., & Constantino, M., 2022).

The following questions can be incorporated in examining the literature to produce a metatheory for future research:

How is behavior modification measured?
How does the attitude towards gaming affect results?

The results from the review of the literature available reveal that there is significant research in the separate areas of gamification, gamification of SETA programs, and behavior modification research. The intersection of all these areas of research will add a new perspective to future research.

A future study to examine a longitudinal multi-dimensional study using analog and digital gamification to study different scenarios for SETA and capture metrics regarding behavior modification and long-term engagement will provide a significant amount of data regarding how to improve SETA in the future.

The following questions can also be asked during this future study to provide answers to gaps in the SETA training in the market today.

How are predictability and repetitiveness addressed in the gamification of SETA programs?
Is there significant behavior change and in what intervals?
How does the gamification of SETA programs in younger audiences affect results?

Once a longitudinal, multi-dimensional research study has been conducted then asking the previous questions will provide even more depth to this area of research. Gamification for the sake of gamification is not the answer to increasing the success of SETA programs. The research studies examined show that gamification of SETA programs can be effective but still have not addressed the problems regarding participation percentages, retention, and behavior modification. The importance of the psychology of changing human behavior and the effect of prior attitudes toward gaming should be part of the research conducted. There is true merit to be found in the balance of gamification, scenario-based learning, and how to keep users interested in the game on a long-term basis. Combining all these factors will produce results that are necessary for understanding how to truly impact SETA programs and increase their effectiveness and participation rates. There is a need to study the impacts of using game theory to increase participation, retention of knowledge and behavior modification over a significant period of time. It is necessary to examine these factors in a longitudinal, multi-dimensional research study to discover the keys to creating impactful SETA training programs.

References

2021 Cybersecurity threat trends: phishing, crypto top the list - Cisco Umbrella. (2021, June 24). Retrieved September 25, 2021, from Cisco Umbrella website: https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list?utm_medium=search-paid&utm_source=google&utm_campaign=UMB_22Q1_NA_EN_GS_Nonbrand_Threats&utm_term=pgm&utm_content=UMB-FY21-Q4-content-ebook-2021-cyber-security-threat-trends&_bt=531409955734&_bk=cybersecurity+threats&_bm=p&_bn=g&_bg=122023015112&gclid=EAIaIQobChMItbrEiuma8wIVi4eRCh38jgYTEAAYASAAEgK1rPD_BwE

Baxter, R. J., Holderness Jr., D. K., & Wood, D. A. (2016). Applying Basic Gamification Techniques to IT Compliance Training: Evidence from the Lab and Field. *Journal of Information Systems, 30(3),* 119–133. https://doi.org/10.2308/isys-51341

Canham, M., Posey, C., & Constantino, M. (2022). Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks. Frontiers in Education, 6. https://doi.org/10.3389/feduc.2021.807277

CSRC Content Editor. (2023). Awareness - Glossary | CSRC. Nist.gov. https://csrc.nist.gov/glossary/term/awareness#:~:text=Source(s)%3A,adverse%20consequences%20of%20its%20failure.

DeCarlo, S. M. (2021). Measuring the application of knowledge gained from the gamification of cybersecurity training in healthcare [ProQuest Information & Learning]. *In Dissertation Abstracts International: Section B: The Sciences and Engineering (Vol. 82, Issue 5–B).*

Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security, 27(6)*, 581–612. https://doi.org/10.3233/JCS-181253

Fearn, N. (2021). How to Get Users to Pay Heed to Security Training: As cyber security risks grow daily, businesses must educate staff about these through cyber awareness training. But how can they ensure employees take this seriously? *Computer Weekly*, 27–31.

Ferguson, A. J. (2005). Fostering E-Mail Security Awareness: The West Point Carronade. EDUCAUSE Quarterly, 28(1), 54–57.

Fogg, B. J., & Euchner, J. (2019). Designing for Behavior Change—New Models and Moral Issues: An Interview with B.J. Fogg. Research Technology Management, 62(5), 14–19. https://doi.org/10.1080/08956308.2019.1638490

Francia, I. G., Thornton, D., Trifas, M., & Bowden, T. (2014). Chapter 5 - Gamification of Information Security Awareness Training. Emerging Trends in ICT Security, 85–97. https://doi.org/10.1016/B978-0-12-411474-6.00005-0

Definition of Gamification - Gartner Marketing Glossary. (2019). Gartner. https://www.gartner.com/en/marketing/glossary/gamification

Gundu, T., Flowerday, S., & Renaud, K. (2019). Deliver security awareness training, then repeat: {deliver; measure efficacy}. 2019 Conference on Information Communications Technology and Society (ICTAS). https://doi.org/10.1109/ictas.2019.8703523

Larson, K. (2020). Serious Games and Gamification in the Corporate Training Environment: a Literature Review. TechTrends: Linking Research & Practice to Improve Learning, 64(2), 319–328. https://doi.org/10.1007/s11528-019-00446-7

Loishyn, A. A., Hohoniants, S., Tkach, M. Y., Tyshchenko, M. H., Tarasenko, N. M., & Kyvliuk, V. S. (2021). Development of the Concept of Cybersecurity of the Organization. TEM Journal, 10(3), 1447–1453. https://doi.org/10.18421/TEM103-57

Lugnet, J., & Ericson, Å. (2022). Scenarios as a Tool for Professional Training in Information Security Dialogues. International Journal of Technology, Knowledge & Society: Annual Review, 18(2), 65–77. https://doi.org/10.18848/1832-3669/CGP/v18i02/65-77

Meyer, C. (2017). How to Utilize Game Theory for Security Awareness: Building classic gaming principles like positive reinforcement and escalating goals into security education can drive new levels of engagement. Security: Solutions for Enterprise Security Leaders, 54(12), 26–27.

The Human Factor 2021 Cybersecurity, Ransomware and Email Fraud in a Year that Changed the World proofpoint.com REPORT. (n.d.). https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf

Rapp, A. (2019). Design fictions for behaviour change: exploring the long-term impacts of technology through the creation of fictional future prototypes. Behavior & Information Technology, 38(3), 244–272. https://doi.org/10.1080/0144929X.2018.1526970

Scholl, M. (2018). Play the Game! Analogue Gamification for Raising Information Security Awareness (Invited Paper). Journal of Systemics, Cybernetics and Informatics, 16(3), 32-35. https://doaj.org/article/db42b46200b64f7981cc396b3aad4032

Yerby, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security. Journal of Management Information Systems, 37(3), 723–757. https://doi.org/10.1080/07421222.2020.1790187https://doi.org/10.3991/ijac.v13i3.17063

Scroxton, A. (2020). How security will be different after Covid: The world of cyber security will probably never return to its pre-pandemic state, with different approaches to securing distributed enterprise systems and staff likely to come to the fore next year. Computer Weekly, 4–7.

Silic, M., & Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. Journal of Management Information Systems, 37(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512

Torraco, R. J. (2016). Writing integrative literature reviews : using the past and present to explore the future. Human Resource Development Review : Thousand Oaks, Calif. [u.A.], 15(4), 404–428.

Ulsamer, P., Schütz, A., Fertig, T., & Keller, L. (2021). Immersive storytelling for information security awareness training in virtual reality. Proceedings of the 54th Hawaii International Conference on System Sciences. https://doi.org/10.24251/hicss.2021.861

Yerby, J., Hollifield, S., Kwak, M., & Floyd, K. (2014). Development of Serious Games for Teaching Digital Forensics. Issues in Information Systems, 15(2), 335–343.