Analyzing the Effectiveness of Gamification in Cybersecurity Trainings for Organizations

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Jason Yu

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Bryn E. Seabrook, Department of Engineering and Society

STS Research Paper

Introduction

Traditional cybersecurity trainings are notoriously boring and ineffective (Reeves et al., 2021), yet organizations have historically relied on traditional security education and training to mitigate cyberattacks. According to a recent TalentLMS survey on the state of cybersecurity training, 61% of employees who took cybersecurity training failed a basic test (Marousis, 2021). Across the board, employees struggle to retain and apply what they learn in cybersecurity trainings to their everyday work lives. In an attempt to make cybersecurity education more engaging and effective, employers are increasingly turning to gamification methods. Gamification is the use of game mechanics and game thinking to engage users in solving problems and to motivate them by introducing elements of competition and reward (Moore, 2017). While gamification is increasingly popular among employers, the effectiveness of gamification is not well-documented. This STS paper applies the Social Construction of Technology (SCOT) framework to answer the question of how effective gamification is in cybersecurity training for organizations.

Research Question and Methods

This STS research paper explores the effectiveness of gamification methods in cybersecurity trainings compared to traditional cybersecurity training methods. To answer this question, this paper employs documentary research methods by compiling and analyzing research from a variety of scholarly articles ranging from articles detailing the current cybersecurity landscape to individual case studies of gamified approaches to cybersecurity training. Research keywords include “cybersecurity,” “training,” “game,” “gamification,” “engagement,” and “effectiveness” since these are most relevant to the research topic. The analysis is organized thematically and begins with an overview of employee perceptions in the current cybersecurity landscape as well as the effectiveness of traditional training programs. Next, the paper details a number of case studies of gamification in cybersecurity training, pinpointing the strengths and weaknesses of each approach, both in terms of employee engagement and actual security outcomes. Expanding the scope of the research question, this paper then seeks to identify inherent limitations of gamification approaches as it relates to employee trainings. Finally, the paper synthesizes the findings from the analyses to offer recommendations for the future of cybersecurity trainings for organizations.

Background Information

Cyberattacks pose major challenges to businesses and organizations. According to PurpleSec's 2021 Cybersecurity Trends Report, over 50% of all cyberattacks are done on small to midsize businesses (SMBs), and enterprises experience approximately 130 security breaches per year, per organization, on average (Firch). In 2021, RiskIQ estimated that businesses worldwide lose $1,797,945 per minute due to cybercrime—and that the average breach costs a company $7.2 per minute (Rosenthal). Human error is one of the primary factors that enables cyberattacks to be successful (Ahola, 2021). In a security context, human error encompasses unintentional actions (or inaction) by employees and users that cause, spread, or allow a security breach to take place. Human error includes a vast range of actions, from downloading a malware-infected attachment to failing to use a strong password (Leal, 2022). According to research from Elevate Security, human behavior had a direct role in 88% of total losses in the largest cybersecurity incidents over the past five years, and about two-thirds of major data breaches are the result of humans (2021). Similarly, phishing is the most common way in which malware is delivered. In fact, a 2019 report by NortonLifeLock found that 92.4% of malware is delivered as an attachment in a malicious email.

To mitigate the human risk element, organizations have historically required traditional security awareness education and training (The Defence Works, 2019). Traditional security awareness trainings methods include models in which large groups of employees periodically attend one-day events (Hadley, 2018) and mandatory security awareness trainings involving reading information from slides and taking knowledge-checking quizzes afterwards (Obudulu, 2022). Unfortunately, traditional methods of cybersecurity training have proven to be largely ineffective. According to a survey on the state of cybersecurity training, 61% of employees who took cybersecurity training failed a basic test (Marousis, 2021). Not only are cybersecurity trainings relatively ineffective, they are also boring. A 2021 paper found that employees generally have a negative attitude toward cybersecurity trainings, citing a lack of interest in the presentation style and a perceived mismatch between the training content and real-world scenarios (Reeves, et al.). Overall, employees often fail to internalize and implement proper cybersecurity practices in their work lives.

In an effort to increase employee engagement with cybersecurity education, employers are increasingly using gamified methods as opposed to traditional methods. Some examples of gamified methods include ThreatGEN's *Red vs. Blue*, a game-based cybersecurity simulation platform that combines a gaming engine with an adversary simulation A.I., theoretically tailoring the content of the game to match the user's skill level (2022) and Centrical's game platform that allows users to complete challenges involving a variety of game narratives (e.g., Hide and Seek, car races, hitting targets) in order to earn coins, badges, and move up on a leaderboard (2022).

This research paper explores the effectiveness of gamification methods in cybersecurity trainings compared to traditional cybersecurity training methods.

Importance of Social Construction of Technology

This research project employs a Social Construction of Technology (SCOT) framework to analyze the relationship between cybersecurity trainings and relevant social groups, which include employees, employers, cyber attackers, cybersecurity professionals, and everyday users. SCOT posits that technology does not determine human action, but rather than human action primarily shapes technology. Originated by Trevor Pinch and Wiebe Bijker, SCOT denies technological determinism and instead recognizes the interplay between the social and technical aspects of technologies (1984).

While the SCOT framework has not yet been used to analyze the gamification of cybersecurity trainings, several scholars have used the framework to explore related fields of study. In a 2002 paper, for example, Jackson, Scott, and Kuhn document the use of SCOT in studies of the workplace, specifically those exploring the relationship between the organizational aspects of workplaces and the design and development of information and communication technologies (ICTs). In this paper, the authors assess the extent to which constructionist views in past studies are successful in providing a framework for understanding ICTs in the workplace. The authors ultimately argue that while social constructionist views have in principle developed an understanding that privileges neither technology nor the workplace, their use in design and implementation have tended to tilt so as to overemphasize either the technological aspects (ICTs) or the social aspects (the workplace).

For example, a paper by Shoshana Zuboff ostensibly used SCOT to provide a social ethnography of the computerization of large paper mills, describing how work that had previously been done by touch, feel, and sight was transformed as the factory was computerized (1988). Jackson, Scott, and Kuhn point out, however, that Zuboff privileges the technological dimension in her analysis, treating the technology as a black box around which members of the organization must reconstruct their work. Conversely, a different paper exploring knowledge management systems in organizations tips toward a social perspective, concentrating on sense-making, communicative connections between individuals, and knowledge processes at the expense of the ways in which technology itself shapes these dimensions (Mentzas, et al., 2001).

In order to overcome these imbalances, Jackson, Scott, and Kuhn recommend taking the imbalance as an empirical question and asking what factors or forces might determine whether organization is the primary mover, whether technology is, or whether they are co-producing each other, cautioning that "without large, representative samples, it is not possible to determine whether a given slant is warranted or not" (2002). In this research paper, the SCOT framework is apt for the topic of gamification in cybersecurity because innovations in cybersecurity trainings are relatively recent developments, and designers currently have substantial flexibility in shaping the future of cybersecurity trainings. This observation aligns with SCOT's tenet of interpretive flexibility, which suggests that technology design is an open process that can produce different outcomes depending on the social circumstances of development (Klein & Kleinman, 2002). Importantly, while this paper primarily analyzes cybersecurity trainings through the lens of SCOT, it is also important to recognize the ways in which the technology associated with cybersecurity trainings shapes employee perceptions and workplace culture.

SCOT has also been used to analyze and propose new systems for information security. Wolter Pieters' 2010 paper, for example, examines the interplay between the technical and social aspects of cybersecurity policies for organizations. Recognizing that information security is both a technical and a social challenge, Pieters writes that the important distinction between these two domains is that the implementation of policies is not deterministic. Working under the assumption that technology is shaped by human use and action, Pieters points out that while a door will always (or with very high probability) let someone in who has the key, a person may act differently in different circumstances, and he or she may only conform to a given policy, say, 60% of the time. By recognizing the role of human agency in shaping the usage of technology and information security policies, Pieters proposes a framework for information containment that is sensitive to the ways in which social aspects shape the effectiveness of cybersecurity policies.

Analyzing the Effectiveness of Gamified Methods

Gamification of cybersecurity trainings is frequently hailed as a superior alternative to traditional cybersecurity training methods (Zides, 2021). However, while various case studies demonstrate that gamification leads to increased employee engagement, empirical data shows that gamification does not necessarily lead to an improvement in actual security outcomes (Capers, 2021). Specifically, the mere conversion of traditional cybersecurity training content into the form of a game will not, in itself, improve security outcomes. That being said, the game medium offers certain advantages over some forms of traditional cybersecurity trainings including greater possibilities for employee engagement, opportunities for group participation, and more effective ways to motivate good cybersecurity practices. This paper recommends that employees who seek to implement gamified training methods must leverage these advantages and consider the specific needs of their employees in order to maximize benefits.

Current Cybersecurity Training Landscape. The current cybersecurity training landscape is characterized by lack of engagement from employees and subpar security outcomes. One study conducted by Reeves, Calic, and Delfabbro identifies factors that influence employee perceptions of traditional cybersecurity trainings, writing that “much of the delivery of the training or advice was considered boring with low production qualities. In online training, for example, interfaces were often described as counterintuitive” (2021). Indeed, respondents reported that they sometimes disagreed with the advice presented in the training, did not perceive it as relevant to their role, received too much information, or did not believe that it captured real-world variability in the workplace. This observation highlights the fact that the content, delivery, and aesthetics matter when presenting cybersecurity awareness trainings. Another factor identified in the paper centers around other people, colleagues, and management. In particular, participants reported being strongly influenced by the behavior of their colleagues or management, either as positive role-models or examples of bad behavior. Some indicated that their colleagues’ poor behavior served as motivation for them to implement secure practices themselves, whereas others reported violating security policies because they were simply doing what everyone else did. It was also common for people to base their behavior on a perceived mid-point between the official policy and observed behavior of others. This finding suggests that problems with security practices may not simply lie in the type of training that employees receive but also in the workplace culture and expectations of adherence to good security practices. Finally, the paper cites preconceptions, experiences, and understandings of cyber threats as an obstacle to increasing employee engagement and retention relating to cybersecurity awareness trainings. For example, some participants believed that they had a sufficient level of understanding regarding cybersecurity threats to make their own decisions regarding their behavior at work, and for this reason they did not comply with the recommendations of cybersecurity training programs. This result emphasizes the need to not only create good training programs but also to highlight the severity of cybersecurity threats in order to properly motivate employee engagement and compliance.

While gamification is an attractive alternative to traditional cybersecurity trainings in that they tend to increase employee engagement, a survey of 573 respondents found a strong correlation between gamified training programs and higher rates of security breaches (Capers, 2021). Indeed, phishing attacks are suffered by 82% of companies that use gamified security training compared to only 67% of those that employee traditional training methods. Similarly, ransomware attacks were reported in 61% of companies that used gamified training methods compared to only 29% of companies that used traditional methods, and data breaches were reported in 59% of companies that used gamified training methods compared to 28% of companies that used traditional methods. Any company that seeks to engage in gamified security awareness training must reckon with these alarming statistics; not only is gamification apparently less effective at preventing security incidents, but companies are putting significantly more resources into gamified training than those providing traditional training. Clearly, the conversion to a game medium is not in itself sufficient to improve security outcomes. Instead, it is important for employers to carefully consider the strengths of gamified approaches and leverage them to optimize security outcomes.

Case Studies of Gamified Methods

This paper now examines several case studies of gamification methods in cybersecurity trainings through the lens of interpretive flexibility, a principle of SCOT that suggests that technology design is an open-ended process that can produce different outcomes depending on the social circumstances of development (Klein & Kleinman, 2002). Given that the emergence of gamification methods in cybersecurity training is relatively recent, it is unsurprising that there are many different ways in which gamification methods have been implemented. One such study by van Steen and Deeleman experimentally tested a cybersecurity game applicable for cybersecurity training against a non-cybersecurity game that did or did not contain cybersecurity information (2021). In the cybersecurity game, participants encountered a number of cybersecurity incidents, ranging from protecting against phishing e-mails to baiting attacks, and were taught what they could do to be more secure. If they did not give the correct response to the incident, there were consequences (e.g., a lower score in the game) and participants were informed of what they should have done instead and why. This stipulation ensured that participants who did not do well learned what they should do in the future, thereby improving cybersecurity knowledge and relevant skills. In the other conditions, participants played a cooperation game that acted as a control game. In this game, participants solved cooperation-focused incidents in which they were asked for help by non-player characters. These incidents were unrelated to cybersecurity. In the "control plus information" condition, cybersecurity information from the cybersecurity game was added to the cooperation game in poster format. Results showed that the cybersecurity game resulted in higher self-reported scores on attitudes, perceived behavioral control, intentions, and behavior compared with both types of non-cybersecurity games.

While the game from this study increased employee engagement and improved scores of perceived cybersecurity awareness, the study was unable to conclude whether this training program was actually more effective in yielding better security results. Indeed, the only measure of success was based on a subjective questionnaire asking employees about their attitudes and perceived behavioral control regarding cybersecurity practices (2021). Importantly, just because an employee is aware about good security practices does not necessarily lead to actual behavioral change. In fact, the authors of the paper note that “one limitation of this study lies in the limited evidence for behavioral change as a result of playing the cybersecurity game that goes beyond the effects of the Theory of Planned Behavior [questionnaire] predictors” (2021). Another limitation is that the format of the “control plus information” condition, a dubious stand-in for traditional cybersecurity trainings, which generally require more than a cursory glance at a poster of information. The advantage of the gamified approach from this case study is that the format of the game improved employee engagement and retention of knowledge, but it is unlikely that this approach actually improves security outcomes, largely because factors such as workplace culture and motivation for good cybersecurity practices went unaddressed.

A second case study by Muhly, Leo, and Caneppele details the creation and testing of a game for social engineering awareness (2021). The authors utilized field observations and interviews to collect data on participants’ engagement, satisfaction and compliance with game instructions. In this study, the game was a tabletop card game. In each iteration of the game, a team simulated an attacker by creating a social engineering attack plan based on the given game materials consisting of a situation plan for a fictitious company, a set of fictitious employee profiles (each with unique characteristics and skills), and an attack plan sheet that guided players through the process. After formulating an attack plan, the teams presented their attacks to the other teams at the game table. Each presenting team received an evaluation from the other teams based on a predefined point scale, and the evaluating teams had the ability to propose attack improvements to earn bonus points.

Much of the feedback about the game centered around improving the game procedures and materials. Interviewees mentioned that they would have appreciated more background information and a deeper introduction to the real-life implications of social engineering. Other participants pointed out that the game should have been digitized to scale it and make it more accessible. Indeed, the authors of the study acknowledge that “the findings suggest that participants enjoyed the game but sometimes had trouble with following the game instructions” (2021). In general, the main drawback of this gamified approach was the lack of comprehensive, straightforward explanations about the game and cybersecurity in general. Another limitation of this study was that there was no follow-up as to whether security outcomes improved for the subjects in the game, and there was no control group to serve as a baseline. That being said, this gamified approach had certain advantages that the previous case study did not. For one, the group-centric nature of this game shows promise as a way to encourage employees to work together towards good security practices. Instead of employees working individually on cybersecurity training modules (as is often the case in traditional trainings), a group game allows employees to discuss what they are learning, fostering a culture of cybersecurity awareness. Similarly, the game’s emphasis on the attacker’s perspective is helpful in motivating employees to be vigilant against social engineering attacks.

The third case study by Adams and Makramalla intentionally focused on motivating employees to take their responsibilities seriously in maintaining good security practices (2015). Specifically, the authors of this paper discuss the use of gamification methods that enable all employees and organizational leaders to play the roles of various types of attackers in an effort to reduce the number of successful attacks due to human vulnerability exploits. By putting participants in the position of attackers, the authors argue that employees will better grasp the seriousness of cyberattacks, gain a deeper understanding of how cyberattackers operate, and become better-equipped to respond to threats. The game proposed in this study specifically identifies various attacker types such as Script kiddies (attackers who depend on existing tools), insiders (attackers who are embedded within the organization they attack), petty thieves (attackers who commit online fraud), professional criminals (attackers who are hired to infiltrate systems), and hacktivists (attackers who are motivated by ideology), among others (2015). By incorporating these roles into a video game complete with a story, real-time feedback, increased challenges, player control, and progress mechanics, the authors assert that such a game will help train all employees and organization leaders to develop cybersecurity skills and better defend against and react to data breaches (2015).

The advantages of such an approach are apparent: an attack-centric perspective motivates employees to change their behavior, and the medium of a well-designed video game is likely to encourage increased participant engagement. However, this approach fails to address the need for a systemic change in the workplace culture. An employee who is required to play such a game may fully understand the learning objectives, but the actual benefit to the organization's security may be minimal due to the fact that there is no guarantee that the employee's peers are compliant, leading to the possibility that behavior is largely unaffected (Gillam, 2020).

Relevant Social Groups

The second component of SCOT is identifying relevant social groups. Importantly, technology development (including the development of cybersecurity trainings) is a process in which multiple groups, each embodying a specific interpretation of an artifact, iteratively negotiate over the artifact's design (Klein & Kleinman, 2002). In the case of cybersecurity training, the relevant social include business executives, team managers, company employees, and end users. A paper by Sabillon, et al. identifies these same major relevant social groups (2019). In this paper, researchers examined and compiled cybersecurity awareness methodologies, frameworks and approaches in order to propose a training model designed to address existing deficiencies in awareness trainings. Specifically, the authors designed the Cybersecurity Awareness TRAining Model to deliver training to different organizational audiences, each of which has unique and separate objectives (2019). For example, an ideal cybersecurity training course for managers would target different learning goals than a training course for IT professionals. Based on a case study in Canada, CATRAM was effective in laying the groundwork for a new cybersecurity training program. According to the authors of the study, "before conducting our case study research, our target organization did not have any cybersecurity awareness model nor any cybersecurity awareness education program whatsoever. The CATRAM delivery allowed the organization to build a strong foundation for a future implementation of a comprehensive cybersecurity awareness training program" (2019). This case study demonstrates that cyber awareness training research must be focused on developing new and interactive ways to keep people engaged based on their own position and needs in order to cultivate consistent cyber defense and proactive behaviors.

Recommendations for Success

The third component of the SCOT framework is closure and stabilization. A multigroup design process can experience controversies when different interpretations lead to conflicting images of an artifact. Design continues until such conflicts are resolved and the artifact no longer poses a problem to any relevant social group (Klein & Kleinman, 2002). As demonstrated by the case studies detailed above, several researchers have attempted to implement gamified methods for cybersecurity training, but unless the gamified approach is engaging, communal, and properly motivated, it is unlikely to yield positive results. One paper by He and Zhang largely confirms these findings (2019). This paper identifies best practices and provides actionable insights (relating cyber awareness to employees' personal life, reinforcing security procedures and guidelines, instilling a “relaxed alert” state of employees, and minimizing security fatigue for employees) that help enterprises develop and implement economical, effective, and engaging cybersecurity training and awareness programs (2019). Relating cyber awareness to employees’ personal life involves motivating employees to take preventative and precautionary action, not just maintaining a cursory sense of cyber awareness. Indeed, there is a difference between knowing of a threat and acting to preventing a threat, largely because people often underestimate the risks (Schwarzer, 1994). Training programs and educational materials need to relate cyber awareness to employees’ personal life, family, and home, in order to be more engaging and to encourage employees to change their cybersecurity behavior. Another aspect identified by the authors is reinforcing security procedures and guidelines. Based on studies of how people learn and retain information, it is generally not sufficient to rely on minimally trained workers to defeat highly motivated hackers. Therefore, the authors recommend that security training programs focus on implementing good security behaviors as defined in formal organizational procedures and guidelines instead of merely telling people what not to do. The third principle is instilling a “relaxed alert” state of employees. In such a state, employees feel relaxed, productive, and able to concentrate, so they can immediately detect something wrong in their environment. The final recommendation from the paper is to minimize security fatigue for employees. Many employees report feeling overwhelmed and experience “security fatigue” on account of an ever-increasing number of security alerts and warnings from a variety of sources such as television, magazines, radio, and social media. Thus, to minimize security fatigue, the authors recommend that successful security training programs should train employees to set up password managers, set up automatic security updates, and how to use advanced cybersecurity solutions to reduce stress and fatigue.

These recommendations align with the findings mentioned above. For one, minimizing security fatigue and reinforcing security procedures and guidelines can be accomplished by a comprehensive and engaging training program. Instilling a “relaxed alert” state of employees relates to creating a workplace culture of cybersecurity awareness and best practices. Finally, relating cyber awareness to employees’ personal life is a practical way to motivate employees to understand the effects of cyberattacks and motivate behavior change.

Wider Context of Gamified Approaches

SCOT emphasizes the need to take into account the wider sociocultural milieu in which artifact development takes place (Klein & Kleinman, 2002). For example, in the case of gamified approaches to cybersecurity trainings, it is important to consider why games in and of themselves do not necessarily lead to positive security outcomes. One explanation is that gamified trainings tend to be less comprehensive than traditional trainings. According to a 2021 survey, non-gamified trainings were more likely to cover important security subjects such as password policies, data privacy, onsite security, and acceptable use compared to gamified trainings (Capers, 2021). But even beyond the subject matter of the trainings themselves, there are several possible explanations for why a gamified approach, though more engaging, does not actually shape employee behavior. One possible reason is that good games require voluntary participation. Author, researcher, and game designer Jane McGonigal describes games as “voluntary attempts to overcome unnecessary obstacles,” and yet this principle does not necessarily hold true if an employee is required to play a game to fulfill their annual security training (2011). If an employee has no vested interest in playing a game, then a gamified approach will be no more engaging or effective than a traditional cybersecurity training; the only aspect that has changed is the format of the content. A second possible explanation relates to the mental disconnect between the real world and the game world. In games and digital media, for example, the ”magic circle” is the space in which the normal rules and reality of the world are suspended and replaced by the artificial reality of a game world. The existence of the magic circle allows people to enter into game worlds to take on various roles or carry out various activities and yet remain relatively unchanged after emerging back into the real world (Klabbers, 2009). The magic circle could explain why employee behavior remains largely unaffected even after an engaging and comprehensive gamified cybersecurity training program. In order to be effective, a game must penetrate from the virtual world into the outside world, and this goal can be effectively accomplished by sufficiently motivating employees and reminding them about the real-world consequences of their actions.

Limitations and Further Exploration

Overall, in order for a gamified approach to be effective, the delivery of the content must be engaging, there must be a communal aspect in order to shape the workplace culture, and the need for good cybersecurity practices must be properly motivated. While these recommendations surrounding gamified approaches are drawn from real-world case studies and empirical data, it remains to be seen whether these recommendations hold true in an experimental study. Further research into this topic should center around the development and controlled testing of a gamified cybersecurity training that follows the recommendations outlined in this paper.

Conclusion

This research paper sought to determine the extent to which gamified approaches to cybersecurity trainings are effective alternatives to traditional cybersecurity trainings. Based on case studies and empirical data, a gamified approach is a viable method as long as the content is thorough and engaging, the game is distributed to the organization’s workforce in such a way that it fosters a more security-aware culture, and the need for best practices is sufficiently motivated. This research is significant because the field of gamified approaches to cybersecurity trainings is relatively new, and while it appears to be an engaging, attractive, and easy alternative to traditional trainings, it is important for employers to seriously consider the factors that influence improved employee behavior and security outcomes as opposed to blindly believing that gamification in itself is the sole solution to improved security.

References

Adams, M., & Makramalia, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review, 5*(1): 5-14. http://doi.org/10.22215/timreview/861

Ahola, M. (2021, February 1). The Role of Human Error in Successful Cyber Security Breaches. *usecure*. https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Capers, Z. (2021, December 12). *Security Isn't a Game—Our Data Shows Traditional Security Awareness Training May Be More Effective Than Gamified*. GetApp. https://www.getapp.com/resources/gamification-security-training/

Centrical. (2022). Gamification for Employee Engagement. *Centrical*. https://centrical.com/platform/gamification/

Elevate Security. (2021, May 11). Elevate Security and Cyentia Institute Launch First Annual Study on Employee Cybersecurity Risk in the Workplace, Finds Current Solutions Do Little to Reduce Human Error. *Elevate Security*. https://elevatesecurity.com/elevate-security-and-cyentia-institute-launch-first-annual-study-on-employee-cybersecurity-risk-in-the-workplace-finds-current-solutions-do-little-to-reduce-human-error/

Firch, J. (2021, April 29). 10 Cyber Security Trends You Can't Ignore In 2021. *PurpleSec*. https://purplesec.us/cyber-security-trends-2021/

Gillam, A., & Foster, W. (2020). Factors Affecting Risky Cybersecurity Behaviors by U.S. Workers: An Exploratory Study. *Computers in Human Behavior, 108*(2020): 106319. https://doi.org/10.1016/j.chb.2020.106319

Hadley, J. (2018, October 31). How Traditional Training Is Weakening Businesses' Cybersecurity. *Forbes*. https://www.forbes.com/sites/jameshadley/2018/10/31/how-traditional-training-is-weakening-businesses-cybersecurity/?sh=1eacd74b4b0c

He, W., & Zhang, Z. (2019). Enterprise Cybersecurity Training and Awareness Programs: Recommendations for Success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4): 249-257. https://doi.org/10.1080/10919392.2019.1611528

Jackson, M., Poole, M., & Kuhn, T. (2002). The social construction of technology in studies of the workplace. *SAGE Publications, Ltd*, https://dx.doi.org/10.4135/9781848608245

Klabbers, J. (2009). *The Magic Circle: Principles of Gaming and Simulation*. Sense Publishers.

Klein, H., & Kleinman, D. L. (2002). The Social Construction of Technology: Structural Considerations. *Science, Technology, and Human Values*, *27*(1): 28-52. https://doi.org/10.1177/016224390202700102

Leal, A. (2022, August 14). Human Factor in Cybersecurity: The Weakest Link? *KuppingerCole*. https://www.kuppingercole.com/events/csls2022/blog/human-factor-in-cybersecurity-the-weakest-link

Marousis, A. (2021, April 6). Cybersecurity training lags, while hackers capitalize on COVID-19. *TalentLMS*. https://www.talentlms.com/blog/cybersecurity-statistics-survey/

McGonigal, J. (2011). *Reality is Broken: Why games make us better and how they can change the world*. Penguin Books.

Mentzas, G., Apostoulou, D., Young, R., & Abecker, A. (2001). Knowledge networking: a holistic solution for leveraging corporate knowledge. *Journal of Knowledge Management*, *5*(1): 94-106.

Moore, M. (2017). Bringing Gamification to Cyber Security Training. *University of San Diego*. https://onlinedegrees.sandiego.edu/bringing-gamification-to-cyber-security-training/

Muhly, F., Leo, P., & Caneppele, S. (2021). A Serious Game For Social Engineering Awareness Creation. *Journal of Cybersecurity Education, Research, and Practice*, *2022*(1): Article 5. https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss1/5

NortonLifeLock, Symantec Global Internet Security Threat Report (2019). Online Paper. https://docs.broadcom.com/doc/istr-24-2019-en

Obudulu, O. (2022, July 5). 7 Ways to Transform Your Cybersecurity Training and Influence Lasting Change. *skillsoft*. https://www.skillsoft.com/blog/7-ways-to-transform-your-cybersecurity-training-and-influence-lasting-change

Pieters, W. (2010). The (Social) Construction of Information Security. *The Information Society, 27*(5): 326-335. https://www.tandfonline.com/doi/full/10.1080/01972243.2011.607038

Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science*, *14*(3): 399-441. http://www.jstor.org/stable/285355

Reeves, A., Calic, D., & Delfabbro, P. (2021). "Get a Red-Hot Poker and Open Up My Eyes, It's So Boring": Employee Perceptions of Cybersecurity Training. *Computers & Security, 106*(2021): 102281. https://doi.org/10.1016/j.cose.2021.102281

Rosenthal, M. (2022, January 12). Must-Know Phishing Statistics: Updated 2022. https://www.tessian.com/blog/phishing-statistics-2020/

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness

TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology, 21*(3): 26-39. https://doi.org/10.4018/JCIT.2019070102

Schwarzer, R. (1994). Optimism, Vulnerability, and self-beliefs as health-related conditions: A systematic overview. *Psychology & Health, 9(3)*: 161-180. https://doi.org/10.1080/08870449408407475

The Defence Works. (2019, February 19). Does Security Awareness Training Work? *The Defence Works*. https://thedefenceworks.com/blog/does-security-awareness-training-work/

ThreatGEN. (2022). Red vs. Blue. *ThreatGEN*. https://threatgen.com/

van Steen, T., & Deeleman, J. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, Behavior, and Social Networking, 24*(9): 593-598. https://doi.org/10.1089/cyber.2020.0526

Zides, M. (2021, March 23). *Why Implement Gamification Into Your Cybersecurity Training?* eLearning Industry. https://elearningindustry.com/why-implement-gamification-into-cybersecurity-training

Zuboff, S. (1988). *In the Age of the Smart Machine: the Future of Work and Power*. New York: Basic.