Increasing Engagement in a Cyber-Awareness Training Game

Robert Wray[1](✉), Lauren Massey[1], Jose Medina[1], and Amy Bolton[2]

[1] Soar Technology, Inc., Ann Arbor, MI 32817, USA
wray@soartech.com
[2] Office of Naval Research, Arlington, VA 33303, USA

Abstract. Today's workforce is generally uneducated in cybersecurity, largely complacent, and fails to embrace the reality that 'a risk to one is a risk to all'. A cyber-aware mindset must be instilled in improved training across the workforce. We are developing a training game designed to improve cyber awareness with the goal of inculcating "cyber mindset" to reduce vulnerabilities to and increase vigilance toward cyber threats. The game stresses critical thinking, intellectual engagement, and countering cognitive biases. We introduce the design and implementation of the training game. Creating effective cyber awareness training is often challenging due to resistance and disinterest from target populations. We outline the current implementation of the training game and introduce additional features or "mechanics" we have developed and also continue to investigate to attempt to improve the game's effectiveness in developing a cyber mindset.

Keywords: Cyber awareness · Cognitive bias · Personalized learning · Adaptive learning

1 Introduction

In today's workforce, most employees operate in the cyber domain, with all systems and all stored data connected to networks at risk. While networked work has contributed to large increases in individual and aggregate productivity [1], networks introduce new risks to individuals and organizations. Every individual now represents a potential attack vector for nefarious actors. A drumbeat of recurring accounts of successful attacks against individuals, companies and organizations, and governments redounds in the media each week [2–12].

While the conduct of cyber warfare increases in scope and sophistication, training for this new reality of risk exposure and vulnerabilities is not keeping pace. The workforce is generally uneducated in cybersecurity, largely complacent, and fails to embrace the reality that 'a risk to one is a risk to all'. To remain vigilant in the face of these threats, a cyber-aware mindset must be instilled in improved training across the workforce [13].

The general workforce typically views cybersecurity as a nuisance that unnecessarily complicates their mission and for which they have little to no direct responsibility. Cybersecurity is "someone else's problem." National and industrial security requires a

D. D. Schmorrow and C. M. Fidopiastis (Eds.): HCII 2020, LNAI 12197, pp. 147–158, 2020.
https://doi.org/10.1007/978-3-030-50439-7_10

more cyber-savvy workforce, where each individual is attuned to the threat, embraces their role in defense, and is able to respond quickly and effectively.

We are researching and developing a training-game prototype designed to improve cyber awareness. We hypothesize that inculcating “cyber mindset” will reduce vulnerabilities to and increase vigilance toward cyber threats without necessitating the development of sophisticated cyber knowledge and expertise. The current training game stresses critical thinking, intellectual engagement, and countering cognitive biases.

This paper introduces the design and implementation of the training game. As we discuss further below, the game allows the player to participate in the game as an attacker, which we hypothesize has a number of benefits for learning. More generally, however, creating effective cyber awareness training is often challenging, for some of the reasons outlined above. Thus, we are investigating design options for subsequent versions of the game that could support greater learner engagement and potential carryover to the everyday activities of learners. Below, we describe the current implementation of the game and then introduce some of the additional features or “mechanics” we are investigating to attempt to improve the game’s effectiveness in developing a cyber mindset. We review three types of design options: specialization for player type, customization based on player demography, and active monitoring of engagement.

2 Training for Cyber Mindset

In previous work, we outlined the theoretical and empirical foundations for the design of the cyber mindset game, focusing on general review of the literature and identification of specific training objectives from that review [13]. In this section, we briefly review other attempts to train cyber awareness and how those attempts inform our approach. We summarize some design elements that we have already included in the game to support engagement and effective learning. The following section then describes the implementation of the game itself.

2.1 Creating Effective Cyber-Awareness Training Is Difficult

Organizations have employed various training methods to raise awareness to employees about the dangers of the internet, network intrusions, and social engineering, typically promoting the notion that staff are the first line of defense against such attacks. Commonly, the training that is employed focuses on cyber awareness training that promotes that staff know their roles and responsibilities to protect the organization’s information. Most existing training does not ensure that the employees are competent in that role of protection or even than they undertake hands-on training [14].

There are various types of cyber training tools that are currently used for general population consumption, including multimedia static content, on-site presentations, and passive computer-based training (CBT). A company may utilize one or several of these tools in their security training program depending on budget and the amount time allotted to training [15]. Static content and instructor led courses tend to have limited individualized effect and any effect may be highly dependent on the content and delivery [16]. Computer-based training allows for some customization to individual learners, but can typically be completed without significant engagement. These methods typically fail to motivate and engage [15], may not connect learning goals to individual and corporate responsibilities [17], and have been demonstrated to commonly fail to change staff behavior even after "successful" completion of the training [18].

The potential use of games for cyber training is not novel. Multiple games have been developed in research labs, although few commercial serious games have made the transition from research labs [19]. The potential advantage of games to introduce basic cyber principles is that they address the challenges of traditional training methods. Games provide an environment in which trainees can actively participant in the learning process, which may motivate and engage them to pay attention and learn [19, 20]. This motivation and hands-on learning setting could then aid transfer [21] of knowledge to daily adherence without the use of "fear as motivation" that is used in many traditional staff-level cyber training programs.

2.2 Design Elements in Support of Engagement and Learning

The design of our cyber awareness training game draws on two primary training-design elements. First, the game introduces conceptual knowledge about cyber threats, seeking to create and and/or extend learner knowledge structures, which, in turn, modulate attention and metacognition to increase vigilance and awareness of potential of cyber attacks. The primary goal of the game is to facilitate development and transfer (to everyday life) of this new awareness or *cyber-aware mindset.* Examples introduced in the game include the cyber-attack concepts such an attack vector and social engineering [17, 22] and specific examples of higher-level concepts, such as phishing and open-source intelligence gathering (a preliminary activity in social engineering).

A second design element focuses emphasizes the need for attention and practice to support the development of these new knowledge structures and the skill to retrieve and apply them in appropriate context. Most existing cyber awareness tools fail to help users make the leap from awareness to changing behavior, limiting their effectiveness [23]. In contrast, our game adopts turn-based but realistic and familiar depictions of household and office environments, rendered in three-dimensions. A game environment generally supports engagement and immersion; such depictions have been shown to offer increases in attention and retention in comparison to non-immersive environments presenting comparable learning content [24, 25]. Further, one of the advantages of the narrative-based game environment is that it encourages replay and additional exploration, increasing exposure to the core concepts and time on task, both of which are correlated with improved learning outcomes [26].

The use of a simulation game itself, rather than more traditional media, has also been observed to have a marked increase on learner self-efficacy (confidence) [27]. This confidence may help learners transfer knowledge gained in the game to greater cyber awareness in everyday life. Similarly, the game employs tiered badges, to provide explicit performance goals within the game. Performance goals are a self-regulatory strategy known to exert a comparatively large learning impact.

2.3 An Active, Adversarial Role for Learners

In the initial scenario we developed, we employed these practices but noted in piloting that participants' interest quickly flagged. The game allowed users to experience various kinds of cyber intrusions, both directly and indirectly, but the participants role was overly passive; they were "waiting for the attack" and had little agency, even though the game was rendered in an interactive, immersive environment.

To attempt to increase engagement and impact, the latest scenario places the trainee in an adversarial role assigned to attack or compromise various systems (within the game environment). As an aggressor, players view potential cyber events from a vantage point less subject to biases; we hypothesize this vantage will result in greater awareness of system vulnerabilities. This change in perspective supports three distinct goals that are directly (and indirectly) designed to promote engagement:

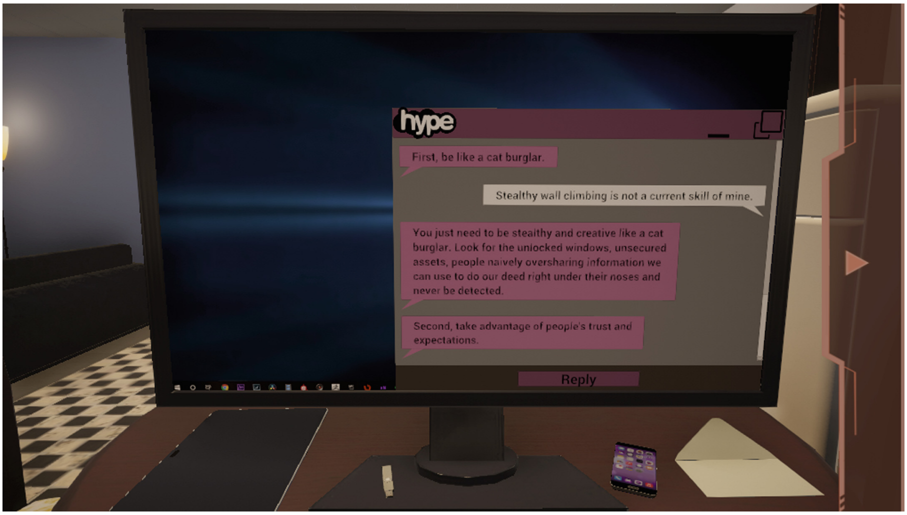
- **Engagement:** Many players are likely to be curious about the possibility of being a cyber attacker and will be surprised by the opportunity to play this role. These elements help engage the player in a subject that is often viewed as boring.
- **Disposition toward action:** A cyber-aware mindset requires pro-active decision and action. Because the player's role is to undertake many actions, this design approach helps associate a propensity for action with a cyber-aware mindset. In the game, the actions are to attack. However, the player is exposed to the ways in which they may be vulnerable in the real-world. Further, they observe differences in the ways various characters they encounter in the game have and have not limited their exposure to potential cyber attacks.
- **Relatability:** The tools and applications introduced in the game are analogs to applications that are likely to be familiar to many players (e.g., online social media platforms). Having players imagine how to exploit applications without introducing specific vectors or vulnerabilities makes the experience relatable to players' everyday activities without being tied to specific tools and vulnerabilities. The intent behind the relatability of the experience is to amplify the cyber-aware mindset around the players' use of such tools outside of the game.

3 The Cyber-RAMPART Training Game

This section overviews the current implementation of the adversary attack scenario. In this scenario, the user engages within a chat application with "Hacker Mo," a virtual character that cajoles the user into executing an attack and then explains, in a guided dialogue, the various options that can be used for an attack.

Figure 1 shows a screenshot from an early part of the dialogue with Hacker Mo. As outlined above, the game is set in a three-dimensional environment. In addition to the monitor, which is where most of the game takes place, there are also some objects in the environment, such as tablet, USB key, and phone. These become relevant in later stages of the scenario.

The orange, arrowed sidebar on the right side of the screen is used to convey detailed information about the concepts Hacker Mo introduces, as well as historical examples. Information in this sidebar "pops out" when Hacker Mo mentions it in the game and the



First, be like a cat burglar.

Stealthy wall climbing is not a current skill of mine.

You just need to be stealthy and creative like a cat burglar. Look for the unlocked windows, unsecured assets, people naively oversharing information we can use to do our deed right under their noses and never be detected.

Second, take advantage of people's trust and expectations.

Fig. 1. Hacker Mo describes the attacker mindset.

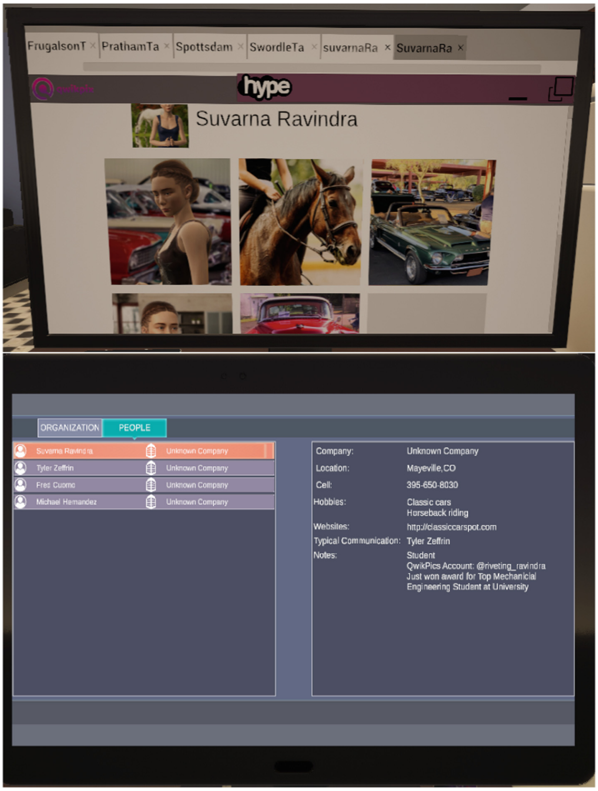
user can review it at any time as well. This mechanic attempts to balance providing a lot of detailed information about cyber attacks to the player, while also minimizing the dynamic, immersive experience of roleplaying as an attacker.

As the scenario progresses, Hacker Mo describes various kinds of ways attacks can be conducted, what kinds of organizations and people might be more or less vulnerable, etc. The second phase of the game involves the player identifying a specific target to attack (an organization) and a particular person associated with that organization. The player makes these choices by conducting a simulation of open-source intelligence gathering, looking at simulated websites, social media sites, and even a phone book to find information.

Figure 2 illustrates an example from the scenario. The top image shows the "quikpix" social media page of a university student. The user can scroll thru the individual posts and glean information about the character. In this case, this person is a student at a local university, likes classic cars, and recently won an award at the university. The user has also determined her cell phone number.

In order to make the game less memory intense and also not require recording information manually, we added a "tablet" that allows the user to readily capture "notes" from the open-source intelligence gathering. In the game, the user clicks on the content of social media and website information and these are automatically added to the correct entries in the notebook. This approach reduces overall learner cognitive load and is designed to help the learner focus on the concepts of cyber attacks rather than the specific information found for each character.

The third and final phase of the scenario involves actually executing an attack. The scenario supports attacks via a phishing email, a text-based attack (vishing), and malware on a USB (sent by mail). When an attack is successful, Hacker Mo turns on a web camera, allowing the user to visualize the impact of the attack on the target (Fig. 3). The success



Suvarna Ravindra

Suvarna Ravindra	Unknown Company
Tyler Zeffrin	Unknown Company
Fred Cuomo	Unknown Company
Michael Hernandez	Unknown Company

Company:	Unknown Company
Location:	Mayeville,CO
Cell:	395-650-8030
Hobbies:	Classic cars Horseback riding
Websites:	http://classiccarspot.com
Typical Communication:	Tyler Zeffrin
Notes:	Student QwikPics Account: @riveting_ravindra Just won award for Top Mechanicial Engineering Student at University

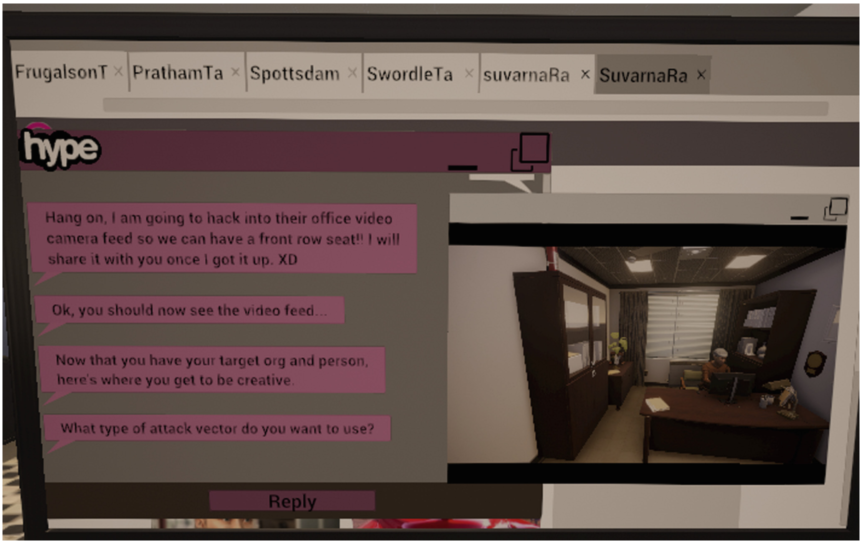
Fig. 2. Gathering open-source intelligence in preparation of an "attack."

of the attack depends on whether the player follows Hacker's Mo guidance in choosing more vulnerable targets as well correctly gathering and using open-source intelligence. For example, for the target illustrated in Fig. 2, a phishing email that focused on "classic cars" or "Congratulations on your recent Mechanical Engineering award" are likely to result in success, while a phishing email about "soccer" (a hobby of another potential target at the university) would fail when sent to this subject.

Two scenarios have been developed for this game to-date and a preliminary evaluation is being undertaken to begin to assess its impact on cyber awareness.

4 Design Alternatives for Increased Engagement

Although initial piloting suggests that the adversarial vantage is helpful and engaging, the training may be perceived as "yet another cyber training exercise," which limits user engagement and thus dampens the potential long-lasting effect on the learner's cyber mindset. In this section, we outline various game-design and adaptation strategies we are currently investigating with goal of enabling still greater engagement and resultant impact. An underlying design philosophy is to align design principles with learner self-regulation functions, so that the game better harnesses the native abilities of players to



Hang on, I am going to hack into their office video camera feed so we can have a front row seat!! I will share it with you once I got it up. XD

Ok, you should now see the video feed...

Now that you have your target org and person, here's where you get to be creative.

What type of attack vector do you want to use?

Fig. 3. A successful attack turns on a webcam.

engage "organically," rather than using artificial or coercive methods common in many computer-based training systems. We focus primarily on intrinsic adaptation (adaptation of content within the game itself). However, intrinsic adaptation introduces the need for additional content authoring, which is expensive and can thus inhibit the use of tailored content. We consider three design alternatives: specialization for player type, demographic personalization, and engagement tailoring.

4.1 Specializing for Player Type

Players like to interact with games in different ways, depending on a variety of factors [28]. Some players may want to explore how a game works; others are motivated by earning badges and maximizing their score, etc. Games that can adapt the way they work to a player's preferred playing style may increase engagement and time spent playing the game [29].

There are a number of frameworks that attempt to categorize and rationalize playing styles for video games. The combination of adapting to both playing style and learning style is still relatively novel, but the ADOPTA framework [30] offers one example. ADOPTA (ADaptive technOlogy-enhanced Platform for eduTAinment) introduces four categories of playing style (Competitor, Dreamer, Logician, and Strategist), which are defined in such a way to be correlated with established learning styles. The developers of ADOTA showed that they could learn to recognize certain features of gameplay according to these learning styles and then adapt gameplay according to the observed playing style, improving engagement for that player. For example, for a "Competitor" in a "gold capture" game they developed, the game increases the speed of movement of various gold pieces (and reward when captured). In contrast, for a "Logician," the adjustment of the degree of difficulty results in more hidden gold pieces and more "puzzles" that must be solved to find the gold. Their results show that adjusting difficulty based on player type improves the subjective experience of gameplay.

One of the advantages of the ADOPTA method is that it can be used to determine player style without the use of questionnaires or other explicit methods which makes the player aware of being "categorized." We envision several ways we could use covert observation of player styles in Cyber-RAMPART. For example, we have observed in piloting that some players enjoy exploring the social media sites somewhat exhaustively, while others, seeking to get to the attack, capture the minimum amount of information. We could adjust the narrative to account for these different styles by encouraging different approaches to open-source intelligence gathering, perhaps using a score and badges for the "Competitor" player to encourage that player type to explore more potential attacks and targets before making a commitment.

4.2 Adaptation Based on Demographic Characteristics

As suggested above, a common complaint of cyber awareness training is that it is somewhat generic and not specific to the organization or individual [15]. We envision the use of player demography to allow the game to customize player experience to contexts and domains relevant to the player.

Potential demographic elements that could be used for customization include the player's age, their position/rank within their organization, and details about their job roles. For example, Hacker Mo could use several different "dialects, somewhat corresponding to age and position. This might result in Mo using text messaging acronyms in conversation much more frequently with younger players than older ones and choosing specific descriptions and word usage mapped to jargon and slang associated with various generational cohorts. Similarly, the social media content and presentation could be adapted to roughly match the age, positions, and job roles of the player. This matching could increase the identification of the player with the potential targets being researched during the open-source intelligence gathering phase. Familiar contexts are likely to both improve learner confidence and attention.

Adapting the scenario based on demographic information is not technically challenging if there is content available to support personalization. However, the content requirements for adaptive learning has proven to be a significant barrier to widespread use in open-ended domains. Rather than hand-create additional content, as we did for the Hacker Mo scenario, we would instead recommend the use of various automated content generation [31] and content repurposing methods to support demographic-based adaptation.

4.3 Engagement Tailoring

Learner engagement has direct corollaries with self-regulatory mechanisms such as attention and persistence [27]. In past work, we have explored how various kinds of passive observation of learner activity can be used as proxies or "markers" to estimate on-going engagement as an experience unfolds [32–34]. Examples of passive observation include assessing the learner's responsiveness to prompts, eye tracking via webcam, and observations of the patterns of mouse movements and hand gestures. Passive observation is less intrusive (and evident) to learners and generally requires little/no additional hardware, making it reasonably inexpensive and easy to deploy.

Via combination of such instrumentation and dynamic content selection, we envision a system capable of producing prompts within the game itself that will encourage sustained engagement and intervene when engagement begins to flag. Consider the conceptual illustration in Fig. 4. As the player participates in the game, the system tracks the estimated level of engagement. When engagement begins to trend toward some minimum arousal threshold, the system introduces an in-game or *intrinsic* prompt such as an unusual comment or unexpected question from Hacker Mo via chat message. For example, Hacker Mo might interrupt a player response by saying, “Hey, you are taking a while here… can we move on?” Intrinsic tailoring (also known as pedagogical experience manipulation) offers the benefit of providing scaffolding and support for the learner without interrupting the immersive experience [35].

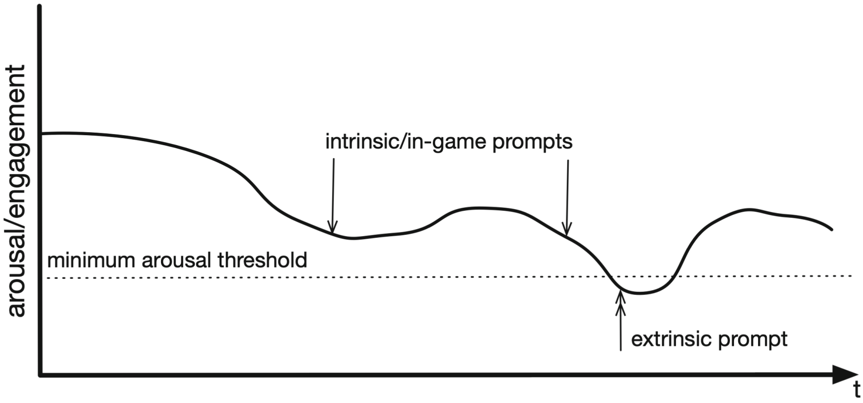


Fig. 4. Tailoring via prompts to sustain engagement.

The intent of these intrinsic prompts is to arrest the falling engagement level, which, in the figure is successful following the initial prompt. As the game progresses, these in-game prompts may lose some power (e.g., the first time Mo surprises a player with a question, it will be a surprise, but less so on the third or fourth use of the same technique). When the intrinsic prompts fail, the game can switch to an extrinsic prompt, such as interrupting the dialogue with Mo to ask the player if they want to continue or take a break.

There are two technical challenges that would need to be addressed to realize this capability in Cyber-RAMPART. First, the level of engagement would need to be estimated, which requires not only the choice of some sensor(s), but also mechanisms for calibrating thresholds for individual players, which may differ substantial from person to person. Second, similar to the previous technique, engagement tailoring also requires additional content authoring. In this case, however, it may be possible to generate prompts and questions somewhat independent of the context at the moment in which they are introduced. This approach would make the authoring requirements straightforward but may be difficult to achieve truly intrinsic prompting with more generic prompting.

5 Conclusions

Effective cyber awareness training is an acute need for today's workforce. Cyber threats are increasing and increasingly calamitous but existing training options commonly are ineffective. In this paper, we introduced an innovative training game that focuses on the development of a cyber mindset by allowing a player to plan and to execute notional examples of various cyber attacks. The attacker perspective offers several advantages that encourage attention and engagement essential for learning, including an engaging and relatable narrative that encourages player action. We also described a number of potential elaborations of the game mechanics to further encourage player engagement and learning.

Acknowledgements. This work was supported by the Office of Naval Research project N68335-18-C-0724 Cyber-RAMPART. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Department of Defense or Office of Naval Research. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon. We thank colleagues and collaborators who have provided insights and operational perspectives in the development of the Cyber-RAMPART including Kelly Neville, Behrooz Mostafavi, Alex Nickels, Larry Flint, Julie Marble, Alice Jackson and Justin Bonny.

References

1. Cortada, J.W.: The Digital Hand: How Computers Changed the Work of American Manufacturing, Transportation, and Retail Industries. Oxford University Press, Oxford (2003)
2. Varol, O., Ferrara, E., Davis, C.A., Menczer, F., Flammini, A.: Online human-bot interactions: detection, estimation, and characterization. In: Proceedings of the Eleventh International AAAI Conference on Web and Social Media (ICWSM 2017). AAAI Press (2017)
3. Schreckinger, B.: How Russia Targets the U.S. Military. Politico (2017)
4. Kettani, H., Wainwright, P.: On the top threats to cyber systems. In: 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT), pp. 175–179 (2019)
5. Howard, P.N., Ganesh, B., Liotsiou, D., Kelly, J., François, C.: The IRA, Social Media and Political Polarization in the United States, 2012–2018. Project on Computational Propaganda, p. 46. Oxford University, Oxford (2018)
6. Adebiaye, R., Alryalat, H., Owusu, T.: Perspectives for cyber-deterrence: a quantitative analysis of cyber threats and attacks on consumers. Int. J. Innov. Res. Sci. Eng. Technol. **5**, 12946–12962 (2016)
7. Suraj, M., Singh, N.K., Tomar, D.S.: Big data analytics of cyber attacks: a review. In: 2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA), pp. 1–7. IEEE (2018)
8. Sumi, F.H., Dutta, L., Sarker, F.: A review on cyberattacks and their preventive measures. Int. J. Cyber Res. Educ. (IJCRE) **1**, 12–29 (2019)

9. Chowdhury, A.: Recent cyber security attacks and their mitigation approaches – an overview. In: Batten, L., Li, G. (eds.) ATIS 2016. CCIS, vol. 651, pp. 54–65. Springer, Singapore (2016). https://doi.org/10.1007/978-981-10-2741-3_5
10. Mezzour, G., Carley, K.M., Carley, L.R.: An empirical study of global malware encounters. In: Proceedings of the 2015 Symposium and Bootcamp on the Science of Security, pp. 1–11 (2015)
11. Thornton-Trump, I.: Malicious attacks and actors: an examination of the modern cyber criminal. EDPACS **57**, 17–23 (2018)
12. Mezzour, G., Carley, L., Carley, K.M.: Global mapping of cyber attacks. SSRN 2729302 (2014)
13. Neville, K., Flint, L., Massey, L., Nickels, A., Medina, J., Bolton, A.: Training to instill a cyber-aware mindset. In: Schmorrow, Dylan D., Fidopiastis, Cali M. (eds.) HCII 2019. LNCS (LNAI), vol. 11580, pp. 299–311. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22419-6_21
14. Amankwa, E., Loock, M., Kritzinger, E.: A conceptual analysis of information security education, information security training and information security awareness definitions. In: The 9th International Conference for Internet Technology and Secured Transactions, London, pp. 248–252. IEEE Press (2014)
15. Aldawood, H., Skinner, G.: Reviewing cyber security social engineering training and awareness programs - pitfalls and ongoing issues. Future Internet **11**, 73 (2019)
16. Ghafir, I., et al.: Security threats to critical infrastructure: the human factor. Supercomputing **74**, 4956–5002 (2018)
17. Hadnagy, C.: Social Engineering: The Art of Human Hacking. Wiley, Hoboken (2010)
18. Caldwell, T.: Making security awareness training work. Comput. Fraud Secur. **2016**, 8–14 (2016)
19. Hendrix, M., Al-Sherbaz, A., Victoria, B.: Game based cyber security training: are serious games suitable for cyber security training? Int. J. Serious Games **3**, 53–61 (2016)
20. McGonigal, J.: Reality Is Broken: Why Games Make Us Better and How They Can Change the World. Penguin Press, New York (2011)
21. De Corte, E.: Transfer as the productive use of acquired knowledge, skills, and motivations. Curr. Dir. Psychol. Sci. **12**, 143–146 (2003)
22. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. J. Inf. Secur. Appl. **22**, 113–122 (2015)
23. Bada, M., Sasse, A., Nurse, J.R.: Cyber security awareness campaigns: why do they fail to change behaviour? In: International Conference on Cyber Security for Sustainable Society, Coventry, UK, pp. 118–131 (2015)
24. Hwang, G.-J., Wu, P.-H., Chen, C.-C., Tu, N.-T.: Effects of an augmented reality-based educational game on students' learning achievements and attitudes in real-world observations. Interact. Learn. Environ. **24**, 1895–1906 (2016)
25. Hamari, J., Shernoff, D.J., Rowe, E., Coller, B., Asbell-Clarke, J., Edwards, T.: Challenging games help students learn: an empirical study on engagement, flow and immersion in game-based learning. Comput. Hum. Behav. **54**, 170–179 (2016)
26. Koedinger, K.R., Booth, J.L., Klahr, D.: Instructional complexity and the science to constrain it. Science **342**, 935–937 (2013)
27. Sitzmann, T., Ely, K.: A meta-analysis of self-regulated learning in work-related training and educational attainment: what we know and where we need to go. Psychol. Bull. **137**, 421–442 (2011)
28. Heeter, C., Winn, B.: Implications of gender, player type and learning strategies for the design of games for learning. In: Kafai, Y., Heeter, C., Denner, J., Sun, J. (eds.) Beyond Barbie and Mortal Kombat: New Perspectives on Gender and Gaming. MIT Press, Cambridge (2008)

29. Heeter, C., Magerko, B., Medler, B., Fitzgerald, J.: Matching game mechanics to player motivation. In: Meaningful Play Conference (2008)
30. Bontchev, B., Vassileva, D., Aleksieva-Petrova, A., Petrov, M.: Playing styles based on experiential learning theory. Comput. Hum. Behav. **85**, 319–328 (2018)
31. Summerville, A., et al.: Procedural content generation via machine learning (PCGML). IEEE Trans. Games **10**, 257–270 (2018)
32. Wearne, A., Wray, R.E.: Exploration of behavioral markers to support adaptive learning. In: Kurosu, M. (ed.) HCI 2018. LNCS, vol. 10903, pp. 355–365. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-91250-9_28
33. Workshop on Brain, Body and Bytes: Psychophysiological User Interaction at CHI 2010, Atlanta, GA (2010)
34. Wray, R.E., Woods, A.: A cognitive systems approach to tailoring learner practice. In: Klenk, M., Laird, J. (eds.) Proceedings of the 2013 Advances in Cognitive Systems Conference, Baltimore, MD (2013)
35. Lane, H.C., Johnson, W.L.: Intelligent tutoring and pedagogical experience manipulation in virtual learning environments. In: Cohn, J., Nicholson, D., Schmorrow, D. (eds.) The PSI Handbook of Virtual Environments for Training and Education, vol. 3. Praeger Security International, Westport (2008)