International Journal of Gaming and Computer-Mediated Simulations
Volume 14 • Issue 1

Engagement and Players’ Intended Behaviors in a Cybersecurity Serious Game

Rana Salameh, Southern Illinois University at Carbondale, USA*

Christian Sebastian Loh, Southern Illinois University at Carbondale, USA

https://orcid.org/0000-0002-6318-3890

ABSTRACT

Serious games have been shown to be effective in engaging end-users for various types of training. However, the research in cybersecurity awareness training with serious games is scarce. The authors are interested in (1) the engagement factors that could predict users’ intended behavior after learning and (2) whether or not playing a game repeatedly can affect engagement. They assessed players’ coping and threat appraisal and measured their multidimensional (i.e., cognitive, affective, behavioral) engagement in cybersecurity awareness. The participants (N=122) in this experiment were randomly assigned to either three or five rounds of gameplay of a commercial cybersecurity awareness serious game. The findings revealed that users’ engagement levels were significantly better sustained through five sessions of gameplay with cognitive (but not affective or behavioral) engagement. Serious game developers should include more activities in the cognitive dimension, rather than the affective or behavioral dimensions to assure high engagement and influence the intended cybersecurity awareness behaviors.

KEYWORDS

Affective Engagement, Behavioral Engagement, Cognitive Engagement, Copying Appraisal, Cybersecurity Awareness, Cybersecurity Intended Behavior, Game-Based Learning, Serious Games, Threat Appraisal

INTRODUCTION

The use of serious games for non-entertainment and ‘serious’ purposes (e.g., education or training) is rather common in today’s learning. Serious games are particularly successful because they make great use of computing technology to enhance inherent interaction features, such as personal communication, narratives, simulations, and just-in-time feedback to players’ in-game choices (Grossard et al., 2017, Baranowski et al., 2016). These games provide a safe and inexpensive platform for learners to experience authentic learning and motivate and help them become more engaged in the learning activities (Ferguson & Colwell, 2018; All et al., 2016; Barnes et al., 2008). Players’ experience and motivation can be enhanced through user-centric authentic activities (e.g., examining objects through exploration, self-discovery, and problem-solving) via a series of scenarios with complex tasks (Serrano-Laguna et al., 2017; Baggio & Beldarrain, 2011). Enjoyable play experiences are key to developing strategic thinking in the learners (Bogost, 2021; Greitzer et al., 2007). Even non-technical audiences (such as minority and female groups) have learned and benefited from using serious games (Poster, 2018; Adams & Makramalla, 2015).

DOI: 10.4018/IJGCMS.313185

*Corresponding Author

Bouvier et al. (2014) defined engagement in serious games as "the willingness to have emotions, affects, and thoughts directed toward and aroused by the mediated activity to achieve a specific objective" (p. 7). When serious game activities connect with the players' perceptual, intellectual, or interactive anticipations, they can impact players' emotions and thoughts. This, in turn, results in the players feeling engaged beyond the activities themselves and continuing to feel engaged even after the activities have ended (Hamari et al., 2016; Alrashidi et al., 2016). In addition, players' information processing abilities can often be enhanced through increased persuasion, attitude change, and awareness (Muhamad & Kim, 2020; Gass & Seiter, 2018). The enhanced information processing abilities make serious games useful in many areas, from a training tool for tactical and operational warfare in the military (Samčović, 2018), to persuading for 'behavioral and/or attitudinal change' in learning. Examples of behavioral change include the promotion of better health (Vlachopoulos & Makri, 2017; Boyle et al., 2016), prevention of diseases (Wiemeyer & Tremper, 2017) and substance abuse (Willmott et al., 2019), and even cybersecurity (Herr & Allen, 2015), which deals with awareness and prevention of fraudulent activities.

The paper proceeds as follows: First, we discuss the motivation and conceptual framework of the study. After that, we describe the data collection methods and research material. Then, present the study's results and findings, and finally, identify the study's limitations.

MOTIVATION

Since cybersecurity (serious) games are created to increase end-user awareness and persuade them to refrain from 'behaviors' that could lead to security threats (Herr & Allen, 2015), an important topic for research would appear to be the influence on behavior and attitude changes from cybersecurity games to increase engagement. Interestingly, literature reviews identified that the studies on cybersecurity game effectiveness remained limited (Bada et al., 2019; Boyle et al., 2016) and that there are problems with many of the training games. Challenges facing these serious games include research gaps from:

- many cybersecurity games focus too heavily on technological information (Mes et al., 2013), which can negatively affect learners' engagement;
- many technical concepts (e.g., cryptography algorithms) discussed are too challenging for the learners and difficult to implement without an information technology background (Galvez et al., 2015), which can negatively impact learners' engagement;
- many earlier studies (before 2017) were not evidence-based (De Bruijn & Janssen, 2017), leading to a gap in research;
- most studies failed to report impacts on learning outcomes because the researchers were not educator-researchers (Alotaibi et al.,2016);
- most studies failed to examine 'training prescription' (i.e., how best to implement training to achieve intended user behaviors); and,
- many studies only investigated user's motivation about cybersecurity threats (Ahmad et al., 2014; Hendrix et al., 2016; Mes et al., 2013) and not the relationship between engagement and the (cybersecurity) game.

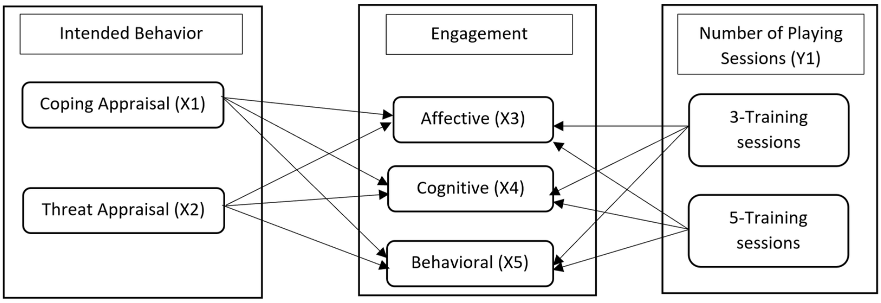
The last point is particularly important because one would expect that serious games that are not as engaging will not be as effective; this means they cannot activate the designed or intended benefits (i.e., change in behaviors and attitudes) as they could in more engaging games. Lacking the research on the relationship between engagement and cybersecurity serious games, no one knows how engaged the players are or what engaged them: contents or gameplay. Furthermore, the literature is not clear on how gameplay affects engagement. For example, many commercial games come with a feature called Game+, where players may replay the same game after completion. Does playing the game more times, so there is repeated exposure to the same/similar content, affect engagement? The literature is unclear in this respect.

The theoretical contribution of this study is to explore a new relationship between concepts (Salamzadeh, 2020). Hence, with a cybersecurity awareness serious game, we investigated the effects of (a) multidimensional engagement levels, and (b) number of gameplay sessions, on the users' intended behaviors (Figure 1). We used two instruments to measure the dependent variables for each participant:

1. The Cybersecurity Intended Behavior (CIBV) scale was used to assess users' PMT factors, specifically, coping appraisal (X1) and threat appraisal (X2) for the intended behaviors (van der Linden, 2014); and,
2. The Multi-Dimension Factors of Engagement (MDFE) was used to assess the affective (X3), cognitive (X4), and behavioral (X5) factors of participants' engagement (Abbasi et al., 2017).

The independent variable in the study is the number of playing sessions (Y_1) assigned for each participant group. We compared (a) the relationships between X_1 and X_2 among X_3, X_4, and X_5, and (b) the relationships for the variable pairings between Y_1 and X_3, X_4, and X_5.

Figure 1. Study conceptual framework model



ENGAGEMENT AND SERIOUS GAMES

Engagement is an important construct in explaining how and why activation of learners' attention and interest during serious games can lead to behavioral and attitudinal change (Qusa & Tarazi, 2021). Furthermore, realistic scenarios are another necessary factor in cybersecurity-based serious games to activate learners' engagement (Flood et al., 2018). Therefore, designers of serious games often use interactive narratives with captivating storylines and realistic scenarios to enhance game engagement and persuade learners towards 'change' (Baslyman & Chiasson, 2016; Nagarajan et al., 2012).

Cybersecurity serious games are designed to make aware to the learners what constitutes cybersecurity threats and what they should, or should not, do to comply with cybersecurity guidelines. An *intended behavior* is the 'desired' behavior to be attained by the end-user. Mainly, it refers to "the motivational factors that influence a given behavior where the stronger the intention to perform the behavior, the more likely the behavior will be performed" (Bada et al., 2015, p. 7). Alqahtani and Kavakli (2020) noted that the primary aim of any cybersecurity awareness program is to strengthen intended behaviors by shaping users' emotions and beliefs. Given the persuasive approach required in cybersecurity awareness training and the persuasive potential of serious games, the combination can form a great approach for delivering cybersecurity awareness instruction (Yasin et al., 2019).

The literature shows three psychological factors that can affect learners' engagement in serious games; namely: (1) affective factors such as emotional response, interest, and enjoyment; (2) cognitive factors, including learning goals, self-regulation, and self-efficacy; and (3) behavioral factors such as effort, participation, and achievement (Alrashidi et al., 2016; Bouvier et al., 2013). Even though many studies in the literature focused on just one engagement factor (i.e., cognitive, affective, or behavioral) to assess the playing experience (for example, Tong et al., 2016; Verkuyl et al., 2022; Galvez et al., 2015), some researchers (O'Brien & Toms, 2010) viewed engagement as a holistic framework that can affect the gameplay experience. For example, a player's knowledge of cybersecurity (cognitive), how strongly they feel about compliance (affective), and if they catch themselves when performing certain actions when using technology (behavior) can all constitute the serious games' (multi-dimensional) 'intended learning outcomes.'

This study applied a multi-dimensional engagement model that combined cognitive, affective, and behavioral factors better to evaluate the learners' cybersecurity gameplay experience. The multi-dimensional engagement model enabled this study to distinguish between (a) the coping appraisal variables, which assess users' motivations to comply with cybersecurity measures, and (b) the threat appraisal variables, which examine users' perception of the vulnerability of the cybersecurity threat and their assessment of the severity of failing to comply with the security measures.

We explore two research questions in this study with a cybersecurity serious game:

1. Do engagement levels affect users' intended behaviors?
2. Does the number of game sessions (i.e., repeated gameplay) affect users' engagement levels?

Null hypotheses:

H_1^o: Engagement levels do not affect users' intended behaviors.
H_2^o: The number of game sessions (i.e., repeated gameplay) does not affect users' engagement levels.

Instead of comparing the group playing the serious game with a control group (which will make this a media comparison), we choose instead to eliminate the need for a control group through a repeated measure design. We explain our rationale in the next section.

MEDIA COMPARISON STUDIES

In instructional design, researchers frequently do not favor "between-group comparisons," called media comparison studies, as they are less meaningful because of confounding variables. In particular, these studies compare one media (or technology, such as serious games) with another media or technology. Examples include face-to-face teaching vs. a control group without instruction; or a traditional classroom vs. a second class playing a serious game).

While media comparison studies are aplenty in the literature, they are 'meaningless' because of confounding variables that make it like comparing 'apples against oranges.' Instructional design researchers have criticized media comparison studies as poor research, as the presence of confounding variables often resulted in findings with "no statistically significant differences" (see Clark, 1994, 2007; Cook et al., 2012; Hastings & Tracey, 2005). Hays (2005) was concerned that these studies could overestimate the digital game-based learning effect when the control group is not engaged in any instructional intervention. Loh and Sheng (2015) dismissed media comparison studies wholeheartedly, citing the approach as one that was "flawed and [which] should be avoided in serious games research" (p. 10). Instead, Loh and Sheng recommended that researchers create two similarly designed serious games to make a 'compatible comparison' (similar to A/B testing).

Hence, to avoid falling into the trap of media comparison, we have opted for a posttest-only, repeated measure design that eliminates the need for a control group. Essentially, a repeated measure design uses the players themselves as an internal control.

MATERIALS AND METHODS

Participants

Since many universities have begun implementing cybersecurity awareness training to comply with external security audits, we reached out to this group of end-users (e.g., students, faculty, staff, and anyone with network access privileges at a university) as potential participants for the study. As a result, a website was created to detail the study's purpose and serve as a link to the online serious game.

We recruited participants through several avenues, such as flyers, emails, word of mouth, the research website, and both locally and internationally. A total of 177 individuals between the ages of 18 and 60, who were fluent in English and able to use a mouse and keyboard to play digital games, signed up for our study via the research website. However, 55 of them did not complete all aspects of the data-collection process (serious games and questionnaires) and were removed from the data set. In total, 122 participants completed all parts of the data-collection process and were included in the final analyses.

A priori power analysis was conducted using G*Power (Faul et al., 2009), based on the following considerations: a medium effect size, 0.80 power, and a 0.05 alpha value (Greenlink, 2015). A sample size of 128 participants was determined by the analysis for the independent samples t-test. Participants were randomly divided into two groups of 64 each. In addition, the 'approved' research period (with developer and IRB) is already over. Unfortunately, we would not be able to collect additional data without violated prior agreements.

After evaluating several commercially available cybersecurity awareness games, we decided that *Info Sentinel*[1] (MAVI Interactive, 2022) best fit the purpose of the studies. *Info Sentinel* was designed to change the end-users' cybersecurity behaviors (for the better) by raising their awareness of cybersecurity threats and vulnerability through real-life scenarios. The study participants assumed the role of a security auditor who was about to inspect a corporate office for cybersecurity violations that could render an organization vulnerable. These violations could include passwords written openly on sticky notes, bootlegged software, confidential documents left in a copier/scanner, and others. Many of the vulnerability and threat scenarios in the game were based on real-life events to reveal blind spots and barriers to the players. The game comprised of the primary module and two supplementary modules. Each module consisted of several vulnerabilities and threat categories that needed to be detected by the player (Table 1).

Table 1. Vulnerabilities and threats categories in Info Sentinel

Sentinel Office Security: (Tutorial + Trainings 1, 2, and 3) 1. Inadequate protection of sensitive data, 2. Unlocked or unsecured cabinets, drawers and storage areas containing sensitive information, 3. Noncompliant destruction of sensitive documents, 4. Risk of intrusion into facilities or a computer network, and 5. Unprotected business hardware.
Sentinel Email Security (Training 4) 1. Phishing, 2. Inappropriate use of email accounts, 3. Insecure transfer of confidential information, 4. Spam or unsolicited email, and 5. "This email is authentic."
Sentinel Social Media Security (Training 5) 1. Disclosure of sensitive information, 2. Risky solicitation or invitation, 3. Insufficient configuration of privacy settings, and 4. Inappropriate communication

The players' scores in *Info Sentinel* were determined by their ability to spot violations in the game environment and correctly identify the threat categories for those violations. Distinctions were made among (1) correctly identifying the violation; (2) identifying the violation but mis-categorizing it; and, (3) misidentifying the violation altogether. The training was deemed complete when participants encountered at least one violation for each category during each game session. The 'success' criterion was a 70% correct identification rate. After gameplay was completed, the game logs were compiled and downloaded for analysis, with access provided by the developer.

Instrument/Measures

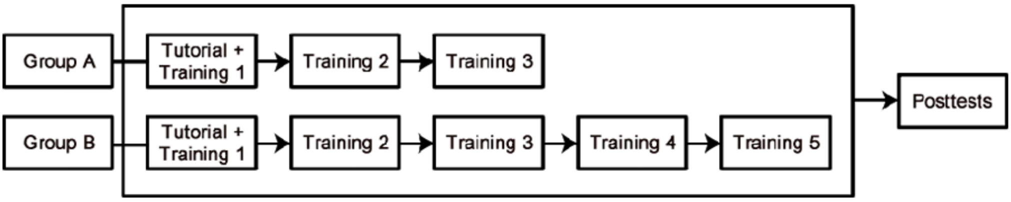
Three surveys were used to obtain users' data for the multi-dimension engagement model. The first was a questionnaire on players' background and demographic information. The second was the MDFE (Abbasi et al., 2016) that used a five-point Likert scale to assess the participants' cognitive, affective, and behavioral factors of engagement. The Cronbach's alphas for the six subscales of MDFE were calculated and deemed high enough to confirm the internal consistency of the instrument: (1) observation (α = .90), (2) conscious attention (α = .90), (3) dedication (α = .92), (4) enthusiasm (α = .93), (5) interaction (α = .89), and (6) social connection (α = .91). The purpose of the MDFE was to assess which factors (viz., cognitive, affective, and/or behavioral) affected the players' engagement levels during gameplay.

The third instrument was the CIBV (van der Linden, 2014). Participants were asked to respond to statements on the CIBV questionnaire regarding their attitudes and intended behaviors on cybersecurity issues after training with the serious game. The Cronbach's alphas for the Coping appraisal (α = .61) and Threat appraisal (α = .82) were likewise high enough to confirm the internal consistency of this instrument (Pallant, 2001). The CIBV was to assess changes in the intended cybersecurity behaviors after gameplay and whether or not playing the game helped change players' thinking.

Data Collection

The participants were randomly assigned to either Group A (three rounds of gameplay) or Group B (five rounds of gameplay), as shown in Figure 2. This arrangement allowed an evaluation of the effects of multiple gameplay sessions on players' engagement levels that was aligned with the serious game design. The main game module constituted the three training sessions, which served as the minimum training (for Group A), whereas the two extra modules together with the main module, constituted the full game, with five training sessions (for Group B).

Figure 2. Playing sessions for two groups



To create the repeated measure design, Group A played Training #1, #2, and #3, lasting approximately 40 minutes. Group B played Training #1, #2, #3, #4, and #5, lasting approximately 60 minutes. Participants were then asked to complete the MDFE and the CIBV questionnaires, which concluded the data collection for the study. We downloaded game logs for analysis.

Data Analysis

Statistical analyses were conducted using IBM SPSS (v. 25). We conducted multiple regression analyses after meeting the conditions needed to satisfy the regression analysis assumptions to answer the first research question. We included the MDFE subscales as the independent variables and the subscales for the CIBV as the dependent variables. We then performed two multiple regression analyses for each dependent variable and applied a Bonferroni adjustment (α-level = .025) to control the overall Type-I error rate.

To address the second research question, we analyzed the relationship between players' engagement levels and intended behaviors in a cybersecurity serious game using an independent-samples t-test. First, we compared the differences in the scores for the engagement levels of the two groups using the number of sessions played (three or five) as the grouping variable and the subscale scores for the MDFE as the dependent variables. Second, since multiple independent-samples t-tests were required for each subscale, the Bonferroni adjustment (α-level = .025) was applied to control the overall Type-I error. An independent-samples t-test followed this to determine which group had a higher MDFE subscale score.

RESULTS AND FINDINGS

Before conducting multiple regression analysis, box plots and standardized residual statistics were used to identify outliers, the Q-Q plot to assess whether variables were normally distributed, the normal probability plot (P-P) to check for systematic biases, and a scatter plot to test for homoscedasticity and the linearity of the relationship between variables and each of the predictors. Finally, multicollinearity was assessed using the correlation matrix, variation inflation factors (VIF), and tolerance values. Based on our assessment of the plots and values, we progressed with the analysis as the main regression analysis assumptions were met.

Multiple regression analyses were conducted for each dependent variable subscale, while t-tests were used to compare the means of the two groups (three vs. five training sessions) and determine whether playing more sessions (i.e., receiving more serious game training) would affect end-users' engagement levels.

Demographic and Descriptive Analyses

The pre-knowledge survey was designed by Whisper Information Security Awareness Quiz and has been adopted by many cybersecurity awareness firms (Webroot, Inc., social engineering). The assessment tool contains seven true/false questions and seven multiple-choice questions. These descriptive statistics represent the mean scores of the participants based on their pre-knowledge initial assessment. Pre-knowledge scores ranged from 7 to 0. The descriptive analysis indicated that the participants did well in the pre-knowledge survey based on the mean (5.40) and standard deviation (1.225). Table 2 shows the distribution of pre-knowledge scores, and the ratio of men to women was: 56.6% and 5.551 (male), vs. 43.4% and 5.226 (female).

Also, in Table 2, the 18-28 age group (5,478) had the highest percentage (54,9%). The 29-34 age group came in second with 5.385 pre-knowledge (21.3%). The 35-40 age group were 15.6% of the

Table 2. Demographic data frequencies, percentages, and means for the participants' age, gender, with the pre-knowledge mean

	Frequency	Percentage	Pre-knowledge Mean	SD
Gender	53	43.4%	5.226	1.339
Female	69	56.6%	5.551	1.118
Male				
Age	67	54.9%	5.478	1.078
18-28 years	26	21.3%	5.385	1.061
29-34	19	15.6%	4.895	1.791
35-40	5	4.1%	6.400	.894
41-49	5	4.1%	5.600	1.140
Over 49				

population with a pre-knowledge mean of 4.895. Age groups 41-49 and over 49 made up 4.1% of the sample. Both age groups had a pre-knowledge mean of 6.400 and 5.600, respectively.

Multiple Linear Regression Analysis

As shown in Table 3, about one-third of the variance in the coping (32%) and threat (33%) appraisal models can be explained by the multi-dimensional engagement factors. The R^2 values for both the coping and threat appraisal models are similarly strong.

Table 3. Standard regression model summary with regression significance values

Model	R	R^2	Adjusted R^2
1	.57	.32	.31
2	.57	.33	.31

1. Dependent variable: Coping appraisal. Predictors: (Constant), Cognitive, Affective, and Behavior. 2. Dependent variable: Threat appraisal. Predictors: (Constant), Cognitive, Affective, and Behavior.

The analysis of variance (ANOVA) results shows that both regression models were statistically significant at the Bonferroni-adjusted α-level of .025 (Tables 4 and 5). In particular, the coping appraisal value is $F(3,118) = 18.67$, $p < .001$, while the threat appraisal value is $F(3,118) = 19.06$, $p < .001$. The findings indicate that the multi-dimensional engagement levels (cognitive, affective, and behavioral engagement) play significant roles in predicting the intended cybersecurity behavioral factors (threat and coping appraisal) among the users.

Table 4. One-way ANOVA results comparing mean cognitive, affective, and behavioral engagement with coping appraisal

Model	Sum of Squares	df	Mean Square	F	p-value
Regression	8.01	3	2.67	18.67	.000
Residual	16.87	118	0.14		

Dependent variable: Coping appraisal. Predictors: (Constant), Behavior, Cognitive, and Affective.

Table 5. One-way ANOVA results comparing mean cognitive, affective, and behavioral engagement with threat appraisal

Model	Sum of Squares	df	Mean Square	F	p-value
Regression	12.85	3	4.28	19.06	.000
Residual	26.51	118	0.23		

Dependent variable: Threat appraisal. Predictors: (Constant), Behavior, Cognitive, and Affective.

PREDICTING END-USERS' INTENDED BEHAVIORS

The individual regression coefficients were used to test whether each predictor (cognitive, affective, and behavior) was significant in predicting the end-users' intended behavior (coping and threat appraisal). The β-value is measured in standard deviations (SD), where the higher the β-value is, the greater the impact of the predictor variable on the criterion variable.

Coping Appraisal

Cognitive engagement is a statistically significant predictor of end-users' coping appraisal ($\beta_{cognitive} = .68$, $t = 4.14$, $p < .001$; see Table 6). The β-value of 0.68 indicates that coping appraisal would increase by .68 SD for every one SD increase in cognitive engagement after holding the other predictor variables constant. Neither affective nor behavioral engagement are significant predictors of coping appraisal. The regression equation for the effect of the multi-dimensional engagement factors on the coping appraisal is, therefore:

Coping Appraisal = 2.60 +.42 × Cognitive – 0.05 × Affective – 0.02 × Behavior

Table 6. Regression coefficients with coping appraisal as the dependent variable

Model	Understudied Coefficient B	Std. Error	Standardized Coefficients Beta (B)	t	p-value
Constant	2.60	.20		13.18	.000
Cognitive	.42	.10	.68	4.14	.000
Affective	−.05	.11	−.09	−.46	.65
Behavior	−.02	.08	−.04	−.28	.78

Dependent variable: Coping appraisal

Threat Appraisal

Cognitive engagement is also a statistically significant predictor of end-users' threat appraisal factor of intended behaviors ($\beta = .37$, $t = 2.24$, $p = .03$; see Table 7). Similarly, neither the affective nor behavioral engagement levels are statistically significant in predicting threat appraisal. The regression equation for the effect of the multi-dimensional engagement factors on threat appraisal is, therefore:

Threat Appraisal = 2.52 + .28 × Cognitive + .09 × Affective + .07 × Behavior

These findings indicate that cognitive engagement alone (but not affective or behavioral engagement) can partially predict the coping and threat appraisal factors in users' intended behaviors with cybersecurity serious games.

Table 7. Regression coefficients with threat appraisal as the dependent variable

Model	Understudied Coefficient B	Std. Error	Standardized Coefficients Beta (B)	T	p-value
Constant	2.52	.25		10.19	.000
Cognitive	.28	.13	.37	2.24	.03
Affective	.09	.13	.13	.66	.51
Behavior	.07	.10	.10	.71	.48

Dependent variable: Threat appraisal

Correlation Between Dependent and Independent Variables

Table 8 shows that both the coping and threat appraisals are significantly correlated with all three levels of engagement: cognitive engagement, affective engagement, and behavioral engagement. The range of r-values (.41 to .56) reveal a moderately strong correlation between appraisal and

Table 8. Bivariate correlations for the criteria and predictor variables

	Cognitive Engagement	Affective Engagement	Behavioral Engagement	p-value
Threat appraisal	.56	.54	.50	.000
Coping appraisal	.56	.47	.41	.000

Note: Significance tests are 2-tailed.

multi-dimensional engagement variables. The bivariate relationships between the intended behavior variables (as predicators) and each multi-dimensional engagement level (as predictors) show that each independent variable alone is significant in predicting the dependent variables—without considering the effects of other independent variables.

Does Repetition Affect Engagement?

Next, we will answer the following research question: Does playing cybersecurity serious games over multiple sessions affect engagement? We conducted an independent-samples t-test to determine whether there are statistically significant differences in the engagement levels (cognitive, affective, and behavior) between Group A and Group B that underwent three and five training sessions of gameplay, respectively.

Due to adding up the alpha levels of Bonferroni adjustments, all the p-values for the engagement levels were greater than .30 (Table 9), meaning that we cannot reject the null hypothesis of equal variance, and we assume that Group A and Group B (each with an equal number of participants, $n = 61$) have equal variance. Table 10 shows the mean (), SD, and independent-samples t-test results for each of the three engagement levels for Groups A and B. There are statistically significant differences between the two groups at all engagement levels (cognitive, affective, and behavioral).

Table 9. Levene's test for the equality of variances

	F	p-value	Reject null hypothesis
Cognitive	.88	.35	No
Affective	.10	.75	No
Behavior	.05	.82	No

Table 10. Means and standard deviations and independent-samples t-tests of the engagement levels for Groups A and B with equal variance assumed

	Group		SD	t-statistic	df	p-value
Cognitive	A	3.80	.69	−4.08	120	.000
	B	4.31	.70			
Affective	A	3.57	.84	−4.43	120	.000
	B	4.21	.76			
Behavior	A	3.49	.77	−4.19	120	.000
	B	4.08	.79			

Given the statistically significant differences between Groups A and B, the null hypothesis for the second research question can be safely rejected. Thus, the findings suggest a difference between the means of the two groups assigned to either three or five training sessions. In other words, the multi-dimensional engagement levels when playing three sessions are not the same as those when playing five sessions.

When considering the descriptive analysis in Table 10, the results show that the players in Group B, with five training sessions, were more engaged in all three levels (i.e., cognitive, affective, and behavior) than the players in Group A, with three training sessions. The greater the number of training sessions, the higher the engagement level among the players.

DISCUSSION OF MAJOR FINDINGS

Demographic and Descriptive Analysis

The participants included 69 males (56%) and 53 females (44%). The lower participation by females could be related to a lack of previous experience in digital gameplay by women (Grevelink, 2015). Younger participants showed greater interest in the study. This observation might be explained by youth having more digital gaming experience than older participants (Ferguson & Colwell, 2018). This finding was consistent with Galgouranas and Xinogalos' (2018) work, showing over 97% of young people preferred playing digital games. Final analysis revealed that the participants had good knowledge of cybersecurity subject matter, especially in social engineering. Females and males aged 41–49 scored the highest when compared to other age groups; however, no significant differences were found between gender and age groups: $t_{gender}(120) = -1.456$, $p = .148$, and $t_{age}(120) = 0.375$, $p = .709$.

Findings of Predictor Variables

Cognitive Engagement

The MDFE instrument was used to measure the effects of cognitive engagement in this study. Based on regression analysis, both the threat appraisals and the coping were significantly predicted by cognitive engagement. In this study, cognitive predictors were partially significant in the model and other predictors (e.g., affective, behavior), but when the predictors were added together, cognitive was significantly greater than affective and behavior (Y. Sheng, personal communication, April 2019). The bivariate correlations (Table 8) indicate that each predictor by itself is moderately and significantly correlated with the intended behavior variables. In other words, there is a degree of overlap between predictor variables, in which affective or behavioral engagement is absorbed by cognitive (Azen & Budescu, 2003).

As a whole, Sentinel Office Security's cognitive engagement activities (including the challenge, graphics, and attainable goals) affected users' intended behavior. Players explored an office to identify cybersecurity threats and vulnerabilities in the game. During each session, several threat categories were hidden in different spots (e.g., inside a file cabinet, under the mouse pad, and in drawers). Therefore, players remained cognitively engaged in identifying and categorizing potential threats. Consequently, cognitive features offered players a mechanism to enhance processing, decision making, and learning (Lamb, 2013; Lamb et al., 2017).

Affective Engagement

The bivariate correlation in Table 8 shows that affective engagement (as a predictor) is moderately and significantly correlated with the desired behaviors variables, with a degree of overlap between engagement levels (Darlington & Hayes, 2017; Azen & Budescu, 2003). Because of their overlap, it is difficult to distinguish between them (Y. Sheng, personal communication, April 2019). Two causes may explain why cognitive engagement outweighed affective engagement. First, the number of training sessions (i.e., total training time) might not have been sufficient to affect participants' emotions. Byun (2012) and Loh and Sheng (2015) concluded that short playing times (less than 10 minutes) and few sessions were insufficient to affect engagement or flow. Short playing times (with only a few sessions) also did not reflect real-world practices since most players spend hours game playing to satisfy their engagement and motivation needs in real life.

Second, the MDEF instrument might not have detected and measured affective engagement. Bouvier et al. (2014) defined self-reports as providing first-person views and data to explain players' emotions, intentions, and decisions during the learning experience. However, the method is not without limitations, as Azevedo (2015) identified. These limitations included the inability to explain the "sequences of actions" chosen by players and record what players thought about during games. According to Kim et al. (2018) tracking instruments (e.g., eye trackers and heart monitors) could track affective factors and detect players' psychophysiological responses during gameplay. A second approach is the "course of actions" methodology developed specifically for serious games analytics by Loh et al. (2016).

Even though affective engagement was not a significant predictor of the end-users' intended behavior in this study, one should still consider affective engagement factors for effective (cybersecurity) training. Those players who achieved affective engagement (i.e., self-efficacy, personal reflection) became fully immersed in the game - an essential step in gaining persuasive experiences related to cybersecurity tasks and future goals (Lu & Lien, 2020). Therefore, the factors that might have influenced affective engagement need further investigation.

Behavior Engagement

In terms of bivariate correlation (in Table 8), there is a certain degree of overlap between the multi-dimensions of engagement, which makes cognitive engagement more significant than behavioral engagement. (Y. Sheng, personal communication, April 2019). When testing users' intended behaviors as combined engagement levels (for both the coping and threat appraisals), behavioral engagement was not found to be a significant predictor. There are two possible causes for this observation. First, the MDFE behavior engagement questions measure social interaction preferences. Sentinel Office Security was a one-player game without social interaction or teamwork. Therefore, certain players might not have enjoyed the social interaction and may not have been satisfied. Schoenau-Fog and Bjoerner (2012) argued that playing with others fosters social interaction. Participants in Schoenau-Fog's (2011) study expressed a sense of involvement with other players during online or console games with multiple players. The playing experience can become an objective in and of itself through multiplayer games. Schoenau-Fog (2011) suggests that players may keep playing and/or returning to the game for social interaction.

Second, the MDEF questionnaire was not designed to track player behavior (decision-making, cognitive activity, or problem-solving). Instead, player performances were captured by tracking their in-game actions and navigational patterns. Before achieving immersion and the self-determination elements (autonomy, self-efficacy, relatedness), players had to become involved in the games (Hallifax et al., 2021). Game constructs and contextual environments (e.g., distractions) can cause players to adjust their playing behaviors to gain control of the situation (Cheng & Tsai, 2020). By tracking players' interactions over time (Time_on_Task) and effort (Accuracy_Rate), we can gain valuable insight into players' interactions, behaviors, and performance in games. Serious games provide 'in-process' assessment tools that can track learning progress. Currently, serious games are facilitated by software that collects gameplay data and transmits it to remote servers (i.e., clouds), stored in a rational database (Loh, 2013). Researchers could cluster and predict players' behaviors using advanced data mining techniques.

We will need more investigation to better understand the factors that might have influenced behavioral engagement. Future researchers might apply a behavioral engagement assessment to track players' performances (i.e., decision-making skills, cognitive abilities, and reasoning patterns). Improved metrics reflecting the unique features of cybersecurity serious games (rather than the generic metrics from other science fields) are required to meet this objective (Loh, 2015). One potential methodology is the "course of actions" process (Loh et al., 2016) that was specifically aimed at serious games analytics research.

The Number of Assigned Training Sessions

Learning how end-user engagement levels change over time instead of over a single session can assist practitioners in prescribing and implementing cybersecurity training. An independent sample t-test was used to examine the statistical differences in engagement between unrelated groups in this study. Groups A and B received three and five training sessions, respectively. The t-test revealed a significantly different engagement pattern between the two groups (cognitive, affective, and behavioral).

The descriptive analysis in Table 10 shows that Group B had more engagement in the three engagement levels (cognitive, affective, and behavioral) than Group A with three training sessions. Participants' engagement level increased with more training sessions assigned. Those players who reached an optimal experience, which satisfied personal goals effectively, continued to play digital games, Choi and Kim (2004) found. In the t-test and based on the definitions of each engagement level, players who received more training sessions expressed that the cybersecurity game helped to improve their observation skills, raise their level of attention (cognitive engagement), improve their level of enthusiasm (affective engagement), and increase their social connections (behavior engagement). However, since the t-test was a non-directional t-test, the researcher could not generalize the results to the rest of the population. Further investigation is needed to identify the factors contributing to this outcome.

Additionally, repeating tasks over time maintains cognitive familiarity and influences the level of automaticity to improve performance (Landers et al., 2017). In repeated training sessions, a novice trainee can gain knowledge and skills to become proficient and competent. Training requires deliberate practice to attain expertise (Loh & Li, 2016). Deliberate practice effect/phenomenon is also widely documented in the expertise literature (Macnamara & Maitra, 2019; Fadde, 2012).

Few researchers specified how frequently end-users should receive cybersecurity training or the appropriate number of training sessions. Leaders of the Information Sharing and Analysis Organization (ISAOs, 2019) have recommended providing ongoing training for systems' end-users because cybercriminals changed tactics and new threats emerge daily. Leaders should implement periodic security training sessions that include information on the latest phishing and social engineering attacks.

CONCLUSION

Cybersecurity serious games (and game-based training) are populated with engagement and motivation features that can positively contribute to the learning process. We, therefore, expect a cybersecurity serious game to affect users' intended behaviors at all levels of engagement (cognitive, affective, and behavioral). However, the findings in this study showed that only cognitive engagement, but not affective and behavioral engagement, is a statistically significant predictor of users' intended behaviors. We suspect this has to do with the limitations of the self-reported instrument, which we discuss in the next section.

Moreover, this study showed a performance difference between the groups that were prescribed a different number of training sessions. Prescription is an important aspect of instructional technology research; in other words, the implementation process of *prescribing* the training is an important key to making the training effective.

Limitations

We believe that the self-reported instruments used in this study may have resulted in several limitations. First, self-reported data has an inherent validity risk since the responses completely depended on the veracity of the participants involved. While we tried to ensure an adequate sample size (determined through G*Power) to establish an adequate power and effect size, any generalization of the findings should be limited to the size of the population. The convenience and purposive sampling may also limit the external validity of the findings. Future research could expand on the current study by duplicating the research with different populations, samples, and contexts.

We suspect that the self-reported instrument may not be sensitive enough to "detect the signals" in this study, specifically, the affective and behavioral engagement generated through playing Sentinel

Office Security (Parry et al., 2021). Loh and Sheng (2014) recommended 1–2 hours per session as an appropriate playtime for serious games research; this contrasts with many studies in the literature that report only 15–30 minutes of gameplay. In this study, Sentinel Office Security can be completed in under an hour due to its setting in an enclosed office. While the play duration is not too short (as with 15–30-minute games), it still fell short of the recommended timeframe of one to two hours. Hence, it is possible that the game may not be long enough to generate the range of affective and behavioral engagement needed for the instrument or that the self-reported instrument may not be sensitive enough to detect the 'weaker 'engagement signals produced in less than one hour of gameplay. In other words, the under 60-minute playtime may have contributed to a weaker signal; therefore, the effects may not be well detected by the self-reported instrument.

Affective and behavioral engagement have both been proposed as crucial factors for learning with serious games. However, this study found that only cognitive engagement, but not affective or behavioral engagement, is a significant predictor of user-intended behavior. One explanation is that the self-reported instrument may have been weak at detecting the signals of affective and behavioral engagement. A better instrument or alternative data-collection methods may be needed to detect the weaker signals properly. For example, researchers may consider employing psychophysiological instruments, such as eye trackers, heart-rate monitors, and facial (emotion) recognition software to better measure affective data. Similarly, automated user-tracking techniques, such as telemetry (Zoeller, 2013) and Information Trails (Loh and Sheng, 2015), maybe more appropriately used to trace players' courses of action in serious games for behavioral engagement analysis.

Suggestions for Future Research

This study indicates that it may be easier to reach younger college males (who showed the greatest interest in the games) than students of other age groups and females using serious games as the instructional tool for cybersecurity training. Practitioners and trainees might use this finding to implement future cybersecurity training, including targeting younger males for initial cybersecurity rollouts. However, while 177 participants indicated their interest in participating in the study, only 122 (68.9%) completed the training successfully. This completion rate means that approximately 30% of the students did not follow through, which may have difficulty attracting and enrolling users who are less motivated in cybersecurity training, even when the training is offered in the format of a serious game.

Incorporating affective engagement (i.e., self-efficacy and personal reflection) into the design of serious games is a much harder task than doing so for cognitive or behavioral engagement. Since affective engagement was also harder to detect in short(er) playing durations, a future study may need to prescribe longer or more training sessions to detect or amplify the weak(er) signal. It is also difficult to assess affective engagement using a self-reported instrument. Game designers would also do well to include cognitive-engagement activities and tasks in future cybersecurity serious games to encourage learning and improve learning outcomes.

Even though behavioral engagement was also an important influencing factor for ensuring players' involvement in activities, this study could not find any evidence to support behavioral engagement as a significant predictor of user-intended behaviors in a cybersecurity serious game. In a future study, designers of cybersecurity serious games may consider adding multiplayer experiences and/or teamwork activities to cater to or satisfy players' sense of autonomy and relatedness, a prerequisite for behavioral engagement. It is possible that the self-reported instrument in this study may have impeded the (weak) signal of behavioral engagement. Rather than reusing generic metrics from other scientific fields to explain the unique features of cybersecurity serious games, it would be better to create novel and improved serious game analytics to cluster players' performances and even identify learners for remediation or (re)training (Loh et al., 2015).

The multifaceted nature of engagement, cognitive, affective, and behavioral, provides a comprehensive understanding of the learning process rather than just a single facet. These factors are not isolated processes; rather, they dynamically overlap and are interrelated. In this study, cognitive engagement absorbed the effect of affective and behavioral factors. The self-reported analysis showed that end-users' engagement levels fluctuated over multiple playing sessions. Players in Group B (who underwent more training sessions) showed greater engagement levels, heightening their observational skills and increasing their conscious attention to the innovative cybersecurity scenarios.

Serious games that can attract players to engage in additional play sessions can satisfy the players' engagement needs, be it cognitive, affective, or behavioral. More serious gameplay sessions not only engage and immerse players in the training but could also increase the "time-on-task" of the players in cybersecurity training, which would help master the subject matter and achieve automaticity. Knowing how often to prescribe training and the length of instructions included in serious games training could further save organizations time and resources, especially because serious games can be costly to produce.

This researcher concluded that the number of training sessions could influence engagement levels. However, more investigation is necessary to reveal the factors or variables that might affect this influence. This limitation represented a viable approach for future studies. Moreover, this researcher did not collect enough demographic data on the participants to study these questions effectively. Future researchers could pair the multi-dimensional engagement model with deep demographic profiles to explore how the interface characteristics of digital games might interact with individual differences. Especially noteworthy is the finding that cognitive, affective, and behavioral dimensions were significantly and moderately correlated in this study. Future research should investigate whether this is specific to the self-reported measures or the cybersecurity context.

The Sentinel Office Security along with Sentinel Email Security and Sentinel Social Media modules were used to present the social engineering threat issues. However, future researchers may consider other serious games with different scenarios and strategies (i.e., defense and offensive strategies and attacker centricity) to present more complex and subtle information security issues, which may target advanced computer security students or information security decision-makers (i.e., cybersecurity while traveling, password protection, and safeguarding data).

More Research About Engagement (and Not Motivation)

Our final recommendation is to divert the focus of future research to attend to engagement in serious games (compared to the past focus on motivation). This aligns with Marcum's (1999) proposal that engagement would be a more appropriate theory for performance improvement than motivation theory, particularly in training. Similarly, Merrill (2013) also advocated that instructional design should be aimed at becoming more effective, efficient, and *engaging*. While engagement is often regarded as closely related to (high) motivation, separating it from motivation theory, as Ge and Ifenthaler (2018) suggested, certainly seems more appropriate for future research with serious games (as a type of instruction). The larger question would be: Could engagement be systematically implemented to change how instructional design occurs in the future, especially in a new era where games, simulations, and virtual and augmented realities thrive? Moreover, this study showed a performance difference between the groups prescribed different numbers of training sessions.

Prescription is indeed an important aspect of instructional technology research. In other words, *how* to prescribe the training is an important key to making the training effective. When prescribing cybersecurity training, it is recommended that more training sessions be included by providing ongoing training for systems' end-users, since cybercriminals are constantly changing tactics, and new threats are emerging almost daily. We have made several recommendations for future studies to incorporate data-analysis techniques to understand participants' interaction and behavior in gameplay. Incorporating analytical methodologies and processes into cybersecurity training using serious games for detailed performance measurement would seem to be a wise next step.

CONFLICT OF INTEREST

The authors of this publication declare there is no conflict of interest.

REFERENCES

Abbasi, A. Z., Ting, D. H., & Hlavacs, H. (2017). Engagement in games: Developing an instrument to measure consumer videogame engagement and its validation. *International Journal of Computer Games Technology*, *7363925*, 1–10. Advance online publication. doi:10.1155/2017/7363925

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1), 5–14. doi:10.22215/timreview/861

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*(2), 357–370. doi:10.1007/s10845-012-0683-0

All, A., Castellar, E. P. N., & Van Looy, J. (2016). Assessing the effectiveness of digital game-based learning: Best practices. *Computers & Education*, *92*, 90–103. doi:10.1016/j.compedu.2015.10.007

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *International Journal for Information Security Research*, *6*(2), 660–666. doi:10.20533/ijisr.2042.4639.2016.0076

Alrashidi, O., Phan, H. P., & Ngu, B. H. (2016). academic engagement: An overview of its definitions, dimensions, and major conceptualizations. *International Education Studies*, *9*(12), 41–52. doi:10.5539/ies.v9n12p41

Alqahtani, H., & Kavakli, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information (Basel)*, *11*(2), 121–125. doi:10.3390/info11020121

Azen, R., & Budescu, D. V. (2003). The dominance analysis approach for comparing predictors in multiple regression. *Psychological Methods*, *8*(2), 129–148. doi:10.1037/1082-989X.8.2.129 PMID:12924811

Azevedo, R. (2015). Defining and measuring engagement and learning in science: Conceptual, theoretical, methodological, and analytical issues. *Educational Psychologist*, *50*(1), 84–94. doi:10.1080/00461520.2015.1004069

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behavior? *Proceedings of the International Conference on Cyber Security for Sustainable Society*.

BadaM.SasseA.NurseJ. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? https://arxiv.org/abs/1901.02672

Baggio, B., & Beldarrain, B. (2011). *Anonymity and learning in digitally mediated communications: Authenticity and Trust in Cyber Education*. IGI Global. doi:10.4018/978-1-60960-543-8

Baranowski, T., Blumberg, F., Buday, R., DeSmet, A., Fiellin, L., Green, S., Kato, P., Lu, A., Maloney, A., Mellecker, R., Morrill, B. A., Peng, W., Shegog, R., Simons, M., Staiano, A. E., Thompson, D., & Young, K. (2016). Games for health for children—Current status and needed research. *Games for Health Journal*, *16*(5), 1–12. doi:10.1089/g4h.2015.0026 PMID:26262772

Barnes, T., Powell, E., & Chaffin, A., & Lipford, H. (2008). Game2Learn. *Proceedings of the 3rd International Conference on Game Development in Computer Science Education - GDCSE '08*. doi:10.1145/1463673.1463674

Baslyman, M., & Chiasson, S. (2016). Smells Phishy? An educational game about online phishing scams. *2016 APWG Symposium on Electronic Crime Research (ECrime)*. doi:10.1109/ECRIME.2016.7487946

Bogost, I. (2021). Persuasive games, a decade later. In T. La Hera, J. Jansz, J. Raessens, & B. Schouten (Eds.), Persuasive Gaming in Context (pp. 29-40). Scienceopen.com. doi:10.5117/9789463728805_ch02

Boyle, E. A., Hainey, T., Connolly, T. M., Gray, G., Earp, J., Ott, M., & Pereira, J. (2016). An update to the systematic literature review of empirical evidence of the impacts and outcomes of computer games and serious games. *Computers & Education*, *94*, 178–192. doi:10.1016/j.compedu.2015.11.003

Bouvier, P., Lavoué, E., Sehaba, K., & George, S. (2013). Identifying learner's engagement in learning games—A qualitative approach based on learner's traces of interaction. In O. Foley, M. T. Restivo, J. O. Uhomoibhi, & M. Helfert (Eds.), *Proceedings of the 5th International Conference on Computer Supported Education, SciTePress* (pp. 339–350). Retrieved from https://hal.archives-ouvertes.fr/hal-00854579

Bouvier, P., Lavoué, E., & Sehaba, K. (2014). A trace-based approach to identifying user' engagement and qualifying their engaged-behaviors in interactive systems: Application to a social game. *User Modeling and User-Adapted Interaction*, *24*(5), 413–445. doi:10.1007/s11257-014-9150-2

Byun, J. (2012). *Effects of character voice-over on players' engagement in a digital role-playing game environment* (UMI No. 552895) [Doctoral dissertation, Southern Illinois University Carbondale]. ProQuest Dissertations. OpenSIUC https://opensiuc.lib.siu.edu/dissertations/595/

Clark, R. E. (1994). Media will never influence learning. *Educational Technology Research and Development*, *42*(2), 21–29. doi:10.1007/BF02299088

Clark, R. E. (2007). Learning from serious games? Arguments, evidence, and research suggestions. *Educational Technology*, *47*, 56–59. https://www.jstor.org/stable/44429512

Cook, D. A., Hamstra, S. J., Brydges, R., Zendejas, B., Szostek, J. H., Wang, A. T., Erwin, P. J., & Hatala, R. (2012). Comparative effectiveness of instructional design features in simulation-based education: Systematic review and meta-analysis. *Medical Teacher*, *35*(1), e867–e898. Advance online publication. doi:10.3109/0142 159X.2012.714886 PMID:22938677

Cheng, H., & Tsai, C. (2020). Students' motivational beliefs and strategies, perceived immersion and attitudes towards science learning with immersive virtual reality: A partial least squares analysis. *British Journal of Educational Technology*, *51*(6), 2140–2159. doi:10.1111/bjet.12956

Choi, D., & Kim, J. (2004). Why people continue to play online games: In search of critical design factors to increase customer loyalty to online contents. *Cyberpsychology & Behavior*, *7*(1), 11–24. doi:10.1089/109493104322820066 PMID:15006164

Darlington, B., & Hayes, F. (2017). Regression analysis and linear models. Academic Press.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. doi:10.1016/j.giq.2017.02.007

DeSmet, A., Shegog, R., Van Ryckeghem, D., Crombez, G., & De Bourdeaudhuij, I. (2015). A systematic review and meta-analysis of interventions for sexual health promotion involving serious digital games. *Games for Health Journal*, *4*(2), 78–90. doi:10.1089/g4h.2014.0110 PMID:26181801

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160. doi:10.3758/BRM.41.4.1149 PMID:19897823

Ferguson, C. J., & Colwell, J. (2018). A meaner, more callous digital world for youth? The relationship between violent digital games, motivation, bullying, and civic behavior among children. *Psychology of Popular Media Culture*, *7*(3), 202–215. doi:10.1037/ppm0000128

Flood, S., Cradock-Henry, N. A., Blackett, P., & Edwards, P. (2018). Adaptive and interactive climate futures: Systematic review of 'serious games' for engagement and decision-making. *Environmental Research Letters*, *13*(6), 063005. doi:10.1088/1748-9326/aac1c6

Galgouranas, S., & Xinogalos, S. (2018). jAVANT-GARDE: A cross-platform serious game for an introduction to programming with Java. *Simulation & Gaming*, *49*(6), 751–767. doi:10.1177/1046878118789976

Galvez, S. M., Shackman, J. D., Guzman, I. R., & Ho, S. M. (2015). Factors affecting individual information security practices. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. ACM. doi:10.1145/2751957.2751966

Gass, R. H., & Seiter, J. S. (2018). *Persuasion: Social Influence and Compliance Gaining* (6th ed.). Routledge. doi:10.4324/9781315209302

Ge, X., & Ifenthaler, D. (2018). Designing engaging educational games and assessing engagement in game-based learning. In Information Resources Management Association (Ed.), Gamification in Education: Breakthroughs in Research and Practice (pp. 1-19). IGI Global. doi:10.4018/978-1-5225-5198-0.ch001

Greene, B. A. (2015). Measuring cognitive engagement with self-report scales: Reflections from over 20 years of research. *Educational Psychologist*, *50*(1), 14–30. doi:10.1080/00461520.2014.989230

Greitzer, F. L., Kuchar, O. A., & Huston, K. (2007). Cognitive science implications for enhancing training effectiveness in a serious gaming context. *Journal of Educational Resources in Computing*, *7*(3), 2–12. doi:10.1145/1281320.1281322

Grevelink, J. (2015). *Serious games for cybersecurity: Investigating the effectiveness of using a persuasive game to influence cybersecurity attitude and behavior* [Master's thesis]. Tilburg University. Communicatie en Informatie. http://arno.uvt.nl/show.cgi?fid=136774

Grossard, C., Grynspan, O., Serret, S., Jouen, A. L., Bailly, K., & Cohen, D. (2017). Serious games to teach social interactions and emotions to individuals with autism spectrum disorders (ASD). *Computers & Education*, *113*, 195–211. doi:10.1016/j.compedu.2017.05.002

Hallifax, S., Serna, A., Marty, J.-C., & Lavoué, E. (2021, April). Dynamic gamification adaptation framework based on engagement detection through learning analytics. *Proceedings of the 11th International Conference on Learning Analytics & Knowledge LAK21.*

Hamari, J., Shernoff, D. J., Rowe, E., Coller, B., Asbell-Clarke, J., & Edwards, T. (2016). Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. *Computers in Human Behavior*, *54*, 170–179. doi:10.1016/j.chb.2015.07.045

Hastings, N. B., & Tracey, M. W. (2005). Does media affect learning: Where are we now? *TechTrends*, *49*(2), 28–30. doi:10.1007/BF02773968

Hays, R. T. (2005). *The effectiveness of instructional games: A literature review and discussion* (Technical Report No. 2005-004). Naval Air Warfare Center, Training Systems Division. https://apps.dtic.mil/dtic/tr/fulltext/u2/a441935.pdf

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game-based cyber security training: Are serious games suitable for cyber security training? *International Journal of Serious Games*, *3*(1), 53–61. doi:10.17083/ijsg.v3i1.107

Herr, C., & Allen, D. (2015). Video games as a training tool to prepare the next generation of cyber warriors. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research.* ACM. doi:10.1145/2751957.2751958

Kim, J., Seo, J., & Laine, T. (2018). Detecting boredom from eye gaze and EEG. *Biomedical Signal Processing and Control*, *46*, 302–313. doi:10.1016/j.bspc.2018.05.034

Klisch, Y., Miller, L. M., Beier, M. E., & Wang, S. (2012). Teaching the biological consequences of alcohol abuse through an online game: Impacts among secondary students. *CBE Life Sciences Education*, *11*(1), 94–102. doi:10.1187/cbe.11-04-0040 PMID:22383621

Lamb, R. L. (2013). *The application of cognitive diagnostic approaches via neural network analysis of serious educational games* [Doctoral dissertation, George Mason University]. Mason Archival Repository Service. https://hdl.handle.net/1920/8342

Lamb, R., Annetta, L., Firestone, J., & Etopio, E. (2017). A meta-analysis with examination of moderators of student cognition, affect, and learning outcomes while using serious educational games, serious games, and simulations. *Computers in Human Behavior*, *80*, 158–167. doi:10.1016/j.chb.2017.10.040

Landers, R. N., Armstrong, M. B., & Collmus, A. B. (2017). How to use game elements to enhance learning: Applications of the theory of gamified learning. In M. Ma & A. Oikonomou (Eds.), Serious Games And Edutainment Applications (pp. 457-483). Springer. doi:10.1007/978-3-319-51645-5_2

Loh, C. S. (2012). Information trails: In-process assessment of game-based learning. Assessment for Game-Based Learning. In Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives (pp. 123-144). Springer. doi:10.1007/978-1-41614-3546-4_8

Loh, C. S. (2013). Improving the impact and return of investment of game-based learning. *International Journal of Virtual and Personal Learning Environments*, *4*(1), 1–15. doi:10.4018/jvple.2013010101

Loh, C. S., & Li, I. H. (2016). Using players' gameplay action-decision profiles to prescribe training: Reducing training costs with serious games analytics. *Proceedings of the 3rd IEEE International Conference on Data Science and Advanced Analytics, DSAA 2016*, 652-661. doi:10.1109/DSAA.2016.74

Loh, C. S., & Sheng, Y. (2015). Measuring expert-performance for serious games analytics: From data to insights. In C. S. Loh, Y. Sheng, & D. Ifenthaler (Eds.), *Serious Games Analytics: Methodologies for Performance Measurement, Assessment, and Improvement* (pp. 101–134). Springer. doi:10.1007/978-3-319-05834-4_5

Loh, C. S., Li, I.-H., & Sheng, Y. (2016). Comparison of similarity measures to differentiate players' actions and decision-making profiles in serious games analytics. *Computers in Human Behavior*, *64*, 62–574. doi:10.1016/j.chb.2016.07.024

Loh, C. S., Sheng, Y., & Ifenthaler, D. (Eds.). (2015). *Serious Games Analytics: Methodologies for Performance Measurement, Assessment, and Improvement*. Springer. doi:10.1007/978-3-319-05834-4

Lu, Y. L., & Lien, C. J. (2020). Are they learning or playing? Students' perception traits and their learning self-efficacy in a game-based learning environment. *Journal of Educational Computing Research*, *57*(8), 1879–1909. doi:10.1177/0735633118820684

Marcum, J. W. (1999). Out with motivation, in with engagement. *National Productivity Review*, *18*(4), 43–46. doi:10.1002/npr.4040180409

Macnamara, B. N., & Maitra, M. (2019). The role of deliberate practice in expert performance: Revisiting Ericsson, Krampe & Tesch-Römer (1993). *Royal Society Open Science*, *6*(8), 190327. doi:10.1098/rsos.190327 PMID:31598236

MAVI Interactive, LLC. (2022). *Sentinel Office Security*. Retrieved from https://www.maviinteractive.com/

Merrill, M. D. (2013). First principles of instruction. *Educational Technology Research and Development*, *50*(3), 43–59. doi:10.1007/BF02505024

Mes, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy & Security*, *9*(1), 47–67. doi:10.1080/15536548.2013.10845672

Muhamad, J. W., & Kim, S. (2020). Serious Games as Communicative Tools for Attitudinal and Behavioral Change. In H. O'Hair & M, O'Hair (Eds.), The Handbook of Applied Communication Research (pp. 141-162). John Wiley & Sons. doi:10.1002/9781119399926.ch9

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. In *Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER 2012)*. IEEE. doi:10.1109/CYBER.2012.6392562

O'Brien, H. L., & Toms, E. G. (2010). The development and evaluation of a survey to measure user engagement. *The American Society for Information Science and Technology*, *61*(1), 50–69. doi:10.1002/asi.21229

Parry, D. A., Davidson, B. I., Sewall, C. J., Fisher, J. T., Mieczkowski, H., & Quintana, D. S. (2021). A systematic review and meta-analysis of discrepancies between logged and self-reported digital media use. *Nature Human Behaviour*, *5*(11), 1535–1547. doi:10.1038/s41562-021-01117-5 PMID:34002052

Pallant, J. (2001). *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using IBM SPSS*. Routledge.

Poster, W. R. (2018). Cybersecurity needs women. *Nature*, *555*(7698), 577–580. doi:10.1038/d41586-018-03327-w

Qusa, H., & Tarazi, J. (2021, January). Cyber-Hero: A gamification framework for cyber security awareness for high schools students. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0677-0682). IEEE. doi:10.1109/CCWC51732.2021.9375847

SalamzadehA. (2020). What Constitutes a Theoretical Contribution? *Journal of Organizational Culture, Communications and Conflicts, 24*(1), 1-2. https://ssrn.com/abstract=3599931

Samčović, A. B. (2018). Serious games in military applications. *Vojnotehnički Glasnik*, *66*(3), 597–613. doi:10.5937/vojtehg66-16367

Serrano-Laguna, Á., Martínez-Ortiz, I., Haag, J., Regan, D., Johnson, A., & Fernández-Manjón, B. (2017). Applying standards to systematize learning analytics in serious games. *Computer Standards & Interfaces*, *50*, 116–123. doi:10.1016/j.csi.2016.09.014

Schoenau-Fog, H. (2011, September). The player engagement process: An exploration of continuation desire in digital games. In *Proceeding of DiGRA International Conference: Think Design Play, University of Utah* (pp. 190-250). Retrieved from: http://www.digra.org/digital-library/publications/the-player-engagement-process-an-exploration-of-continuation-desire-in-digital-games/

Schoenau-Fog, H., & Bjoerner, T. (2012). "Sure, I would like to continue" a method for mapping the experience of engagement in video games. *Bulletin of Science, Technology & Society*, *32*(5), 405–412. doi:10.1177/0270467612469068

Tong, T., Chignell, M., Tierney, M., & Lee, A. (2016). Serious game for clinical assessment of cognitive status: Validation study. *JMIR Serious Games*, *4*(1), e7. doi:10.2196/games.5006 PMID:27234145

van der Linden, J. (2014). *Protection motivation theory and cybersecurity awareness: The effect of serious games* [Unpublished Bachelor thesis]. Tilburg University.

Verkuyl, M., Djafarova, N., Mastrilli, P., & Atack, L. (2022). Virtual gaming simulation: Evaluating players' experiences. *Clinical Simulation in Nursing*, *63*, 16–22. doi:10.1016/j.ecns.2021.11.002

Vlachopoulos, D., & Makri, A. (2017). The effect of games and simulations on higher education: A systematic literature review. *International Journal of Educational Technology in Higher Education*, *14*(1), 1–33. doi:10.1186/s41239-017-0062-1

Wiemeyer, J., & Tremper, L. L. (2017). Edutainment in sport and health. In R. Nakatsu, M. Rauterberg, & P. Ciancarini (Eds.), *Handbook of Digital Games and Entertainment Technologies* (pp. 883–908). Springer. doi:10.1007/978-981-4560-50-4_67

Willmott, T., Russell-Bennett, R., Drennan, J., & Rundle-Thiele, S. (2019). The impact of serious educational gameplay on adolescent binge drinking intentions: A theoretically grounded empirical examination. *Health Education & Behavior*, *46*(1), 114–125. doi:10.1177/1090198118780493 PMID:30027760

Yasin, A., Liu, L., Li, T., Fatima, R., & Jianmin, W. (2019). Improving software security awareness using a serious game. *IET Software*, *13*(2), 159–169. doi:10.1049/iet-sen.2018.5095

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2016). The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, *32*(3), 215–257. doi:10.1080/10447318.2016.1136177

Zoeller, G. (2013). Game development telemetry in production. In M. Seif El-Nasr, A. Drachen, & A. Canossa (Eds.), *Game Analytics: Maximizing the Value of Player Data* (pp. 111–135). Springer., doi:10.1007/978-1-4471-4769-5_7

ENDNOTE

[1] See https://maviinteractive.com/video_info_sentinel.html.

Rana Salameh is an Assistant lecturer of computer science. Her research interests include Serious Game Analytics, User's performance and behavior assessment and cybersecurity awareness training. She received her MS in Computer Science at Southern Illinois University at Carbondale in 2002. In 2019 she received her Ph.D. in Instructional Design and technology from Southern Illinois University at Carbondale. CRediT: Conceptualization, Investigation, Formal analysis, Writing – original draft.

Christian Sebastian Loh is Professor of Instructional Design & Technology at the Southern Illinois University Carbondale. His research and professional interests include Serious Games Analytics, performance assessment and decision-making with virtual environments, and expert-novice performance. He serves on the editorial boards of several international journals and is the lead editor of Serious Games Analytics: Methodologies for Performance Measurement, Assessment, and Improvement. CRediT: Supervision, Methodology, Writing – Reviewing and Editing.