The current reference for this work is as follows:

> Mario Silic and Paul Benjamin Lowry (2019). "Using design-science based gamification to improve organizational security training and compliance," ***Journal of Management Information Systems (JMIS)*** (accepted 01-Aug-2019)

If you have any questions, would like a copy of the final version of the article, or would like copies of other articles we've published, please contact any of us directly, as follows:

- **Dr. Mario Silici**
  - Email: mario.silic@unisg.ch
  - Website: https://www.alexandria.unisg.ch/persons/6160
- **Professor Paul Benjamin Lowry**
  - Email: Paul.Lowry.PhD@gmail.com
  - Website: https://sites.google.com/site/professorlowrypaulbenjamin/home
  - System to request Paul's articles: https://seanacademic.qualtrics.com/SE/?SID=SV_7WCaP0V7FA0GWWx

Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance

AUTHOR BIOS AND CONTACT INFORMATION

Dr. Mario Silic is a post-doctoral researcher at the Institute of Information Management, University of St. Gallen, Switzerland. He holds a Ph.D. from University of St Gallen, Switzerland. His research motivation focuses on the fields of information security, open source software, human-computer interaction and mobile. He has published research in *Journal of Management Information Systems*, *Security Journal*, *Information & Management*, *Computers & Security*, *Computers in Human Behavior*, and others.

University of St. Gallen
Institute of Information Management
University of St. Gallen
Mueller-Friedberg-Str. 8
9000 St. Gallen
Switzerland
mario.silic@unisg.ch

Dr. Paul Benjamin Lowry is the Suzanne Parker Thornhill Chair Professor and Eminent Scholar in Business Information Technology at the Pamplin College of Business at Virginia Tech. He is a former tenured Full Professor at both City University of Hong Kong and The University of Hong Kong. He received his Ph.D. in MIS from the University of Arizona. He has published 120+ journal articles in *Journal of Management Information Systems*, *MISQ*, *ISR*, *JAIS*, *ISJ*, *EJIS*, *JSIS*, *JIT*, and others. In 2019, he was recognized as the most productive scholar in the world for the top-6 IS journals, in the last 5 years (and second for the top-4 journals). He is a department editor at *Decision Sciences J*. He also is an SE at *J. of MIS*, *J. of the AIS*, and *Information System J.*, and an AE at the *European J. of Information Systems.* His research interests include (1) organizational and behavioral security and privacy; (2) online deviance, online harassment, and computer ethics; (3) HCI, social media, and gamification; and (4) business analytics, decision sciences, innovation, and supply chains.

Department of Business Information Technology
Pamplin College of Business
Virginia Tech
Pamplin Hall, Suite 1007
880 West Campus Drive
Blacksburg, VA 24061 USA
Paul.Lowry.PhD@gmail.com

Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance

ABSTRACT

We conducted a design-science research project to improve an organization's compound problems of (1) unsuccessful employee phishing prevention and (2) poorly received internal security training. To do so, we created a gamified security training system focusing on two factors: (1) enhancing intrinsic motivation through gamification and (2) improving security learning and efficacy. Our key theoretical contribution is proposing a recontextualized kernel theory from the hedonic-motivation system adoption model that can be used to assess employee security constructs along with their intrinsic motivations and coping for learning and compliance. A six-month field study with 420 participants shows that fulfilling users' motivations and coping needs through gamified security training can result in statistically significant positive behavioral changes. We also provide a novel empirical demonstration of the conceptual importance of "appropriate challenge" in this context. We vet our work using the principles of proof-of-concept and proof-of-value, and we conclude with a research agenda that leads toward final proof-in-use.

Keywords: Gamification; design science research (DSR); hedonic-motivation system adoption model (HMSAM); immersion; flow; security compliance; security education, training, and awareness (SETA)

INTRODUCTION

Information technology (IT) security compliance deals with techniques and processes that motivate employees to behave more securely when engaging with organizational systems and information [cf. 14]. Such compliance is of increasing concern for management and executives because of the global explosion of organizational security issues. Generally, IT security compliance has three objectives: (1) to mitigate or avoid security incidents and risks often caused by negligent employees [22, 65, 102], (2) to thwart criminal security behavior and computer abuse [65, 101, 102], and (3) to encourage prosocial and protective security behaviors in employees [45, 84]. A number of promising studies have applied various techniques to motivate employees to adopt secure intentions and behavior—from deterrence techniques [26, 101, 102] and discouraging employee neutralization [e.g., 91] to increasing the awareness of the risks

and potential costs of noncompliance [e.g., 14], to increasing accountability [94, 95], to leveraging positive psychology or affect [15, 28], and even using more explicit threats and fear appeals [11, 52, 83]. Despite these efforts, employees remain the "weakest link" in organizational IT security because employee behavior can easily undermine it [102]; moreover, it is ultimately the employees' responsibility to comply, and they often do not [22, 83].

Understandably, researchers have questioned whether extant organizational security approaches are efficacious. For example, deterrence techniques were designed for criminal behavior and may be inappropriate for security policy noncompliance [26, 102]. Techniques that employ threats and intensified risks can have unintended consequences, including negative employee reactance [63, 65].

In contrast, security education, training, and awareness (SETA) programs can leverage a more positive approach. SETA programs aim to provide employees with the knowledge and motivation necessary to comply with security policies when confronted with a security risk [21]. However, it is evident that many of the current compliance-related training approaches are relatively ineffective; many employees continue to be noncompliant [102]. This is troubling, as SETA programs have long been considered fundamental to organizational security governance, and despite repeated calls to address this promising research area, researchers have not examined how to make SETA programs more effective, with a few promising exceptions [e.g., 21].

Employee training is notorious for failing, as even though it often delivers the right content, employees often lack the motivation to embrace the training and apply it in their everyday work, thus causing performance and even reputational failures [67]. Employees also have difficulty focusing on lengthy training sessions, especially when they are concerned about their actual work tasks. This is especially true in the context of security, in which most employees are not experts and lack efficacy. Most employees do not recognize the importance of caring about security in the context of everyday work. Thus, changing users' security-related behaviors through training is highly complex and prone to failure [57]. This is a common problem in employee training, during which employees lack conscientiousness and thus do not develop the efficacy needed to apply what they have learned [67]. Ferguson [36]

essentially declared SETA programs useless after conducting an experiment involving four hours of training, as the participants were generally unmotivated and 90% failed to detect a phishing attack.

Rather than similarly concluding that SETA programs are ineffective, we instead aim to improve them. We propose that a solution must begin with the recognition that most security training is not enjoyable or motivating—it is perfunctory, arcane, and outside employees' normal practice and expertise. We posit that security training based on *gamification* principles[i] (e.g., game-like features applied to nongaming contexts) is an effective approach for improving intrinsic motivation, learning, coping skills, and subsequent security compliance. People are more motivated and conscientious when they have an enjoyable, immersive experience. However, a recent cross-sectional study complicates our proposition: although Baxter et al. [8] established that their gamified security training system was fun, enjoyable, and preferred over other methods, no statistically significant evidence showed that the gamified system actually increased the users' knowledge.[ii]

With the final goal of improving security training in organizations, our study strengthens the promising foundation of this literature and applies an approach to gamification grounded in both motivation theory and design-science research (DSR). Our aim is to improve not only the delivery of organizational security training through gamification, but also the security-related motivations, efficacy, learning, intentions, and behaviors of employees receiving such training. Our six-month field study in an actual organization with 420 participants shows that fulfilling users' motivations and coping needs through gamified security training can result in statistically significant changes—including an improved ability to efficaciously respond to actual phishing attempts.

GAMIFICATION LITERATURE REVIEW

Gamification applies knowledge from gaming theory and *flow theory* [23, 24, 92] to nongaming contexts. Thus, *gamification* is "the application of lessons from the gaming domain in order to change stakeholder behaviors and outcomes in non-game situations" [85, p. 352]. Gamification was first implemented in an organizational context during the "Cold War" when workers and factories in the Soviet Union used a points-based system of competition to increase productivity (which was detached from economic reality

and thus backfired) [71]. In 1984, Coonradt [19] became one of the first researchers to apply gamification to a business context to motivate employees by including frequent feedback, clear goals, personal choice, and gaming features. Although gamification emerged from the flow literature as it applied to gaming, scholars have not reached a consensus regarding gamification's definition [92]. Similarly, Liu et al. [59] concluded

> The common themes that emerge from the various definitions over the past decade are: gamified systems must have specific user engagement and instrumental goals, and the way to achieve these is by the selection of game design elements (p. 3).

Another key gamification concept is that a game-like user experience activates users' individual motives [22, 61].[iii] Summarizing the various definitions of gamification in the literature, we propose the following working definitions of gamification:

- ***Gamification*** *is the use of game-like IT design artifacts and system processes to strengthen motivations and encourage specific behavioral changes in users for specific instrumental goals.*
- ***Security gamification*** *is applying game-like design artifacts and system processes to strengthen employees' motivations to encourage learning, efficacy, and increased employee compliance with organizational security initiatives.*

Previous research has suggested that game design can include the use of goals, rewards, and storytelling [53] to stimulate experiences of challenge and curiosity [33] and that the conceptualization of gaming elements is highly important for user–game engagement [58]. However, Bui et al.'s [13] review of gamification design artifacts offered two interesting conclusions: (1) most studies did not explain the technological elements of the gamified systems, such as how these artifacts foster gamification, and (2) there is a

> ...large gap in research of potential relevance to organizations... more research is needed on employees interacting with group systems resulting in collaboration dynamics and longer-term behavioral outcomes [13, p. 11].

Bui et al.'s review supports three of our study's core assumptions. First, a careful DSR approach should be used to create gamified systems. Second, gamification must be applied in a realistic organizational context using longer-term approaches that focus on *meaningful engagement* to produce meaningful results. Third, the DSR kernel theory must be carefully contextualized to the instrumental goal of the

gamification task—in our context, improving organizational security through training interventions.[iv]

Several researchers have posited that gamification can foster employees' training and subsequent compliance with organizational security [e.g., 2, 8]. These studies are reviewed in Online Table A.1. This research stream faces several challenges, which we address fully in our research: (1) the majority of the studies used one-time cross-sectional data, and none used long-term or longitudinal data; (2) the participants were mainly students, and thus many of the tasks had no ecologically valid relationship to actual organizational security in practice [cf. 60]; (3) the research designs lacked control groups, so there was no way to empirically establish that the gamification context was an improvement over the status quo; (4) actual behaviors were not measured; (5) many studies did not use theory, and none developed a cohesive theoretical foundation; (6) most did not involve a working system; and (7) most did not achieve *meaningful engagement*[v] or articulate the importance of instrumental (e.g., improved IT security compliance) and interaction outcomes (e.g., measurable increased immersion) [cf. 59].[vi]

DSR APPLIED TO GAMIFIED SECURITY TRAINING

Given the compelling opportunities in the literature, we argue that an improved approach is needed. Likewise Liu et al. [59] concluded that the gamification literature in general does not explain

> **how** these design elements should be chosen for **specific tasks**, and **how** they interact among themselves and create the desired user interactions that **engage the user** and lead to the intended **instrumental goals** (p. 3) [emphasis added]

We thus propose that gamified security training represents a natural opportunity to apply a DSR approach to bridge the related opportunities in design, theory, methodology, and practice from our introduction.

Overview of Our DSR Approach

Previous gamification studies have largely lacked a systematic DSR approach [13] to the security context. In a non-gamified security context, Vance et al. [95] explained that although there is no single, authoritative approach to DSR, a common expectation of DSR is that the solution can be described and evaluated in terms of proof-of-concept and proof-of-value [e.g., 38, 41, 77, 93]:

> ***Proof-of-concept*** is the point at which enough evidence exists to show that the described conceptual solution of design is feasible and promising, at least in a limited context.... In contrast,

> ***proof-of-value*** is achieved when researchers show that an IT artifact actually works in reality [95, p. A6] [emphasis added].

Similar approaches to proof-of-concept and proof-of-value have recently been introduced in contexts such as cyberbullying [64], autonomous scientifically controlled screening systems [93], and a video-based screening system [82]. However, according to [75, p. 16], the third concept of *proof-of-use* can also be applied to DSR. To support our DSR approach, we adhered to a DSR methodology that closely follows the method advocated by Nunamaker Jr et al. [76] and elaborated on by Peffers et al. [81].

We systematically established proof-of-concept and proof-of-value and moved toward ongoing proof-of-use by implementing a system actually used in practice. Next, we explain how we systematically combined relevance with theoretical rigor, leveraging additional DSR principles to embody the principles of the "last research mile" as advocated by Nunamaker Jr et al. [75]. This involved an extensive, iterative process based on the security gamification literature, DSR, system development, and feedback from the target organization. Despite its iterative nature, the DSR process we leveraged can be described in the following seven steps (two final steps are addressed in the discussion section).

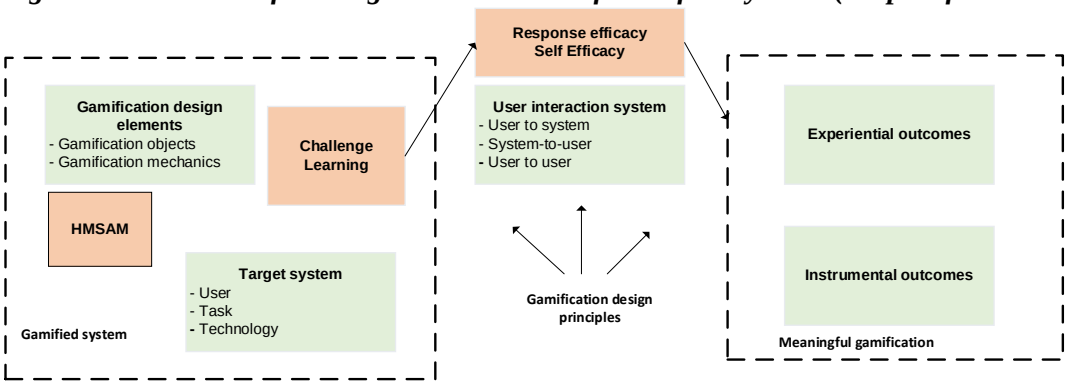
1. Establish the Gamified Design as an Artifact

We followed Liu et al. [59], who proposed a key gamification design principles illustrated by a running case (HealthyMe). Although we applied the majority of their design principles, some were inapplicable to our organizational security context or specific design choices.[vii] Figure 1 depicts our final design framework in which we were able to focus on *design as an artifact* [cf. 41]. Liu et al. [59] suggested focusing on the design and development of the gamified system before focusing on the outcomes. We did so following the DSR approach advocated by Nunamaker Jr et al. [76] and shown in Figure A.1 (Appendix A): (1) theory building, (2) systems development, (3) experimentation, and (4) observations. These steps encapsulate several subprocesses, such as those of Peffers et al. [81].

2. Focus on Design Problem Relevance

Our research started when the French company invited one of the authors to help create a system that would encourage better employee IT security compliance through online training. The company had faced

Figure 1. Framework for Design and Research of Gamified Systems (adapted from Liu et al. [59])



an ongoing problem of employee carelessness regarding security issues, including falling for phishing attacks. Their existing email-based training system was not positively viewed within the firm.

Moreover, our literature review revealed that the traditional approach of encouraging IT security compliance through sanctions is inconsistent and can backfire. We also learned that gamification could potentially positively influence employee training and motivation. However, no prior research has established clear empirical evidence that employees' security learning and efficacy perceptions could be positively influenced by gamification.

3. Create Objectives for Design Evaluation

Our objectives were to build a gamified training system based on a native information systems (IS) motivational theory as the kernel theory that was tested in an ecologically valid manner using a long-term field experiment. We thus undertook an iterative process of design and development, balancing concepts, designs, and concepts from the literature with the client's training requirements. We unit tested the system and then ran a pilot test with human subjects to further evaluate the design objectives.

4. Apply a DSR Kernel Theory Contextualized to Gamification

A key step of designing a gamified system is to carefully choose the gamification design principles that serve as the bridge between the system and meaningful engagement [59]. This step establishes the user-interaction processes that occur between user-system-user actors. We first analyzed kernel theories [73] that would support and motivate the employees' security learning and behavioral change. We surmised that the *hedonic-motivation system adoption model* (HMSAM) [62] was particularly suitable as a kernel

theory and evaluation model when extended to the security context and coping support. This extended model consisted of two main components that further inspired design principles: (1) *motivation fulfillment* to inspire gamified systems use and (2) *coping support* so the users can deal with security issues and engage in security-related behavioral change.

To proceed with context-specific theorizing, we used a framework similar to the one suggested by Hong et al. [43], which suggests that the technology artifact is an additional element in theorizing that should be considered. In IS research, contextualization usually involves the introduction of contextual features into previously established general models, as in the contextualization of the unified theory of acceptance and use of technology [96] to the adoption and use of collaboration technologies [12]. Our most important contextualization consisted of adding context-specific factors—learning, security response efficacy, and security self-efficacy—to HMSAM.

5. Propose Guiding Design Principles to Bridge DSR Design Objectives and the DSR Kernel Theory

Following DSR, the subsequent design principles needed to rely on carefully chosen design elements. Thus, we proposed the first design principle:

> **Design principle #1:** The gamified training system should incorporate different design elements that increase employees' motivation and fulfillment.

Regarding coping support, it is crucial that the new system has features that sustain and leverage employees' knowledge in such a way that employees will not only be intrinsically motivated through enjoyment but will also acquire the new knowledge effectively. This led to the second design principle:

> **Design principle #2:** The gamified training system should provide new knowledge through a learning process that is meaningful, entertaining, and fun.

Here, there are three conceptual design issues that need to be addressed [73]: The first is the "conceptual distance between a latent independent variable (cause) and its corresponding design items" [73, p. 311], which in our case translates into the potential for both intrinsic and extrinsic motivations to positively influence security learning and behavioral change. Both intrinsic and extrinsic motivations can positively influence an individual's security behavioral change [e.g., 14, 40]. However, extrinsic

motivations may provide only temporary compliance [55] and intrinsic motivations are more powerful in driving employee's behaviors [78]. Likewise, intrinsically motivated learners were found to demonstrate higher achievements in learning [9]. To satisfy this meta-requirement, we focused primarily on intrinsic motivations when designing the system, although there may be some spillover into extrinsic motivations.

The second issue concerns the "conceptual distance between a latent dependent variable (effect) and its corresponding measurements" [73, p. 312]. Here, the challenge involves choosing the right measurement items, which is especially important for DSR so that design evaluation and research rigor can be established [41]. We thus carefully reviewed the literature and, whenever possible, selected established measures, as further documented in the method section.

The third and final conceptual design issue concerns the "potential interdependence of simultaneously implemented design items" [73, p. 312]. This is the problem of confounding design elements that may have different effects on the artifact evaluation. For example, we had to decide whether to guide the learning process through a recorded video or through a series of brief, interactive lessons that used graphical examples of phishing mistakes typically made by employees. Here, the design decision influenced the evaluation of the artifact. Our target organizations placed a premium on simplicity; thus, we chose short informative lessons. Such decisions can influence the "solution space for other design decisions; however, this may lead to lock-in situations with respect to the final artifact" [73, p. 312].

6. Establish Proof-of-Concept

We followed four primary steps to establish ***proof-of-concept*** [cf. 81] before we proceeded to empirical testing. The company was pleased by the positive results, and the feedback from employees was highly positive. Thus, the solution worked well in practice, which provided evidence of proof-of-concept [80].

Step 1: Before creating a working prototype, we reviewed the gamified security literature to learn about gamification features that may work well in a security context and understand why this is the case.

This review is detailed in Appendix A (see Tables A.1–A.2).

Step 2: We then created Table A.3 to propose how gamification elements should be implemented in our context and that we followed to implement multiple versions of our security training system. We

also mapped these elements to the various ways that flow (in our context, *immersion*) can be fostered [24] and mapped the elements to the intrinsic motivations they could potentially fulfill.

Step 3: We then further bridged design and theory by systematically applying our kernel theory, HMSAM, by mapping the derived gamification element relationships to HMSAM constructs, as shown in Table A.4. This allowed us to conceptually check whether our design could fulfill intrinsic motivations and provide an "appropriate challenge."

Step 4: Finally, in Table A.5 we mapped specific motivations to each of the gamification design elements. We used a taxonomy of major motivations for system use in [61] where the motivations were suited for the security training context. By analyzing mappings from Table A.4 and Table A.5, we observed the same relationships with motivations. For example, play/enjoyment/fun can be found in 11 gamification design elements (Table A.5.).

7. Establish Proof-of-Value

To establish proof-of-value, once the system was deemed ready, we first formally pilot tested it and the kernel theory with students. However, the key step in establishing proof-of-value involved a long-term field experiment with actual employees using the gamified security training system. These details, and the subsequent rigorous analyses, are addressed fully in the section after the next section. Before addressing the full proof-of-value methodologies and analyses, the next section details how we operationalized our kernel theory, HMSAM, to develop testable hypotheses for empirically establishing proof-of-value.

KERNEL THEORY FOUNDATION FOR PROOF-OF-CONCEPT AND PROOF-OF-VALUE

The key role of our kernel theory, HMSAM, was twofold: to guide the design and help establish proof-of-concept, and to be operationalized to test it for further proof-of-value. Again, this process was iterative such that what we learned in developing hypotheses informed design, and vice versa. Here, our focus is on the derived operationalized hypotheses and the logic behind them.

HMSAM was chosen primarily because it is a native IS theory that focuses heavily on intrinsic motivations in systems use [62], which we found to be a natural fit for our gamified context. Namely, HMSAM was designed to explain how fulfilling *motivations* can lead to increased immersion and

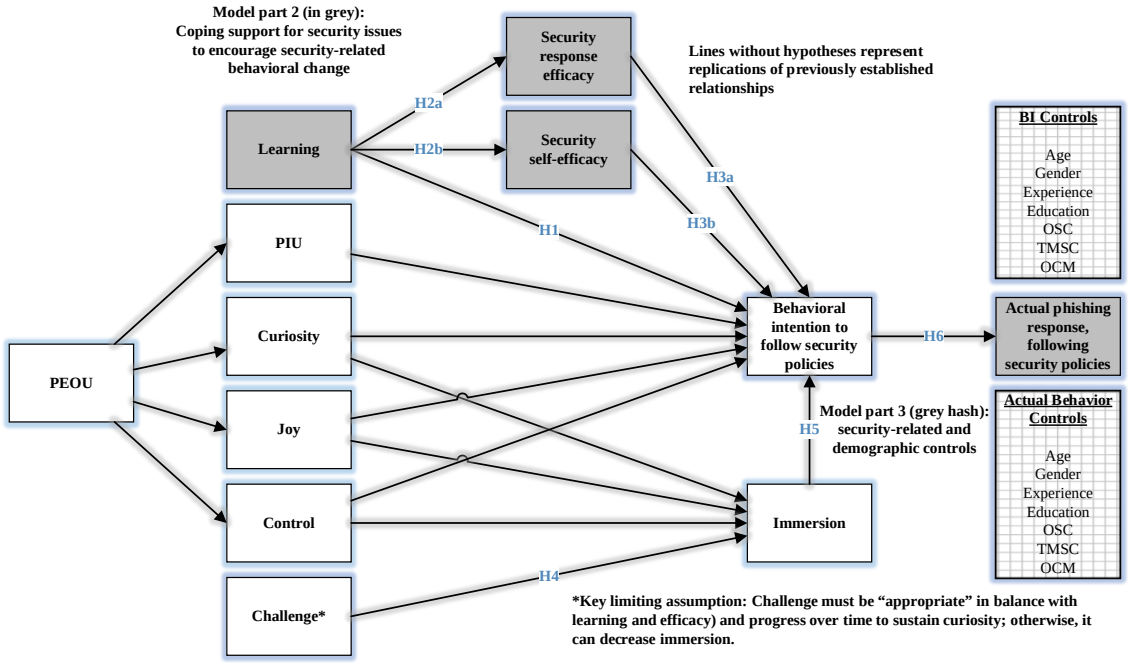
behavioral intention (BI) and ultimately to behavioral change [62]. These explanations are more theoretically powerful and appropriate predictors of BI than traditional factors, such as perceived ease of use (PEOU) or joy [62]. HMSAM builds on flow theory by re-envisioning the original conceptualization of cognitive absorption (CA) developed in [3]. The CA construct was inspired by flow theory, which was not proposed with systems in mind, and is defined as a deep state of involvement with systems (i.e., immersive systems use). Gamified systems thus represent an ideal setting in which to investigate CA, which has affective and cognitive components and is an intrinsic motivator. Whereas the original conceptualization of CA assumed that its components (curiosity, joy, control, and immersion) occurred simultaneously as one formative construct [3], HMSAM examines CA's components independently and explains how the fulfillment of intrinsic motivations fosters associated BI (or, in the original HMSAM, system acceptance intentions). Lowry et al. [62] argued that this approach is more consistent with flow theory's understanding of flow as a process that unfolds over time and involves multiple constructs. HMSAM also leverages the technology acceptance model (TAM) to explain that intrinsic TAM elements are lower-order factors in the creation of immersion and BI. Consequently, HMSAM is a process-variance model in which intrinsic TAM elements, like PEOU and enjoyment, are lower-order elements that precede immersion and combine to change BI.

Figure 2 depicts the HMSAM that we extend for the new context of BI related to security learning and compliance. Our extensions are shown as hypotheses; all remaining paths are replications of HMSAM. Our model suggests that the factors of improved security learning, efficacy perceptions, and the ability to cope with security challenges encourage positive behavioral change by strengthening employees' intentions to follow security policies and improving their phishing-response behaviors.

Core Kernel Theory Assumptions for Achieving Immersion

A core assumption of our operationalized kernel theory is that the experience of flow (and thus, in our context, *immersion*) arises from the satisfaction of three conditions: (1) clear goals, (2) unambiguous feedback, and (3) a balance of challenges and skills [29]. The first condition indicates the importance of ***instrumental goals***, as stressed by Liu et al. [59], which suggests that the gamification system should

Figure 2. Operationalized and Extended Kernel Theory: HMSAM



PEOU = perceived ease of use; PIU = perceived intrinsic usefulness; BI = behavioral intention to follow security policies; OSC = organization security communication; TMSC = top management security commitment; OCM = organization computer monitoring.

enable the accomplishment of dual goals, in which both sides can see benefits (e.g., improved security knowledge for the employee and fewer security breaches for the company). ***Unambiguous feedback*** can be delivered by providing gamified feedback in the training itself. In the gamified system, this could be augmented with leaderboards, points, measurement against goals, features that convey a sense of general progress, and the presence of a gamemaster [2, 8, 42]. Balancing ***challenge and skills***, fostered through learning and the efficacy and coping derived from it, is a core focus of the remainder of this section.

Infusing Learning and Security Coping into Our Context

Like motivations, positive coping skills can foster behavioral change. A key way to deliver coping skills is through SETA programs [e.g., 21]. Our gamified environment provides common SETA-based training related to organizational security systems, particularly to help employees learn how to identify and avoid phishing attacks and suspicious emails. Research has found a link between learning and behavioral engagement [44]. The more employees learn, the more they will be prepared to implement protective security behaviors [cf. 84]. Employees who have a deeper knowledge of security risks and ways to thwart

them are more likely to believe they can comply and protect their organizations. Conversely, employees who have little knowledge in this area are more likely to be uncertain and make poor security decisions. Research shows that the learning process strengthens one's abilities; as a result, one pays more attention to the context, content, and environment, all of which must be properly assessed to make effective security decisions [51]. Thus,

> *H1. Increased perceived learning in a gamified security training context is associated with increased BI.*

Such learning fosters general coping abilities, most commonly termed "security response efficacy" and "security self-efficacy" [e.g., 11, 52]. *Response efficacy* is "the belief that the adaptive response will work, that taking the protective action will be effective in protecting the self or others" [37, p. 411]. *Self-efficacy* is the degree to which individuals believe they are capable of preventing threats [11]. Security researchers have reconceptualized these concepts extensively and from several perspectives [11, 49, 52, 99, 100]. In our context, *security response efficacy* means that employees believe that what they were told to do in their security/phishing training will work to prevent the threat, and *security self-efficacy* means that they believe they can deal with the security response themselves. Thus, if employees learn a new protocol that is purported to mitigate phishing attacks and they believe the process is efficacious, they will be more likely to follow it.

Research [79] has also found that goal-oriented individuals demonstrate higher levels of task-specific efficacy. Our gamified environment fosters a goal orientation with a clear task objective and concrete feedback. Performance and achievement lead to higher levels of self-efficacy, and an informal social learning environment directly influences employee efficacy levels [68]. This suggests that employees will not only demonstrate higher levels of efficacy but also be more certain of their ability to apply newly acquired knowledge in practice. Learning also leads to greater efficacy, which in turn generates more interest and more learning [51]. Thus, it is likely that there are feedback mechanisms between efficacy and learning. However, for concision, we predict:

> *H2a–b. Increased perceived learning in a gamified security learning context is associated with increased (a) security response efficacy and (b) security self-efficacy.*

Coping and Behavioral Change

Research has demonstrated the importance of improving coping skills as a means of encouraging behavioral changes in employees that result in better adherence to security policies [e.g., 11, 14, 52, 100]. Recent research [100] has identified a clear link between coping adaptiveness (e.g., task-focused coping) and perceived phishing detection efficacy. This is partially supported by recent findings that awareness and motivation are crucial for security compliance [16].

Efficacy should increase not only as a result of learning but also specifically as a result of learning through a gamified system, because such systems make learning more efficacious. Gamified systems provide "powerful social psychological processes such as self-efficacy... [that] provide rewards... [and] drive most of the long-term participation" [31, p.16]. Per Bandura [6], setting and assigning goals (e.g., badges or levels in gamified systems) enhances self-efficacy. Thus, the increased self-efficacy and response efficacy resulting from gamified systems should lead to an increased intention to act securely, as more employees will feel capable of acting securely and believe that the desired security decision will be effective.

> *H3a–b. Both (a) increased security response efficacy and (b) security self-efficacy in a gamified security training context are associated with increased BI.*

Balancing Skills and Challenges

Again, the third condition of achieving immersion, per Davis and Csikszentmihalyi [29], is balancing skills and challenges. In gamified contexts, flow occurs when perceived skill and challenge levels are balanced; however, if such levels are initially low, apathy instead of engagement can occur [20]. Likewise, a key role of gamified components is to stimulate experiences of both curiosity and challenge [33], with challenges driving immersive engagement [47]. Thus, "if stimuli from an experience are either too challenging or not challenging enough, interest and curiosity decline" [61, p. 539].

Thus, we add to HMSAM the concept of challenges, which when met can fulfill motivations and ultimately facilitate immersion. However, the key limiting assumption of this addition is that a challenge is most likely to be useful if it takes the form of an *appropriate challenge*, which is "the degree to which

the perceived positive challenge of an activity matches the perceived skills of the user" [61, p. 539]. Thus, as it relates to an employee's instrumental goals, learning, and efficacy, a gamified training task should be neither too challenging nor too facile. The greater the challenge, the greater the behavioral engagement required to overcome it [89]. Likewise, we assume that the challenge should become more difficult (e.g., "levels up") as the employee learns and becomes more efficacious [e.g., 7]. Otherwise, curiosity will be undermined, and boredom can ensue.

Meng et al. [69] argued that the optimal challenge leads to optimal immersion. We likewise argue that (1) good gamification delivery involves progressive challenges, but (2) such challenges must be appropriate, and thus, a challenge might become "too much" for an end user and cause diminishing returns. This state represents an inverted U-shaped relationship in which a "relationship exists if the dependent variable Y first increases with the independent variable X at a decreasing rate to reach a maximum, after which Y decreases at an increasing rate" [39, p. 4]. A recent study [66] employed the two-player StopWatch game to confirm through electrophysiological evidence that this inverted U-shaped relationship exists between perceived challenges and one's intrinsic motivation. Namely, in situations in which the challenge is optimal, one's immersion should increase up to the apex of the curve, whereas further increases of the challenge beyond the optimal point should lead to decreased immersion. Thus,

> *H4. Perceived challenge will have a positive and curvilinear (inverted U-shaped) relationship with perceived immersion in a gamified security training context.*

Fulfilling Motivations for Behavioral Change

CA theory [3] predicts that immersion is positively associated with BI, which has been replicated in HMSAM gaming research [62]. However, we have extended HMSAM, such that BI is parallel to our context and thus involves the intention to follow security policies, not the intention to use a system. This is a theoretically reasonable extension, because HMSAM's behavioral predictions are rooted in TAM, which is rooted in the *theory of reasoned action* (TRA) [5]. TAM, the TRA, and the related *theory of planned behavior* (TPB) [4] consistently exhibit a strong link between attitude formation, intention, and behavior that extends far beyond mere system usage. This is the case regardless of shifts in the behavioral

target, as long as the target is in the same context.

Gamification and immersion are powerful influences on behavioral change in individuals, and they should be especially apt in our gamified security training context. An earlier study [72] predicted, but did not empirically show, that meaningful gamification should motivate and lead to long-term behavioral changes. A key reason for this is that motivations can be fulfilled through immersion. Immersion in gaming contexts is the experience of being engaged in the game-playing experience while having partial awareness of reality [62]. In learning contexts, immersion occurs as a result of appealing to intrinsic motivations, such as learning new things and being engaged [35].

Immersion is an experience of total involvement that causes external demands to be ignored [3, 62]. This increased focus, combined with the fulfillment of motivations, creates ideal conditions for learning and behavioral change. Research [98] has found that higher levels of immersion lead to greater usage intentions than lower levels of immersion. By influencing the state of flow/immersion, gamification positively and continuously influences intentions and actual behaviors. Numerous studies have found that intrinsic motivations are strong predictors of meaningful user behavioral change outcomes, such as satisfaction, continuance intentions, and perceived performance [25, 61].

The underlying causal mechanisms are not just cognitive, as inferred by the TRA, but also physiological. Thus, they are surprisingly powerful. Prior research has identified several neurological causal mechanisms involved in flow and gaming, showing that games lead to numerous neurological changes: (1) the brain releases more dopamine, which is associated with pleasure and consequently increases motivation [54]; (2) testosterone is increased, affecting energy, mood, and self-esteem [34]; and (3) memory is improved by training the amygdala, the brain's memory and decision center, to better respond to similar situations in the future [10]. These factors can lead to dramatic behavioral changes.[viii] Thus, assuming that the underlying mechanisms of the TRA and of the gamification of intrinsic motivations and learning hold true in our context, employees should be motivated to strengthen their context-related intentions when they have a more immersive learning experience.

H5. Increased immersion in a gamified security training context is associated with increased BI

to comply with the security policies employees are learning.

Moreover, both the TRA [5] and the TPB [4] predict a strong link between intention and behavior. In the information security context, several studies have suggested that it is more realistic and valid to measure actual behaviors than intentions [11, 22, 60]. It is particularly important to measure actual behaviors, as it is clear that good intentions do not always lead to good behaviors in organizational security contexts, as employees often have conflicting roles and motivations with respect to security requirements [11, 22, 83]. Measuring behaviors is an excellent way to further determine whether gamification can result in meaningful security training and behavioral changes. Thus,

H6. Increased BI should be associated with an increased actual phishing response, when following the same security policies.

Modeling Counter-explanations Through Control Variables

Testing counter-explanations of other possible predictors has pragmatic relevance in IS security research [83]. We do so by modeling common demographic covariates and alternative security constructs, as follows: age, gender, experience, education, organization computer monitoring (OCM) [27], organization security communication (OSC) [17, 88]; and top management security commitment (TMSC) [46].

PROCEDURES FOR DESIGN EVALUATION FOR PROOF-OF-VALUE

Pilot Study for Proof-of-Value

Once we deemed the system to have achieved reasonable proof-of-concept, we prepared to rigorously establish its proof-of-value. Thus, we first conducted a pilot study with university students (N = 45). The study spanned three months and included monthly data collection. This allowed us to refine the procedures and test the instruments' validity and reliability.[ix]

Main Study Design for Proof-of-Value in Actual Use

The final study for formal proof-of-value in actual use was designed as a controlled field experiment using an unbalanced design of two treatment and one control groups. A total of 800 employees from a large international French company were invited to participate, who were confirmed from HR records to have not received security training. Only offices in which English was the main language (i.e., the United

Kingdom, the United States, and Australia) participated to prevent potential language issues and website localization. The 488 employees who positively responded[x] were randomly assigned to one of two groups: the gamified system treatment group (420 employees) or the email treatment group (68 employees); they were determined to be demographically equivalent. The control group (38 employees) was not explicitly invited so they would not know they were used as controls; this was created using a random sample from the organization's HR database of employees. The participation rate of over 50% is high for organizational field studies. Thirty-six participants were removed because of implausibly short response times [under eight minutes], incomplete answers, and illogical response patterns. The final sample included 384 responses. The average age of the participants was 33.4 years (SD = 11.2 years); 52% were male and 48% were female.

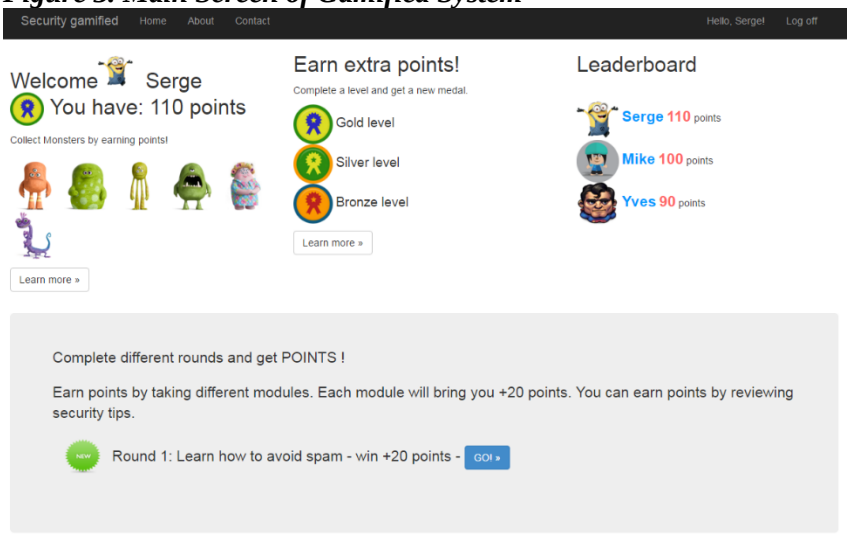
Notably, the control group received no training or notifications. However, the gamification and email groups received the same training content and the same frequency of training, reminders /notifications, and quizzes. These two sets of participants were invited to take a quiz after completing each training session. This allowed for a cleaner manipulation between gamified interaction versus non-gamified email interaction. A custom Web-based gamification application was created by one of the researchers using.NET technology, and all design elements were developed based on previously identified game mechanics.

Gamified System and Procedures

The gamified system's objective was to educate users about security topics using various game design elements. In the first step, users registered for and signed in the website. Next, users chose an avatar (Appendix B, Figure B.1), and after completion, users were redirected to the main screen (see Figure 3).

At the first login, the gamemaster appeared and explained the game mechanics (e.g., how to earn points). The gamemaster appeared at different stages/levels of the game. For example, if the user had not logged in for over one week, the gamemaster sent an email (the same notification frequency was used for the email group) inviting the user to continue and providing the user with information about current achievements and top scorers (via the leaderboard). The objective of the game was to complete quizzes

Figure 3. Main Screen of Gamified System



and read different tips related to security education about malicious software (malware), spam, and especially how to avoid falling victim to phishing attempts. By playing different rounds, users accumulated points that allowed them to receive additional incentives in the form of monsters (monsters represented trophies) and to advance to another level (bronze, silver, and gold). In addition, a leaderboard of top employees with their corresponding scores was displayed on the main menu interface. Different rounds with quizzes and other educational elements were offered to users every two weeks (again, the same frequency was used for the email group). This gave users time to educate themselves about different security and phishing topics and to acquire the knowledge necessary to correctly answer questions.

The participants in the email control group did not participate in the controlled field experiment but followed a more traditional security education approach limited to email communication. Email communication (Figure B.5) offered the same content as the gamified system, but the format was less visually appealing and contained more textual explanations. Nonetheless, the content of the email communication was useful, clearly written, and easy for employees to understand.

We chose phishing as a key focus of the training because it is a much more urgent concern for management than behaviors like reading spam or failing to check for viruses. Moreover, responding to a phishing attack is an objectively auditable security behavior. Participants completed a survey at three months and at the end of the game (i.e., six months). To measure users' security behaviors, we sent a

phishing email to employees' inboxes without their knowledge. This process was administered by a third-party company that specializes in phishing testing/training. An email was sent to employees asking them to change their passwords by clicking on the internal company's link (the link led to the third party's website, which tracked a lack of compliance). Employees' decisions were coded as binary variables ('0' for not clicking or '1' for clicking), which measured users' security behaviors. To establish anonymity, and a link between each employee's security gamification platform presence and the phishing email, a unique random number was created for each participant and that number was used for the survey.

Measures for Design Evaluation

The measurement items were borrowed or adapted from previous studies (see Table C.1). All scales were reflective, using a seven-point Likert-type scale ranging from completely disagree (1) to completely agree (7). A new measure was created for challenge, which corresponded to the perception of the game's level of difficulty. The actual phishing behavior construct was a binary value (0 or 1).

ANALYSIS FOR FINAL PROOF-OF-VALUE

Measurement Model

First, a confirmatory factor analysis was conducted. The results indicated that some items' standardized regression weights were lower than 0.60 (e.g., JOY1 and PEOU1) and were thus removed. After rerunning the model, all other factor loadings were higher than the recommended 0.60 value. Next, the average variance extracted (AVE) values were checked to ensure that all values exceeded 0.50.

According to all tests, the measurement model exhibited good reliability, and convergent validity and discriminant validity[xi] were established. Table D.1, in online Appendix D, details the loadings. Table D.2 summarizes the discriminant validity and AVEs for the model. Table D.7 presents the statistics used to assess the quality of the measurement model's measures. We confirmed that the Cronbach's α values for all scales were higher than 0.70 and found that multicollinearity was not an issue.[xii] In addition to taking several measures to prevent common methods bias, we conducted two tests to demonstrate that it was likely not a factor in our data (see "CMB and Multicollinearity" in Appendix D).

Structural Model Results

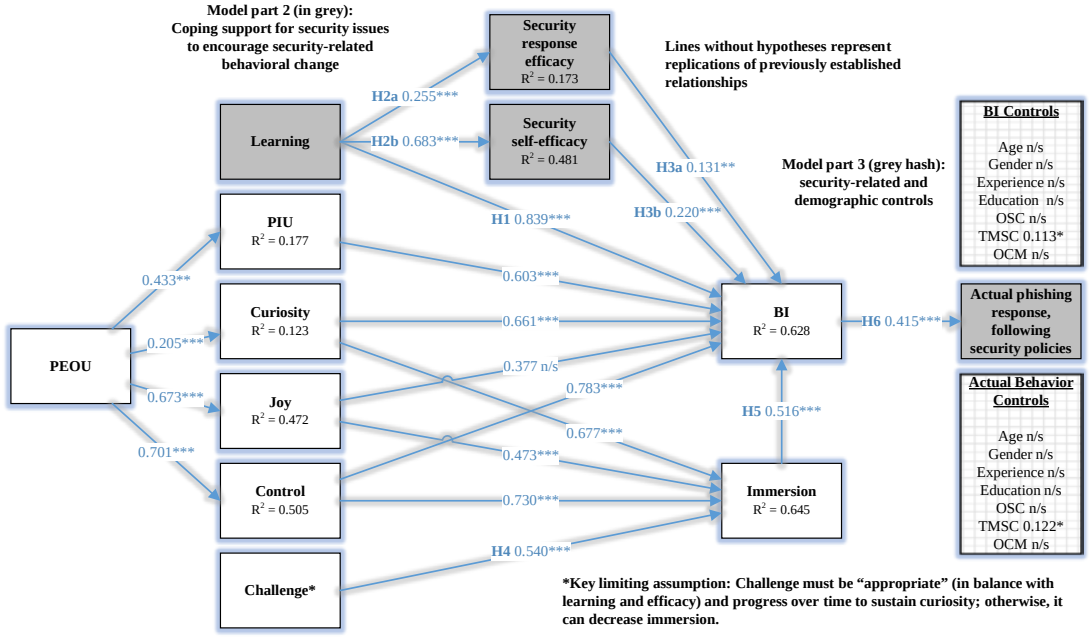
We used Mplus 7 software, a covariance-based structural equation modeling (CB-SEM) tool, to test the model. Mplus 7 allowed for the theory and hypotheses to be assessed for model fit and provided a logistic regression analysis for the dichotomous outcome variable (i.e., actual phishing response behavior). Age, gender, experience, and education were included in the analysis as controls for intentions and behaviors; the organizational security constructs of TMSC, OSC, and OCM were added as counter-explanations. Figure 4 depicts the structural model results. Table D.8 summarizes the full structural model testing details, which included three stages of model testing: Model part 1 (HMSAM replication only), Model part 2 (extension to add coping and challenge), and Model part 3 (full model with controls and theoretical counter-explanations). All HMSAM replications were supported, except joy to BI and control to immersion. All hypotheses were supported (H4 is addressed last); our results at month three were similar, but not as strong (Table D.3). When we modeled the data for the email treatment alone, the results were much worse (see Tables D.4 and D.5). Interestingly, the email treatment results worsened or remained the same between the initial three-month period and the six-month period.

Finally, H4 was supported, but because H4 was hypothesized as a nonlinear relationship, we first ran the model with original indicators and then estimated the construct that had the proposed nonlinearity. We then performed the transformation through a squared term and entered this new variable in the SEM model, in which both the main effect and the squared term were related to the same dependent variable. A similar approach was used in [70], which tested a curvilinear model with covariance-based SEM. The variance inflation factors (VIFs) increased and ranged from 1.945 to 9.453 with the model fit RMSEA 0.062, SRMR 0.069, CFI 0.929, and TLI 0.923 for the gamification treatment and RMSEA 0.072, SRMR 0.078, CFI 0.905, and TLI 0.902 for the email treatment. Although the model fit and VIFs worsened, the values were still within the acceptable ranges and are expected to worsen when including a squared term.

Manipulation Checks of Instrumental Goals

Given that the field experiment was conducted to determine whether the gamified training system could increase learning and immersion as well as decrease employee susceptibility to phishing, a crucial piece

Figure 4. Structural Model Testing Results of the Operationalized Kernel Theory at Six Months[xiii]



of the analysis was the manipulation checks, as they indicated whether the gamified system delivered on its instrumental goals to improve security learning and compliance. This was confirmed by the two manipulation checks. First, we compared the degree to which the small group of randomly selected employees (those in the control group who did not participate in the gamified group or email group) and the gamified treatment group were successfully phished. The results in Tables 1 and 2 indicate that there was a significant difference in the expected direction. Strikingly, those with email training performed no better than those who received no training at all.

Table 1. Summary of Who Was and Was Not Phished in the Control and Treatment Groups

Group	Phished (*n* = 149)	Not phished (*n* = 341)
Control group* (*n* = 38)	17 (44.7%)	21 (55.3%)
Gamified group (*n* = 384)	105 (27.3%)	279 (72.7%)
Email group (*n* = 68)	27 (39.7%)	41 (60.3%)

* Note: The control group was a randomly selected group of employees who had not received training through gamification or email. The *n*'s represented in this table were used for the analysis after all data drops.

Table 2. Comparisons between the Treatment and Control Groups

Comparison	Phished (Z-score)*
Gamified vs. control	2.2561*
Gamified vs. email	2.0664*
Control vs. email	0.5041 n/s

* Note: A result is significant at $p < 0.05$ (assuming a two-tailed hypothesis test).

The treatment effects that occurred between the email and gamified groups in terms of the model

variables were also examined. A multivariate analysis of variance (MANOVA)[xiv] was run to compare the values for significant differences. Crucially, our group (i.e., cell) sizes were different; thus, we carefully checked to ensure that we adhered to the assumptions of MANOVA, which included the confirmation of Box M (see "Box M and MANOVA assumptions" Appendix D). Table D.9 summarizes the means and

SDs comparing these two groups at the end of six months (Tables D.6 and D.7 provide the respective correlations). To compare the actual behaviors between the two groups, the Z-score (2.2561, $p < 0.05$) was calculated, confirming that the two groups' actual behaviors were significantly different and in the expected direction.

DISCUSSION

The discussion of our study is guided by the structural example provided by Abbasi et al. [1] and the DSR evaluation principles of Hevner et al. [41]. We also lean heavily on inspiration found in following Liu et al. [59], Nunamaker Jr et al. [76], Peffers et al. [81], and Gregor and Hevner [38].

Recap of Our General DSR Study Goals

The goals of our DSR study were pragmatically driven from the serendipitous confluence of several opportunities: First, we were approached by a French international company that wanted help improving their internal SETA program to increase organizational security compliance. Second, we saw gamified security training as a way to improve their training, but we observed that previous research efforts in this area were incomplete, with too little focus on the design artifact, long-term data, objective behavioral assessment, use with actual employees, and so on. Third, the recent gamification editorial by Liu et al. [59] pointed to similar issues in the gamification literature that has thus far largely failed bridge theory, design, and methodology. Fourth, previous gamification studies in a security context have largely lacked a systematic DSR approach. Consequently, we thus proposed that gamified security training represents a natural opportunity to apply a DSR approach to bridge the related opportunities in design, theory, methodology, and practice.

Applying our goals to practice, we followed rigorous and systematic DSR principles, and created a working gamified SETA system based on an iterative application of theory, extant literature,

prototyping, and feedback from the target organization. In the field, the goal of our study was to extend and recontextualize kernel theory (i.e., HMSAM) to explain how organizations can positively bring about security learning and associated behavioral changes in employees, specifically in a gamified security training context. We aimed to do so through the novel application of two parallel factors: (1) focusing on positive interventions through gamified training (as opposed to traditional manipulations of punishments, fear, and threats) and (2) improving employees' security learning and efficacy to strengthen their ability to cope with security challenges (in our context, phishing). Together, these two factors were predicted to result in positive behavioral change in employees through their increased intentions to follow security policies and the alignment of their actual phishing response behaviors with the organizational security policies in which they were trained.

Recap of Our DSR Approach

To support our DSR approach, we adhered to a DSR methodology that closely followed the method advocated by Nunamaker Jr et al. [76] and elaborated on by Peffers et al. [81]. This involved an extensive, iterative process based on the security gamification literature, DSR, system development, and feedback from the target organization. In doing so, we followed a rigorous but highly iterative process that can be best described in nine steps: (1) established the gamified security training system as an artifact; (2) focused on the design problem relevance; (3) created objectives for design evaluation; (4) applied a DSR kernel theory that is contextualized to gamification; (5) proposed design principles that bridge DSR design objectives and the DSR kernel theory; (6) established proof-of-concept through multiple methods; (7) established proof-of-value through multiple methods; (8) created a working foundation in which proof-in-use can be established over time; and (9) evaluated the results rigorously according to multiple DSR evaluation guidelines.

Establishing Proof-of-Concept

Before moving to proof-of-value, we carefully followed the steps for proof-of-concept suggested by Peffers et al. [81], as detailed extensively earlier in the paper. Of the many discoveries and design artifacts that were created through this process, perhaps the most fundamental outcome was driven by the ideas

from Liu et al. [59] that a key step of designing a gamified system is to carefully choose the gamification design principles that serve as the bridge between the system and meaningful engagement. This step establishes the user-interaction processes that occur between user-system-user actors. We see this approach as key to tying the design to a meaningful kernel theory (i.e., HMSAM) that further explains meaningful engagement and measures that can be used to evaluate it. We posit that these ideas are core to fostering proof-of-concept.

Thus, HMSAM provided the basis for our kernel theory and evaluation model, which consisted of two main components that further inspire design assumptions and principles: (1) the importance of designing for *motivation fulfillment* to inspire meaningful and engaged gamified systems use and (2) the importance of designing for *coping support* so the users can deal with security issues and thus encourage security-related behavioral change. These ideas also inspired the two design principles we carefully applied in building our training artifact. These principles were systematically applied with the literature and iterative design sessions, finally yielding a strong case for proof-of-concept, as detailed in our earlier DSR section and the appendices.

Establishing Overall Proof-of-Value

To establish proof-of-value, once the system was deemed ready, we first formally pilot tested it and the kernel theory with students. However, the key step in establishing proof-of-value involved a long-term field experiment with actual employees using the gamified security training system. Our overall proof-of-value is demonstrated in that the DSR artifact worked as intended and as theorized. Their SETA program was thus improved. Going forward, we discuss proof-of-value in three details respects: (1) in actual practice, (2) in research, and (3) in theory.

Establishing Proof-of-Value in Actual Practice

Our proof-of-value in actual practice was demonstrated in multiple respects. First, our long-term study demonstrated both strong *ecological validity*[xv] and *meaningful engagement* [59]. Achieving meaningful engagement is an important factor of building gamified information systems and should be addressed in view of both instrumental and experiential benefits [59]. Not only did the participants use the

gamified system over six months during their normal course of work, but also a third party phished the unwitting participants and control group to objectively assess whether they followed the phishing response outlined by the organization's security policies.

Likewise, the employees' learning, efficacy, and behaviors were strongly and positively influenced (and thus the SETA program), thereby demonstrating the utility of our extended model as well as the value of the gamified design elements included in the system. Aside from the strong manipulations and statistical results of our design, we received positive feedback from the organizational leadership and participating employees. Again, we focused solely on manipulating positive motivations and improving participants' coping responses and did not use typical approaches involving deterrence, threats, or fear.

Gamified system design elements contributed to a more immersive experience and appealed to powerful motivations while building employees' coping capabilities. We thus demonstrated that a gamified security training system approach offers a new and unique way to improve employee security learning and compliance and can be implemented without the usual "carrots and sticks." Although threats, fear, sanctions, and costs/benefits may have an appropriate place in organizations [e.g., 11, 27, 52], these approaches also run the risk of backfiring, causing reactance, a sense of injustice, or employee engagement in "malicious compliance" or other microaggressions [63, 65]. Most employees prefer to work in an enjoyable and supportive work environment rather than one laden with rules, regulations, fear, and punishments. This is also an important consideration when choosing the design characteristics of an organizational e-training system. We demonstrated that adding the abovementioned design elements could improve a system's efficacy and lead to higher levels of motivation.

If our results hold, their implications for security training in practice are noteworthy. Our study provides empirical evidence that email training and email notifications designed to help employees avoid phishing attacks might be largely futile. This was particularly useful information for the French company with whom we worked, as they used email training extensively and thought it was more efficacious than our results indicated. It was no surprise that this contrasting approach yielded far less motivation and immersion; after all, it was not a gamified system. However, we were surprised that there was no

statistically significant difference in terms of the actual behavior of the email group and the pure control group. The emails were thoughtfully constructed, and they used the same content and many of the same visuals as the gamification system; however, employees who received the email treatment had the same outcomes as those who received no training. This is clear evidence that pushing security content to end users via email is not effective in this context; in contrast to a gamified training system, it neither fosters motivations nor strengthens coping.

Following Baxter et al.'s [8] conclusions, and in consultation with the French company, we also realized that conducting training in short, spaced-out segments is more helpful and natural to employees than long training segments. Traditional training in corporate environments can be highly disruptive, time-consuming, unmotivating, and even irritating. We suspect this is also likely true with gamification itself: it is more likely to remain novel and fresh if introduced in short segments that provide welcome relief from normal work duties.

These overall results provide proof-of-value in actual practice—not just because our system worked as intended, but because meaningful pragmatic change was introduced to improve the client organization through improved systems and practices.

Establishing Proof-of-Value in Research

Aside from providing proof-of-value in actual practice, our value extends to challenging and extending gamified security research. We do so by offering a study that uniquely involves all of the following—thus addressing compelling research gaps and opportunities in this area: (1) long-term data collection; (2) actual working employees in large, international for-profit organizations; (3) control and treatment conditions; (4) a mix of perceptual and objective measurement; (5) being grounded in a native IS kernel theory (i.e., HMSAM) that was contextualized to gamified organizational security training; (6) an actual working gamified training system rigorously designed and developed through DSR principles; (7) actual empirical demonstration of "meaningful engagement" (e.g., improved IT security compliance) and interaction outcomes (e.g., measurable increased immersion) [cf. 59].

Notably, we are the first to use a long-term study in a gamified security context. This approach

has long been recommended for researching technology-related training in the workplace [97]. As noted, related attempts at one-off, cross-sectional SETA [36] and gamified security training [8] have failed to produce increased learning and behavioral change. We argue that the likely reasons for this failure are simple: fulfilling motivations, inducing a state of immersion, fostering learning, and developing coping responses all take time, so it is exceedingly difficult to produce these outcomes over the course of a brief cross-sectional study. We conclude that gamification should be studied using a long-term approach because flow and immersion occur in stages rather than simultaneously [e.g., 48, 62].

Another research contribution is that actual security compliance was measured and a positive relationship between BI and employee actions in response to the phishing attempts they were trained to recognize was confirmed. This finding is in line with previous studies in non-security contexts, and researchers have called for additional studies confirming the link between intentions and actual security behaviors in various security contexts [22]. Our study is the first to examine this important relationship in a gamified security context.

Establishing Proof-of-Value in Theory

We not only were able to demonstrate an effective DSR kernel theory with our HMSAM application, but we also did so in a manner that can contribute to theory development beyond DSR. Our first key contribution here is the extension of HMSAM to a gamified security training and compliance context. To do so, we added new constructs to the original model (i.e., security self-efficacy, security response efficacy, challenge, learning, and actual security behavior). The addition of new constructs was crucial, as it enabled us to build a working prototype that could empirically establish proof-of-value.

As a further empirical demonstration of our theoretical contribution, the R^2 for BI in our baseline replicated HMSAM model was 0.318; furthermore, our modeling extensions (excluding the trivial contributions of the control variables) literally doubled the R^2 for BI to 0.638. In terms of a pragmatic effect size, this change is statistically *huge* ($f^2 = 0.884$) and pseudo *F*-test results show that the change is highly significant ($F = 328.84$, $p < 0.001$).[xvi] Moreover, we added the demographic controls and the counter-explanations of TMSC, OSC, and OCM. Only TMSC was significant, and it contributed only to

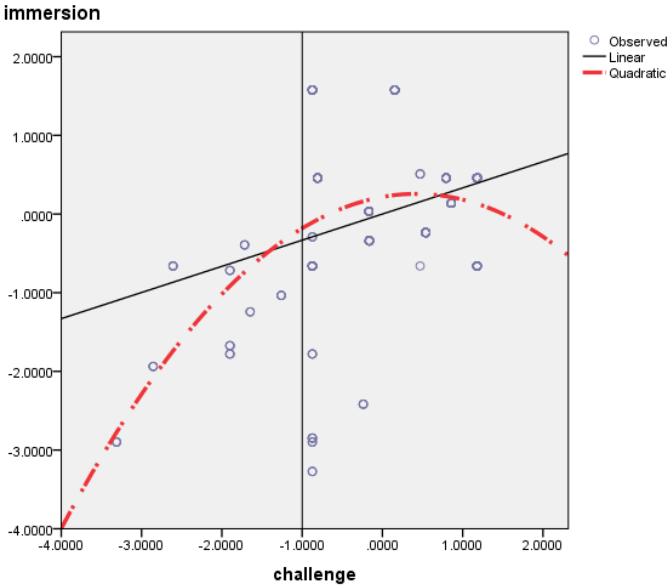
an extremely small increase in R^2. As with all of these additions, the R^2 for BI only went from 0.638 to 0.645. This change is statistically *trivial* ($f^2 = 0.019$).[xvii] Because a pseudo *F*-test may not be strictly correct and can have limited value, we also used the method to compare nested models by calculating AIC/BIC values for the nested models. We found fit statistics of 2,945.3 (Akaike's information criterion [AIC]) and 2,988.1 (Schwarz's Bayesian information criterion [BIC]) for true treatment and fit statistics of 2,231.4 (AIC) and 2,362.3 (Schwarz's BIC) for email treatment. Overall, these tests provide further evidence that our theoretical contribution is both statistically significant and meaningful in terms of its application in the field of highly efficacious gamification interventions.

Moreover, the challenge-related findings led to a couple of unexpected key contributions that have the capacity to improve theory, research, and practice in gamified security training. We showed that challenge did lead to immersion, but this finding comes with a crucial theoretical limitation: if the challenge is not appropriate, the results might be undermined. This has long been an underlying assumption of gamification and flow theory [24]. Researchers in these fields [29] have explained that to experience flow (or *immersion*), three conditions should be satisfied: clear goals, unambiguous feedback, and a balance of challenges and skills. However, to the best our knowledge, what constitutes an appropriate challenge has never been empirically confirmed. Reviewer feedback on our paper led us to realize that if this limiting assumption indeed holds, there is a point at which a challenge becomes detrimental to fostering immersion—it becomes overly challenging and thus inappropriate. If this continues to hold elsewhere, the relationship between challenges and immersion should not be linear; instead, it should be curvilinear and ideally a quadratic, inverted U-shaped curve that reaches a diminishing marginal return at a certain apex.

We thus conducted a follow-up analysis to run two contrasting regression models—one presenting challenge and immersion as a linear relationship and another presenting it as a curvilinear relationship. The curvilinear model was statistically superior, yielding a statistically higher increase in R^2 (a nearly twofold increase).[xviii] This means that the relationship between challenge and immersion is in fact ideally modeled as curvilinear. When we visually depicted this relationship with fitted regression

lines, the best fit was shown by an inverted U-shaped curve (see Figure 5). This is the first empirical evidence for two long-held notions: (1) good gamification delivery involves progressive challenges, but (2) such challenges must be appropriate and thus there is a certain point at which a challenge can overwhelm an end user and cause diminishing returns.

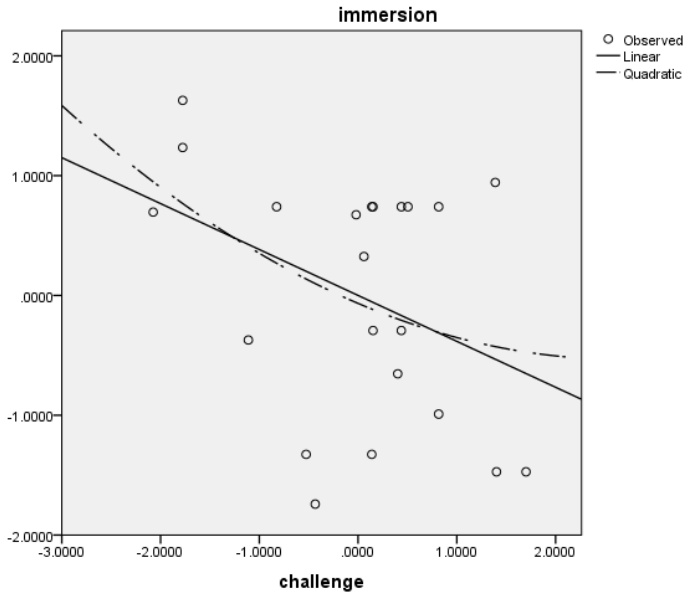
Figure 5. The Curvilinear and Inverted U-shaped Relationship between Challenge and Immersion



Note: All the statistics used in this figure are standardized. Challenge is on the x-axis and immersion is on the y-axis. This shows that challenges are helpful to immersion, but only to a certain point.

Given that *challenge* is essential to our gamification context, we also suspected that challenge would not have a similarly beneficial relationship in the non-gamified email treatment. We thus conducted a similar analysis to test whether the relationship between challenge and immersion in this case was curvilinear. We found two unexpected and fascinating results. First, there was no significant difference in this context between linear or curvilinear modeling;[xix] thus, we can conclude that in our non-gamified email training context, the relationship between challenge and immersion was linear. We also found that this was a negative relationship, such that challenge was a detrimental factor (see Figure 6). This makes sense, as an email training environment does not offer the gamified features that can turn a challenge into a positive factor, with the result that challenge in an email training environment simply becomes a source of frustration for many employees.

Figure 6. The Linear and Negative Relationship Between Challenge and Immersion in a Non-gamification Context



Finally, we learned that the "time dimension" does not favor email treatment. From the initial three months (Table D.4) to six months (Table D.5), we observed stable or decreasing statistical power as time passed, meaning that the effects of the email treatment diminished over time. The time factor appeared to play an important role in the gamified systems (see Figures 5 and 6) because it added a new dimension that should be carefully positioned and built into the gamified system. The right balance among time, play, and learning should be carefully designed and chosen so that users do not lose their motivation to learn and play. Our conclusion thus is that the key to improving the French company's security climate was through gamified security training that offered an appropriate challenge and thus led to a more rewarding and immersive experience that fostered actual behavioral change. If this holds, the theoretical implications are compelling.

A Research Agenda to Establish Proof-of-Use

Beyond demonstrating proof-of-concept and proof-of-value, according to [75, p. 16], a third concept, *proof-of-use* can also be applied to DSR. ***Proof-of-use*** is demonstrated when DSR

> *seeks to create self-sustaining and growing communities of practice around a generalizable solution, and to demonstrate that practitioners can successfully create and gain value from their own instances of the generalizable solution.*

Thus, proof-of-use is perhaps the greatest limitation and future research opportunity for this research. The first obvious issue and opportunity here is that of generalizability. Although we obtained a high degree of ecological validity by using an actual organization and an actual gamified security training system, using one organization limits the generalizability of our results. Each organization has slightly different and unique security and compliance climates, just as the executives, managers, and employees vary widely. For example, in some organizations, a "shadow IT culture" is widespread [90]. This could produce different results, as the security expectations in these organizations are higher than average. Such organizations could exhibit differences in how employees learn and comply based on individual-level and national-level cultural differences.

Likewise, building a working prototype was an iterative process in which we actively involved the French organization, as we sought to receive meaningful feedback on the prototype to align it as closely as possible to organizational realities and needs. Consequently, the working prototype may need further modifications if adapted to another organization. Regardless, our design principles and kernel theory need to be further modified, applied, and tested, such that the broader practice community is further positively influenced—not just the French organization.

Another consideration that needs to be examined for proof-in-use is that we cannot entirely know what outcome would have occurred had traditional manipulations of extrinsic security motivations been used in this setting, as we intentionally did not use them. Again, we took this approach because research indicates that extrinsic motivations are inherently weaker than intrinsic motivations [30, 61] and can backfire in organizational settings. However, mixed motivations are common and can be dealt with effectively in systems use [61]; thus, it might be possible to create a security environment where the outcomes are maximized through a careful combination of extrinsic and intrinsic motivations. For example, a prize scheme for top performers (e.g., salary increase, bonus payment, or recognition as "security employee of the quarter") could facilitate further investigations of whether and how these types of motivation influence behaviors. It is also important to determine which kinds of extrinsic motivations are the most problematic for this setting.

We also believe this study offers an ideal opportunity for the kind of future interdisciplinary and programmatic research called for by Nunamaker et al. [74]. For example, our work was conducted over the course of six months with a continual infusion of fresh material. What would happen if the use was extended and the fresh material ran out, such that novelty and challenge diminished? At what point would learning and behavioral change deteriorate? Further research should explore these issues and apply HMSAM to other gamification and compliance contexts in which intrinsic motivations and immersion play strong roles. Moreover, the extended gamified HMSAM model could likely be applied to other areas of compliance training, such as those related to corporate governance, risk assessment, audit, and other financial controls. Our extensions might also work in a compelling manner for iterative IS development processes and requirements engineering.

Moreover, for further proof-in-use, more research needs to examine each element involved in gamified security training. We studied an entire system, but each part should also receive further attention. For example, each of the gamification elements in Table A.3 could be studied as its own dependent variable with a highly contextualized model and series of studies. Thus, researchers could examine the kinds of avatars that are more likely to enhance a loss of self-consciousness and that are the most autotelic. Or the gamemaster could be the subject of many models and studies. The lack of a gamemaster is a drawback of traditional e-training systems that focus on completion rates or on quantity over quality. The gamemaster, who plays the role of a "positive virtual mentor," could motivate increased participation. Most employees would likely prefer to be supported by a positive person or positive virtual mentor than nagged by a negative virtual mentor. Based on the analysis of quantitative answers, the gamemaster could provide an individual improvement activity in which learners could improve their knowledge by taking additional quizzes/tests. The gamification effects should then be more effective and the overall motivation to participate and learn should increase. Consequently, Table A.3 alone points to many possibilities for programmatic research. Another related avenue for future research is to examine in more detail how various levels of media richness (e.g., the use of video, sound, or animation in the communication media) may further influence the individual's security learning process.

CONCLUSION

We conducted a DSR project that theoretically and empirically demonstrates that careful design with selected gamified IT artifacts can improve extant organizational security training systems. Namely, we show through a long-term field experiment that gamification can be used to foster training systems that are less invasive of employees' everyday work routines, that provide intrinsic motivation to learn and comply with security efforts, and that provide the efficacy necessary so that employees will actually comply. We also demonstrated improvement in actual anti-phishing behaviors by hiring a third-party firm that phished the employees as a natural experiment to test their reactions. We also provide a novel empirical demonstration of the conceptual importance of "appropriate challenge" in this context. We conclude that a mix of DSR, carefully contextualized kernel theory, and long-term research in an empirical field setting is a promising way to effectively implement gamification in organizations.

REFERENCES

1. Abbasi, A; Zhang, Z; Zimbra, D; Chen, H; and Nunamaker Jr, JF. Detecting fake Websites: the contribution of statistical learning theory. *MIS Quarterly*, 34, 3 (2010), 435-461.
2. Adams, M and Makramalla, M. Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, 5, 1 (2015), 5-14.
3. Agarwal, R and Karahanna, E. Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly*, 24, 4 (2000), 665-694.
4. Ajzen, I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 2 (1991), 179-211.
5. Ajzen, I and Fishbein, M. *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice-Hall, 1980.
6. Bandura, A. Perceived self-efficacy in cognitive development and functioning. *Educational Psychologist*, 28, 2 (1993), 117-148.
7. Banfield, J and Wilkerson, B. Increasing student intrinsic motivation and self-efficacy through gamification pedagogy. *Contemporary Issues in Education Research*, 7, 4 (2014), 291-298.
8. Baxter, RJ; Holderness, DK; and Wood, DA. Applying basic gamification techniques to it compliance training: evidence from the lab and field. *Journal of Information Systems*, 30, 3 (2016), 119-133.
9. Benware, CA and Deci, EL. Quality of learning with an active versus passive motivational set. *American Educational Research Journal*, 21, 4 (1984), 755-765.
10. Boot, WR; Kramer, AF; Simons, DJ; Fabiani, M; and Gratton, G. The effects of video game playing on attention, memory, and executive control. *Acta Psychologica*, 129, 3 (2008), 387-398.
11. Boss, SR; Galletta, DF; Lowry, PB; Moody, GD; and Polak, P. What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39, 4 (2015), 837-864.
12. Brown, SA; Dennis, AR; and Venkatesh, V. Predicting collaboration technology use: Integrating technology adoption and collaboration research. *Journal of Management Information Systems*, 27, 2 (2010), 9-54.

13. Bui, A; Veit, D; and Webster, J. Gamification–a novel phenomenon or a new wrapping for existing concepts? In Proceedings of *International Conference on Information Systems*, Fort Worth, US, 2015.
14. Bulgurcu, B; Cavusoglu, H; and Benbasat, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34, 3 (2010), 523-548.
15. Burns, AJ; Roberts, TL; Posey, C; and Lowry, PB. Examining the influence of organizational insiders' psychological capital on information security threat and coping appraisals. *Computers in Human Behavior*, 68, March (2017), 190-209.
16. Chen, X; Chen, L; and Wu, D. Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems*, 58, 4 (2018), 312-324.
17. Chen, Y; Ramamurthy, K; and Wen, K-W. Organizations' information security policy compliance: stick or carrot approach? *Journal of Management Information Systems*, 29, 3 (2012), 157-188.
18. Chin, W; Marcolin, B; and Newsted, P. A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic Mail Emotion/Adoption Study. *Information Systems Research*, 14, 2 (2003), 189-217.
19. Coonradt, C. *The Game of Work: How to Enjoy Work As Much As Play*. Layton, Utah: Gibbs Smith, 2007.
20. Cowley, B; Charles, D; Black, M; and Hickey, R. Toward an understanding of flow in video games. *Computers in Entertainment (CIE)*, 6, 2 (2008), 20.
21. Crossler, RE and Bélanger, F. The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage. *Journal of Information System Security*, 5, 3 (2009),
22. Crossler, RE; Johnston, AC; Lowry, PB; Hu, Q; Warkentin, M; and Baskerville, R. Future directions for behavioral information security research. *Computers & Security*, 32, (2013), 90-101.
23. Csikszentmihalyi, M. *Finding Flow: The Psychology of Engagement with Everyday Life*. New York, NY: Basic Books, 1997.
24. Csikszentmihalyi, M. *Beyond Boredom and Anxiety*. San Francisco, CA, US: Jossey-Bass, 2000.
25. Cyr, D; Head, M; and Ivanov, A. Perceived interactivity leading to e-loyalty: Development of a model for cognitive-affective user responses. *International Journal of Human Computer Studies*, 67, 10 (2009), 850-869.
26. D'arcy, J and Herath, T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, 20, 6 (2011), 643-658.
27. D'Arcy, J; Hovav, A; and Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20, 1 (2009), 79-98.
28. D'Arcy, J and Lowry, PB. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29, 1 (2019), 43-69.
29. Davis, M and Csikszentmihalyi, M. *Beyond Boredom and Anxiety: The Experience of Play in Work and Games*. Washington, DC: Amer Sociological Assoc, 1977.
30. Deci, EL and Ryan, RM. *Intrinsic Motivation and Self-determination in Human Behavior*. New York, NY: Plenum Press, 1985.
31. Deterding, S. Gamification: Designing for motivation. *Interactions*, 19, 4 (2012), 14-17.
32. Deterding, S; Dixon, D; Khaled, R; and Nacke, LE. From game design elements to gamefulness: defining gamification. Presented at *15th international academic MindTrek conference: Envisioning future media environments*, Tampere, Finland, 2011, pp. 9-15.
33. Domínguez, A; Saenz-de-Navarrete, J; De-Marcos, L; Fernández-Sanz, L; Pagés, C; and Martínez-Herráiz, J-J. Gamifying learning experiences: Practical implications and outcomes. *Computers &*

Education, 63, April (2013), 380-392.
34. Edwards, DA; Wetzel, K; and Wyner, DR. Intercollegiate soccer: saliva cortisol and testosterone are elevated during competition, and testosterone is related to status and social connectedness with teammates. *Physiology & Behavior*, 87, 1 (2006), 135-143.
35. Fassbender, E; Richards, D; Bilgin, A; Thompson, WF; and Heiden, W. VirSchool: The effect of background music and immersive display systems on memory for facts learned in an educational virtual environment. *Computers & Education*, 58, 1 (2012), 490-500.
36. Ferguson, AJ. Fostering e-mail security awareness: The West Point carronade. *EDUCASE Quarterly*, 28, 1 (2005), 54-57.
37. Floyd, DL; Prentice-Dunn, S; and Rogers, RW. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30, 2 (2000), 407-429.
38. Gregor, S and Hevner, AR. Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37, 2 (2013), 337-355.
39. Haans, RF; Pieters, C; and He, ZL. Thinking about U: Theorizing and testing U-and inverted U-shaped relationships in strategy research. *Strategic Management Journal*, 37, 7 (2016), 1177-1195.
40. Herath, T and Rao, HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47, 2 (2009), 154-165.
41. Hevner, AR; March, ST; Park, J; and Ram, S. Design science in information systems research. *MIS Quarterly*, 28, 1 (2004), 75-105.
42. Ho, SM and Warkentin, M. Leader's dilemma game: An experimental design for cyber insider threat research. *Information Systems Frontiers*, 19, 2 (2015), 1-20.
43. Hong, W; Chan, FK; Thong, JY; Chasalow, LC; and Dhillon, G. A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, 25, 1 (2013), 111-136.
44. Hsu, C-Y; Tsai, C-C; and Wang, H-Y. Facilitating third graders' acquisition of scientific concepts through digital game-based learning: The effects of self-explanation principles. *The Asia-Pacific Education Researcher*, 21, 1 (2012), 71-82.
45. Hsu, JS; Shih, S; Hung, YW; and Lowry, PB. The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, 26, 2 (2015), 282-300.
46. Hu, Q; Dinev, T; Hart, P; and Cooke, D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43, 4 (2012), 615-660.
47. Hwang, G-J; Wu, P-H; and Chen, C-C. An online game approach for improving students' learning performance in web-based problem-solving activities. *Computers & Education*, 59, 4 (2012), 1246-1256.
48. Jennett, C; Cox, AL; Cairns, P; Dhoparee, S; Epps, A; Tijs, T; and Walton, A. Measuring and defining the experience of immersion in games. *International Journal of Human-computer Studies*, 66, 9 (2008), 641-661.
49. Jensen, ML; Dinger, M; Wright, RT; and Thatcher, JB. Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, 34, 2 (2017), 597-626.
50. Johns, G. The essential impact of context on organizational behavior. *Academy of Management Review*, 31, 2 (2006), 386-408.
51. Johnson, RD and Marakas, GM. Research report: the role of behavioral modeling in computer skills acquisition: toward refinement of the model. *Information Systems Research*, 11, 4 (2000), 402-417.
52. Johnston, AC; Warkentin, M; and Siponen, M. An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, 39, 1 (2015), 113-134.
53. Kapp, KM. *The gamification of learning and instruction: game-based methods and strategies for training and education*. San Francisco, US: John Wiley & Sons, 2012.
54. Koepp, MJ; Gunn, RN; Lawrence, AD; Cunningham, VJ; Dagher, A; Jones, T; Brooks, DJ; Bench, C; and Grasby, P. Evidence for striatal dopamine release during a video game. *Nature*, 393, 6682

(1998), 266-268.
55. Kohn, A. Why incentive plans cannot work. *Harvard Business Review*, 71, 5 (1993), 54-60.
56. Kühn, S; Gleich, T; Lorenz, R; Lindenberger, U; and Gallinat, J. Playing Super Mario induces structural brain plasticity: gray matter changes resulting from training with a commercial video game. *Molecular Psychiatry*, 19, 2 (2014), 265-271.
57. Kumaraguru, P; Sheng, S; Acquisti, A; Cranor, LF; and Hong, J. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10, 2 (2010), 1-31.
58. Li, M; Jiang, Q; Tan, C-H; and Wei, K-K. Enhancing user-game engagement through software gaming elements. *Journal of Management Information Systems*, 30, 4 (2014), 115-150.
59. Liu, D; Santhanam, R; and Webster, J. Toward meaningful engagement: A framework for design and research of gamified information systems. *MIS Quarterly*, 41, 4 (2017), 1011-1034.
60. Lowry, PB; Dinev, T; and Willison, R. Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems*, 26, 6 (2017), 546-563.
61. Lowry, PB; Gaskin, J; and Moody, GD. Proposing the multimotive information systems continuance model (misc) to better explain end-user system evaluations and continuance intentions. *Journal of the Association for Information Systems*, 16, 7 (2015), 515-579.
62. Lowry, PB; Gaskin, J; Twyman, N; Hammer, B; and Roberts, T. Taking 'fun and games' seriously: Proposing the hedonic-motivation system adoption model (HMSAM). *Journal of the Association for Information Systems*, 14, 11 (2013), 617-671.
63. Lowry, PB and Moody, GD. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal*, 25, 5 (2015), 433-463.
64. Lowry, PB; Moody, GD; and Chatterjee, S. Using IT design to prevent cyberbullying. *Journal of Management Information Systems*, 34, 3 (2017), 863-901.
65. Lowry, PB; Posey, C; Bennett, RJ; and Roberts, TL. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, 25, 3 (2015), 193-230.
66. Ma, Q; Pei, G; and Meng, L. Inverted u-shaped curvilinear relationship between challenge and one's intrinsic motivation: Evidence from event-related potentials. *Frontiers in Neuroscience*, 11, (2017), 131.
67. Martocchio, JJ and Judge, TA. Relationship between conscientiousness and learning in employee training: mediating influences of self-deception and self-efficacy. *Journal of Applied Psychology*, 82, 5 (1997), 764.
68. Mathieu, JE; Martineau, JW; and Tannenbaum, SI. Individual and situational influences on the development of self-efficacy: Implications for training effectiveness. *Personnel Psychology*, 46, 1 (1993), 125.
69. Meng, L; Pei, G; Zheng, J; and Ma, Q. Close games versus blowouts: optimal challenge reinforces one's intrinsic motivation to win. *International Journal of Psychophysiology*, 110, December (2016), 102-108.
70. Moody, GD; Lowry, PB; and Galletta, DF. It's complicated: explaining the relationship between trust, distrust, and ambivalence in online transaction relationships using polynomial regression analysis and response surface analysis. *European Journal of Information Systems*, 26, 4 (2017), 379-413.
71. Nelson, MJ. Soviet and American precursors to the gamification of work. Presented at *Proceedings of the 16th International Academic MindTrek Conference*, Tampere, Finland, 2012, pp. 23-26.
72. Nicholson, S. A recipe for meaningful gamification. *Gamification in Education and Business*. Switzerland: Springer International Publishing, 2015, pp. 1-20.
73. Niehaves, B and Ortbach, K. The inner and the outer model in explanatory design theory: the case of designing electronic feedback systems. *European Journal of Information Systems*, 25, 4 (2016), 303-

316.
74. Nunamaker, JF; Twyman, NW; Giboney, JS; and Briggs, RO. Creating high-value real-world impact through systematic programs of research. *MIS Quarterly*, 41, 2 (2017), 335-351.
75. Nunamaker Jr, JF; Briggs, RO; Derrick, DC; and Schwabe, G. The last research mile: Achieving both rigor and relevance in information systems research. *Journal of Management Information Systems*, 32, 3 (2015), 10-47.
76. Nunamaker Jr, JF; Chen, M; and Purdin, TD. Systems development in information systems research. *Journal of Management Information Systems*, 7, 3 (1990), 89-106.
77. Nunamaker Jr., JF and Briggs, RO. Toward a broader vision for information systems. *ACM Transactions on Management Information Systems*, 2, 4 (2011), 1-12.
78. Osterloh, M and Frey, BS. Motivation, knowledge transfer, and organizational forms. *Organization Science*, 11, 5 (2000), 538-550.
79. Payne, SC; Youngcourt, SS; and Beaubien, JM. A meta-analytic examination of the goal orientation nomological net. *Journal of Applied Psychology*, 92, 1 (2007), 128.
80. Peffers, K; Gengler, CE; and Tuunanen, T. Extending critical success factors methodology to facilitate broadly participative information systems planning. *Journal of Management Information Systems*, 20, 1 (2003), 51-85.
81. Peffers, K; Tuunanen, T; Rothenberger, MA; and Chatterjee, S. A design science research methodology for information systems research. *Journal of Management Information Systems*, 24, 3 (2007), 45-77.
82. Pentland, SJ; Twyman, NW; Burgoon, JK; Nunamaker Jr, JF; and Diller, CB. A video-based screening system for automated risk assessment using nuanced facial features. *Journal of Management Information Systems*, 34, 4 (2017), 970-993.
83. Posey, C; Roberts, TL; and Lowry, PB. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32, 4 (2015), 179-214.
84. Posey, C; Roberts, TL; Lowry, PB; Bennett, RJ; and Courtney, J. Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, 37, 4 (2013), 1189-1210.
85. Robson, K; Plangger, K; Kietzmann, J; McCarthy, I; and Pitt, L. Understanding gamification of consumer experiences. *Advances in Consumer Research*, 42, (2014), 352-356.
86. Rousseau, DM and Fried, Y. Location, location, location: Contextualizing organizational research. *Journal of Organizational Behavior*, 22, 1 (2001), 1-13.
87. Ryan, RM and Deci, EL. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, 55, 1 (2000), 68.
88. Sen, R; Subramaniam, C; and Nelson, ML. Determinants of the choice of open source software license. *Journal of Management Information Systems*, 25, 3 (2008), 207-240.
89. Shernoff, DJ; Kelly, S; Tonks, SM; Anderson, B; Cavanagh, RF; Sinha, S; and Abdi, B. Student engagement as a function of environmental complexity in high school classrooms. *Learning and Instruction*, 43, (2016), 52-60.
90. Silic, M and Back, A. Shadow IT–A view from behind the curtain. *Computers & Security*, 45, (2014), 274-283.
91. Siponen, M and Vance, A. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, (2010), 487-502.
92. Treiblmaier, H; Putz, L-M; and Lowry, PB. Setting a definition, context, and research agenda for the gamification of non-gaming systems. *Association for Information Systems Transactions on Human-Computer Interaction*, 10, 3 (2018), 129-163.
93. Twyman, NW; Lowry, PB; Burgoon, JK; and Jay F. Nunamaker, J. Autonomous scientifically controlled screening systems for detecting information purposely concealed by individuals. *Journal of Management Information Systems*, 31, 3 (2014), 106-137.
94. Vance, A; Lowry, PB; and Eggett, D. Using accountability to reduce access policy violations in

information systems. *Journal of Management Information Systems*, 29, 4 (2013), 263-289.
95. Vance, A; Lowry, PB; and Eggett, D. A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly*, 39, 2 (2015), 345-366.
96. Venkatesh, V; Morris, MG; Davis, GB; and Davis, FD. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27, 3 (2003), 425-478.
97. Venkatesh, V and Speier, C. Computer technology training in the workplace: A longitudinal investigation of the effect of mood. *Organizational Behavior and Human-Decision Processes*, 79, 1 (1999), 1-28.
98. Wakefield, RL and Whitten, D. Mobile computing: a user study on hedonic/utilitarian mobile device usage. *European Journal of Information Systems*, 15, 3 (2006), 292-300.
99. Wang, J; Li, Y; and Rao, HR. Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, 17, 11 (2016), 759.
100. Wang, J; Li, Y; and Rao, HR. Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences. *Information Systems Research*, 28, 2 (2017), 378-396.
101. Willison, R; Lowry, PB; and Paternoster, R. A tale of two deterrents: Considering the role of absolute and restrictive deterrence in inspiring new directions in behavioral and organizational security. *Journal of the Association for Information Systems*, 19, 12 (2018), 1187-1216.
102. Willison, R and Warkentin, M. Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly*, 37, 1 (2013), 1-20.

[i] Generally, gamification is the application of game-like features to nongaming systems to help foster a useful outcome other than entertainment [32, 92]. The features include design elements, such as points, levels, leaderboards, and badges.

[ii] Namely, they statistically rejected the associated hypotheses "H2: Individuals who receive gamified training will exhibit greater knowledge acquisition than individuals who receive non-gamified training or no training." See page 20 of their text for statistical details.

[iii] Ultimately, users' behaviors should be influenced by the gamified tasks in which a flow experience—or "immersion" in the systems version [3, 22]—is the objective. This objective can be achieved either through intrinsic or extrinsic motivation, but intrinsic motivation tends to be stronger for an instrumental goal [61, 87]. Intrinsic motivation can be involved in the task itself, whereas extrinsic motivation results from external factors (e.g., financial rewards or career goals).

[iv] We aim for both application to practice but also to tackle the challenge of integrating our unique gamified security learning context into theory [50]. This is challenging because contextualization is about "linking observations to a set of relevant facts, events, or points of view that make possible research and theory that form part of a larger whole" [86, p. 1]. Following Johns [50], we carefully evaluated, designed, and implemented the implications of contextual appreciation for both theory building and practice to achieve the best possible match between theoretical relevance and practical implications.

[v] *Meaningful engagement* in this context refers to the outcomes of the gamification design. That is, the gamified system should foster (1) enjoyment, (2) interaction/engagement, and (3) enhanced instrumental task outcomes [59].

[vi] Other studies have implemented several of the gamification design principles, but typically in fields like computer science. Such studies are especially important for advancing gamification-related design and algorithms. However, most either used student subjects, did not advance a "cohesive theoretical foundation," or did not focus on achieving meaningful engagement, as suggested by Liu et al. [59].

[vii] The organization we worked with preferred to have a simple system implemented without too much interaction between employees to prevent distractions from their normal work. Thus, we did not apply pie/bar charts, activity stream, giving kudos, social networking, forming teams, providing cash incentives, personalized goals, or social support.

[viii] For example, a study found that playing the Super Mario Bros. game resulted in a significant gray matter increase, impacting spatial navigation, strategic planning, and working memory [56]. Another example is the use of video games by public safety and military organizations to recruit and train soldiers and to treat their psychological

disorders by literally improving their coping and cognitive processes.

[ix] A couple of the more notable improvements we made included two major adjustments: (1) the number of times a participant could take a quiz was limited because some pilot participants had used automatic clicking tools (such as AutoClicker) as a workaround to earn additional points, and (2) a gamemaster role was implemented, as this role can be an important motivational factor for users.

[x] We have no further survey data on the employees who opted to not participate. However, as an accepted surrogate test to assess nonresponse bias, we tested to ensure that there was no statistical difference between "early" and "late" respondents. We used time stamps of when they accepted joining the project. We grouped early and late respondents and compared their responses to the Likert-type scale questions using a MANOVA test. The results did not reveal any statistical significance ($F = 1.976$, $p = 0.313$).

[xi] The second step of model validation was to test for discriminant validity. Here, we first considered whether there was any discriminant overlap in the items in the factor analysis, and we consequently dropped two more items that yielded poor discriminant validity. We then examined overall discriminant validity by placing the square root of the reflective construct's AVE on the diagonal line and the correlations between the constructs below it. The square root value of the AVE should be higher than all latent constructs, which was the case.

[xiii] PEOU = perceived ease of use; PIU = perceived intrinsic usefulness; BI = behavioral intentions to follow security policies; OSC = organization security communication; TMSC = top management security commitment; OCM = organization computer monitoring.

[xiv] As the design is unbalanced, we tested the equality of covariance matrices using Box's M test. The result was not significant.

[xv] Ecological validity should not be confused with external validity. *Ecological validity* indicates the degree to which the findings of a research study can be generalized to real-life settings, often because they are collected or generated in real-life settings (e.g., actual employees trying to solve real work tasks). Although this form of validity—unlike internal and external validity—is not strictly required for a study to be valid, it is a particularly meaningful but often overlooked consideration for research areas that are highly intertwined with practice, such as security and privacy research [cf. 60].

[xvi] To demonstrate these points empirically, we followed Chin et al. [18] The effect of adding our contextualized improvements to HMSAM (step 2 of model building) was calculated as follows [18]: f^2 (Cohen's effect size) = $R^2_{\text{extended model}} - R^2_{\text{HMSAM}}$) (.320) / (1 - $R^2_{\text{extended model}}$) (.362). In this case, $f^2 = 0.884$, which is a "huge" effect size (anything above 0.35 is considered "large"), is rarely seen in the organizational security literature. To test the statistical significance of this increase, we conducted a pseudo F-test as follows: f^2 (Cohen's effect size) * (n – k – 1), where n is the sample size and k is the number of independent variables. In our case, n = 384; and we conservatively set k to 11 for all of the constructs preceding BI. This resulted in F = 328.84, $p < 0.001$.

[xvii] f^2 (Cohen's effect size) = $R^2_{\text{covariate model}} - R^2_{\text{extended model)}}$ (.007) / (1 - $R^2_{\text{extended model}}$) (.362). In this case, $f^2 = 0.019$, which is a "trivial" effect size ("small" requires a size of 0.20 or greater).

[xviii] The model summary statistics between Model 1 (linear) and Model 2 (curvilinear; quadratic) are listed in the following table:

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	Change Statistics		
					R^2 Change	*F* Change	Sig. *F* Change
1	.332[a]	.111	.109	.945	.111	55.903	.000
2	.438[b]	.192	.188	.902	.081	45.070	.000

[a] = predictors (constant), challenge; [b] = predictors (contact), challenge, $challenge^2$ (quadratic relationship)

[xix] Using only the data in the email treatment, the model summary statistics between Model 1 (linear) and Model 2 (curvilinear; quadratic) are listed in the following table:

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	Change Statistics		
					R^2 Change	*F* Change	Sig. *F* Change
1	.383[a]	.147	.104	.9687208	.147	3.444	.078
2	.391[b]	.153	.064	.9903298	.006	.137	.716

[a] = predictors (constant), challenge; [b] = predictors (contact), challenge, $challenge^2$ (quadratic relationship)

The current reference for this work is as follows:

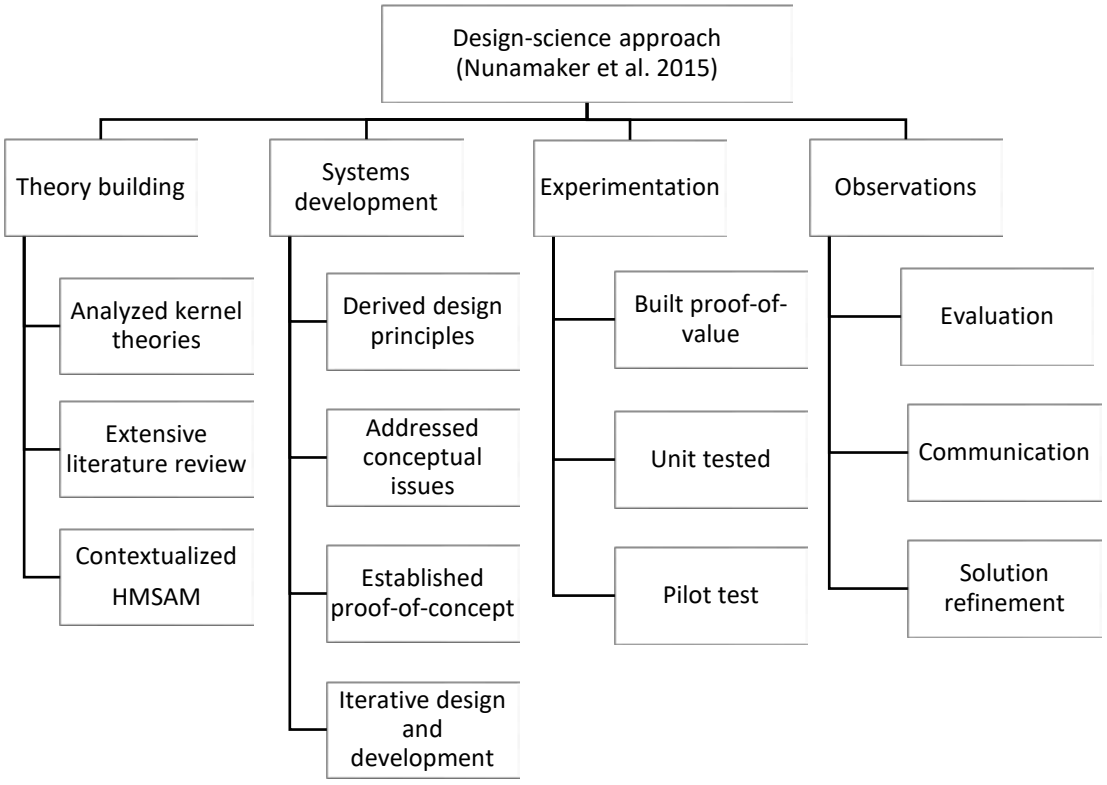
> Mario Silic and Paul Benjamin Lowry (2019). "Using design-science based gamification to improve organizational security training and compliance," ***Journal of Management Information Systems (JMIS)*** (accepted 01-Aug-2019)

If you have any questions, would like a copy of the final version of the article, or would like copies of other articles we've published, please contact any of us directly, as follows:

- **Dr. Mario Silici**
  - Email: mario.silic@unisg.ch
  - Website: https://www.alexandria.unisg.ch/persons/6160
- **Professor Paul Benjamin Lowry**
  - Email: Paul.Lowry.PhD@gmail.com
  - Website: https://sites.google.com/site/professorlowrypaulbenjamin/home
  - System to request Paul's articles: https://seanacademic.qualtrics.com/SE/?SID=SV_7WCaP0V7FA0GWWx

ONLINE APPENDIX A. GAMIFICATION REVIEW, DEFINITIONS, AND DESIGN ARTIFACTS IN THE LITERATURE

Figure A.1. The Design-science Approach We Followed from Nunamaker Jr et al. [61]



Gamification Definitions Review

By reviewing the somewhat disjointed literature, we draw several conclusions: (1) the purpose of gamification is not clearly articulated and is inconsistent across different studies; (2) virtually all definitions include game-design artifacts but not necessarily the same ones; and 3) most definitions are primarily based on the early works of Deterding et al. [23] and Huotari and Hamari [36], although the two sources have several fundamental differences. For Huotari and Hamari [36], gamefulness (i.e., playful elements of games) results from the psychological consequences through the gamified system with the overall objective to invoke psychological experiences. In contrast, Deterding et al. [23] argued that gamefulness results from the system design and focuses on applying "game elements" to non-game contexts.

Another key difference stems from the gamification objective. Deterding et al.'s [23] definition is less clear about gamification's objectives, whereas Huotari and Hamari [36] suggested that gamification involves changing psychological and behavioral user states (e.g., it has instrumental goals). Given its greater clarity regarding objectives, the latter proposal was adopted, noting that gamification in an information security context should leverage the hedonic experience by focusing on motivational aspects in which psychological outcomes should be reframed by the system design to shape one's behaviors (e.g., improve security behaviors). This can be achieved by adding game design elements (e.g., challenge, levels, points, and leaderboards) to non-gaming contexts to ultimately influence behaviors for desired outcomes.

Gamification Security Literature Review Details

To identify all gamification studies that relate to the information security context we used the following publication sources: ACM, IEEE, AISeL, EBSCOhost, Google Scholar, ScienceDirect, ISI Web of Knowledge, Proquest,

SSRN/Research Gate for working papers and various other security related workshops (e.g., Dewald Roode Workshop on Information Systems Security). We searched through all databases by using the terms (("gamification security*" OR (game* security) OR (gami* security) OR (gami* security) OR (gami* information) OR (gami* organizational)) to search through the title, abstract and keywords of all articles published in the respective databases to find all publications. Search time was not restricted. To be more comprehensive and ensure all important prior work is included, we used Google Scholar with combination of information / gamification / security keywords. Our last step was a backward/forward search as suggested by Webster and Watson [82].

Table A.1 summarizes all of the studies we found that used gamification in a security context. Table A.2 further overviews the different gamification studies related to the information security context. Each study brought some new and interesting findings, yet at the same time, there were several conceptualizations and operationalization issues with the gamification elements. We carefully studied each in detail to discern what could be learned from them to improve our study and the creation of our corresponding gamified system. We note our detailed findings as follows.

For example, Baxter et al. [8] used several gamification elements (story, role-playing, goals, feedback, progress), as part of an existing third-party system (True Office), and conducted two studies: 1) a controlled laboratory experiment with students and 2) field study with bank employees. The first challenge that arises from this approach is the fact that study could not change, adapt, or modify the third-party system. This could explain the results that found the gamified system to be more fun and enjoyable; but did not find any connection between the knowledge acquisition and the use of gamified vs non-gamified learning module. The study does explain that the third-party system was lacking elements such as competition based on points and leaderboards, achievement badges or levels, and virtual currencies. We argue that by not having these important elements could have led to study's contradictory results by not being a properly gamified system. Clearly, this could have influenced the motivational aspects. Indeed, creating a game-like user experience to activate individual user motives [36] is one of the gamification aims. Another issue with the study design is that it focused on the study elements (e.g., story) as being the main driving and influencing factor. Although story is an important element in the game design literature, many people do not like 'story-based' games, and thus there is a decline in this type of game [51]. Thus, we argue that focusing too much on the story element, in the information security context, can hinder the importance of other elements. That is, story is an important element as long as it stays short, simple and efficient. This is particularly true in the organizational context where employees generally do not have time to read the story, nor to be experience the story immersion.

Next, Trinkle et al. [79] investigated the factors influencing an employee's willingness to play online games by evaluating employee's intentions through vignette-based approach. Although, the study did not specifically use any gamification elements, it is interesting to see that employees were less likely to participate in playing online games in the presence of social media policy. This suggests that for an effective gamification system, a good information security policy is needed to leverage and support playing games activities that are approved by the organization. However, the study suggests a surprising result indicating that in presence of logging and monitoring, employees tend to play online games less in absence of the social media policy. Clearly, if the importance of the gamified system is clearly communicated and explained to employees, this could enhance the system effectiveness where elements such as fun, could receive a new dimension.

Meanwhile, another study used a simulation experiment by using an online game to understand how organizational trust relationships can be identified in the insider threat context [33]. Although the study offers a novel approach to understand how to be more compliant from an employee perspective, we argue that its main challenge is its applicability and scalability to the organizational context. The study does use several gamification elements that are inter-connected by the Game-Master concept, which is a core game mechanism. Although this is an interesting concept, applying it to a gamification system that should be both, scalable and easily applicable, which can be quite challenging. However, we believe that this concept can be an important aspect when building a gamification system. Indeed, game mastering, also referred to as Orchestration [75], could be an important part of the gamification system, especially in the organizational context, as the role of the game-master would be to organize the game, engage participants, schedule sessions, track progress, and manage participants activities to create an interaction effect between all other gamification elements.

The avatar element is another interesting concept suggested by Adams and Makramalla [1], which highlights the importance of identifying attacker characteristics that should lead to improving employees' abilities in preventing or reacting to data breaches. While this study suffers from lack of empirical evidence, we believe that understanding attacker characteristics is an important aspect that was already confirmed by past studies [15, 25, 47]. However, associating avatar to attacker types or characteristics could be potentially misleading as the main role of avatar, above all, is to represent people's identity which is their customized image that bears similarity to their real

selves [55]. In this context, we argue that avatar element should simply be implemented as one's representation of selves in which users should be able to construct a sense of self (using natural or idealized avatar). More importantly, past research has found that avatars that are cartoon-like seem to be more appealing, attractive, and credible to users [60]. Hence, in the gamified system avatars, in our view, should be represented through a fun dimension (e.g., cartoony approach) which should influence gaming attractiveness.

Interestingly, the study by Dabrowski et al. [20] used a very different approach when compared to the approach as suggested by Adams and Makramalla [1]. Dabrowski et al. showed that by using various gamification design elements, students' motivation, efforts and extra work can be increased positively. Interestingly, the study claims that students' knowledge increased, which conflicts with the findings by Baxter et al. [8]. However, the knowledge and self-efficacy increase findings in [6, 20] should be treated with caution, as these are based on students' self-assessment rather than on actual knowledge gain measurements and statistics.

It seems that web-based security games can be an interesting new direction to learn cybersecurity skills and increase student's knowledge. This is suggested by the Code Hunt framework [24], an educational game platform, in which two interesting concepts are proposed: Clue and Hint system and Just-in-time learning. Although these concepts are similar with the (immediate) feedback [1, 8, 67, 76], we argue that the two concepts should be separated into two elements: 1) immediate feedback and 2) tips or hint elements. Another interesting element is fun that should be part of the gamification system as not only fun creates the necessary psychological link between the user and the system [2], but it also brings the entertaining effect which influences player enjoyment that is one of the important issues in successful game design [37]. Importantly, rarely did studies use a control group (versus a treatment group) to assess the gamification elements. We found two studies that had a control and treatment—one by Vail [80] and one by Ophoff and Janowski [62]. Vail [80] study provided evidence that students' are more engaged and experience more fun. Ophoff and Janowski [62] demonstrated that students will choose a stronger password in presence of the gamification design elements such as leaderboard.

We derive several limitations and challenges from reviewing these past studies. First, a lack of empirical evaluation is present in most of the papers [e.g., 3, 9, 24, 43]. Although the focus of many papers is the gamification of the students' learning process, the majority of the papers fail to provide any empirical evidence that would support the design elements they propose. Second, the majority of these studies focus on students. This is not a problem in the context in which most of these studies were conducted (e.g., course learning). However, the applicability and generalizability of their findings is highly questionable in an organizational security context, in which employees have different tasks and motivations, and react differently to learning situations. Third, all of the studies were collected data as one-time snapshot, which could reveal to be quite problematic in the gamification context. Indeed, a player plays a game not just at one particular time point, but rather it is an increasing time spectrum, where player will either 1) abandon playing the game or 2) will become addict. Therefore, to be able to measure the gamification effectiveness, the data collection has to occur over different points in time and hence, be longitudinal in the approach. This could explain some of the contradictory results that past studies suggested. Fourth, lack of the control group is another limitation of several past studies where gamification was applied without any comparison to the control sample. Fifth, from this review we could see not only, a quite inconsistent way of implementing different gamification elements, but also different interpretations of a gamification element definition.

Table A.1. Gamification Studies Related to Information Security Context (Part 1)

Source	Research context	Findings	Concept under study	Participants + sample size	Method	Dependent Variable	Theory or framework	Gamification Design element
Adams and Makramalla [1]	The use of gamification methods that enable all employees and organizational leaders to play the roles of various types of attackers is discussed	Two separate streams are discussed: gamification and entrepreneurial perspectives – for the purpose of building cybersecurity skills	Security education	N/A	Essay (discussion paper)	N/A	N/A	Progress mechanics, player control, problem solving, story
Amorim et al. [3]	Discusses how to better offer training while considering new developments that involve both multimedia production and the "gamification" of training	Paper suggests the gamification to be used as a new training approach	Privacy	N/A	Essay (discussion paper)	N/A	Game Development Framework	N/A
Banfield and Wilkerson [6]	Assessed gamification as a method of experiential learning theory (ELT) on student motivation and self-efficacy to perform System Engineering/Information Assurance (IA) tasks.	Results indicated high intrinsic motivation and self-efficacy from the students 96 interviewed	General security	96 interviews with students	Direct observation method, semi-structured interviews One-time	Intrinsic motivation, self-efficacy	Experiential learning theory	Problem solving, challenge, scoreboard, leaderboard, competition, story, goals, objectives
Baxter et al. [8]	Laboratory and field experiment on data privacy and a field study to test whether a training environment with basic gamification elements results in greater trainee satisfaction and knowledge acquisition	Basic gamification results in higher satisfaction levels in the lab and field, but only marginally significant improvements in learning	Data privacy training	Study 1: 33 students in True Office, 38 in Thomson Reuters group, 45 control group Study 2: 856 Employees	Lab experiment Field study Survey One-time	Trainee satisfaction Knowledge acquisition	General gamification theory	Story, goals, feedback, progress
Boopathi et al. [9]	A game is developed which is divided into various levels and at each level the knowledge of students in Cyber security concepts is tested	Gaming approach in Cyber security education will be a big step forward in training more students in computer security and create a secure online world	Cyber security	N/A	Simulation One-time	Security knowledge level	Game theory	Levels, storyline, competition, problem solving
Dabrowski et al. [20]	Game-like course setup is presented and evaluated through the unique approach through student surveys	Well-established gaming-like competitive approach is not only highly appreciated by students but also raises their interest and motivation to put more effort and extra work into their security education.	Security education	One generic course survey with 130 students and a specific Internet Security course survey with 183 Students	Survey One-time	N/A	N/A	Storyline, challenge, scoring, incentives, leaderboard, badges, privileges

Fouché and Mangle [24]	Student's interest in cybersecurity is analyzed through the Code Hunt framework by adding the gaming model	Leveraging Code Hunt's structured gaming model can address these weaknesses and makes cybersecurity training more accessible	Cyber security	N/A	Design principles	N/A	N/A	N/A
Ho and Warkentin [33]	Simulation of an insider betrayal scenario for analyzing organizational trust relationships	Leader's dilemma game is built to provide methodological approach	Insider threat	N/A	Simulation One-time Experimental design	Team-Leaders trustworthiness	Theory of trustworthiness attribution	Progress, goals, award system
Lee and Manners [43]	Discussed how elements of games can be used in penetration testing	Penetration testing represents a game	Cyber security	N/A	Essay (discussion paper)	N/A	N/A	Objectives, rules, points, skills, brotherhood, addictiveness, fun
Melki and Chatrieh [53]	Describe the experience of the University of Balamand in adopting gamification as a means to provide community education in the field of cyber security	In the case of Lebanon, the majority of internet users are outside the regular outreach of any training or awareness program. This fact is a challenge for cybersecurity education in Lebanon.	Cyber security	N/A	Essay (discussion paper)	N/A	N/A	N/A
Ophoff and Janowski [62]	Investigates how gamification can be used to effectively motivate users to choose stronger passwords	Results found that there was a significant difference between the mean password strength of the group without feedback and other groups. Gamification can be used to motivate users to choose stronger passwords	Individual security	581 students	Online experiment, Survey One-time	Password Strength	N/A	Badges, Leaderboard, Baseline meter, Avatar
Ruboczki [67]	Essay about providing more efficient cloud computing training awareness	General discussion about the possible gamification use in cloud computing context	Cloud computing	N/A	Essay (discussion paper)	N/A	Game theory	Progress mechanics, narrative, player control, feedback, problem solving, levels, social connection
Thornton and Francia III [76]	Paper discusses gamification, the application of gaming elements in non-game contexts, with regard to information systems and information security	Results indicate positive student attitudes toward gamified approaches, as well as improved attendance and success rate	Security education	150 students + 150 control group	Ethnography Survey Longitudinal	N/A	Flow theory	Leaderboard, levels, guidance, experience points, geometric rewards, feedback, team assignment,

	training in the classroom							
Trinkle et al. [79]	By using accountability and boundary theories, factors influencing employees to play OSN games on company-owned computers	The presence of a social networking policy, logging awareness, and monitoring practices reduced participants' likelihood of playing OSN games on company-owned computers	Social networking	193 employees	Online factorial survey One-time	Likelihood to play games	Accountability and boundary theories	N/A
Vail [80]	An Information Security Management course was selected to use as a case study to investigate if an interactive game would engage learners	The study found that students found the class more enjoyable, and at least 46% felt engaged due to the introduction of gamification	General security	15 students as treatment group + 20 students for control group	Case study Survey, exploratory comparative study One-time	Engagement Levels of learning gains	Problem-based learning	Goals, problem solving, objectives

Table A.1. Gamification Studies Related to Information Security Context (Part 2)

Source	**Long-term?**	**Used employees?**	**Used control groups?**	**Actual behaviors?**	**Theory was used?**	**Addressed Six aspects of Meaningful Engagement***						
						EEF	**EEM**	**EIIEF**	**EIIEM**	**EIT**	**EITM**	**Engagement asssessment**
Adams and Makramalla [1]	No	N/A	N/A	N/A	No	No	No	No	No	No	No	Little evidence
Amorim et al. [3]	No	No	No	No	No	No	No	No	No	No	No	Little evidence
Banfield and Wilkerson [6]	No	No	No	No	Yes	No	No	Yes	Yes	No	No	Partial implementation
Baxter et al. [8]	No	Yes (for 1 of 2 studies)	Yes	No	No	Yes	Yes	No	Yes	No	Yes	Instrumental task was not enhanced as learning was not improved
Boopathi et al. [9]	No	No	No	No	Yes	Yes	No	Yes	No	No	No	Discussion paper
Dabrowski et al. [20]	No	No	No	No	No	Yes	Yes	Yes	No	Yes	No	Partly achieved as EIIEM and EITM were not measured
Fouché and Mangle [24]	No	No	No	No	No	No	No	No	No	No	No	Little evidence
Ho and Warkentin [33]	No	No	N/A	No	Yes	No	No	No	No	No	No	Little evidence
Lee and Manners [43]	No	No	No	No	No	No	No	No	No	No	No	Little evidence
Melki and Chatrieh [53]	No	No	No	No	No	No	No	No	No	No	No	Little evidence
Ophoff and Janowski [62]	No	No	No	No	No	Partly	No	No	No	Yes	Yes	Focused only on motivating users to choose stronger passwords.
Ruboczki [67]	No	N/A	No	No	Yes	No	No	No	No	No	No	Little evidence
Thornton and Francia III [76]	No	No	No	No	Yes	No	No	No	No	Yes	Yes	Limited observed as only instrumental task was enhanced
Trinkle et al. [79]	No	Yes	No	No	Yes	No	No	No	No	No	No	Little evidence
Vail [80]	No	No	No	No	Yes	Yes	No	Yes	No	No	No	Assessed only through fostering of enjoyable and immersive experiences.

*NOTE: EEF: Enjoyable experience fostered; EEM: Enjoyable experience measured; EIIEF: Engaging/interactive/immersive experience fostered; EIIEM: Engaging/interactive/immersive experience measured; EIT: Enhanced instrumental task; EITM: Enhanced instrumental task measured

Table A.2. Overview and Critical Review of Gamification Studies Related to Information Security Context

Source	Element(s) used	Element implementation	Relation to study	Empirical results review
Adams and Makramalla [1]	Avatar Challenges Feedback Mastery Mechanics Player control Problem solving Progress Story	Story is based on the attacker types that are combined with its characteristics (e.g., insiders) to propose avatars (bricolage, effectuation, causation, social, hubris and emancipation). Problem solving allows trainees to learn and retain new information.	All elements are used to promote the gamified cybersecurity skills training allows the trainees to experience an attack through the eyes of a cyber-attacker and therefore from entrepreneurial perspectives.	Paper does not have any empirically validated results but instead is a discussion paper.
Amorim et al. [3]	Boundary Holistic Structural Temporal	Game elements are classified into four categories: 1) holistic (game instance, game session, play session and extra-game activities); 2) boundary (rules, modes of play, goals and sub goals); 3) temporal (actions, events, closures and sub closures, end conditions and evaluation functions) and 4) structural interface, game elements, players, game facilitator and game time.	The framework for the development of a serious game for training on privacy by design is presented that should include four categories of gamification elements.	No empirical study was conducted.
Banfield and Wilkerson [6]	Challenge Competition Knowledge test Scoreboard	Computer science students were provided an IP address and expected to find the subnet mask and range of available IP addresses, and perform some networking tasks. Seven web servers were used as different levels and whiteboard was shown in front of students.	Gamification was used as a teaching pedagogy in Information Assurance classes to increase intrinsic motivation and self-efficacy in students. The results indicate an increase in both student intrinsic motivation and self-efficacy.	No control group was used to compare the results. Students need to be graded for the final certificate which could be a limiting factor.
Baxter et al. [8]	Feedback Goals Progress Role playing Story	A commercially-developed gamified platform (True Office) was used in which different elements existed through the training environment. A story of a fictional investigation of a breach of security, where an international bank's customer data was compromised, was used. Learning objectives with various milestones were presented to the user along with the role playing where an employee acts as an investigator, making assessments of the fictional employee's statements and the objects. To take a post-training quiz various milestones (e.g., interviewing people to confirm that one has read policy documents) needed to be completed.	Two studies were run: 1) a controlled laboratory experiment compared game-style approach of True Office with Thomson Reuters non-gamified learning module and a condition with no training; 2) a field study with a large international bank focusing only on US employees.	Empirical results provide contradictory results as the gamified system was found to be more fun, enjoyable and preferred method over other others; however, no statistically significant evidence showed that the gamified system increased the user's knowledge. Also, study lacks other gamification techniques such as competition based on points and leaderboards, achievement badges or levels, or virtual currencies.
Boopathi et al. [9]	Addictiveness Levels Story Tests	The game is divided in 4 levels with knowledge tests. Level difficulty increases with level completion. Once all 4 levels are completed, team is eligible for Hackathon competition which consists in set of challenges.	The gamified approach is used to test students' knowledge in various computer security concepts. A game is developed and divided into different levels.	No empirical study was conducted.
Dabrowski et al. [20]	Badges Challenges Competition Deadline	Students are introduced a funny story of secret missions, big companies, helicopters, and so on. Students, assigned a pseudonym, have to complete a challenge which increases	Cyber security game-like course setup is built including several game design elements to increase students' interest and motivation. Results indicate that	Two points limit the paper's generalizability: 1) being enrolled in the IT course, students were already tech-savvy which could influence their gamification experience and

	Feedback Forum Hierarchy Incentive Leaderboard Mastery Negative feedback Peer pressure Privileges Pseudonym Story	over time. Leaderboards are displayed to all students that can acquire badges and additional privileges more successful they are. For every challenge students solve, they move up in the hierarchy (from Nobody to Master Guru). Students are provided with instant grading feedback allowing reinforcing the positive feelings of mastering a challenge. Also, peer pressure and deadline negative feedback are used to as additional design elements.	game design elements support more effort and extra work from students, improving their motivation when engaged in the security course.	subsequent security learning, and 2) students need to be graded for the final certificate which could be an extrinsic motivating factor.
Fouché and Mangle [24]	Challenges Clue and Hint system Competition Just-in-time learning Tests	Elements are implemented within an educational gaming platform where competition. Description on how exactly elements are implemented is missing.	Code Hunt, an interactive educational gaming platform that aims to develop program- ming skills, is proposed to improve cybersecurity trainings and program- ming skills.	No empirical study was conducted.
Ho and Warkentin [33]	Assignments Competition Goals Reward Roles Scenario	Controlled online game environment was created where competition between teams (each team has several categories of players: Game-Master, Team-Leader and Team Members) was created to understand the insider betrayal scenario. Each team has to work on group assignments to achieve pre-determined goals. Teams are led by team leaders and the entire game dynamics is supervised by the Game-Master. The first team that resolves the task get a financial reward.	Simulation of the insider threat scenarios was run through an experimental design where an online game method was used. The Leader's Dilemma Game through the scenario approach enables analyzing organizational trust relationships.	Study used game approach to better understand the insider threat issue arguing that the violation of trust in a focal actor's trustworthiness level can be identified based on the social network. One of the key challenges with the study's approach is its applicability and implementation in the organizational context. Not only it would be rather complex to setup similar game simulations in the organizational context, but there would be also scalability and deployment challenges.
Lee and Manners [43]	Addictiveness Brotherhood Fun Objective Points Rules Skills	Elements are described through the penetration testing approach which is considered to be a game. Objectives and rules are agreed between different parties. Penetration tester can occur points as a result of finding vulnerabilities which have different levels. A sense of brotherhood is seen through building a community of security experts. The penetration process creates addictiveness and brings fun to players.	Penetration testing process is presented as a game-like experience where penetration testers go through different phases of game, from having clear objectives and rules to betting addicted and having fun.	No empirical study was conducted.
Melki and Chatrieh [53]	Not specified	Not applicable	Use of educational games as a means for community education to address the human weakness in cybersecurity	No empirical study was conducted.
Ophoff and Janowski [62]	Avatar Badges Baseline meter Leaderboard	Students were invited to register to an online website through 4 different sign-up forms: no-feedback, badges, leaderboard and baseline meter.	Influence of Gamification on individual's password strength choice was investigated. The mean password strength for gamified sign-up form (e.g., leaderboard) was higher than no-feedback form.	Study used one-time approach where students were not protecting their own information but were asked to sign-up an artificial form.

Ruboczki [67]	Immediate feedback Narrative Opportunities for collaborative problem solving Opportunities for mastery, and leveling up Player control Progress mechanics Social connection	None	Elements were not implemented but just their use was discussed	No empirical study was conducted.
Thornton and Francia III [76]	Award points Geometric awards Immediate feedback Leaderboard Levels Multiplayer Multiple learning paths Privileges	Elements are implemented as part of the gamification of information systems and security training on teachers and students. Students study does not contain information on how different elements were implemented.	The study provided an initial attempt to understand how game-based curriculum modules can leverage students motivation.	Empirical results are mixed as results indicate that differences between control group and gamification group are not significant. Students stayed in the course 61%, compared to a control of 54%. Student attendance 30 days per semester, compared with a control of 26 days.
Trinkle et al. [79]	Role-playing Story	Story and role-playing elements were used to employee's decision on playing online games.	Vignette based instrument was used where participants have to read the story and, depending on the role they are assigned to, decide what to do: play online games or not.	Results suggest that in presence of the social media policy, employees' are less likely to violate security policy. Also, logging and monitoring of employees is more effective in absence of the social media policy.
Vail [80]	Feedback Objectives Scenario Story Triggers	CyberCIEGE (Simcity like game) is used to teach students cybersecurity. Game is built around a scenario definition language that describes scenarios in terms of users, information, user goals, attacker motives and initial security settings. In-game triggers are used to provide feedback and explain objectives.	Gamification was used in the information security management course. The study indicates that students found the class more enjoyable and bringing more engagement due to the introduction of gamification. Also, the average assessment score for the class utilizing CyberCIEGE was higher than the control class.	The study relied on one-time data collection and did not use longitudinal approach to understand how students' would react in different points in time. Also, the sample was small (20 control group) and 15 (treatment).

Table A.3. Summary of Elements Implemented in the Gamified System with Corresponding Intrinsic Motivations

Element (supporting security gamified studies)	**How the element should be implemented in a gamified system**	**How element fosters flow or immersion per** Csikszentmihalyi [19]	**Types of intrinsic motivation the design element can fulfill**	**Reason for motivation support**
Avatar Li and Lwin [44], Ophoff and Janowski [62]	Element should be implemented as one's representation of self; users should be able to construct a sense of self using cartoon-like representations. **Example**: Avatar is chosen among different Disney cartoons.	• #2 person feels in control • #8 loss of self-consciousness • #9 autotelic, purely intrinsic in nature	• Entertainment • Escape, relaxation • Explore, discover • Play, enjoyment, fun	Players choose avatars for fun but also to escape from normal self-presentation in real life. Avatars provide a new dimension for players, where they will achieve faster immersion into the game through the explore/discover motivation and the lack of inhibition due to being someone else.
Challenge/levels	Every challenge or level should be easily achievable and constructed	• #1 challenging but accessible task	• Challenge • Entertainment	One of the important motivation factors that supports challenge/levels is the

Boopathi et al. [9]	in a visually appealing way so that the learning process is facilitated through examples. **Example**: This week's challenge is to discover how visiting unknown websites can put in danger your data.	• #2 person feels in control • #3 full immersion possible • #5 task goals clear • #6 immediate feedback • #9 autotelic, purely intrinsic in nature	• Escape, relaxation • Explore, discover • Gaming achievement • Knowledge acquisition • Play, enjoyment, fun • Satisfy curiosity, pique interest	knowledge acquisition that supports the entire learning process, which is the end goal of the gamification system: to increase players' security knowledge.
Competition Dabrowski et al. [20], Ho and Warkentin [33]	Competition should be implemented through different mechanisms, such as leaderboards, incentives, points, and progress. It should be system-driven but can also be communicated to an outside audience to benefit from network effects. **Example**: Email communication could be sent within the entire organization announcing first week top scorers.	• #1 challenging but accessible task • #3 full immersion possible • #5 task goals clear • #6 immediate feedback • #7 transformation of time • #9 autotelic, purely intrinsic in nature	• Affiliation with community of interest • Challenge • Collaboration • Computer-skill acquisition • Entertainment • Escape, relaxation • Explore, discover • Gaming achievement • Improve reputation, receive approval • Influence others • Knowledge acquisition • Leading effective, successful experiences • Play with others • Play, enjoyment, fun • Satisfy curiosity, pique interest • Social communication	Competition is the essence of game play. Players not only compete with others but also with themselves. Competition must incorporate all possible motivations, where a higher number of intrinsic motivations is linked to a higher likelihood of immersion event.
Feedback/guidance Baxter et al. [8], Thornton and Francia III [76]	Immediate feedback should be provided to participants when overcoming a challenge. **Example:** Every wrong Quiz answer is accompanied by an instant feedback and suggestions on how to deal with similar situations.	• #1 challenging but accessible task • #2 person feels in control • #4 freedom to focus on task • #5 task goals clear • #6 immediate feedback	• Autonomy, freedom • Being informed • Computer-skill acquisition • Entertainment • Explore, discover • Gaming achievement • Knowledge acquisition • Play, enjoyment, fun • Satisfy curiosity, pique interest	Feedback/guidance is influenced by the same motivations as goals/objectives. As such, it provides an additional layer of motivation but is used more as an engaging factor that keeps players "in the game" rather than demotivating them, for example, by lack of knowledge or extreme difficulty.
Fun Agarwal and Karahanna [2], Lee and Manners [43]	Element of fun should be represented through the entire gamified system. **Example:** Fun can be implemented through the combination of avatar choice + visually appealing system design + easy to use system + competition against colleagues	• #3 full immersion possible • #7 transformation of time • #8 loss of self-consciousness • #9 autotelic, purely intrinsic in nature	• Entertainment • Explore, discover • Play, enjoyment, fun	Fun is a key factor in entertainment, play, and exploring dimensions. As such, it is embedded in the core of the gamification system.

Game-master Thompson et al. [75]	The game-master is a responsible person (or intelligent agent) who organizes the game, engages participants, schedules sessions, tracks progress, and manages participants' activities. **Example:** Project manager acts as game-master and drives the entire training program.	• #1 challenging but accessible task • #2 person feels in control • #5 task goals clear • #6 immediate feedback	• Escape, relaxation • Gaming achievement • Improve reputation, receive approval • Play, enjoyment, fun • Satisfy curiosity, pique interest	The game-master assumes the role of motivating others to play but also manages the overall gaming platform by encouraging motivational factors, such as fun or curiosity.
Goals/objectives Baxter et al. [8], Ho and Warkentin [33]	Goals or objectives should be clearly communicated, explained, and achievable. **Example:** Your objective is to complete all 6 levels by completing different tasks that will bring you points. Finally, you have to pass the final exam.	• #1 challenging but accessible task • #4 freedom to focus on task • #5 task goals clear • #6 immediate feedback	• Being informed • Challenge • Computer-skill acquisition • Entertainment • Explore, discover • Gaming achievement • Knowledge acquisition • Play, enjoyment, fun • Satisfy curiosity, pique interest	This element has three main components: 1) have fun, 2) be challenging, and 3) learn. The goals/objectives element is supported by several motivations that directly influence the degree of the players' addiction and interest to continue being engaged in the learning experience.
Incentives Dabrowski et al. [20], Thornton and Francia III [76]	Element implementation should have short- and long-term incentives that are intrinsic in nature (e.g., points and badges). Short-term incentives should correspond to points and possibilities to earn extra points. Long-term incentives should be proposed to participants once they complete certain levels (e.g., badges). **Example:** Earn extra points by reading the following link. You will get black belt badge if you achieve 100 points.	• #4 freedom to focus on task • #5 task goals clear • #6 immediate feedback • #9 autotelic, purely intrinsic in nature	• Challenge • Entertainment • Explore, discover • Gaming achievement • Improve reputation, receive approval • Play, enjoyment, fun • Satisfy curiosity, pique interest	Incentives can be short-term (similar to points/scoring motivations) or long-term in which improving reputation and gaming achievements are the driving factors.
Leaderboard Dabrowski et al. [20], Ophoff and Janowski [62], Thornton and Francia III [76]	Element should always be visible to all participants and include top performers. **Example:** Top 3 performers are displayed and visible to all users.	• #4 freedom to focus on task • #5 task goals clear • #6 immediate feedback	• Affiliation with community of interest • Challenge • Collaboration • Entertainment • Explore, discover • Gaming achievement • Improve reputation, receive approval • Influence others • Play with others • Play, enjoyment, fun	The leaderboard represents one of the most important gamification design elements, as it stimulates several different motivations. It is a rare element that is "public" and thus has a social component that communicates other players' achievements. It creates a positive effect of influencing others, as it directly promotes competition and consequently leads to faster immersion and connection with others.

			• Satisfy curiosity, pique interest • Social communication	
Points/scoring Dabrowski et al. [20], Ophoff and Janowski [62], Thornton and Francia III [76]	Simple and clear scoring system that provides possibilities to earn extra points by completing additional tasks should be implemented. **Example:** Each level completed brings you 50 points. Each quiz solved bring 10 points. Reading additional tips brings you 2 points.	• #2 person feels in control • #5 task goals clear • #6 immediate feedback • #9 autotelic, purely intrinsic in nature	• Challenge • Entertainment • Explore, discover • Gaming achievement • Improve reputation, receive approval • Play, enjoyment, fun • Satisfy curiosity, pique interest	Points/scoring system element is a critical part of the gamification system, as it can increase but also decrease players' motivation. When increasing motivation, the various motivation types are stimulated, particularly the play/enjoyment/fun, challenge, and curiosity factors.
Progress Adams and Makramalla [1], Baxter et al. [8], Dabrowski et al. [20]	Progress should be visually represented with statistics related to the overall performance of users. **Example:** User total number of points would be displayed together with user's current ranking.	• #2 person feels in control • #4 freedom to focus on task • #5 task goals clear • #6 immediate feedback	• Challenge • Entertainment • Explore, discover • Gaming achievement • Improve reputation, receive approval • Leading effective, successful experiences • Play, enjoyment, fun • Satisfy curiosity, pique interest	Motivations of the progress element are mainly related to having fun, being challenged, and understanding how well players perform. Other motivations (e.g., explore or successful experience) influence players' satisfaction with their current game results and stimulate further participation.
Story Baxter et al. [8], Ho and Warkentin [33]	Element should be simple, entertaining, and short and should convey clear goals and objectives. **Example:** You have six weeks to complete 10 different levels. At each level you get points by completing taks. Additional points can be attributed. Best performers will get a prize.	• #3 full immersion possible • #7 transformation of time • #8 loss of self-consciousness • #9 autotelic, purely intrinsic in nature	• Entertainment	The story is linked to entertainment motivation, where its initial objective is to provide the general game overview to the player.
Tips/hint system Fouché and Mangle [24], Ophoff and Janowski [62]	Tips or hint system should be implemented to facilitate the learning process. **Example:** Tips page provides a resource to learn about the sub-topic that level is studying.	• #4 freedom to focus on task • #6 immediate feedback	• Autonomy, freedom • Being informed • Computer-skill acquisition • Explore, discover • Knowledge acquisition • Satisfy curiosity, pique interest	Tips/hint system is an important learning design element that provides curiosity motivation in which players aim to improve learning by gaining further knowledge. It also helps them overcome frustration when they are stuck.

According to Csikszentmihalyi [19], for an optimal experience, at least one of the following nine elements should exist: 1) challenging but accessible task to be completed; 2) person feels fully in control; 3) full immersion as the task is achieved; 4) person has freedom to concentrate on the task; 5) task has clear goals; 6) immediate feedback is received once the task is completed; 7) transformation of time, where people lose track of time and perception is distorted; 8) loss of self-consciousness, where sense of identity lessens; and 9) an autotelic, intrinsically rewarding experience that suggests that the activity in itself is a reason for performing it. In this context, there is a clear link between games and flow [19].

Table A.4. Gamification Elements' Relationships with HMSAM Constructs

Gamification element	Relationship to HMSAM constructs						
	PEOU?	**PIU?**	**Curiosity?**	**Joy?**	**Control?**	**Immersion**	**Example Ref.**
Avatar	Yes	Yes	No	Yes	No	Yes	[63]
Challenge/Levels	Yes	Yes	Yes	Yes	Yes	Yes	[14]
Competition	Yes	Yes	Yes	Yes	Yes	Yes	[30]
Feedback/guidance	Yes	Yes	Yes	No	Yes	Yes	[77]
Fun	No	No	No	Yes	No	Yes	[11]
Game-Master	No	No	No	Yes	Yes	No	[81]
Goals/objectives	Yes	Yes	Yes	Yes	No	Yes	[74]
Incentives	Yes	Yes	Yes	Yes	Yes	Yes	[30, 36]
Leaderboard	Yes	Yes	Yes	Yes	Yes	Yes	[52]
Points/Scoring	Yes	Yes	Yes	Yes	Yes	Yes	[52, 72]
Progress	Yes	Yes	Yes	Yes	Yes	Yes	[85]
Story	Yes	Yes	Yes	No	No	Yes	[85]
Tips/Hint system	Yes	Yes	Yes	Yes	Yes	Yes	[59, 84]

Note: the references are nonexhaustive examples from the literature and do not represent every relationship combination.

Table A.5. Gamification Elements Relationships with Motivations

Motivation category	General motivation (desire for)	Specific motivation (desire for)	Ref.	1	2	3	4	5	6	7	8	9	10	11	12	13	Total
Hedonic	System pleasure	Play/enjoyment/fun	[86]	•		•	•	•	•		•	•	•	•	•	•	11
		Entertainment	[70]		•	•	•	•	•		•	•	•	•	•	•	11
		Sex/lust/pleasure	[29]														0
		Escape/relaxation	[87]	•		•									•	•	4
	System arousal	Challenge	[10],					•			•	•	•	•	•	•	7
		Satisfy curiosity/pique interest	[39]	•				•	•	•	•	•	•	•	•	•	10
		Explore/discover	[7]			•	•	•	•	•	•	•	•	•	•	•	11
		Stimulate utilitarian experience	[45]					•	•		•	•	•	•	•	•	8
		Sex/lust/arousal	[29]														0
Intrinsic (non-hedonic)	System accomplishment	Influence others	[58]											•		•	2

Motivation category	General motivation (desire for)	Specific motivation (desire for)	Ref.	1	2	3	4	5	6	7	8	9	10	11	12	13	Total
	System learning	Altruism	[13]														0
		Improve reputation/receive approval	[34]	•							•	•	•	•		•	6
		Leading effective/successful experiences	[21]								•					•	2
		Gaming achievement	[27]	•				•	•		•	•	•	•	•	•	9
		Autonomy/freedom	[58]						•	•							2
		Knowledge acquisition	[42]					•	•	•					•	•	5
		Knowledge sharing	[13]														0
		Computer-skill acquisition	[26]					•	•	•						•	4
		To be informed	[58]					•	•	•						•	4
	System socialization	Affiliation with community of interest	[5]											•		•	2
		Social communication	[66]											•		•	2
		Collaboration	[48]											•		•	2
		To play with others	[54]											•		•	2
		Romance/dating	[16]														0
		Total		5	1	4	3	10	10	6	9	8	8	13	9	18	104

*1) Game-Master 2) Story 3) Avatar 4) Fun 5) Goals/ objectives 6) Feedback/guidance 7) Tips/Hint system 8) Progress 9) Points/Scoring 10) Incentives 11) Leaderboard 12) Challenge Levels 13) Competition

Gamification vs Flow theory

The reason that games, and consequently game-like features, can have such a strong, positive motivational influence on people can be partially explained by flow theory. It posits that people performing an activity (i.e., playing a game) can achieve feelings of complete and energized focus with a high level of enjoyment and fulfillment under certain conditions [19]. Playing engaging and enjoyable games helps people reach a state of flow (i.e., being 'in the zone') in which they experience deep immersion in the experience. Accordingly, flow is a key reason that people play games [57] because games create an entertainment effect through intrinsic motivation, leading to a state of flow [17]. Crucially, this flow effect can also be found in many non-gaming contexts (e.g., education, music, sports, religion and spirituality, exploratory learning, completing crowdsourcing tasks online for pay)

Flow theory was proposed outside of a system's context and describes the experiences of intrinsically motivated people who are engaged in an activity chosen for its own sake [18, 22]. Although flow theory was not constructed with systems in mind [50], it was later applied to various systems environments, including online user and consumer behavior [2, 40] and hedonic motivation systems [e.g., 35, 72].

Gamification Design Artifacts Inspiring Motivation

We argue that the gamification elements implemented in our system (e.g., points/scores, leaderboard) are natural ways to inspire intrinsic motivations, although they may also encourage extrinsic motivations. For example, we designed the use of points and other associated gamification features (e.g., avatars, levels, feedback, fun, gamemaster, goals, leaderboard, progress, points, story, tips/hints) as a purely virtual mechanism with the French company, because these were not tied to bonuses, raises, annual reviews, threats, and so on. This created an environment that, in most people, better fosters intrinsic motivation than extrinsic motivation, although some people may still experience both (e.g., take points seriously, even though they had no actual direct effect on their careers). Moreover, employees were encouraged to pick an avatar and associated nickname to render their participation "nearly" fully anonymous (the email was known to the site administrator but was used only to send automated email reminders). The avatars and nicknames were thus used as another form of intrinsic motivation and fun.
A leaderboard may have more strongly fostered extrinsic motivations if the employees' full names and photos had been used, which could have served as the basis of public shaming. The motivations may also have been more extrinsic if actual rewards had been associated with the leaderboards in terms of money, raises, promotions, certificates, awards, or other direct career consequences. However, none of these were provided. Because the leaderboard was anonymous and only a given employee could identify his/her own avatar on the leaderboard, it is much more plausible that the leaderboard design elements mostly (if not entirely) drove employees' intrinsic motivations, because individual employees were aware of their ranking compared others. Thus, we suggest that employee behavior was most likely to be motivated by an internal desire for accomplishment, meeting a challenge for the sake of growth [10], or even gaming achievement (another key intrinsic motivation) [27], with the result that employees could see their avatars climb in the leaderboard ranking. Given the voluntary and mostly anonymous nature of the participation, it is also more plausible that the employees were motivated to participate in the activity by curiosity [39], joy, learning [42], self-improvement [10], wanting to affiliate and "play" with others [54], the desire for mastery [41], and the like—not because they felt they needed to respond to an external inducement.

Nonetheless, although we test these assumptions indirectly through manipulation checks and actual testing of hypotheses, our design does not allow us to characterize the inner workings of individuals' actual motivations—whether intrinsic or extrinsic. Doing so is a difficult cognitive psychology task that lies beyond the scope of our study. Thus, we cannot claim that participants were only intrinsically motivated. Mixed motivations are highly common in systems-use contexts [49] and are likewise expected for gamification [78]. Moreover, in our target organization, the employees would have been subject to the ever-present extrinsic motivations of doing their normal work and adhering to general company policies and procedures. Thus, in organizations, gamified security training cannot operate independently of extrinsic motivations. We thus argue that organizations can boost intrinsic motivations by implementing different gamification elements—some of which participants will perceive as eliciting both intrinsic and extrinsic motivation—within their e-learning system.

ONLINE APPENDIX B. EXAMPLE GRAPHICAL INTERFACES FROM SYSTEMS

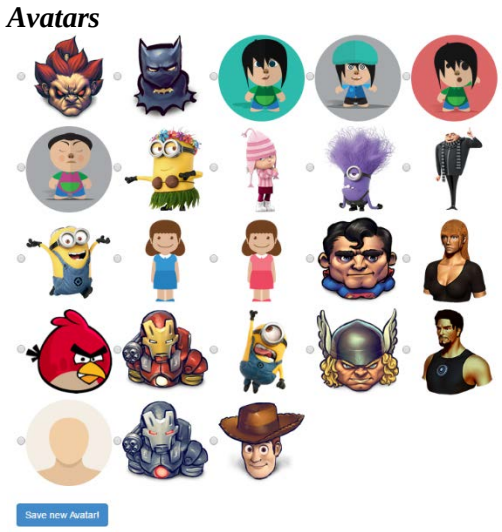


Figure B.1. Example System

Figure B.2. Example of a Round

Figure B.3. Example of a Training Tip

Figure B.4. Example of a Training Test

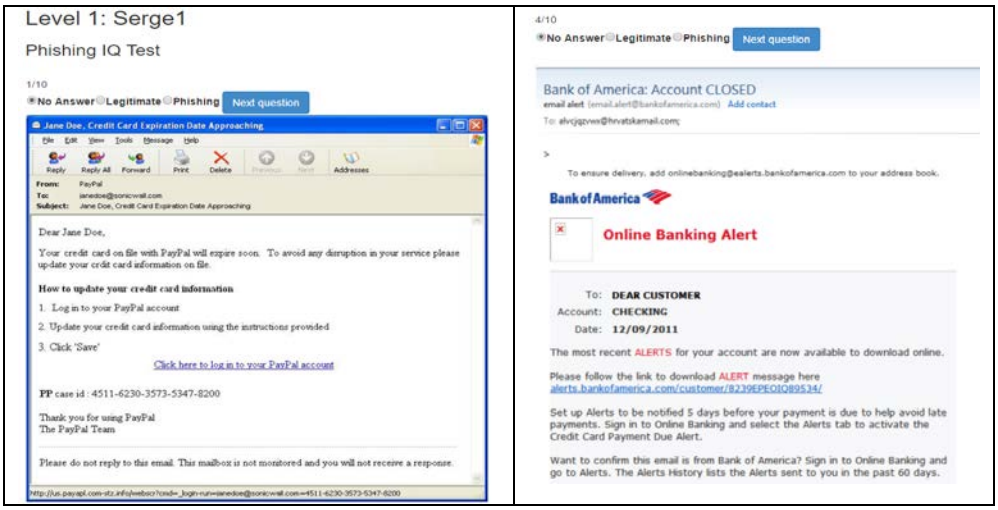


Figure B.4. Examples of a Learning/Training Process

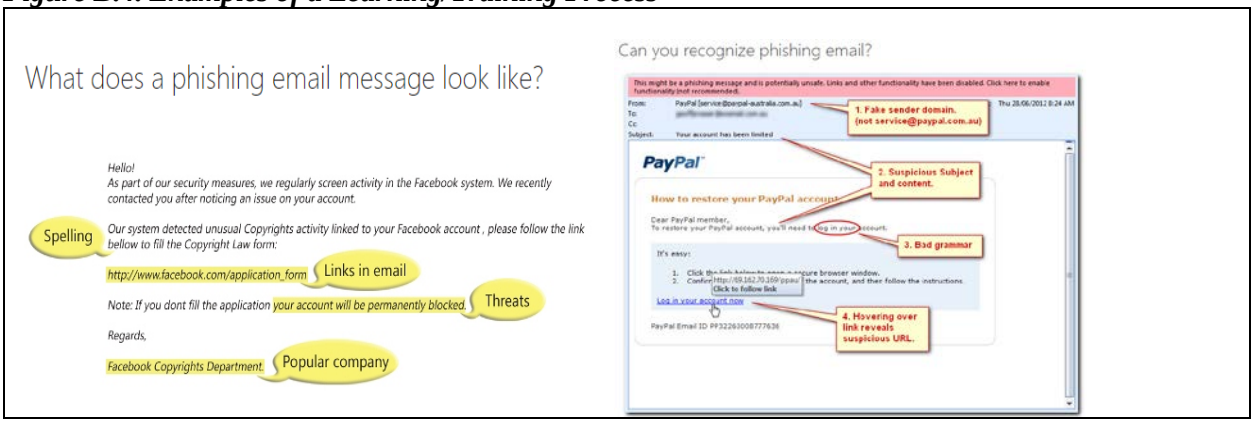
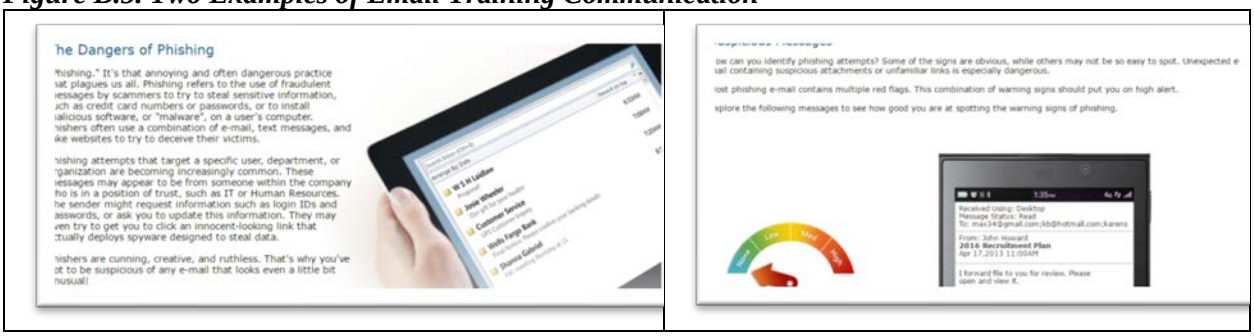


Figure B.5. Two Examples of Email Training Communication



ONLINE APPENDIX C. MEASUREMENT ITEMS FOR OUR RESEARCH

Table C.1. Measurement Items for Gamification and Email Treatments*

Constructs [treatments]	Items	Adapted from
Perceived ease-of-use (PEOU) [gamification treatment]	**Prompt [for gamification]**: Your recently engaged in a series of Web-based game-like training that taught you about organizational security. We would like your honest opinions about this training. For the remainder of the questions, please give us your opinion on how effective you think this systems-based training was. There are no wrong/right answers. PEOU1. My interaction with the web system was clear and understandable. PEOU2. Interacting with the web system did not require a lot of my mental effort. PEOU3. I found the web system to be trouble free. PEOU4. I found it easy to get the web system to do what I want it to do. PEOU5. It was simple to do what I wanted with the web system. PEOU6. It was easy for me to become skillful at using the web system. PEOU7. I found the platform easy to use.	Agarwal and Karahanna [2] and Lowry et al. [50]
Perceived ease-of-use (PEOU) [email treatment]	**Prompt [for email]**: Your recently engaged in a series of email training that taught you about organizational security. We would like your honest opinions about this email training. For the remainder of the questions, please give us your opinion on how effective you think these emails were. There are no wrong/right answers. PEOU1. My interaction with the training emails was clear and understandable. PEOU2. Interacting with the training emails did not require a lot of my mental effort. PEOU3. I found the training emails to be trouble free. PEOU4. I found it easy to get the training emails to do what I want them to do. PEOU5. It was simple to do what I wanted with the training emails. PEOU6. It was easy for me to become skillful at using the training emails. PEOU7. I found the training emails easy to use.	Agarwal and Karahanna [2] and Lowry et al. [50]
Perceived intrinsic usefulness (PIU) [gamification treatment]	PIU1. The web system decreased my stress. PIU2. The web system helped me better pass time. PIU3. The web system provided a useful escape. PIU4. The web system helped me think more clearly. PIU5. The web system helped me feel rejuvenated.	Lowry et al. [50]
Perceived intrinsic usefulness (PIU) [email treatment]	PIU1. The training emails decreased my stress. PIU2. The training emails helped me better pass time. PIU3. The training emails provided a useful escape. PIU4. The training emails helped me think more clearly. PIU5. The training emails helped me feel rejuvenated.	Lowry et al. [50]
Behavioral intention to	BI1. I am likely to follow organizational security policies.	Herath and Rao [31]

follow security policies (BI) [both treatments]	BI2. It is possible that I will comply with organizational IS security policies to protect the organization's information systems. BI3. I am certain that I will follow organizational security policies.	
Joy [gamification treatment]	JOY1. I found playing the game on the web portal to be enjoyable. JOY2. I had fun using the web portal. *JOY3. Using the web portal was boring. *JOY4. The web portal really annoyed me JOY5. The web portal experience was pleasurable. *JOY6. The web portal left me unsatisfied.	Lowry et al. [50]
Joy [email treatment]	JOY1. I found using the training emails to be enjoyable. JOY2. I had fun reading the training emails. *JOY3. Using the training emails was boring. *JOY4. The training emails really annoyed me JOY5. The training emails experience was pleasurable. *JOY6. The training emails left me unsatisfied.	Lowry et al. [50]
Control (CTL) [both treatments]	**Prompt [for gamification]**: Again, in terms of the training system you used …Please state your agreement, with the following: **Prompt [for email]**: Again, in terms of the training emails we sent you…Please state your agreement, with the following: CTL1. I had a lot of control CTL2. I could choose freely what I wanted to see or do. *CTL3. I had little control over what I could do. CTL4. I was in control. *CTL5. I had no control over my interaction. CTL6. I was allowed to control my interaction	Lowry et al. [50]
Immersion (aka focused immersion) (FI) [gamification treatment]	FI1. I was able to block out most other distractions FI2. I was absorbed in what I was doing. FI3. I was immersed in the web portal. *FI4. I was distracted by other attentions very easily.	Lowry et al. [50]
Immersion (FI) [email treatment]	FI1. I was able to block out most other distractions FI2. I was absorbed in what I was doing with the training emails. FI3. I was immersed in the training emails. *FI4. I was distracted by other attentions very easily.	Lowry et al. [50]
Curiosity (CUR) [both treatments]	CUR1. This experience excited my curiosity. CUR2. This experience made me curious. CUR3. This experience aroused my imagination.	Agarwal and Karahanna [2] and Lowry et al. [50]

Security self-efficacy (SEF) [both treatments]	PSE1: If I wanted to, I am confident that I could perform proper information security behaviours. PSE2: If I wanted to, I could protect my computer by following proper information security behaviours PSE3: If I wanted to, I would be able to perform proper information security behaviours	Anderson and Agarwal [4] and Herath and Rao [32]
Security response efficacy (REF) [both treatments]	REF1: Exercising proper information security behavior is a good way to reduce the risk of compromising organizational data REF2: If I were to exercise proper information security behavior each time a potential security threat arises, I would lessen my chances of compromsing organizational data	Milne et al. [56]
Learning (LER) [gamification treatment]	LER1: All things considered, the game system helped me learn new things. LER2: All things considered, the game system helped me master new concepts LER3: All things considered, the game system helped me acquire innovative ideas.	Chang et al. [12] and Wei et al. [83]
Learning (LER) [email treatment]	LER1: All things considered, the training emails helped me learn new things. LER2: All things considered, the training emails helped me master new concepts LER3: All things considered, the training emails helped me acquire innovative ideas.	Chang et al. [12] and Wei et al. [83]
Challenge (CHA) [gamification treatment]	CHA1: Completing different training rounds was challenging. CHA2: The different training rounds were demanding. CHA3: It was easy for me to complete knowledge tests in the system*	Newly created measure based on Sen et al. [69]
Challenge (CHA) [email treatment]	CHA1: Reading different training emails was challenging CHA2: Reading different training emails was demanding CHA3: It was easy for me to enhance my knowledge on security from the training emails*	Newly created measure based on Sen et al. [69]

*=reverse scaled; all scales were reflective and used a Likert-type seven-point scale anchored on “Strongly Disagree” to “Strongly Agree.” Because the target system and interactions were different between the gamification and email training treatments, several of these measures had to be adapted to both.

ONLINE APPENDIX D. MODEL VALIDATION AND SUPPLEMENTARY ANALYSES

Table D.1. Item Loadings (Full data)

Item	BI	CHA	CM	CTL	CUR	FI	JOY	LER	PEOU	PSE	PIU	REF	SM	TMC
BI1	0.909	0.247	0.327	0.325	0.458	0.333	0.699	0.631	0.165	0.087	0.431	0.078	0.105	0.242
BI2	0.921	0.268	0.056	0.408	0.369	0.269	0.401	0.425	0.221	0.018	0.378	0.204	0.086	0.205
BI3	0.934	0.252	0.172	0.225	0.352	0.311	0.389	0.497	-0.067	-0.108	0.287	0.264	0.071	0.029
CHA1	0.407	0.903	0.173	0.535	0.359	0.541	0.424	0.461	0.180	0.369	0.688	0.201	-0.120	0.361
CHA2	0.085	0.915	0.212	0.498	0.234	0.509	0.410	0.245	0.190	0.494	0.591	0.457	-0.055	0.046
CHA3	0.111	0.892	0.486	0.435	0.233	0.315	0.171	0.243	0.085	0.558	0.341	0.157	-0.017	0.229
CM1	0.043	-0.218	0.982	0.015	0.412	0.288	0.349	0.032	0.511	0.230	0.497	0.115	0.174	0.490
CM2	0.047	-0.093	0.976	-0.038	0.088	0.136	0.106	0.471	0.158	0.278	0.390	0.023	0.052	-0.087
CTL3	0.217	0.401	0.164	0.822	0.455	0.261	0.739	0.031	0.629	0.225	0.398	0.219	-0.021	0.237
CTL4	0.271	0.478	-0.113	0.883	0.193	0.095	0.352	0.117	0.557	0.192	0.607	0.093	-0.051	0.404
CTL5	0.363	0.415	0.135	0.871	0.274	0.054	0.393	0.106	0.534	0.112	0.579	0.305	-0.015	0.240
CTL6	0.321	0.735	0.601	0.735	0.254	0.332	0.342	0.305	0.347	0.499	0.577	0.232	0.105	0.786
CUR1	0.437	0.087	0.480	0.144	0.901	-0.050	0.547	0.113	0.215	0.157	0.115	-0.026	-0.119	-0.111
CUR2	0.381	0.481	0.272	0.467	0.956	0.289	0.727	0.339	0.458	0.356	0.305	0.171	-0.047	-0.093
FI1	0.252	0.541	0.346	0.264	0.168	0.892	0.437	0.504	0.162	0.384	0.358	0.259	-0.120	0.190
FI2	0.361	0.505	0.402	0.152	0.094	0.901	0.418	0.594	0.119	0.271	0.427	0.473	-0.132	-0.018
FI3	0.289	0.523	0.263	0.193	0.189	0.940	0.463	0.601	0.055	0.415	0.386	0.202	-0.099	0.136
JOY2	0.516	0.163	0.185	0.175	0.571	0.277	*0.604	0.261	0.192	0.096	0.143	-0.141	-0.056	0.257
JOY3	0.347	0.469	0.230	0.522	0.544	0.419	0.891	0.342	0.439	0.373	0.441	0.302	0.001	0.006
JOY4	0.480	0.564	-0.072	0.477	0.519	0.544	0.830	0.571	0.307	0.515	0.595	0.324	0.120	0.220
JOY5	0.473	0.213	0.006	0.608	0.536	0.352	0.888	0.212	0.664	0.135	0.259	0.264	0.101	0.438
JOY6	0.424	0.295	0.461	0.405	0.674	0.316	0.890	0.289	0.364	0.343	0.331	0.203	-0.050	0.122
LER1	0.546	0.298	0.097	0.132	0.295	0.508	0.343	0.914	-0.044	0.408	0.399	0.040	-0.077	0.219
LER3	0.516	0.442	0.023	0.157	0.205	0.639	0.427	0.938	-0.081	0.382	0.639	0.204	-0.104	0.283
PEOU3	0.187	0.218	0.604	0.444	0.451	0.114	0.473	0.031	0.835	0.021	0.270	0.116	-0.135	-0.300
PEOU5	-0.021	0.084	0.252	0.570	0.126	0.076	0.311	0.083	0.802	0.202	0.161	0.378	0.130	0.556
PEOU6	0.054	-0.260	0.006	0.157	-0.108	-0.054	0.145	-0.059	0.825	-0.088	-0.189	0.406	0.054	0.400
PSE1	0.012	0.525	0.234	0.360	0.405	0.397	0.429	0.322	0.251	0.975	0.400	0.474	0.104	0.668
PSE2	-0.041	0.348	0.244	0.418	0.464	0.332	0.399	-0.025	0.514	0.912	0.190	0.413	0.175	0.741
PSE3	0.037	0.240	0.068	0.344	0.519	0.224	0.408	-0.080	0.445	0.933	0.099	0.351	0.114	0.680
PIU1	0.403	0.662	0.531	0.658	0.386	0.441	0.477	0.506	0.371	0.451	0.948	0.417	-0.177	-0.201
PIU2	0.387	0.604	0.473	0.508	0.303	0.408	0.341	0.603	0.196	0.396	0.913	0.368	-0.185	0.265
PIU3	0.421	0.665	0.262	0.577	0.327	0.383	0.502	0.594	0.193	0.456	0.927	0.332	0.164	-0.259
PIU4	0.269	0.711	0.350	0.328	0.224	0.413	0.187	0.535	-0.106	0.428	0.801	0.447	0.145	0.281
PIU5	0.274	0.535	0.456	0.678	0.356	0.308	0.369	0.357	0.347	0.285	0.879	0.506	0.151	0.252
REF1	-0.074	0.312	0.095	0.266	0.116	0.313	0.305	0.131	0.308	0.424	0.423	0.965	0.132	0.132
REF2	-0.038	0.329	0.126	0.229	0.074	0.356	0.195	0.137	0.231	0.420	0.444	0.968	0.062	0.111
SC1	-0.037	-0.065	-0.036	0.028	0.081	-0.021	-0.082	-0.002	-0.050	-0.046	-0.029	-0.023	0.978	-0.069
SC2	-0.103	-0.131	0.139	0.035	-0.122	-0.141	-0.028	-0.128	-0.112	0.115	-0.185	0.093	0.822	0.106
SC3	-0.036	-0.005	0.073	0.018	-0.040	0.060	0.012	-0.001	-0.079	0.060	-0.031	0.022	0.944	0.035
SC4	0.016	0.061	-0.064	0.066	0.073	0.069	0.041	0.025	0.076	-0.040	0.067	-0.085	0.866	-0.009
SC5	0.017	0.007	-0.019	0.003	0.016	-0.008	0.054	0.011	0.014	-0.001	-0.009	-0.030	0.929	0.018
SC6	-0.060	-0.028	0.067	0.027	-0.031	-0.097	-0.056	-0.050	0.018	0.032	-0.081	0.030	0.886	0.064
TMC1	-0.152	0.038	0.364	0.480	-0.075	0.219	0.308	0.001	0.081	0.762	-0.205	0.050	0.146	0.909
TMC2	0.102	0.163	0.427	0.379	0.134	0.017	0.199	0.151	0.116	0.523	-0.116	-0.086	0.128	0.912
TMC3	0.031	-0.273	0.481	0.100	0.397	0.015	-0.059	-0.023	0.529	0.538	-0.359	0.423	0.060	*0.662

* item dropped to improve discriminant validity

Table D.2. Discriminant Validity (Inter-Correlations) of Variable Constructs (Full data)

Latent Construct	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
Behavioral intention (1)	.921													
Challenge (2)	-.433	.817												
OCM (3)*	-.041	-.206	.941											
Control (4)	.016	.353	.019	.891										
Curiosity (5)	.251	.543	-.401	.172	.944									
Immersion (6)	-.180	.357	-.271	-.192	-.641	.830								
Joy (7)	.129	.478	-.336	.405	.484	-.161	.929							
Learning (8)	.240	.181	.040	.580	-.730	.430	-.537	.911						
PEOU (9)	.136	.367	.503	.725	.187	-.059	.708	-.514	.808					
PIU (10)	-.370	.631	.239	.293	-.251	-.007	.523	.035	-.349	.926				
Security response-efficacy (11)	-.382	.305	.485	.141	-.010	.324	.140	-.213	.027	.297	.967			
Security self-efficacy (12)	-.418	.543	.112	.305	.326	.207	.214	-.663	.181	.046	.537	.868		
OSC (13)*	-.096	-.088	.168	.022	-.090	-.119	-.013	-.110	-.102	.133	-.169	.102	.941	
TMSC (14) *	-.010	-.005	.500	.400	-.107	.105	.196	.058	-.161	.729	-.257	.126	.137	.835

Note: Diagonal values are square roots of the AVEs (bolded and underlined). All data (gamification and email) is included which explains why some of the correlations are contrary to the direction with our final gamification model. * = construct that was used solely as a covariate to BI and actual behaviors in the model; OSC = organization security communication; TMSC = top management security commitment; OCM = organization computer monitoring.

Table D.3. Data Collection (Survey After Three Months)

Relationships tested	**Model 1 (HMSAM replication)**	**Model 2 (add coping and challenge)**	**Model 3 (full model with controls)**
Replication: PEOU → PIU	0.422 (4.206***)	0.432 (4.243***)	0.433 (3.066**)
Replication: PEOU → curiosity	0.198 (4.612***)	0.202 (4.833***)	0.205 (4.736***)
Replication: PEOU → joy	0.645 (29.845***)	0.680 (30.144***)	0.673 (30.189***)
Replication: PEOU → control	0.700 (40.007***)	0.710 (42.304***)	0.701 (43.221***)
Replication: PIU → BI	0.618 (5.374***)	0.621 (5.388***)	0.603 (5.051***)
Replication: Curiosity → BI	0.626 (21.452***)	0.672 (22.299***)	0.661 (20.203***)
Replication: Curiosity → immersion	0.674 (14.268***)	0.680 (15.366***)	0.677 (17.635***)
Replication: Joy → BI	0.371 (1.334 n/s)	0.382 (1.434 n/s)	0.377 (1.398 n/s)
Replication: Joy → immersion	0.472 (12.547***)	0.479 (12.613***)	0.473 (12.001***)
Replication: Control → BI	0.799 (10.096***)	0.799 (10.402***)	0.783 (10.304***)
Replication: Control → immersion	-0.451 (1.644 n/s)	-0.442 (1.782 n/s)	-0.441 (1.803 n/s)
H1. Learning → BI	n/a	0.839 (10.504***)	0.730 (10.381***)
H2a. Learning → Security response efficacy	n/a	0.261 (6.432***)	0.255 (6.302***)
H2b. Learning → Security self-efficacy	n/a	0.677 (32.344***)	0.683 (39.302***)
H3a. Security response efficacy → BI	n/a	0.131 (2.368*)	0.131 (2.632**)
H3b. Security self-efficacy → BI	n/a	0.232 (5.142***)	0.220 (5.244***)
H4. Challenge → immersion	n/a	0.541 (12.487***)	0.540 (13.504***)
H5. Immersion → BI	n/a	0.532 (11.274***)	0.516 (12.104***)
H6. BI → actual security behavior	n/a	0.414 (17.366***)	0.415 (17.904***)
Control: age → BI	n/a	n/a	0.011 (1.303 n/s)
Control: gender → BI	n/a	n/a	0.029 (1.556 n/s)
Control: experience → BI	n/a	n/a	-0.023 (1.166 n/s)
Control: education → BI	n/a	n/a	0.025 (1.675 n/s)

Control: OSC → BI	n/a	n/a	0.044 (1.633 n/s)
Control: TMSC → BI	n/a	n/a	0.113 (2.102*)
Control: OCM → BI	n/a	n/a	-0.021 (1.652 n/s)
Control: age → actual security behavior	n/a	n/a	0.029 (1.349 n/s)
Control: gender → actual security behavior	n/a	n/a	0.041 (1.598n/s)
Control: experience → actual security behavior	n/a	n/a	-0.062 (1.139 n/s)
Control: education → actual security behavior	n/a	n/a	0.081 (1.719 n/s)
Control: OSC → actual security behavior	n/a	n/a	0.039 (1615 n/s)
Control: TMSC → actual security behavior	n/a	n/a	0.122 (2.034*)
Control: OCM → actual security behavior	n/a	n/a	-0.031 (1.554 n/s)
Equation-level fit statistics (variance explained or R^2) and Model-level fit statistics, based on the estimated model of the original sample			
R^2 for PIU	0.188	0.185	0.177
R^2 for curiosity	0.130	0.131	0.123
R^2 for joy	0.478	0.475	0.472
R^2 for control	0.512	0.519	0.505
R^2 for security response efficacy	n/a	0.166	0.173
R^2 for security self-efficacy	n/a	0.482	0.481
R^2 for immersion	0.466	0.613	0.645
R^2 for BI	0.274	0.621	0.628
Root mean square error of approximation (RMSEA)	0.066	0.062	0.063
Standardized root mean residual (SRMR)	0.081	0.083	0.081
Comparative fit index (CFI)	0.920	0.922	0.923
Tucker-Lewis index (TLI)	0.921	0.921	0.924

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, n/s = not significant; R^2 for actual security behavior cannot be calculated because it is categorical (successfully phished: yes/no); PEOU = perceived ease of use; PIU = perceived intrinsic usefulness; BI = behavioral intentions to follow security policies; OSC = organization security communication; TMSC = top management security commitment; OCM = organization computer monitoring

Table D.4. Data Collection (Survey After Three Months) – Email Treatment Data Only

Relationships tested	**Model 1 (HMSAM replication)**	**Model 2 (add coping and challenge)**	**Model 3 (full model with controls)**
Replication: PEOU → PIU	0.152 (2.732**)	0.155 (2.088*)	0.149 (2.214*)
Replication: PEOU → curiosity	0.151 (3.698*)	0.162 (3.704*)	0.162 (3.603*)
Replication: PEOU → joy	0.332 (12.501***)	0.321 (12.689***)	0.354 (12.345***)
Replication: PEOU → control	0.504 (26.536***)	0.506 (26.512***)	0.492 (26.214***)
Replication: PIU → BI	-0.341 (1.298 n/s)	-0.358 (1.345 n/s)	-0.331 (1.315 n/s)
Replication: Curiosity → BI	0.211 (5.368***)	0.232 (5.457***)	0.222 (5.475***)
Replication: Curiosity → immersion	-0.229 (1.402 n/s)	-0.221 (1.506 n/s)	-0.235 (1.498 n/s)
Replication: Joy → BI	-0.031 (1.031 n/s)	-0.022 (1.026 n/s)	-0.058 (1.125 n/s)
Replication: Joy → immersion	-0.645 (1.222 n/s)	-0.664 (1.169 n/s)	-0.674 (1.122 n/s)
Replication: Control → BI	0.201 (2.356*)	0.214 (2.302*)	0.192 (2.314*)
Replication: Control → immersion	-0.389 (1.615 n/s)	-0.356 (1.457 n/s)	-0.314 (1.687 n/s)
H1. Learning → BI	n/a	-0.024 (1.523 n/s)	-0.021 (1.598 n/s)
H2a. Learning → Security response efficacy	n/a	-0.138 (1.378 n/s)	-0.119 (1.299 n/s)
H2b. Learning → Security self-efficacy	n/a	-0.051 (1.195 n/s)	-0.031 (1.147 n/s)
H3a. Security response efficacy → BI	n/a	-0.135 (1.311 n/s)	-0.122 (1.314 n/s)
H3b. Security self-efficacy → BI	n/a	-0.114 (1.698 n.s)	-0.132 (1.559 n.s)
H4. Challenge → immersion	n/a	0.198 (8.614***)	0.198 (8.317***)
H5. Immersion → BI	n/a	-0.212 (1.623 n/s)	-0.201 (1.485 n/s)
H6. BI → actual security behavior	n/a	0.147 (2.745*)	0.132 (2.474*)
Control: age → BI	n/a	n/a	0.009 (1.432 n/s)
Control: gender → BI	n/a	n/a	0.021 (1.344 n/s)
Control: experience → BI	n/a	n/a	-0.011 (1.647 n/s)

Control: education → BI	n/a	n/a	0.021 (1.387 n/s)
Control: OSC → BI	n/a	n/a	0.039 (1.696 n/s)
Control: TMSC → BI	n/a	n/a	0.119 (2.205*)
Control: OCM → BI	n/a	n/a	-0.022 (1.687 n/s)
Control: age → actual security behavior	n/a	n/a	0.012 (1.478 n/s)
Control: gender → actual security behavior	n/a	n/a	0.013 (1.322 n/s)
Control: experience → actual security behavior	n/a	n/a	-0.009 (1.636 n/s)
Control: education → actual security behavior	n/a	n/a	0.014 (1.314 n/s)
Control: OSC → actual security behavior	n/a	n/a	0.039 (1.591 n/s)
Control: TMSC → actual security behavior	n/a	n/a	0.121 (2.259*)
Control: OCM → actual security behavior	n/a	n/a	-0.021 (1.457 n/s)
Equation-level fit statistics (variance explained or R^2) and Model-level fit statistics, based on the estimated model of the original sample			
R^2 for PIU	0.138	0.139	0.139
R^2 for curiosity	0.043	0.045	0.041
R^2 for joy	0.119	0.123	0.118
R^2 for control	0.323	0.320	0.321
R^2 for security response efficacy	n/a	0.135	0.121
R^2 for security self-efficacy	n/a	0.156	0.155
R^2 for immersion	0.354	0.374	0.315
R^2 for BI	0.249	0.259	0.244
Root mean square error of approximation (RMSEA)	0.065	0.105	0.102
Standardized root mean residual (SRMR)	0.082	0.102	0.115
Comparative fit index (CFI)	0.909	0.918	0.918
Tucker-Lewis index (TLI)	0.908	0.919	0.928

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, n/s = not significant; R^2 for actual security behavior cannot be calculated because it is categorical (successfully phished: yes/no); PEOU = perceived ease of use; PIU = perceived intrinsic usefulness; BI = behavioral intentions to follow security policies; OSC = organization security communication; TMSC = top management security commitment; OCM = organization computer monitoring

Table D.5. Data Collection (Survey After Six Months) – Email Treatment Data Only

Relationships tested	Model 1 (HMSAM replication)	Model 2 (add coping and challenge)	Model 3 (full model with controls)
Replication: PEOU → PIU	0.148 (2.645**)	0.142 (2.095*)	0.140 (2.201*)
Replication: PEOU → curiosity	0.159 (3.714*)	0.158 (3.688*)	0.156 (3.633*)
Replication: PEOU → joy	0.312 (12.405***)	0.318 (12.405***)	0.313 (12.411***)
Replication: PEOU → control	0.495 (26.518***)	0.494 (26.488***)	0.487 (26.125***)
Replication: PIU → BI	-0.347 (1.301 n/s)	-0.344 (1.256 n/s)	-0.333 (1.222 n/s)
Replication: Curiosity → BI	0.218 (5.497***)	0.223 (5.332***)	0.221 (5.562***)
Replication: Curiosity → immersion	-0.226 (1.318 n/s)	-0.228 (1.422 n/s)	-0.225 (1.533 n/s)
Replication: Joy → BI	-0.032 (1.033 n/s)	-0.022 (1.033 n/s)	-0.043 (1.136 n/s)
Replication: Joy → immersion	-0.634 (1.216 n/s)	-0.634 (1.131 n/s)	-0.639 (1.119 n/s)
Replication: Control → BI	0.195 (2.314*)	0.192 (2.297*)	0.186 (2.246*)
Replication: Control → immersion	-0.375 (1.605 n/s)	-0.343 (1.591 n/s)	-0.376 (1.634 n/s)
H1. Learning → BI	n/a	-0.012 (1.573 n/s)	-0.014 (1.552 n/s)
H2a. Learning → Security response efficacy	n/a	-0.121 (1.324 n/s)	-0.116 (1.291 n/s)
H2b. Learning → Security self-efficacy	n/a	-0.049 (1.187 n/s)	-0.039 (1.133 n/s)
H3a. Security response efficacy → BI	n/a	-0.122 (1.302 n/s)	-0.121 (1.245 n/s)
H3b. Security self-efficacy → BI	n/a	-0.118 (1.683 n.s)	-0.129 (1.541 n.s)
H4. Challenge → immersion	n/a	0.187 (8.562***)	0.186 (8.203***)
H5. Immersion → BI	n/a	-0.210 (1.602 n/s)	-0.204 (1.422 n/s)
H6. BI → actual security behavior	n/a	0.122 (2.604*)	0.114 (2.392*)
Control: age → BI	n/a	n/a	0.005 (1.378 n/s)
Control: gender → BI	n/a	n/a	0.012 (1.301 n/s)

Control: experience → BI	n/a	n/a	-0.009 (1.618 n/s)
Control: education → BI	n/a	n/a	0.011 (1.312 n/s)
Control: OSC → BI	n/a	n/a	0.033 (1.639 n/s)
Control: TMSC → BI	n/a	n/a	0.116 (2.128*)
Control: OCM → BI	n/a	n/a	-0.021 (1.652 n/s)
Control: age → actual security behavior	n/a	n/a	0.005 (1.423 n/s)
Control: gender → actual security behavior	n/a	n/a	0.012 (1.301 n/s)
Control: experience → actual security behavior	n/a	n/a	-0.008 (1.613 n/s)
Control: education → actual security behavior	n/a	n/a	0.011 (1.305 n/s)
Control: OSC → actual security behavior	n/a	n/a	0.037 (1.594 n/s)
Control: TMSC → actual security behavior	n/a	n/a	0.119 (2.138*)
Control: OCM → actual security behavior	n/a	n/a	-0.022 (1574 n/s)
Equation-level fit statistics (variance explained or R^2) and Model-level fit statistics, based on the estimated model of the original sample			
R^2 for PIU	0.135	0.138	0.138
R^2 for curiosity	0.042	0.044	0.042
R^2 for joy	0.119	0.120	0.119
R^2 for control	0.320	0.321	0.329
R^2 for security response efficacy	n/a	0.130	0.129
R^2 for security self-efficacy	n/a	0.157	0.156
R^2 for immersion	0.310	0.318	0.317
R^2 for BI	0.243	0.249	0.232
Root mean square error of approximation (RMSEA)	0.058	0.058	0.058
Standardized root mean residual (SRMR)	0.071	0.073	0.072
Comparative fit index (CFI)	0.902	0.902	0.903
Tucker-Lewis index (TLI)	0.902	0.904	0.903

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, n/s = not significant; R^2 for actual security behavior cannot be calculated because it is categorical (successfully phished: yes/no); PEOU = perceived ease of use; PIU = perceived intrinsic usefulness; BI = behavioral intentions to follow security policies; OSC = organization security communication; TMSC = top management security commitment; OCM = organization computer monitoring

Table D.5. Correlations for Only Gamification Data

Latent Construct	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Behavioral intention (1)	.907													
Challenge (2)	.643	.803												
OCM (3)	.038	-.206	.803											
Control (4)	.229	.271	.019	.870										
Curiosity (5)	.596	.407	.401	-.375	.943									
Immersion (6)	.429	.607	.270	.152	.468	.918								
Joy (7)	.546	.557	.338	.205	.608	.576	.847							
Learning (8)	.721	.658	.028	.341	.545	.647	.286	.841						
PEOU (9)	.538	.696	.504	.163	.721	.188	.554	.386	.780					
PIU (10)	.733	.390	.485	.465	.577	.689	.573	.608	.264	.836				
Security response-efficacy (11)	.362	.354	.112	.205	.320	.130	.241	.408	.145	.341	.973			
Security self-efficacy (12)	.397	.257	.310	.260	.344	.033	.035	.180	.509	.485	.466	.923		
OSC (13)	-.096	-.088	.168	.022	-.090	-.119	-.013	-.110	-.102	.133	-.169	.102	.833	
TMSC (14)	-.010	-.005	.500	.400	-.107	.105	.196	.058	-.161	.729	-.257	.126	.137	.835

Diagonal values are square roots of the AVEs (underlined); OSC = organization security communication; TMSC = top management security commitment; OCM = organization computer monitoring.

Table D.6. Correlations for Only Email data

Latent Construct	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Behavioral intention (1)	.889													
Challenge (2)	-.529	.807												
OCM (3)	-.038	-.206	.952											
Control (4)	.213	.082	.019	.800										
Curiosity (5)	.105	.136	-.229	-.375	.906									
Immersion (6)	-.609	-.250	-.462	-.793	.468	.772								
Joy (7)	.112	-.079	.067	.279	-.769	.286	.715							
Learning (8)	-.205	.218	.552	-.171	-.115	-.184	-.467	.926						
PEOU (9)	-.402	.129	.221	.024	-.780	.520	-.168	.386	.702					
PIU (10)	-.317	.241	.192	-.716	-.584	-.212	-.538	.608	-.348	.883				
Security response-efficacy (11)	-.562	.049	.029	-.215	.004	.010	-.454	-.381	.152	-.341	.913			
Security self-efficacy (12)	-.419	.645	.005	.066	-.137	.181	-.698	.001	-.463	.052	-.467	.882		
OSC (13)	-.095	-.087	.167	.022	-.090	-.119	-.010	-.110	-.102	.133	-.169	.102	.777	
TMSC (14)	-.010	-.005	.500	.400	-.107	.105	.196	.058	-.161	.729	-.257	.126	.137	.895

Diagonal values are square roots of the AVEs (underlyined); OSC = organization security communication; TMSC = top management security commitment; OCM = organization computer monitoring.

Table D.7. Statistics Used to Assess the Quality of the Measurement Model's Measures

Latent construct	Average	SD	AVE	Composite reliability	Cronbach's alpha (α)
Behavioral intentions (BI)	6.08	0.86	0.823	0.933	0.896
Challenge	5.78	0.95	0.646	0.843	0.749
Control	5.61	1.44	0.758	0.925	0.894
Curiosity	5.69	0.94	0.891	0.942	0.878
Immersion	6.13	1.03	0.844	0.942	0.907
Joy	6.13	1.03	0.719	0.926	0.897
Learning	6.03	0.69	0.708	0.827	0.722
Organization computer monitoring (OCM)*	5.73	0.87	0.795	0.854	0.885
Organization security communication (OSC)*	6.31	0.50	0.887	0.894	0.817
Perceived ease of use (PEOU)	5.99	0.73	0.609	0.824	0.783
Perceived intrinsic usefulness (PIU)	5.83	0.82	0.700	0.921	0.922
Security response efficacy	6.13	1.05	0.948	0.974	0.946
Security self-efficacy	6.00	0.78	0.852	0.945	0.939
Top management security commitment (TMSC)*	5.51	1.06	0.698	0.872	0.773

Note: These are the combined averages and standard deviations (SDs) for the gamification and email treatments (Table D.9 categorizes the SDs by treatment). * Indicates constructs that were used only as control variables.

Table D.8. Data Collection (Survey after Six Months)

Relationships tested	Model 1 (HMSAM replication)	Model 2 (add coping and challenge)	Model 3 (full model with controls)
Replication: PEOU → PIU	0.439 (3.190***)	0.441 (3.371***)	0.440 (3.075**)
Replication: PEOU → curiosity	0.210 (4.514***)	0.207 (4.742***)	0.210 (4.865***)
Replication: PEOU → joy	0.681 (30.215***)	0.679 (30.143***)	0.677 (30.265***)
Replication: PEOU → control	0.712 (43.321***)	0.705 (43.214***)	0.702 (43.255***)
Replication: PIU → BI	0.603 (5.112***)	0.612 (5.123***)	0.610 (5.056***)
Replication: Curiosity → BI	0.659 (21.015***)	0.661 (21.124***)	0.655 (21.198***)
Replication: Curiosity → immersion	0.656 (17.268***)	0.654 (17.333***)	0.646 (17.655***)
Replication: Joy → BI	0.384 (1.306 n/s)	0.391 (1.411 n/s)	0.375 (1.465 n/s)
Replication: Joy → immersion	0.437 (11.659***)	0.445 (11.873***)	0.429 (12.009***)
Replication: Control → BI	0.798 (10.015***)	0.810 (10.304***)	0.802 (10.216***)
Replication: Control → immersion	-0.421 (1.469 n/s)	-0.397 (1.581 n/s)	-0.369 (1.855 n/s)
H1. Learning → BI	n/a	0.839 (10.412***)	0.741 (10.401***)
H2a. Learning → security response efficacy	n/a	0.239 (6.209***)	0.222 (6.125***)
H2b. Learning → security self-efficacy	n/a	0.715 (39.704***)	0.702 (39.693***)
H3a. Security response efficacy → BI	n/a	0.160 (2.786**)	0.132 (2.648**)
H3b. Security self-efficacy → BI	n/a	0.254 (5.312***)	0.224 (5.262***)
H4. Challenge → immersion	n/a	0.537 (13.722***)	0.541 (13.698***)
H5. Immersion → BI	n/a	0.533 (11.531***)	0.509 (11.455***)
H6. BI → actual security behavior	n/a	0.431 (18.645***)	0.416 (18.101***)
Control: Age → BI	n/a	n/a	0.012 (1.312 n/s)
Control: Gender → BI	n/a	n/a	0.022 (1.624 n/s)
Control: Experience → BI	n/a	n/a	-0.019 (1.152 n/s)
Control: Education → BI	n/a	n/a	0.023 (1.734 n/s)
Control: OSC → BI	n/a	n/a	0.039 (1.837 n/s)
Control: TMSC → BI	n/a	n/a	0.111 (2.017*)
Control: OCM → BI	n/a	n/a	-0.023 (1.658 n/s)
Control: Age → actual security behavior	n/a	n/a	0.021 (1.334 n/s)
Control: Gender → actual security behavior	n/a	n/a	0.038 (1.655 n/s)
Control: Experience → actual security behavior	n/a	n/a	-0.067 (1.142 n/s)
Control: Education → actual security behavior	n/a	n/a	0.083 (1.734 n/s)
Control: OSC → actual security behavior	n/a	n/a	0.041 (1.736 n/s)
Control: TMSC → actual security behavior	n/a	n/a	0.113 (2.209*)
Control: OCM → actual security behavior	n/a	n/a	-0.029 (1.634 n/s)
Equation-level fit statistics (variance explained or R^2) and model-level fit statistics, based on the estimated model of the original sample			
R^2 for PIU	0.184	0.179	0.179
R^2 for curiosity	0.129	0.125	0.126
R^2 for joy	0.485	0.472	0.473
R^2 for control	0.511	0.498	0.497
R^2 for security response efficacy	n/a	0.175	0.176
R^2 for security self-efficacy	n/a	0.483	0.482
R^2 for immersion	0.441	0.654	0.655
R^2 for BI	0.318	0.638	0.645
Root mean square error of approximation (RMSEA)	0.042	0.045	0.044
Standardized root mean residual (SRMR)	0.062	0.065	0.064
Comparative fit index (CFI)	0.970	0.974	0.973
Tucker-Lewis index (TLI)	0.970	0.972	0.973

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, n/s = not significant; R^2 for actual security behavior cannot be calculated because it is categorical (successfully phished: yes/no)

Table D.9. Construct Comparisons between Gamification and Email Treatments

	Gamification group		Email group		Results of comparisons	
Latent construct	**AVG**	**SD**	**AVG**	**SD**	**MANOVA F statistic**	**Gamified is better?**
BI	6.08	0.86	5.16	0.97	10.435***	Yes
Challenge	5.78	0.95	5.09	0.98	40.633***	Yes
Control	5.61	1.44	5.20	1.54	18.014***	Yes
Curiosity	5.69	0.94	5.38	1.01	18.784***	Yes
Immersion	6.13	1.03	4.42	1.43	3.166*	Yes
Joy	6.13	1.03	5.06	1.17	20.107***	Yes
Learning	6.03	0.69	5.55	0.97	14.035***	Yes
PEOU	6.15	0.73	5.94	0.75	30.105***	Yes
PIU	6.06	0.82	5.87	0.70	27.819***	Yes
Security response efficacy	6.13	1.05	5.83	1.34	2.601*	Yes
Security self-efficacy	6.00	0.78	5.82	1.19	4.832*	Yes

CMB and Multicollinearity

To address the potential CMB issue, recommendations from Podsakoff et al. [64] were followed. To minimize the potential social desirability effects, full anonymity was ensured for all participants. They were told that there were no right/wrong or good/bad answers, so honesty was expected. Several items were reversed to minimize automatic responses and to detect lack of attentiveness, if applicable.

Two methods were used to check for CMB. The first was Harman's single-factor test [65]. Because this test has several limitations [38, 64], the unmeasured latent method construct (ULMC) method was used, as advocated by Podsakoff et al. [64] and first implemented in IS by Liang et al. [46]. Although the efficacy of this approach has been debated, recent research has further affirmed its use [68]. This approach involves creating an ad hoc unmeasured latent construct that consists of all other items and running it against the separate constructs in the model to parse out the degree to which each construct is influenced by the common factor (thus, CMB). The results did not reveal any significant variance that would be explained by the latent construct. The average difference of the model's standardized loadings was 0.031 (maximum 0.056) and no items that loaded significantly on the latent construct were identified. Thus, CMB likely does not represent an issue.

To detect the presence of multicollinearity issues, variance inflation factor (VIF) scores were calculated. A VIF score provides a measure of the increases in the variance of the estimated beta coefficients and its impacts due to collinearity. The calculated VIFs were all below the recommended value of 10 [28]. All of our VIFs are below this most stringent guideline, as they ranged from 1.767 to 4.478 without the squared-term, and from 1.945 to 9.453 with the squared-term. Therefore, multicollinearity was not an issue for this study.

To address the potential CMB issue, recommendations from Podsakoff et al. [64] were followed. To minimize the potential social desirability effects, full anonymity was ensured for all participants. They were told that there were no right/wrong or good/bad answers, so honesty was expected. Several items were reversed to minimize automatic responses and to detect lack of attentiveness, if applicable.

Two methods were used to check for CMB. The first was Harman's single-factor test [65]. Because this test has several limitations [38, 64], the unmeasured latent method construct (ULMC) method was used, as advocated by Podsakoff et al. [64] and first implemented in IS by Liang et al. [46]. Although the efficacy of this approach has been debated, recent research has further affirmed its use [68]. This approach involves creating an ad hoc unmeasured latent construct that consists of all other items and running it against the separate constructs in the model to parse out the degree to which each construct is influenced by the common factor (thus, CMB). The results did not reveal any significant variance that would be explained by the latent construct. The average difference of the model's standardized loadings was 0.031 (maximum 0.056) and no items that loaded significantly on the latent construct were identified. Thus, CMB likely does not represent an issue.

Box M and MANOVA Assumptions

We followed the leading guidelines on MANOVA assumptions [28, 71, 73]:

First, MANOVA assumes normal distributions of the data, but it is actually extremely robust to non-normal data unless it has a platykurtic distribution (plateau-like), which is not the case with our data. Moreover, MANOVA is virtually immune to this assumption when a cell has 20–30 observations, which we exceeded.

Second, MANOVA requires a sample size of n in each cell to be greater than the number of DVs, which we greatly exceeded.

Third, MANOVA also assumes independence of the observations, which was the case with our data, given our design.

Fourth, MANOVA is very sensitive to extreme numerical outliers, but Likert-type data does not produce these kinds of outliers because the numbers literally range from 1 to 7.

Fifth, MANOVA assumes homogenous variance in each person's score on the dependent variables. MANOVA is extremely robust to violations of this assumption, except that if group sizes are dramatically different, it can make such violations more problematic. Our group sizes were different, but they fulfilled the other assumptions; thus, they would likely not qualify as "dramatically different." Nonetheless, there is a conservative test that can be applied to determine whether the covariance matrices are still equal (a key MANOVA assumption) when the group sizes are different. It is like Levene's test for ANOVA, but the MANOVA instantiation of this test is called the Box M test (see https://en.wikiversity.org/wiki/Box%27s_M). We ran the Box M test which resulted in *F*

= 12.131, p = .318. This means that we could support the assumption of equal covariance matrices—and thus, different group sizes were not detrimental.

Sixth, MANOVA assumes there is no multicollinearity among the variables. To be very conservative, we also tested all the IV–DV relationships. To detect the existence of multicollinearity issues, VIF scores were calculated. A VIF score provides a measure of the increases in the variance of the estimated beta coefficients and its impacts due to collinearity. The calculated VIFs were all below the recommended value of 10 [28]The calculated VIFs were all below the recommended value of 10 [28] for reflective constructs, which ranged from 1.767 to 4.478. Therefore, multicollinearity was not an issue for this study.

Seventh, MANOVA assumes only moderate correlations between pairs of variables, such that none are correlated at the .800 or .900 level or higher. That was also the case with our data.

REFERENCES FOR ONLINE APPENDICES

1. Adams, M and Makramalla, M. Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, 5, 1 (2015), 5-14.
2. Agarwal, R and Karahanna, E. Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly*, 24, 4 (2000), 665-694.
3. Amorim, JA; Ahlfeldt, R-M; Gustavsson, PM; and Andler, SF. Privacy and Security in Cyberspace: Training Perspectives on the Personal Data Ecosystem. Presented at *2013 European Intelligence and Security Informatics Conference*, Uppsala, Sweden, 2013, pp. 139-142.
4. Anderson, CL and Agarwal, R. Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34, 3 (2010), 613-643.
5. Au, YA; Carpenter, D; Chen, X; and Clark, JG. Virtual organizational learning in open source software development projects. *Information & Management*, 46, 1 (2009), 9-15.
6. Banfield, J and Wilkerson, B. Increasing student intrinsic motivation and self-efficacy through gamification pedagogy. *Contemporary Issues in Education Research*, 7, 4 (2014), 291-298.
7. Barnes, S. Virtual worlds as a medium for advertising. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 38, 4 (2007), 45-55.
8. Baxter, RJ; Holderness, DK; and Wood, DA. Applying basic gamification techniques to it compliance training: evidence from the lab and field. *Journal of Information Systems*, 30, 3 (2016), 119-133.
9. Boopathi, K; Sreejith, S; and Bithin, A. Learning cyber security through gamification. *Indian Journal of Science and Technology*, 8, 7 (2015), 642-649.
10. Bryan Foltz, C. Cyberterrorism, computer crime, and reality. *Information Management & Computer Security*, 12, 2 (2004), 154-166.
11. Cairns, P; Cox, AL; Day, M; Martin, H; and Perryman, T. Who but not where: The effect of social play on immersion in digital games. *International Journal of Human-Computer Studies*, 71, 11 (2013), 1069-1077.
12. Chang, C-M; Yen, C-H; and Cheng, H-L. Trust-building mechanisms and knowledge sharing in virtual communities. Presented at *Proceedings of the 9th International Conference on Electronic Business*, Macau, 2009, pp. 1070-1079.
13. Chen, C-J and Hung, S-W. To give or to receive? Factors influencing members' knowledge sharing and community promotion in professional virtual communities. *Information & management*, 47, 4 (2010), 226-236.
14. Chen, Y-M; Hsu, T-H; and Lu, Y-J. Impact of flow on mobile shopping intention. *Journal of Retailing and Consumer Services*, 41, (2018), 281-287.
15. Colwill, C. Human factors in information security: The insider threat–Who can you trust these days? *Information Security Technical Report*, 14, 4 (2009), 186-196.
16. Couch, D and Liamputtong, P. Online dating and mating: The use of the internet to meet sexual partners. *Qualitative Health Research*, 18, 2 (2008), 268-279.
17. Crossler, RE; Johnston, AC; Lowry, PB; Hu, Q; Warkentin, M; and Baskerville, R. Future

directions for behavioral information security research. *Computers & Security*, 32, (2013), 90-101.
18. Csikszentmihalyi, M. *Finding Flow: The Psychology of Engagement with Everyday Life*. New York, NY: Basic Books, 1997.
19. Csikszentmihalyi, M. *Beyond Boredom and Anxiety*. San Francisco, CA, US: Jossey-Bass, 2000.
20. Dabrowski, A; Kammerstetter, M; Thamm, E; Weippl, E; and Kastner, W. Leveraging competitive gamification for sustainable fun and profit in security education. Presented at *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, Washington, D.C., 2015.
21. David, GC; Chand, D; Newell, S; and Resende-Santos, J. Integrated collaboration across distributed sites: the perils of process and the promise of practice. *Outsourcing Global Services*: Springer, 2008, pp. 127-150.
22. Davis, M and Csikszentmihalyi, M. *Beyond Boredom and Anxiety: The Experience of Play in Work and Games*. Washington, DC: Amer Sociological Assoc, 1977.
23. Deterding, S; Dixon, D; Khaled, R; and Nacke, LE. From game design elements to gamefulness: defining gamification. Presented at *15th international academic MindTrek conference: Envisioning future media environments*, Tampere, Finland, 2011, pp. 9-15.
24. Fouché, S and Mangle, AH. Code hunt as platform for gamification of cybersecurity training. Presented at *Proceedings of the 1st International Workshop on Code Hunt Workshop on Educational Software Engineering*, Baltimore, MD, USA, 2015, pp. 9-11.
25. Gold, S. Understanding the hacker psyche. *Network Security*, 2011, 12 (2011), 15-17.
26. Gravill, JI; Compeau, DR; and Marcolin, BL. Experience effects on the accuracy of self-assessed user competence. *Information & Management*, 43, 3 (2006), 378-394.
27. Griffiths, MD; Davies, MN; and Chappell, D. Breaking the stereotype: The case of online gaming. *CyberPsychology & Behavior*, 6, 1 (2003), 81-91.
28. Hair, JF; Anderson, RE; Babin, BJ; and Black, WC. *Multivariate data analysis: A global perspective*. 7. Upper Saddle River, NJ: Pearson, 2010.
29. Hald, GM and Malamuth, NM. Self-perceived effects of pornography consumption. *Archives of sexual behavior*, 37, 4 (2008), 614-625.
30. Hamari, J; Shernoff, DJ; Rowe, E; Coller, B; Asbell-Clarke, J; and Edwards, T. Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. *Computers in Human Behavior*, 54, January (2016), 170-179.
31. Herath, T and Rao, HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47, 2 (2009), 154-165.
32. Herath, T and Rao, HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18, 2 (2009), 106-125.
33. Ho, SM and Warkentin, M. Leader's dilemma game: An experimental design for cyber insider threat research. *Information Systems Frontiers*, 19, 2 (2015), 1-20.
34. Hsu, C-L and Lin, JC-C. Acceptance of blog usage: The roles of technology acceptance, social influence and knowledge sharing motivation. *Information & management*, 45, 1 (2008), 65-74.
35. Hsu, C-L and Lu, H-P. Why do people play on-line games? An extended TAM with social influences and flow experience. *Information & Management*, 41, 7 (2004), 853-868.
36. Huotari, K and Hamari, J. Defining gamification: A service marketing perspective. In Proceedings of *Proceedings of the 16th International Academic MindTrek Conference*, Tampere, Finland, 2012, pp. 17-22.
37. Jegers, K. Pervasive game flow: Understanding player enjoyment in pervasive gaming. *ACM Computers in Entertainment*, 5, 1 (2007), 1-11.
38. Kemery, ER and Dunlap, WP. Partialling factor scores does not control method variance: A reply to Podsakoff and Todor. *Journal of Management*, 12, 4 (1986), 525-530.
39. Kim, S; Na, E-K; and Ryu, M-H. Factors affecting user participation in video UCC (User-Created

Contents) services. *Communities and Technologies 2007*: Springer, 2007, pp. 209-224.
40. Koufaris, M. Applying the technology acceptance model and flow theory to online consumer behavior. *Information Systems Research*, 13, 2 (2002), 205-223.
41. Kumar, J. *Gamification at Work: Designing Engaging Business Software*. Denmark: The Interaction Design Foundation 2013.
42. Lee, MK; Cheung, CM; and Chen, Z. Acceptance of Internet-based learning medium: the role of extrinsic and intrinsic motivation. *Information & Management*, 42, 8 (2005), 1095-1104.
43. Lee, N and Manners, D. Gamification of penetration testing. *Counterterrorism and Cybersecurity*. Switzerland: Springer International Publishing, 2015, pp. 343-347.
44. Li, BJ and Lwin, MO. Player see, player do: Testing an exergame motivation model based on the influence of the self avatar. *Computers in Human Behavior*, 59, June (2016), 350-357.
45. Li, X; Hsieh, JP-A; and Rai, A. A motivational account for post-acceptance routine and innovative use: Introducing the concept of tri-dimensional intrinsic motivation. (2009),
46. Liang, H; Saraf, N; Hu, Q; and Xue, Y. Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, 31, 1 (2007), 59-87.
47. Liu, S and Cheng, B. Cyberattacks: Why, what, who, and how. *IT Professional Magazine*, 11, 3 (2009), 14.
48. Lowry, P; Roberts, T; Dean, D; and Marakas, G. Toward building self-sustaining groups in PCR-based tasks through implicit coordination: The case of heuristic evaluation. (2009),
49. Lowry, PB; Gaskin, J; and Moody, GD. Proposing the multimotive information systems continuance model (misc) to better explain end-user system evaluations and continuance intentions. *Journal of the Association for Information Systems*, 16, 7 (2015), 515-579.
50. Lowry, PB; Gaskin, J; Twyman, N; Hammer, B; and Roberts, T. Taking 'fun and games' seriously: Proposing the hedonic-motivation system adoption model (HMSAM). *Journal of the Association for Information Systems*, 14, 11 (2013), 617-671.
51. Lyengard, G. The decline of video game narratives. Lyengard.com, 2015.
52. Mekler, ED; Brühlmann, F; Opwis, K; and Tuch, AN. Do points, levels and leaderboards harm intrinsic motivation?: an empirical analysis of common gamification elements. Presented at *Proceedings of the First International Conference on gameful design, research, and applications*, Toronto, Ontario, Canada, 2013, pp. 66-73.
53. Melki, AM and Chatrieh, MG. Gamification to support cyber security community education in lebanon. In Proceedings of *New Horizons in Industry, Business and Education*, Skiathos, Greece, 2015, pp. 172-177.
54. Meredith, A; Hussain, Z; and Griffiths, MD. Online gaming: a scoping study of massively multi-player online role playing games. *Electronic Commerce Research*, 9, 1-2 (2009), 3-26.
55. Messinger, PR; Ge, X; Stroulia, E; Lyons, K; Smirnov, K; and Bone, M. On the relationship between my avatar and myself. *Journal For Virtual Worlds Research*, 1, 2 (2008), 1-17.
56. Milne, S; Orbell, S; and Sheeran, P. Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, 7, 2 (2002), 163-184.
57. Murphy, C. Why games work and the science of learning. Presented at *MODSIM World 2011 Conference and Expo*, Virginia B, USA 2011, pp. 260-272.
58. Nardi, BA; Schiano, DJ; and Gumbrecht, M. Blogging as social activity, or, would you let 900 million people read your diary? Presented at *Proceedings of the 2004 ACM conference on Computer supported cooperative work*, 2004, pp. 222-231.
59. Neill, T. Serious games: learning for the i generation. *Development and Learning in Organizations: An International Journal*, 23, 4 (2009), 12-15.
60. Nowak, KL and Rauh, C. The influence of the avatar on online perceptions of anthropomorphism, androgyny, credibility, homophily, and attraction. *Journal of Computer-Mediated Communication*, 11, 1 (2005), 153-178.

61. Nunamaker Jr, JF; Briggs, RO; Derrick, DC; and Schwabe, G. The last research mile: Achieving both rigor and relevance in information systems research. *Journal of Management Information Systems*, 32, 3 (2015), 10-47.
62. Ophoff, J and Janowski, M. Examining Gamification as a Driver of Individual Information Security Behavior. Presented at *2015 Dewald Roode Workshop on Information Systems Security Research*, Albuquerque, NM, 2015.
63. Ortiz, A; del Puy Carretero, M; Oyarzun, D; Yanguas, JJ; Buiza, C; Gonzalez, MF; and Etxeberria, I. Elderly users in ambient intelligence: Does an avatar improve the interaction? *Universal access in ambient intelligence environments*: Springer, 2007, pp. 99-114.
64. Podsakoff, PM; MacKenzie, SB; Lee, J-Y; and Podsakoff, NP. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88, 5 (2003), 879.
65. Podsakoff, PM and Organ, DW. Self-reports in organizational research: Problems and prospects. *Journal of Management*, 12, 4 (1986), 531-544.
66. Ridings, CM and Gefen, D. Virtual community attraction: Why people hang out online. *Journal of Computer-mediated communication*, 10, 1 (2004), JCMC10110.
67. Ruboczki, ES. How to develop cloud security awareness. Presented at *2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, Romania, 2015, pp. 323-326.
68. Schwarz, A; Rizzuto, T; Carraher-Wolverton, C; Roldán, JL; and Barrera-Barrera, R. Examining the impact and detection of the 'urban legend' of common method bias. *Database for Advances in Information Systems*, 48, 1 (2017), 93-119.
69. Sen, R; Subramaniam, C; and Nelson, ML. Determinants of the choice of open source software license. *Journal of Management Information Systems*, 25, 3 (2008), 207-240.
70. Shang, R-A; Chen, Y-C; and Shen, L. Extrinsic versus intrinsic motivations for consumers to shop on-line. *Information & Management*, 42, 3 (2005), 401-413.
71. Stevens, JP. *Applied Multivariate Statistics for the Social Sciences*. Mahwah, NJ: Lawrence Erblaum, 2002.
72. Sweetser, P and Wyeth, P. GameFlow: a model for evaluating player enjoyment in games. *Computers in Entertainment (CIE)*, 3, 3 (2005), 3-3.
73. Tabachnick, BG and Fidell, LS. *Using Multivariate Statistics*. New York: Harper & Row, 1983.
74. Tan, JL; Goh, DH-L; Ang, RP; and Huan, VS. Participatory evaluation of an educational game for social skills acquisition. *Computers & Education*, 64, (2013), 70-80.
75. Thompson, MK; Weal, MJ; Michaelides, DT; Cruickshank, DG; and Roure, D. MUD slinging: Virtual orchestration of physical interactions. *University of Southampton, Working Paper, ECSTRIAM03-007*, (2003), Date last accessed: June 7, 2016, retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.6617&rep=rep1&type=pdf
76. Thornton, D and Francia III, G. Gamification of information systems and security training: issues and case studies. *Information Security Education Journal*, 1, 1 (2014), 16-24.
77. Tillema, HH; Smith, K; and Leshem, S. Dual roles–conflicting purposes: a comparative study on perceptions on assessment in mentoring relations during practicum. *European Journal of Teacher Education*, 34, 2 (2011), 139-159.
78. Treiblmaier, H; Putz, L-M; and Lowry, PB. Setting a definition, context, and research agenda for the gamification of non-gaming systems. *Association for Information Systems Transactions on Human-Computer Interaction*, 10, 3 (2018), 129-163.
79. Trinkle, BS; Crossler, RE; and Warkentin, M. I'm game, are you? Reducing real-world security threats by managing employee activity in online social networks. *Journal of Information Systems*, 28, 2 (2014), 307-327.
80. Vail, J. Gamification of an information security management course. Presented at *EdMedia: World Conference on Educational Media and Technology*, Montreal, Quebec, Canada, 2015, pp. 1720-1731.

81. Waern, A; Montola, M; and Stenros, J. The three-sixty illusion: designing for immersion in pervasive games. Presented at *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2009, pp. 1549-1558.
82. Webster, J and Watson, RT. Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly*, 26, 2 (2002), xiii-xxiii.
83. Wei, K-K; Teo, H-H; Chan, HC; and Tan, BC. Conceptualizing and testing a social cognitive model of the digital divide. *Information Systems Research*, 22, 1 (2011), 170-187.
84. Williamson, B and Facer, K. More than'just a game': the implications for schools of children's computer games communities. *Education, Communication & Information*, 4, 2-3 (2004), 255-270.
85. Wouters, P; Van Oostendorp, H; Boonekamp, R; and Van der Spek, E. The role of Game Discourse Analysis and curiosity in creating engaging and effective serious games by implementing a back story and foreshadowing. *Interacting with Computers*, 23, 4 (2011), 329-336.
86. Wu, J; Li, P; and Rao, S. Why they enjoy virtual game worlds? An empirical investigation. *Journal of electronic commerce research*, 9, 3 (2008), 219-230.
87. Yee, N. Motivations for play in online games. *CyberPsychology & behavior*, 9, 6 (2006), 772-775.