Virtual World-Based Information Security Learning: Design and Evaluation

Jungwoo Ryoo *

Division of Business, Engineering
and Information Sciences and Technology
Penn State University, USA
E-mail: jryoo@psu.edu

Angsana A. Techatassanasoontorn

Department of Business Information Systems
Faculty of Business and Law, Auckland University
Newzealand
E-mail: angsana@aut.ac.nz

Dongwon Lee

College of Information Science and Technology
Penn State University, USA
E-mail: dongwon@psu.edu

ABSTRACT

There has been a growing interest and enthusiasm for the application of virtual worlds in learning and training. This research proposes a design framework of a virtual world-based learning environment that integrates two unique features of the virtual world technology, immersion and interactivity, with an instructional strategy that promotes self-regulatory learning. We demonstrate the usefulness and assess the e?ectiveness of our design in the context of information security learning. In particular, the information security learning module implemented in Second Life was incorporated into an Introduction to Information Security course. Data from pre- and post- learning surveys were used to evaluate the e?ectiveness of the learning module. Overall, the results strongly suggest that the virtual world-based learning environment enhances information security learning, thus supporting the e?ectiveness of the proposed design framework. Additional results suggest that learner traits have an important in?uence on learning outcomes through perceived enjoyment. The study o?ers useful design and implementation guidelines for organizations and universities to develop a virtual world-based learning environment. It also represents an initial step towards the design and explanation theories of virtual world-based learning environments.

Keywords: Virtual World, Second Life, Information Security Learning, Design Evaluation, Self-regulatory Learning

1. INTRODUCTION

There has been a dramatic increase in the use of information technology (IT) in teaching and learning. These technologies are often referred to as technology-mediated learning (TML). TML is defined as an environment in which the learner's interactions with learning materials, peers, and/or instructors are mediated through advanced information technologies (Alavi & Leidner, 2001). Various forms of TML environments that have been broadly studied are computer-based collaborative learning (Alavi, 1994; Hashaim, Rathnam, & Whinston, 1992), distance learning (Hiltz & Turo, 1993; Webster & Hackley, 1997), and more recently Internet-based learning environments (Piccoli, Ahmad, & Ives, 2001; Santhanam, Sasidharan, & Webster, 2008).

In recent years, there has been a growing interest and enthusiasm for the application of virtual worlds in education. Virtual worlds can enhance learning with their ability to provide stimulating 3D environments, complex and realistic simulations, and active engagement through embodied persona (i.e., avatars) (Leidner & Jarvenpaa, 1995; Schultze et al., 2008). In such environments, learners can construct their own knowledge through their experience with a topic. Since virtual worlds have recently been developed, much of the research attention has a broad focus on the potential applications of virtual worlds and their expected benefits (e.g., Ives & Junglas, 2008; Mennecke et al., 2008; Schultze et al., 2008). Therefore, there is a fundamental need for rigorous research to understand how to use virtual worlds as an effective teaching and learning mechanism.

In this research, drawing on the TML research framework (Alavi & Leidner, 2001), virtual environment perspectives (Steuer, 1992; Witmer & Singer, 1998), and self-regulatory learning theory (Schunk & Ertmer, 1999; Zimmerman, 1989; Zimmerman, 1995), we propose a design framework of a virtual world-based learning environment and evaluate its effectiveness on learning in the context of information security education using Second Life. Although our study investigates the subject of information security in a particular environment (i.e., Second Life), we believe that the proposed research framework has a broad utility in other virtual world environments and learning subjects as well.

2. VIRTUAL WORLDS AND SECOND LIFE

Virtual worlds are 3D, computer-simulated environments that users inhabit and use to interact with other users through graphical representations of themselves called avatars or through software agents (Ives & Junglas, 2008; Kumar et al., 2008). Virtual worlds can be broadly classified into online games and metaverses. Online games or massively multiplayer online games (MMOGs), similar to video games, offer environments that have been created by their producers with an overarching set of objectives for players. Users come together to participate in various genres of activities (e.g., defeating enemies, capturing treasures). EVE Online (www.eveonline.com) and World of Warcraft (www.worldofwarcraft.com) are two of such popular games.

The second type of virtual worlds, metaverses, are also known as multi-user virtual environments, virtual social worlds, or synthetic worlds. They are immersive virtual spaces that differ from online games in at least three ways. First, unlike online games, metaverses provide seamless persistent worlds where users can roam around without predefined objectives. Second, there are no clearly defined character roles for users; therefore, users can freely choose to create their avatars to have similar appearances to themselves, animals, or even fantasy-like creatures. Third, users can generate and retain the ownership of contents and objects, which allows them to later sell their objects in the meta-verse economy. In recent years, there has been an increasing growth in the number of metaverses with varying functions and usages. For example, Forterra Systems (www.forterrainc.com) is a private metaverse with an emphasis on staff training and collaborative decision making activities. Other metaverses are open to all users, such as Active Worlds (www.activeworlds.com), There (www.there.com), and Second Life (www.secondlife.com).

Second Life, created by Linden Labs in 2003, has been one of the most popular metaverses with 21.3 million registered users as of November 2010. Because of its general purpose and open environment, Second Life enables a broad range of activities and usages among organizations, such as virtual team collaboration (e.g., IBM), product announcements and showcases (e.g., Cisco), customer interactions (e.g., BMW, Lacoste, Toyota), and product design and development (e.g.,

Starwood Hotels). Another exciting area of application that virtual worlds can offer significant opportunities in is education and training (Pollitt, 2008; Mennecke et al., 2008). It was reported that more than 100 universities have held classes or some sessions in Second Life (Schultze et al., 2008).

Despite the growing interest and potential values of the virtual world-based learning environments, very little research has examined the design of a virtual world-based learning environment and the assessment of its effectiveness on learning. Much of the research that examined the role of virtual worlds in learning was exploratory and descriptive in nature and reported inconclusive findings. For example, Wagner (2008) concluded that students at a university in Hong Kong demonstrated considerable learning and were enthusiastic about learning in a virtual world. However, a small pilot study at the New Jersey Institute of Technology reported that most of the students did not like the Second Life environment due to the frustration with the user interface, limited interaction capabilities, and the complex avatar controls (Schultze et al., 2008).

As suggested by several researchers (Clark, 1994; Leidner & Jarvenpaa, 1995; Piccoli, Ahmad, & Ives, 2001), technology alone does not necessarily determine learning outcomes. An important question is "How can we design an IT-enabled learning environment that enhances and improves learning?" Next, we discuss our framework that proposes a design of a virtual world-based learning environment with a strong emphasis on the intricate influence of technology features, an instructional strategy, and psychological processes on learning.

3. RESEARCH FRAMEWORK

The motivation for using technology in learning is to facilitate learning processes, which in turn in influences positive learning outcomes. Therefore, IT-enabled learning research needs to move beyond the study of a simple examination of surface features of IT on learning to the study of deeper structures of the relationships among IT, an instructional strategy, and psychological learning processes and their influence on learning outcomes (Alavi & Leidner, 2001; Piccoli, Ahmad, & Ives, 2001). We share this view and conceptualize a design

framework of a virtual world-based environment by integrating unique features of the virtual world technology with an instructional strategy that promotes self-regulatory learning. We demonstrate the usefulness and assess the effectiveness of our design framework in the context of information security learning using Second Life.

3.1. Design of a Virtual World-based Learning Environment

We adopt a constructivist view of learning which argues that meaningful learning is considered as a collaborative and active engagement in an authentically rich and realistic environment (Jonassen, 1999). There is strong empirical evidence that, in TML contexts, collaborative learning has superior learning effects in comparison to individual learning (Lim, Ward, & Benbasat, 1997; Lou, Abrami, & D'Apollonia, 2001). This is because group learning facilitates social interactions among learners and forces them to engage in deeper-level thinking (Alavi & Leidner, 2001). Virtual worlds facilitate constructivist learning through their ability to simulate a more realistic context and to support learning-by-doing (Leidner & Jarvenpaa, 1995). Such simulated learning environments are particularly useful for information security learning because they allow learners to make mistakes (e.g., an insecure router setup, a weak password choice, or purchases from insecure Web sites) without risking negative consequences when those same mistakes occur in the real environment. Figure 1 illustrates the design of a virtual world-based, simulated, collaborative learning environment in the context of information security learning in Second Life.

3.1.1. Virtual World Features

Research concludes that two features distinguishing virtual environments from other technologies are: immersion and interactivity (Steuer, 1992; Walsh & Pawlowski, 2002; Witmer & Singer, 1998). Immersion refers to the extent of representational richness and the range of sensory modalities employed (Steuer, 1992). For example, a virtual world that supports both textual and audio chat capabilities is more immersive than another virtual world that supports only a textual chat capability. It is important to recognize that these

immersive features describe technology characteristics, not an individual's responses to the technology (Slater, 1999). The terms *system immersion* and *psychological immersion* are often used to distinguish the former concept from the latter. Despite their distinctiveness, the system immersion and psychological immersion concepts are strongly related. In particular, system immersion promotes a sense of psychological immersion or "a psychological state characterized by perceiving oneself to be enveloped by, included in, and interacting with an environment that provides a continuous stream of stimuli and experiences" (Witmer & Singer, 1998). Table 1 illustrates our application of immersive features in Second Life. These include team avatars and custom-made physical structures and objects that provide high fidelity with the scenario described in Figure 1. Figures 2-4 show a Second Life store, a message board, portals, and an information security readiness scoreboard, respectively. These are key objects to facilitate learning in our Second Life environment. Figure 5 shows an online store from which the teams can purchase their products.

Interactivity refers to the extent to which a user can participate in a virtual environment by modifying the form and content of the environment in real time (Steuer, 1992). Interactivity is a prominent feature of a virtual environment. More specifically, it enables users to maintain active involvement and adjust the mediated environment according to their interests. Suh and Lee (2005), for example, found that a virtual environment enhances consumer learning about products. In this study, we incorporated interactivity through avatar customization and several forms of avatar-object interactions (see Table 1).

3.1.2. Self-Regulation

Self-regulation refers to a general skill to direct and sustain efforts toward the attainment of one's goals through goal setting, progress evaluation, and goal and strategy adaptation to ensure success (Zimmerman, 2000). There is a strong body of evidence suggesting that learners who self-regulate their learning have higher academic achievements (Pintrinch & Degroot, 1990; Zimmerman, Bandura, & Martinez-Pons, 1992). This study adopts the social cognitive perspective on self-regulation in which learners play an active role in enacting self-regulation towards learning (e.g., setting learning goals, choosing learning strategies, having sufficient motivation to learn). The social cognitive theory (Bandura, 1986) emphasizes a learners' personal agency and suggests that, in addition to cognitive engagement, self-efficacy and motivation are critical components in self-regulatory processes and learning outcomes.

We propose that instructional strategies in virtual worlds should include interventions that guide learners to apply self-regulation in their learning. Some of the interventions include, among other things, formulating appropriate goals, enhancing their motivation to learn, and using feedback to adjust learning goals and strategies. In particular, we draw on Zimmerman's (1998) process of self-regulation model in which three cyclical phases of self-regulation are distinguished: (1) the forethought phase, (2) the performance control phase, and (3) the self-reflection phase.

The forethought phase occurs before learning and provides opportunities to prepare learners to set realistic goals and outcome expectations, plan strategies, and develop a positive mindset towards learning. The performance control phase involves processes during learning. During this phase, self-evaluation and external feedback are critical to encourage learners to continue their learning efforts. The self-reflection phase involves reflection or evaluation of outcomes compared to goals after performance. We implemented a number of interventions across all three self-regulated learning phases as summarized in Table 2.

3.2. Evaluation of a Virtual World-based Learning Environment

Following the proposed design framework of a virtual world-based learning environment, we developed an information security learning environment in Second Life. Next, we evaluated the effectiveness of the design framework on learning outcomes and investigated the extent to which different psychological traits of students (e.g., learning goal orientation, computer learning self-efficacy) affect learning experience and outcomes.

Both learner performance and satisfaction have been widely used as measures to evaluate the effectiveness of learning environments (Alavi, 1994; Piccoli, Ahmad, & Ives, 2001). However, previous research in IT training suggests that performance does not offer a complete explanation on future behaviors. Self-efficacy (Bandura, 1986) which refers to individuals' belief in their ability

Goal: A learning module to help learners obtain a basic understanding of how businesses and individuals can protect themselves against key security threats. The focus is on both technical security measures (appropriate router and firewall setup and maintenance) and safe on-line behaviors (choices of online stores with appropriate access controls).

Learning Objectives: At the end of the learning module, students should be able to:

- Appropriately configure a router and its built-in firewall to strengthen computer and network security;
- Understand the implications of a weak security configuration of a router; Appropriately choose strong passwords;
- Understand the implications of using weak passwords;
- Appropriately choose Web sites that provide strong access control;
- Understand the differences and benefits of the key access control mechanisms (CAPTCHA, clipping levels, security images, and out of band communications); and
- Understand the implications of interacting with Web sites that do not provide strong access control.

Scenario: Student teams are in charge of opening a new virtual store in Second Life. Their main tasks are to (1) purchase a router from an online store, (2) install/configure it for the Second Life store, (3) choose a type of products to sell (i.e., furniture or electronics), and (4) stock the store with the products purchased from trustworthy online stores. These tasks need to be accomplished with a limited budget. There are two team assets given at the beginning of this learning module:

- $5,000 of cyber money to acquire necessary computing/networking equipment and products for the team's Second Life store; and
- An initial information security readiness score of 0. Information security readiness scores are evaluated periodically and calculated as an average of the technical security readiness score and the online purchase behavior score. At the end of this learning module, the team that spends the least amount of money and has the highest information security readiness score wins the game.

Fig. 1 A virtual world-based simulated, collaborative learning environment

Table 1. Virtual World Features: Immersion and Interactivity

| Feature	Definition	Design Instantiations in Second Life	Usage/Purpose
Immersion	The extent of representational richness and the range of sensory modalities employed	Team avatars	Each team is assigned an avatar with the same look and clothing.
		Store building	A team is provided with an empty space of a Second Life storefront with a basic building structure and furniture.
		Routers and computers	A team is given one computer and one router in the IT room section of a Second Life store.
		Team message boards	Each team has a message board for an instructor to communicate with teams regarding various security attack scenarios (e.g., a breached router due to an untimely firmware upgrade or a hacked router password).
		Security readiness scoreboard	A scoreboard shows an overall in formation security readiness score for each team. The scores are updated every time teams make security-relevant decisions such as changing their router password or firewall settings.
		Product portals	A portal serves as a connection between the Web and Second Life. Products purchased from online stores on the Web are de livered through portals in Second Life.
Interactivity	The extent to hich a user can participate in a virtual ronment by modifying the form and content of the environment in real time	Avatar customization	A team is encouraged to customize the look, clothing, and accessories of its avatar.
		Avatar-object interaction - real world simulated object manipulation	A team avatar activates a Web interface of a router setup (similar to a real-life router setup interface) by clicking on a virtual router in Second Life.
		Avatar-object interaction - virtual world object manipulation	A team avatar customizes its Second Life store by adding additional objects (e.g., rooftop, decorative items).
			A team avatar interacts with a portal to pick up purchased products and put them in a Second Life store.
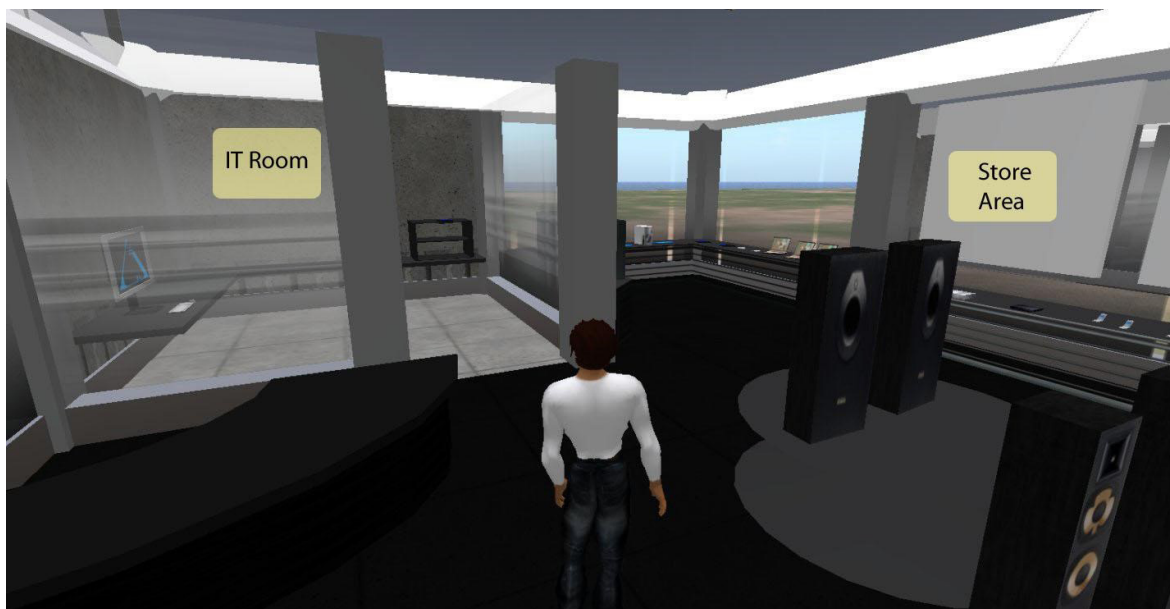
Fig. 2 A team Second Life store

Fig. 3 A team message board

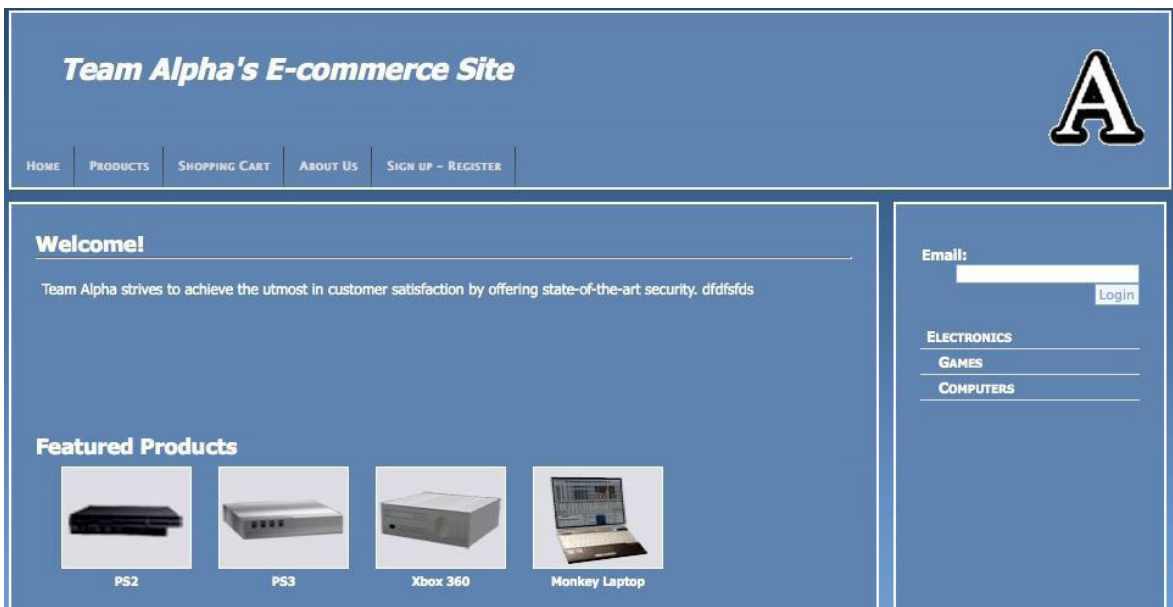**Fig. 4** An information security readiness scoreboard (left) and portals (right)

Fig. 5 An online store

Table 2. Self-Regulatory Interventions

Phase	Interventions
Forethought	• Discuss the specific goals of the information security learning module. • Provide a list of what learners should have learned at the end of the learning module. • Provide a detailed list of tasks that need to be accomplished. • Use one class session to introduce Second Life through a short lecture, a video clip, and hands-on activities with an avatar (e.g., walking, flying, chatting finding a team store, etc.) to enhance interest in learning through Second Life.
Performance Control	• Provide periodic feedback of information security readiness scores. Teams can then use the information to evaluate their performance and, if necessary, adjust their strategies. • Motivate teams (particularly those that earn relatively low information security readiness scores) to rethink their strategies. • Remind learners to take notes and pay attention to their purchase activities and router setup details.
Self-reflection	• Provide a detailed breakdown of a team's technical security score and an online purchase behavior score. • Explain the criteria used to calculate the scores. • Ask teams to make a brief presentation to reflect on their learning processes and answer the question "If you could redo the learning module, what would you do differently?" • Summarize common security mistakes that different teams make and discuss key technical measures and safe online behaviors learned.

to perform behavior has been found to be an important predictor of behaviors when confronting a task that requires individuals to apply the acquired IT skills. Therefore, in this research, effectiveness is measured by learning outcomes (performance and self-efficacy) and satisfaction. We discuss the hypotheses put forth in our research next.

Virtual world-based learning environments provide rich information and enable more interactions with learning contents and other learners. Research reported that rich, interactive, and engaging presentations of information enhance learning among consumers (Li, Daugherty, & Biocca, 2001; Suh & Lee, 2005). The high degree of interactivity enables learners to have higher control of the learning environment and facilitates active learning. Higher degrees of learner control improve learner performance and lead to higher satisfaction (Merrill, 1994). As discussed earlier, there is strong evidence that self-regulatory learning through goal setting, feedback, and self-reflection affects learning outcomes (Schunk, 1991; Schunk & Ertmer, 1999). In some cases, virtual world features can promote self-regulatory learning processes leading to positive learning outcomes. For example, the information security scoreboard allows learners to view their own team's score as well as those from other teams. This enables learners to monitor their progress against their goals as well as evaluate their relative progress with other teams. Perceived progress promotes self-efficacy and motivation, which enhances learning. Hence, we propose the following hypothesis:

H1: The design of a virtual world-based learning environment that leverages unique virtual world features and incorporates design interventions to promote self-regulatory learning will enhance learning outcomes.

Learning goal orientation is a motivational variable that explains how individuals respond to new learning environments (Brett & VandeWalle, 1999). In other words, learning goal orientation relates to the use of learning strategies in new learning situations (i.e., virtual world-based learning environments). The concept of learning goal orientation is critical in high-order skills learning (such as information security learning) because it requires the use of more complex learning

strategies in which learners associate the new information with other more familiar materials (Fisher & Ford, 1998). Individuals with high learning goal orientation set challenging goals for themselves and pursue adaptive learning strategies in which they are persistent in their learning e orts. They also report enjoyment with the challenge (Brett & VandeWalle, 1999). Thus, we propose the following hypothesis:

H2a: In a virtual world-based learning environment, learning goal orientation will be positively associated with perceived enjoyment.

Self-efficacy is a critical variable that affects all phases of self-regulation (Schunk & Ertmer, 1999). Students who are familiar with traditional classroom environments were reported to have difficulty in managing different delivery methods (Gall & Hannafin, 1994). Although some may argue that self-efficacy beliefs towards learning in a technology-mediated environment may have a direct influence on learning outcomes, evidence from previous TML studies did not find support for the relationship. In e-learning environments, Santhanam, Sasidharan, and Webster (2008), for example, reported that self-efficacy beliefs towards learning in a technology-mediated environment do not explain differences in changes in declarative knowledge and hands-on performance. In contrast, research evidence seems to suggest that perceived enjoyment mediates the influence of self-efficacy beliefs on learning outcomes. For example, several students reported having difficulty and frustration during their learning process in the new Web-based virtual learning environments (Piccoli, Ahmad, & Ives, 2001). Thus, we propose the following hypothesis:

H2b: In a virtual world-based learning environment, computer learning self-efficacy will be positively associated with perceived enjoyment.

Research has shown that psychological characteristics such as motivation and a degree of effort are positively correlated with learning outcomes (Alavi & Leidner, 2001). It is expected that individuals who experience enjoyment while interacting with a virtual world-based learning environment are motivated to put more efforts towards learning tasks, thus enhancing learning

outcomes. Perceived enjoyment is related to the notion of ow (Hoffman & Novak, 1996) and research suggests that flow leads to several positive outcomes including increased learning and satisfaction with the experience. Therefore, we propose the following hypotheses:

H3a: In a virtual world-based learning environment, perceived enjoyment will be positively associated with learning outcomes.

H3b: In a virtual world-based learning environment, perceived enjoyment will be positively associated with satisfaction.

4. RESEARCH METHOD

4.1. The Learners
The virtual world-based information security learning module using Second Life was incorporated into an "Introduction to Information Security" course at a major university in Fall 2008. The students (52 males, 7 females) were undergraduate students enrolled in the course at two campuses. The small number of female students is a reflection of the 13% female enrolment at this college during that period. Most of the students are experienced computer users with an average experience of 11.9 years. About one-third (33.3%) of students have no prior experience with Second Life.

4.2. Procedure
All students attended a semester-long course. The course met twice a week for a period of seventy-five minutes. Students were divided into teams of four to work on the virtual world-based information security learning module during the two week period of classes. To control for potential biases, an identical set of procedures, materials, and classroom protocols were used by the instructors of the two classes.

Before their engagement with the module, students were introduced to the virtual world in general and Second Life in particular through a class lecture, a short video clip, and a brief hands-on exercise. A written description and instruction about the activities were used to provide information about learning objectives, the scenario, team assets, and activities. During the rest of the two-week class periods, the teams were given a set

of interrelated tasks to open a new virtual store in Second Life.

4.3. Measures

4.3.1. Dependent variables

Consistent with previous TML research (Piccoli, Ahmad, & Ives, 2001), the dependent variables are measured by learning outcomes (learners' performance and information security self-efficacy) and satisfaction. Learners' performance is measured with a conceptual knowledge test and hands-on information security readiness scores (technical security readiness and online purchase behavior scores). In this study, the conceptual knowledge test included thirteen multiple choice questions. Satisfaction was measured through a validated scale (Piccoli, Ahmad, & Ives, 2001). Information security self-efficacy was measured by adapting validated scales from Chai et al. (2006).

4.3.2. Pre-learning survey

A questionnaire capturing the learners' gender, self-rated computer experience, virtual world experience, learning goal orientation, and computer learning self-efficacy was administered at the beginning of the learning module. Learners were also asked to respond to the questions that test their information security knowledge and capture their self-efficacy before learning. Both learning goal orientation and computer learning self-efficacy were measured through the original scales from Zweig and Webster (2004) that were also used in Santhanam, Sasidharan, and Webster's (2008) e-learning study.

4.3.3. Post-learning survey

At the end of the learning module, learners were asked to respond to another questionnaire to capture their information security knowledge and self-efficacy after learning, perceived enjoyment, and satisfaction. Perceived enjoyment was measured through a validated scale from Deci et al. (1994).

5. DATA ANALYSIS AND RESULTS

5.1. Measurement Model Validation

Two related analysis procedures were used to test the effectiveness of the virtual world-based information security learning module. Paired t-test was used to test the pre- and post-learning outcomes. Partial Least Square (PLS) was used to evaluate the influence of psychological learning variables on learning outcomes. To determine the appropriateness of analysis at an individual level, we calculated the Intra-Class Correlation (ICC) (Shrout & Fleiss, 1979) and evaluated the possible team-level effects. The ICC is derived from a nested ANOVA test that assesses whether or not members in the same team produce more similar outcomes. The ICC score of 1.0 indicates that all the team members have the same score, and the ICC score of 0.0 indicates that people within a team are no more similar than people from different teams. In other words, the lower value of the ICC indicates that the team level does not have any significant effect and the analyses can be conducted at an individual level. The ICC values for this study are from 0.007 to 0.42 with an average of 0.18 which were below the suggested theoretical guideline of 0.5 for considering the team effects (McGraw & Wong, 1996). Thus, all the analyses were conducted at an individual level.

Construct validity was evaluated before conducting further analysis. Since all of the constructs with the exception of information security performance are reflective constructs, the conventional construct validity assessment using a common factor analysis is used. The convergent validity and reliability were evaluated by examining item loadings and composite reliability. Among the twenty eight measures, an item loading for one measure is significant at $p < 0.10$ and the other twenty one and six measures are significant at $p < 0.01$ and $p < 0.05$ respectively. The composite reliability values are high, ranging from 0.84 (information security self-efficacy) to 0.96 (perceived enjoyment).

Discriminant validity was evaluated by examining the loadings and cross-loadings of item-construct loadings, and average variance extracted (AVE). Discriminant validity is established when items load higher on their hypothesized constructs than on other constructs and when the square root of a construct's AVE is larger than its correlations with other constructs (Gefen & Straub, 2005). All items load higher on their constructs than on other constructs, and the square root of each construct's AVE is higher than its correlations with other constructs.

5.2. Results

We first performed paired t-test to evaluate Hypothesis 1 concerning the effectiveness of the virtual world-based information security learning on learning outcomes. As shown in Table 3, the results indicated significant improvement in both information security knowledge (p < .01) and information security self-efficacy (p < .05) between pre- and post-test measures. This suggests that the virtual world-based learning environment that integrates unique virtual world features with the self-regulatory learning interventions enhances information security learning.

To better understand the psychological learning process through which learning occurs, we performed PLS analysis to evaluate learner traits on learning outcomes. In particular, we performed a bootstrap analysis with 500 subsamples using PLS Graph 3.0 to estimate the path coefficients and their significance. Figure 6 presents the path coefficients and the explained variances.

The results support all the hypothesis except H2a - Learning goal orientation is positively associated with perceived enjoyment. Computer learning self-efficacy is positively related to perceived enjoyment (= 0.49, p < .01), supporting H2b. Perceived enjoyment is positively related to information security performance (= 0.37, p < .01) and satisfaction (= 0.79, p < .01), supporting H3a and H3c. Overall, computer learning self-efficacy predicts perceived enjoyment (R^2 = 0.27). Perceived enjoyment predicts information security performance (R^2 = 0.35) and satisfaction (R^2 = 0.63). These results lead us to conclude that learner traits have an important influence on learning outcomes. In other words, learners who have higher self-efficacy with the virtual world learning environment are likely to have enjoyment experience during the learning process, which in turn enhances learning and overall satisfaction.

6. DISCUSSION AND CONCLUSION

Virtual worlds have attracted growing interests among organizations and educational institutions as a new learning platform because, unlike other technologies, they offer several unique characteristics (e.g., 3D immersive game-like environments) that can potentially enhance learning and training outcomes. In this research, we proposed an effective design of a virtual world-based learning environment that integrates unique virtual world features (i.e., immersion and interactivity) with self-regulatory learning interventions to offer a rich, authentic, and active learning environment. We implemented the design framework and evaluated the effectiveness of the virtual world-based learning environment in the context of information security learning in the Second Life environment.

Consistent with the previous TML research (Alavi, 1994; Alavi, Marakas, & Yoo, 2002), our results support the tenet of constructive learning: effective learning processes are those in which teams of learners acquire knowledge via problem solving. Overall, the virtual world-based learning environment leads to higher levels of conceptual security knowledge and skills development and information security self-efficacy.

According to Gagne and Briggs (1979), instructional activities can be designed to activate learners' psychological processes required to achieve learning outcomes. The key instructional events are gaining attention, presenting the stimulus material, and providing feed-

Table 3. Second Life Security Learning Module: Paired t-test of Learning Outcomes

Measures	Mean outcome score (SD)		t-value
	Pre-learning	Post-learning	
Conceptual knowledge (Max= 13)	9.59 (2.42)	12.66 (2.15)	3.17***
Information efficacy (7-point Likert scale)	5.98 (1.33)	6.38 (0.79)	1.85**
The significance levels are *p < .10, **p < .05, ***p < .01			

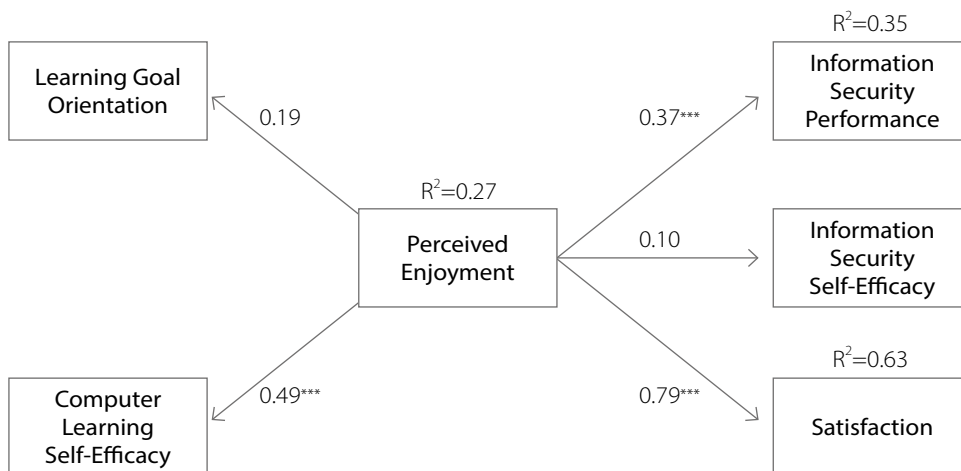**Fig. 6** Results of the influence of psychological learning variables on learning outcomes
The significance levels are: * p < :10, ** p < :05, *** p < :01

back about performance. Our design supports all these instructional events. For example, the learning scenario that requires learners to open a virtual store in Second Life grasps the attention of learners who are more familiar with traditional classroom learning. The 3D objects, team avatars, and avatar-object interactions provide rich presentations of the information and promote active engagement and motivation during the learning process, leading to effective learning outcomes. External feedback through an information security scoreboard enables learners to adjust their strategies to improve their scores, if necessary.

Consistent with Santhanam, Sasidharan, and Webster (2008), we also found that the incorporation of self-regulatory interventions encouraged learners to apply more self-regulatory strategies, leading to positive learning outcomes. In some cases, the interaction between virtual world features (e.g., an information security scoreboard) and self-regulatory interventions (e.g., reminders to pay attention to router configuration and choices of online stores) reinforces psychological processes that facilitate learning.

TML research has concluded that student characteristics have an important influence on learning outcomes.

We found that individuals' psychological traits influence learning outcomes through perceived enjoyment. Our results provide explanation why Santhanam, Sasidharan, and Webster (2008) did not find the effects of individual psychological traits on learning outcomes. However, we did not find support for the influence of perceived enjoyment on information security self-efficacy. One possible explanation is that the students in our study reported high levels of information security self-efficacy before learning. Therefore, additional studies are needed with various population groups to evaluate the relationship between these two constructs. Also, the influence of learning goal orientation on perceived enjoyment was not supported. This points to the value of virtual world-based environments to a more general population regardless of their learning orientation.

There are a few limitations in this study. The sample size is relatively small compared to other TML studies. This is due to the limitation of the Second Life technology. We found that Second Life system performance significantly degrades when more than 50 students simultaneously access the common learning platform built on an island in Second Life. Wagner (2008) reported similar problems in his classroom use. Another

limitation is the generalizability of our findings to other learning contexts. Although we believe that the design framework is applicable to other learning contexts, replications in other virtual world technologies and subject areas are strongly encouraged.

This study has contributed to both theory and practice. According to Alavi and Leidner (2001), there is a strong need for theoretically grounded and rigorous research to guide the development of TML environments. Much of TML research has primarily focused on conducting comparative studies of multiple TML learning environments (e.g., Alavi, Marakas, & Yoo, 2002) or a TML learning environment and a traditional learning environment (e.g., Piccoli, Ahmad, & Ives, 2001). Although these studies provide insights to understand relative effectiveness of a new technology, they do not offer guidelines to develop effective learning environments with a new technology. This research represents an initial step towards the design and explanation theories of virtual world-based learning environments (Gregor, 2006). One avenue for future research is to develop an integrated theoretical model to examine the mutual influence of virtual world features, self-regulatory learning strategies, and psychological processes on learning outcomes.

Castranova (2007) predicted that, similar to the Web, avatar-mediated interactions will become part of mainstream activities in the near future. Organizations and universities have constantly looked for novel learning and training environments to enhance learning outcomes. We believe that virtual worlds are promising platforms for effective learning. However, we agree with other researchers (e.g., Alavi & Leidner, 2001; Turo & Hiltz, 1995) that a novel learning environment should not be a mere automated version of a traditional learning environment. Therefore, this study offers useful design and implementation guidelines for organizations and universities to develop a virtual world-based learning environment of their own.

REFERENCES

Alavi, M. (1994). Computer-mediated collaborative learning: An empirical evaluation. *MIS Quarterly 18*(2), 159-174.

Alavi, M., & Leidner, D. E. (2001). Research commentary: Technology-medicated learning - A call for greater depth and breadth of research. *Information Systems Research 12*(1), 1-10.

Alavi, M., Marakas, G. M., & Yoo, Y. (2002). A comparative study of distributed learning environments on learning outcomes. *Information Systems Research 13*(4), 404-415.

Bandura, A. (1986). *Self-efficacy, social foundations of thought and action: A social cognitive theory.* Englewood Cliffs, NJ: Prentice-Hall.

Brett, J. F., & VandeWalle, D. (1999). Goal orientation and goal content as predictors of performance in a training program. *Journal of Applied Psychology 84*(6), 863-873.

Castranova, E. (2007). *Exodus to the virtual world: How online fun is changing reality.* New York, NY: Palgrave Macmillan.

Chai, S. et al. (2006). Role of perceived importance of information security: An exploratory study of middle school children's information security behavior. *Proceedings of Informing Science + Information Technology Education Conference* (pp. 127-135). Greater Manchester: England.

Clark, R. E. (1994). Media will never influence learning. *Educational Technology Research and Development 42*(2), 21-29.

Deci, E. L., et al. (1994). Facilitating internalization: The self-determination theory perspective. *Journal of Personality 62*(1), 119-142.

Fisher, S. L., & Ford, J. K. (1998). Differential effects of learner effort and goal orientation on two learning outcomes. *Personnel Psychology 51*(2), 397-420.

Gagne, R. M., & Briggs, L. J. (1979). *Principles of instructional design*. 2nd ed. New York: Holt, Rinehart, and Winston.

Gall, J. E., & Hannafin, M. J. (1994). A framework for the study of hypertext. *Instructional Science 22*, 207-232.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the AIS 16*, 91-109.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly 30*(3), 611-642.

Hashaim, S., Rathnam, S., & Whinston A. (1992). CATT: An Argumentation-based groupware system for enhancing case discussions in business

school. *Proceedings of 12th Annual International Conference of Information Systems*, 371-385.

Hiltz, S. R., & Turo, M. (1993). *The network nation: Human communication via computer.* Cambridge, MA: MIT Press.

Hoffman, T. P., & Novak, D. L. (1996). Marketing in hypermedia computer-mediated environments: Conceptual foundations. *Journal of Marketing 60*, 50-68.

Ives, B., & Junglas, I. (2008). APC Forum: Business implications of virtual worlds and serious gaming. *MIS Quarterly Executive 7*(3), 151-156.

Jonassen, D. H. (1999). Designing constructivist learning environments. In C. M. Reigeluth (Ed.), *Instructional-design theories and models, Vol. 2.* Mahwah, NJ: Lawrence Erlbaum Associates.

Kumar, S. et al. (2008). Second Life and the new generation of virtual worlds. *IEEE Computer 41*(9), 46-53.

Leidner, D. E., & Jarvenpaa, S. L. (1995). The use of information technology to enhance management school education: A theoretical view. *MIS Quarterly 19*(3), 265-291.

Li, H., Daugherty, T., & Biocca, F. (2001). Characteristics of virtual experience in electronic commerce: A protocol analysis. *Journal of Interactive Marketing 15*(3), 13-30.

Lim, K. H., Ward, L. M., & Benbasat, I. (1997). An empirical study of computer system learning: Comparison of co-discovery and self-discovery methods. *Information Systems Research 8*(3), 254-272.

Lou, Y., Abrami, P. C., & D'Apollonia, S. (2001). Small group and individual learning with technology: A meta-analysis. *Review of Educational Research 71*(3), 449-521.

McGraw, K. O., & Wong, S. P. (1996). Forming inferences about some intraclass correlation coefficients. *Psychological Methods 1*(1), 30-46.

Mennecke, B. E., et al. (2008). Second Life and other virtual worlds: A roadmap for research. *Communications of the Association for Information Systems 22*, 371-388.

Merrill, M. D. (1994). *Instructional design theory.* Englewood Cliffs, NJ: Educational Technology Publications.

Piccoli, G., Ahmad, R., & Ives, B. (2001). Web-based virtual learning environments: A research frame-

work and a preliminary assessment of effectiveness in basic IT skills training. *MIS Quarterly 25*(4), 401-426.

Pintrinch, P., & Degroot, E. (1990). Motivational and self-regulated learning components of classroom academic performance. *Journal of Educational Psychology 82*(1), 33-40.

Pollitt, D. (2008). Learn-while-you-play program gets IBM recruits up to speed. *Training & Management Development Methods 22*(1), 401-403.

Santhanam, R., Sasidharan, S., & Webster, J. (2008). Using self-regulatory learning to enhance e-learning-based information technology training. *Information Systems Research 19*(1), 26-47.

Schultze, U., et al. (2008). Using synthetic worlds for work and learning. *Communications of the Association for Information Systems 22*, 351-370.

Schunk, D. H. (1991). Goal setting and self-evaluation: A social cognitive perspective on self-regulation. In M.L. Machr & P.R. Pintrich (Eds.), *Advances in motivation and achievement* (pp. 85-113). Greenwich, CT: JAI Press.

Schunk, D. H., & Ertmer, P. A. (1999). Self-regulatory processes during computer skill acquisition: Goal and self-evaluative influences. *Journal of Educational Psychology 91*(2), 251-260.

Shrout, P. E., & Fleiss, J. L. (1979). Intraclass correlations: Uses in assessing rater reliability. *Psychological Bulletin 86*(2), 420-428.

Slater, M. (1999). Measuring presence: A response to the Witmer and Singer Presence questionnaire. *Presence: Teleoperators and Virtual Environments 8*(5), 1-13.

Steuer, J. (1992). Defining virtual reality: Dimensions determining telepresence. *Journal of Communication 42*(4), 73-93.

Suh, K., & Lee, Y. E. (2005). The effects of virtual reality on consumer learning: An empirical investigation. *MIS Quarterly 29*(4), 673-697.

Turo, M., & Hiltz, S. R. (1995). Software design and the future of the virtual classroom. *Journal of Information Technology for Teacher Education 4*(2), 197-215.

Wagner, C. (2008). Learning experience with virtual worlds. *Journal of Information Systems Education 19*(3), 263-266.

Walsh, K. R., & Pawlowski, S. D. (2002). Virtual reality:

A technology in need of IS research. *Communications of the Association for Information Systems 8*, 297-313.

Webster, J., & Hackley, P. (1997). Teaching effectiveness in technology mediated distance learning. *Academy of Management Journal 40*(6), 1282-1309.

Witmer, B. G., & Singer, M. J. (1998). Measuring presence in virtual environments: A presence questionnaire. *Presence 7*(3), 225-240.

Zimmerman, B. J. (1989). A social cognitive view of self-regulated academic learning. *Journal of Educational Psychology 81*(3), 329-339.

Zimmerman, B. J. (2000). *Attaining self-regulation: A social cognitive perspective*. Ed. by Boekarts M., Pintrich P., and Zeidner M. San Diego, CA: Academic Press, 2000.

Zimmerman, B. J. (1998). Developing self-fulfilling cycles of academic regulation: An analysis of exemplary instructional models. In D. H. Schunk & B. J. Zimmerman, *Self-regulated learning: From teaching to self-reflective practice* (pp. 1-19). New York, NY: Guilford Press.

Zimmerman, B. J. (1995). Self-regulation involves more than metacognition: A social cognitive perspective. *Educational Psychologist 30*(4), 217-221.

Zimmerman, B. J., Bandura, A., & Martinez-Pons, M. (1992). Self-motivation for academic attainment: The role of self-efficacy beliefs and personal goal setting. *American Educational Research Journal 29*(3), 663-676.

Zweig, D., & Webster, J. (2004). Validation of a multidimensional measure of goal orientation. *Canadian Journal of Behavioral Science 36*(3), 232-243.

Appendix A

A.1 Information Security Conceptual Knowledge Test Questions (Pre- and Post-learning)

1. Which of the following attack categories fit phishing the best?
   (a) Brute force attack
   (b) War driving
   (c) Dictionary attack
   (d) Social Engineering

2. Which of the following does not make a password stronger?
   (a) Longer length
   (b) More secrecy
   (c) Regular changes
   (d) More variations of symbols used including numbers, special characters, etc.

3. What is a generic name for a router Operating System (OS)?
   (a) Firmware
   (b) Shareware
   (c) Freeware
   (d) Malware

4. Which of the following are Internet applications that are rarely used due to their known security vulnerabilities?
   (a) SSH
   (b) Telnet
   (c) SMTP
   (d) HTTP

5. To prevent Internet access to a particular application running on your computer, _____ can be blocked.
   (a) Protocols
   (b) Signals
   (c) Ports
   (d) IP addresses

6. Which of the following is the best password choice for limiting access to your router?
   (a) Manufacturer-provided default password
   (b) Any custom password created by a user, which is short, simple, therefore, easy to remember
   (c) No password at all
   (d) Randomly generated, long password (at least 10-characters long) that is frequently changed

7. Which of the following protocols are used to automatically configure network settings of computers in a certain network?

 (a) DHCP

 (b) HTTP

 (c) SNMP

 (d) ARP

8. What does the phrase "clipping level" mean?

 (a) The number of trials allowed for entering correct passwords

 (b) The number of password changes one person can make during a certain period of time

 (c) The minimum number of characters allowed for a given password

 (d) The maximum number of characters allowed for a given password

9. Which of the following is a spam filtering technology?

 (a) CAPTCHA

 (b) Security token

 (c) Pass phrase

 (d) Kerberos

10. Which of the following cannot be used to hinder phishing attempts?

 (a) Secret images pre-stored by a user

 (b) Security questions whose answers were provided by a user

 (c) The use of embedded links in an e-mail

 (d) Spam filtering

11. Using a separate communication channel (e.g., using an e-mail instead of a Web page) for resetting a password is referred to as:

 (a) Broad band

 (b) Out-of-band

 (c) Base band

 (d) Infini-band

12. Which of the following is an example of a strong password?

 (a) Password

 (b) J*p2le04>F

 (c) Your real name

 (d) PennState

13. What is phishing?

    (a) A type of computer virus

    (b) An example of a strong password

    (c) "Spoofed" e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords

    (d) A type of encryption method

Table 4. Details on the Technical Security Readiness Score Calculation

Technical Security Readiness Score	Score Calculation
Router password setup	0 through 100 points computed by a password strength test algorithm based on the time it takes to crack a given password
Firmware upgrade practices	100 points if a team upgrades a router firmware when it becomes available and zero point other-wise
Firewall port settings	25 points if HTTP is enabled 25 points if SSH is enabled 25 points if FTP is disabled 25 points if Telnet is disabled

Note: The technical security readiness score is a weighted average of the router password setup (20%), firmware upgrade practices (30%), and firewall ports setting (50%).

A.2 Information Security Readiness Score Computation

All teams have an initial information security readiness score of 0. The scores are evaluated periodically and calculated as an average of the technical security readiness score and the online purchase behavior score. The technical security readiness score is broken down into three components: a router password setup (twenty points), firmware upgrade practices (thirty points), and firewall port settings (fifty points). Table 4 provides additional details on the technical security readiness score calculation.

An online purchase behavior score is based on a team's choices of online stores to make their product purchase. Online stores have varying levels of access control from no access control up to the maximum of four access control features. The four access control features are CAPTCHA, clipping levels, security images, and out-of-band communications. A team that makes a purchase from an online store that has no, one, two, three, or four access control features receives zero, 20, 40, 80, or 100 points, respectively. For example, if a team makes all its purchases from two online stores, one with no access control and another with two access control features, its online purchase behavior score will be $20 = \frac{(0+40)}{2}$.

B QUESTIONNAIRE ITEMS

Items are anchored on seven-point Likert scales: 1= strongly disagree to 7= strongly agree.

B.1. Learning Goal Orientation

1. The opportunity to learn new things is important to me.

2. The opportunity to do challenging work is important to me.

3. I prefer to work on tasks that force me to learn new things.

4. If I don't succeed on a difficult task, I plan to try harder the next time.

5. In learning situations, I tend to set fairly challenging goals for myself.

6. I am always challenging myself to learn new concepts.

7. The opportunity to extend my range of abilities is important to me.

B.2   Computer Learning Self-Efficacy

1. I feel con dent using a computer to learn about and apply new concepts.

2. Using a computer is an efficient way for me to learn new things.

3. I could apply new concepts that I learned from a computerized training program such as the Second Life learning module.

4. I don't feel that I could learn new skills from a computerized training program such as the Second Life learning module. (REVERSE)

5. It would be easy for me to become skillful at tasks learned from a computerized training program such as the Second Life learning module.

6. I would be comfortable using a computerized training program such as the Second Life learning module.

7. I could successfully use a computerized training program such as the Second Life learning module.

B.3   Perceived Enjoyment

1. I enjoyed doing this activity very much.

2. This activity was fun to do.

3. I thought this was a boring activity. (REVERSE).

4. This activity did not hold my attention at all. (REVERSE).

5. I would describe this activity as very interesting.

6. I thought this activity was quite enjoyable.

7. While I was doing this activity, I was thinking about how much I enjoyed it.

B.4   Information Security Self-Efficacy (Pre- and Post-learning)

1. I feel confident that I can make passwords difficult for others to guess

2. I feel confident that I can keep my personal information secret from other Internet users whom I don't trust

3. I feel confident that I can use technical security mechanisms to address security threats

4. I feel confident that I engage in safe online behaviors to prevent from security threats

B.5   Satisfaction

How do you feel about your overall experience of the Second Life security learning module?

1. Coordinated/Uncoordinated

2. Confusing/Understandable

3. Satisfying/Dissatisfying

C CONSTRUCT CONVERGENT VALIDITY

Construct	Item	Mean	Std. Dev.	Loading	t-stat	
Learning goal orientation (Learn_O) *Composite Reliability = 0.94*	Learn_O1	6.48	1.09	0.66	2.91	***
	Learn_O2	6.02	1.18	0.79	4.13	***
	Learn_O3	6	1.15	0.84	4.66	***
	Learn_O4	6.29	1.11	0.84	4.12	***
	Learn_O5	5.88	1.17	0.74	3.43	***
	Learn_O6	5.8	1.13	0.65	2.49	**
	Learn_O7	6.43	1.06	0.54	1.98	**
Computer learning self-efficacy (Learn_SE) *Composite Reliability = 0.90*	Learn_SE1	6.57	0.74	0.41	1.94	*
	Learn_SE2	6.45	0.74	0.53	2.43	**
	Learn_SE3	5.6	1.52	0.79	4.94	***
	Learn_SE4	4.38	1.71	0.74	3.72	***
	Learn_SE5	5.64	1.25	0.55	2.71	***
	Learn_SE6	5.76	1.54	0.9	7.24	***
	Learn_SE7	6.03	1.09	0.67	3.21	***
Perceived enjoyment (Enjoy) *Composite Reliability = 0.96*	Enjoy1	5.07	1.61	0.96	78.29	***
	Enjoy2	5.36	1.62	0.94	37.84	***
	Enjoy3	3.64	1.95	0.78	9.45	***
	Enjoy4	3.81	1.63	0.73	5.52	***
	Enjoy5	5	1.5	0.9	20.92	***
	Enjoy6	5.07	1.61	0.95	43.82	***
	Enjoy7	4.4	1.7	0.9	24.43	***
Information security self-efficacy (Sec_SE) Composite Reliability = 0.84	Sec_SE1	6.76	0.62	0.69	3.22	***
	Sec_SE2	6.48	0.77	0.72	2.15	**
	Sec_SE3	6.17	0.96	0.7	2.5	**
	Sec_SE4	6.43	0.91	0.76	3.33	***
Satisfaction (Satis) *Composite Reliability = 0.86*	Satis1	4.4	1.38	0.51	2.5	**
	Satis2	4.5	1.58	0.98	5.75	***
	Satis3	6.76	0.62	0.62	3.05	***

The significance levels are: * p < :10, ** p < :05, *** p < :01.

D

D.1   Correlations among Latent Constructs and AVE (shown in diagonal)

	Learning_O	Learning_SE	Enjoy	Sec_SE	Satis
Learning_O	0.71				
Learning_SE	0.02	0.56			
Enjoy	0.18	0.48	0.78		
Sec_SE	0.01	0.02	0.09	0.58	
Satis	0.2	0.27	0.72	0.06	0.53

D.2 Item-Construct Loadings and Cross Loadings

	Learning_O	Learning_SE	Enjoy	Sec_SE	Satis
Learn_O1	0.79	0.02	0.03	0.03	0.17
Learn_O2	0.9	0.05	0.13	0.04	0.09
Learn_O3	0.93	0.03	0.15	0.04	0.15
Learn_O4	0.95	0.05	0.24	0.01	0.29
Learn_O5	0.83	0.04	0.06	0.03	0.05
Learn_O6	0.76	0.1	0.02	0.03	0.04
Learn_O7	0.69	0.06	0.01	0.02	0.14
Learn_SE1	0.02	0.55	0.11	0.17	0.25
Learn_SE2	0.07	0.62	0.19	0.28	0.07
Learn_SE3	0.1	0.86	0.37	0.08	0.3
Learn_SE4	0.09	0.79	0.4	0.07	0.15
Learn_SE5	0.04	0.66	0.1	0.1	0.08
Learn_SE6	0.08	0.91	0.53	0.05	0.29
Learn_SE7	0.04	0.79	0.17	0.07	0.05
Enjoy1	0.16	0.58	0.96	0.07	0.5
Enjoy2	0.16	0.47	0.93	0.13	0.47
Enjoy3	0.04	0.33	0.78	0.12	0.52
Enjoy4	0.13	0.26	0.72	0.08	0.44
Enjoy5	0.22	0.44	0.92	0.09	0.47
Enjoy6	0.21	0.45	0.95	0.05	0.51
Enjoy7	0.16	0.37	0.9	0.03	0.56
Sec_SE1	0.05	0.06	0.08	0.95	0.07
Sec_SE2	0.14	0.14	0.03	0.56	0.06
Sec_SE3	0.02	0.25	0.03	0.73	0.03
Sec_SE4	0.02	0.11	0.04	0.75	0.04
Satis1	0.06	0.05	0.15	0.03	0.57
Satis2	0.22	0.29	0.83	0.03	0.98
Satis3	0.05	0.06	0.08	0.51	0.66

http://www.jistap.org