Sun, J. C.-Y., Kuo, C.-Y., Hou, H.-T., & Lin, Y.-Y. (2017). Exploring Learners' Sequential Behavioral Patterns, Flow Experience, and Learning Performance in an Anti-Phishing Educational Game. *Educational Technology & Society, 20* (1), 45–60.

Exploring Learners' Sequential Behavioral Patterns, Flow Experience, and Learning Performance in an Anti-Phishing Educational Game

Jerry Chih-Yuan Sun[1*], Cian-Yu Kuo[1], Huei-Tse Hou[2] and Yu-Yan Lin[1]

[1]Institute of Education, National Chiao Tung University, Taiwan // [2]Graduate Institute of Applied Science and Technology, National Taiwan University of Science and Technology, Taiwan // csun@nctu.edu.tw // metilda_kuo@kingston.com.tw // hthou@mail.ntust.edu.tw // aoisora.nagi@gmail.com

[*]Corresponding author

(Submitted September 10, 2015; Revised December 15, 2015; Accepted January 26, 2016)

ABSTRACT

The purposes of this study were to provide a game-based anti-phishing lesson to 110 elementary school students in Taiwan, explore their learning behavioral patterns, and investigate the effects of the flow states on their learning behavioral patterns and learning achievement. The study recorded behaviour logs, and applied a pre- and post-test on phishing knowledge and a flow state measurement to analyze the learning process. The study used lag sequential analysis to infer the students' behavioural patterns. The results showed that the learning materials used in this study can enable learners' flow experience, whereby they can acquire anti-phishing knowledge through trial and error via a repeated "learning with gaming" behavioral pattern. We recommend that future educators and researchers on this topic appropriately increase the level of difficulty of the games used, and design learning materials with flexible difficulty based on learners' flow states.

Keywords

Game-based learning, Anti-phishing, Behavioral patterns, Flow experience, Sequential analysis

Introduction

As of 2014, there were 2.4 billion Internet users globally (Internet World Stats, 2014). However, studies show that Internet users are often unaware of the dangers of the phishing attacks they are exposed to (Arachchilage & Love, 2013). As of 2013, Internet phishing through email scams had decreased by 16% from 2012 (Fossi et al., 2013); however, Internet scams using social sites had increased by 3% (Anti-Phishing Working Group, 2013). Social networking websites are gradually replacing emails as the new primary means for Internet scams (Fossi et al., 2013). Victims of Internet phishing include people of all age groups, among which young people constitute the most vulnerable group (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). Statistics from Livingstone and Haddon (2009) showed that 60% of all social site users were between 9–16 years old, while more recent data from 2013 further showed that the number of young people who were social sites users increased by 29% in one year and was continuing to increase (Harper, 2014). This heavy use of social sites accentuates young people's vulnerability to phishing through these sites.

Tools for detecting phishing may not provide effective defenses (Kumaraguru et al., 2007a). Therefore, some academics deem anti-phishing education, in which users learn correct Internet phishing concepts and defense methods and are equipped with basic defense abilities, to be the most effective means of combating phishing (Kumaraguru et al., 2007b; Kumaraguru et al., 2010; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010; Sheng et al., 2007) as well as fostering good general Internet safety, operating habits, and awareness (Wirth, Rifon, LaRose, & Lewis, 2007). Defense against Internet phishing is a problem-solving process that requires judgment and reasoning abilities (Kumaraguru et al., 2007a). The advantage of game-based learning materials is the construction of life-like situations of phishing and game-based learning scenarios; therefore, game-based learning is an effective teaching method to help learners enhance their anti-phishing abilities (Kiili, 2005; Sheng et al., 2007). The game-based learning method affects learners' flow experience and problem solving abilities, and can promote effective learning behaviors; for example, simulation games help learners enter a flow state during the computational problem solving activities (Liu, Cheng, & Huang, 2011) and facilitate the flow experience when playing games as a group in an interactive social game environment (Inal & Çağıltay, 2007). There have been previous studies focusing on the use of anti-phishing games in teaching among university students (Yang, Tseng, Lee, Weng, & Chen, 2012), but there has been no study exploring the effective learning behavior of children or teenagers through anti-phishing educational games. Therefore, the present study, using young people as the research subjects and an anti-phishing game as the teaching method, sought to understand whether the flow experience in games can contribute to effective learning behaviors.

Mayer (1992) proposed that it is relatively difficult for teachers to understand learners' metacognitive processes such as learning strategies through summative assessment (e.g., learning achievement tests), and that it is therefore difficult to improve learners' learning states or enhance their learning achievement using these methods. Thus, it may be more effective to help educators understand and improve learners' learning states and strategies using quantified dynamic learning behavior, presented in the form of a time order (Liu et al., 2011), as well as applying sequential analysis to explore the correlation between learners' behaviors and to infer overall behavioral patterns (Bakeman & Gottman, 1997). Learning behavior patterns are beneficial in terms of identifying the reason for unsatisfactory learning states and learning achievement, which can in turn help teachers provide learners with suitable guidance for better learning outcomes (Hou, 2012b). On this basis, this study makes use of a game-based learning scenario and sequential analysis to explore learning behaviors in order to enhance young people's anti-phishing abilities on social sites. During online learning activities, if the learning state reaches the condition of flow experience, learners will have greater learning achievement (Choi, Kim, & Kim, 2007; Skadberg & Kimmel, 2004). Liu et al. (2011) analyzed learning behavioral patterns in game-based learning and discovered that learners tended to use behavioral strategies learned from mistakes. Based on the above findings, a stronger understanding of the correlation between flow states and learning behavioral patterns in game-based learning should help future educators guide the learning behaviors of students and help them reach a higher level of learning achievement. Therefore, the purpose of this study was to examine differences between learners in terms of their learning behavioral patterns and learning achievement given different flow experiences relating to game-based anti-phishing learning materials.

Literature review

Young people and Internet phishing on social sites

"Internet phishing" refers to the illegal act of attackers making use of fake emails, websites, or browsers to deceive victims and obtain their private information when they click on links or fill in personal information (Sheng et al., 2007). According to past studies, approximately 90% of all Internet users eventually click on links to phishing sites within eight hours of the time the fake emails are sent, and thus fall victim to these illegal acts (Kumaraguru et al., 2009; Kumaraguru et al., 2007a); furthermore, most users are relatively unconcerned about issues relating to Internet phishing (Fossi et al., 2013). Social sites provide Internet users with communication channels to develop interpersonal relationships, generally free of charge (Gao et al., 2010); at the same time, they also create complicated social connections which facilitate phishing victimization (Boshmaf, Muslukhov, Beznosov, & Ripeanu, 2011).

Although children and youths are a digitally native generation, they are at greater risk from Internet phishing than are adults due to their lack of experience and knowledge relating to Internet scams (Fire, Goldschmidt, & Elovici, 2014). Young people are most frequently attacked by Internet scams on social sites (Wirth et al., 2007). Quilliam, Rifon, and Larose (2006) highlighted the fact that over 60% of young people fail to regularly look for privacy policies, 58% do not clear their browser history, 37.7% fail to check if online forms are secure, and 50% do not set their browsers to reject cookies; some youths even authorize third-party software or websites to obtain their personal information without reading the user agreements on those sites (Wirth et al., 2007). Therefore, a comprehensive anti-phishing curriculum is needed to help young people build their knowledge of Internet phishing so as to equip them with the needed defensive abilities and prevent them from becoming victims (Wirth et al., 2007).

Most current studies related to anti-phishing education have used university students as their teaching subjects, and only a few have focused on conducting Internet information safety education for children. Jansson and von Solms (2013) designed an educational training method focused on phishing mail that allowed learners to acquire anti-phishing related knowledge from simulated phishing attacks by receiving emails. The study by Robila and Ragucci (2006) taught university students awareness of the content of phishing attack websites through classroom discussions. Yang et al. (2012) developed an Anti-Phishing Education Game to develop university students' knowledge of anti-phishing techniques; their results showed that students showed significant progress in their ability to identify phishing web pages. Moreover, with children aged between 9 and 12 as subjects and by means of questionnaires and behavioral observation, Wishart, Oades, and Morris (2007) explored whether online role-play activities could help children receive and remember the key Internet safety message.

To sum up the above observations, young people are the primary users of social sites, but at the same time lack knowledge and skills relating to Internet safety, and the ability to defend themselves against social site phishing, and therefore run a very high risk of becoming victims. Among the current studies of anti-phishing or Internet

information safety education, there are few focusing on anti-phishing education among children and teenagers. Research findings from Wishart et al. (2007) only listed the important concepts of Internet safety that children learned from role-play activities, such as: 'Don't give out personal details' and 'Don't trust what people say in chatrooms/on the Internet;' they did not, however, investigate the learners' behavioral process in the course of role-play. As such, this study targets youths with an intervention to enhance their Internet safety awareness through anti-phishing game-based instruction, and to equip them with the ability to identify and defend against Internet phishing, while also examining their behavior patterns during the learning process.

Flow experience in game-based learning

Csíkszentmihályi (2000) considered flow to be the optimal experience, whereby actors are completely absorbed in flow activities, with their consciousness focused within a narrow range and automatically filtering out perceptions and feelings that are not related to the activity at hand. In a flow state, actors have a sense of control over their environment and are focused on specific goals and clear feedback. In the three-channel model of flow (flow, anxiety, and boredom) proposed by Csíkszentmihályi (2000), "flow" is a feeling of balance between skill and challenge, and its force can drive actors into challenging activities at a higher level. Figure 1 is an illustration of the three-channel model. When there is a balance between the level of challenge of the learning activity and the actor's skill, the actor will experience a flow state; when an actor of low skill faces high-difficulty challenges, he or she will enter into an "anxiety state"; and when their skill is higher than the difficulty of the challenge, they will not be fully focused on the activity and will enter into a "boredom state" (Csíkszentmihályi, 2000). There are different techniques for measuring flow. One is the use of a psychological scale to detect the aspects of perceived control, engagement, and enjoyment following the conclusion of an activity (Pearce, Ainley, & Howard, 2005; Webster, Trevino, & Ryan, 1993), as an overall measure of flow state. Another method is to monitor learners' skill-challenge balance during the activity, as an indicator of the flow state process (Pearce et al., 2005). Massimini and Carli (1988, p.269) describe this method as "theoretically, the most meaningful reference point for the presence or absence of flow." Fang, Zhang, and Chan (2013) argued that all flow elements (including preconditions, flow state, and its outcomes) should be measured so that one can understand whether learners actually achieve the flow state. However Inal and Çağıltay (2007) found that children failed to understand some questions in the flow scale, such as the sub-factors of autotelic experience, time distortion and playability. Therefore, when considering young people's comprehension ability, and to minimize the level of intervention in the learning process, this study used the method of measuring skill-challenge balance to explore learners' flow state. Furthermore, this study focused on the correlation between flow state and behavior outcome in the learning process, so other flow related factors (such as preconditions) were not included in the measurement.

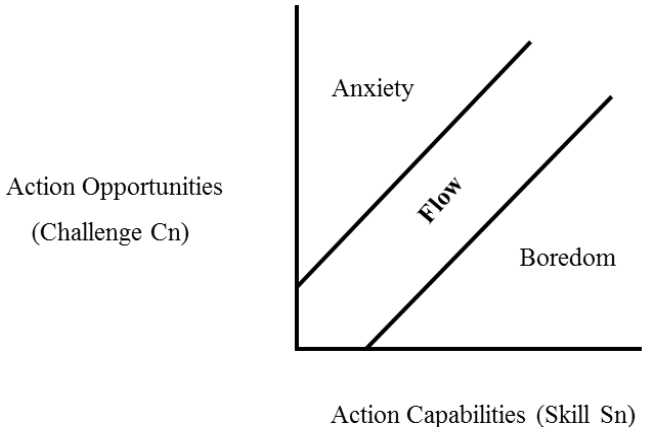

Figure 1. Three-channel model of the flow state (Csíkszentmihályi, 2000, p.45)

Although flow is an optimal experience, Csíkszentmihályi (1975) found that it only existed among certain kinds of activities such as climbing, chess and basketball. Among these specific activities in which people might experience flow, playing a game is an activity that allows one to undergo an excellent flow experience (Csíkszentmihályi, 1975, p. 36). As a result, this study considered game-based learning a suitable environment for designing the activities to facilitate flow experience. In digital learning, a game-based curriculum is viewed as computer-assisted scenario teaching and an effective tool for enhancing learning problem solving abilities (Liu et al., 2011). Game-based learning seeks to induce learners to repeatedly practice the concepts learned and to focus on learning tasks (Hou, 2012b) while striking a balance between skills and challenges (Sweetser &

Wyeth, 2005). Games provide appropriate levels of scaffolding and difficulties, enhancing learners' performance in problem-solving abilities (Hung, Kuo, Sun, & Yu, 2014), while the challenge in games helps learners achieve better flow experience (Hung, Sun, & Yu, 2015). In a game-based learning environment, flow experience is a suitable factor for exploring the learning state of learners (Kiili, 2005; Liu et al., 2011). Therefore, the present study suggests that in a game-based learning environment, flow theory helps to illuminate the learning process and effectively categorize learners, and hence uses the three-channel model of flow to examine the differences in behavioral patterns of flow experience and their correlation with learning achievement.

The relation of flow experience with learning behavioral patterns and learning achievement

Educational games can promote effective learning behaviors (Inal & Çağıltay, 2007). Hou and Li (2014) suggested that game-based learning stimulated learning motivation using game-based learning materials, thereby encouraging learners to voluntarily engage in the activity at hand and achieve flow experience, as well as enhancing their learning achievement by providing enjoyable experiences and challenging goals. If learners are fully focused on the activity while maintaining a desire to achieve the goal (Inal & Çağıltay, 2007), they will be more effective at learning (Hoffman & Novak, 1996; Hou & Li, 2014). Therefore, maintaining the flow state can be considered an effective way of promoting game-based learning achievement (Liu et al., 2011). Pearce et al. (2005) discovered a positive correlation between flow experience and learning achievement, as flow experience enabled learners to achieve higher levels of learning achievement. It is thus no surprise that measuring the flow experience of learners in an online learning scenario is indeed beneficial to understanding learning state (Choi et al., 2007; Skadberg & Kimmel, 2004). This study expects that in a game-based environment, learners who have achieved a flow state will focus on the learning activities and proactively face challenges, allowing better learning achievement.

On the other hand, game-based learning also provides the opportunity to explore suitable learning methods through learners' experiences (Liu et al., 2011). Therefore, studying learning behavioral patterns and related processes will help us discover the reasons behind unsatisfactory learning achievement and identify means of improvement (Hou, 2012b). Derived from the basis of observation of the learning process, learning behavioral patterns summarize the learners' behavioral characteristics (Hou, 2013). Liu et al. (2011) analyzed learning behavioral patterns in game-based learning and discovered that learners tended to use behavioral strategies learned from mistakes: Learners who were less capable of understanding the questions and considering solutions would lose motivation and more easily fall into a state of anxiety, in turn prolonging their learning duration and reducing their learning achievement. A study by Hou (2013) pointed out that in game-based learning, learners with more prior knowledge were more confident at interacting with others and discussing questions, and achieved greater enjoyment, whereas learners with less prior knowledge lacked the confidence to interact with others and were more prone to choose to learn on their own. Based on the above findings, a stronger understanding of the correlation between flow states and learning behavioral patterns in game-based learning should help future educators guide the learning behaviors of students based on their flow experience, and help them reach a higher level of learning achievement. Therefore, this study uses game-based learning materials, and categorizes the flow state of learners based on the three-channel model of flow in order to analyze differences in learners' learning behavioral patterns and learning achievement by flow experience.

Research methods

Participants and instructional design

This study is a causal-comparative research study. The participants were students in grades 5 and 6, aged between 9 and 12, with an average age of 11.23. There were 110 students altogether, of whom 62 were boys and 48 were girls. The research data were collected in December 2014. In order to control the learning environment to ensure that the students would not be influenced by external factors, we conducted a two-hour lesson in a computer lab, and the entire process was recorded on video.

A pre-test on phishing knowledge about social sites was conducted before the start of the lesson to collect information on the learners' prior knowledge. Following that, the learners were informed of the learning task and its goals. The task required the students to learn according to their own methods during the anti-phishing game-based lesson; however, they were required to successfully pass the game challenge at least once before they could complete the learning task. Learners started challenging the learning task once the lesson started; they were allowed to try different learning behaviors, such as reading the learning materials, referring to practical

examples, and consulting forums until they succeeded in their challenge. Learning behaviors during the lesson were logged and coded automatically through the computer system. The lesson ended once the challenges were completed successfully, at which point an active survey was conducted immediately in order to measure the learners' flow experience (Novak, Hoffman, & Yung, 1998), as was a post-test on phishing knowledge about social sites, to collect information on after-lesson learning achievement. The experimental procedures and scenarios are shown in Figures 2 and 3.

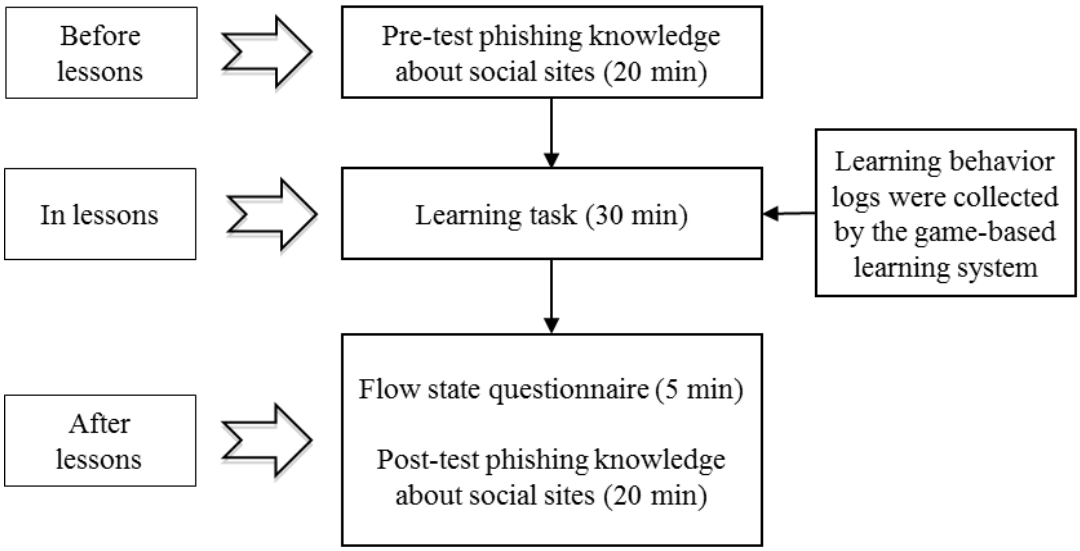

Figure 2. Experimental design

Figure 3. Game scenario of anti-phishing

The anti-phishing game-based lesson used in this study required learners to learn independently using digital learning materials, with both the lesson and the test being conducted entirely on computers. The anti-phishing game-based learning materials were related to phishing on social sites; the main system functions covered can be classified into six types, namely user identification, the learning material, practical examples, games, forums, and leader boards. Learners were able to register and log into the system through the user identification function. Learners tried to pass the game challenges by answering the questions, and were then rewarded with treasure. The questions were designed based on the anti-phishing concepts and were presented randomly. Prior research showed that game-based learners tend to learn from their mistakes (Liu et al., 2011), so this study was designed to allow the learners to continually work on the game challenges. During the learning process, they acquired knowledge related to phishing attacks on social sites by reading the learning materials, experiencing the practical examples and games, and using the forum for discussion with peers; they were also able to view the learning achievement of their peers through the leader board.

Instruments

The data-gathering tools used by this study were the flow state measurement, a pre- and post-test on phishing knowledge about social sites, and learning behavioral coding. We used the study of Pearce et al. (2005) as a reference for the flow state measurement, which measured the learners' flow state during the activities using the challenge and skill questions. Learners were asked to answer two questions based on their feelings during the learning experience: (1) *Do you feel that your skills were suitable for solving the tasks in this activity?* and (2) *How do you feel about the task's level of challenge in this activity?* The measurement used a five-point Likert-type scale (*1 = highly unsuitable; 5 = highly suitable*). The measurement is a type of technique to probe the flow state of learning process, similar to the research of Pearce et al. (2005). In this research, one question was used for each of the two dimensions of skill and challenge to probe students' flow space. Nevertheless, due to limitations of the course duration and to prevent interference with learners' discussions with their peers during the learning process, reading and teaching materials, challenge games and flow state measurements were only determined following the completion of a learning task (that is, after successfully getting through one level of the game) as an indicator of flow space location.

The pre- and post-test on phishing knowledge about social sites (for summative evaluation) used the same questions—ten questions consisting of a mix of multiple-choice and yes/no questions, in a different sequence in the pre- and post-tests. We referred to social-site-phishing-related events for the question propositions, which were further examined and repeatedly corrected by experts in digital learning. A preliminary test was taken by twelve youths to ascertain the item discrimination and difficulty level of the test. Based on the Ebel and Frisbie (1986) criterion, we amended two multiple-choice questions, as their difficulty levels were too high, and one giveaway multiple choice question, whose difficulty level was too high and whose item discrimination was insufficient. After the revision, the average difficulty level of the test was 0.56, and the discrimination power of D value was 0.54, which achieved excellent quality. Cronbach's α was .64, acting as the minimum acceptable level of reliability for preliminary research (Nunnally, 1967) and reflecting learning achievement derived from these game-based anti-phishing learning materials related to social sites (Nunnally & Bernstein, 1994). The final test questions on phishing in social network sites are listed in Appendix 1.

Concerning the validity of the learning achievement test, three experts in digital learning and behavioral patterns examined the validity of the test questions so as to ensure expert validity. Expert A's research focuses on coding learning behavior processes. He has investigated various models of learning behavior through quantitative content analysis and sequential analysis. Expert B's research interests are in integrating information technology into teaching, designing digital teaching materials and action learning. Expert C's research field includes teaching technology, interactive learning, online learning and course design, and designing multimedia teaching. The experts in digital learning and behavioral patterns reviewed the study and defined four behavioral dimensions (Reading, Interaction with peers, Game, and Test) before conducting the experiment. The students' learning behaviors were then automatically recorded by the system in the anti-phishing curriculum (Hou, 2012a; 2013; Tsai, Yu, & Hsiao, 2007). Detailed definitions of the codes are provided in Appendix 2.

Statistical analyses

Upon completion of the data collection, the learners were first grouped based on information from the flow state measurement: learners with equal skill and challenges were grouped into the flow state; if skill was greater than challenge, the learners were grouped into the boredom state; if skill was lower than challenge, they were grouped

into the anxiety state. The data were analyzed by SPSS 17.0 and the Mepa 4.9 statistical software following file conversion. Frequency distribution was used for descriptive analysis, while one-way analysis of variance (ANOVA) was used to examine whether different flow experiences had any basis in differences in prior knowledge in the pre-test on phishing knowledge about social sites. Subsequently, a paired-samples *t*-test was performed to examine the average scores of different flow experiences in the post-test on phishing knowledge about social sites. In addition, we used sequential analysis to calculate a behavioral frequency conversion matrix for different flow experience states and converted the behavioral code information of the various groups into the *z*-score, followed by the export of the frequency transition tables and adjusted residuals tables. The *z*-score in the table was then used to determine the significance between the behavioral sequential relations ($z > 1.96$ indicated that the sequential relation reached the significance level of $p < .05$) (Bakeman & Gottman, 1997). Lastly, the results were organized into a learning behavioral patterns chart.

Research results

Descriptive statistics

Grouping the learners according to the flow state measurement showed that there were 60 learners in the Flow Group (32 boys and 28 girls, with an average age of 11.32), 32 learners in the Anxiety Group (19 boys and 13 girls, with an average age of 11.25), and 18 learners in the Boredom Group (11 boys and 7 girls, with an average age of 11.11). In terms of gaming experience, the respective numbers of learners with one year, two years, three years and more than three years of gaming experience were 40, 8, 14 and 48. In addition, 30 learners had used social networking sites previously, while the remaining 80 learners had not.

In this study, we collected a total of 2,362 behavioral codes (Flow Group: 1242, Anxiety Group: 721, Boredom Group: 399). In terms of dimensional difference, given the different numbers of learners in each group, after deducting the (game) success (Y) and failure (N) codes, the frequency distribution of their learning behaviors across various dimensions is shown in Table 1. In terms of the Reading (9%, 10%, and 11%) and Test (36%, 33%, and 38%) dimensions, the three groups were similar; as for peer Interaction, the behaviors of the Flow Group and the Anxiety Group were similar, while the level of interaction was notably lower in the Boredom Group. However, the Boredom Group's interaction in the Game dimension was also notably higher than that for the other two groups.

Table 1. Summary of learner behaviors by frequency

Groups	Dimensions				
	Reading	Interaction with peers	Game	Test	Total
Flow	107 (9%)	163 (14%)	492 (41%)	480 (36%)	1242
Anxiety	64 (10%)	84 (13%)	289 (44%)	284 (33%)	721
Boredom	41 (11%)	9 (2%)	177 (49%)	172 (38%)	399

Learning behavioral patterns in different flow states

We first performed sequential analysis on the Flow Group, and the residual table was then adjusted based on the dimensions: significant sequences for $p < .05$ were Test→Test ($z = 26.18$), Reading→Reading ($z = 4.65$), Interaction→Reading ($z = 5.15$), Interaction→Interaction ($z = 26.60$) and Game→Game ($z = 21.07$). The learning behavioral patterns chart is shown in Figure 4. The Flow Group had three notably significant behavioral sequences: (1) the behavior of performing multiple Tests indicated that the learners had completed all the tests; (2) learners would keep the Game playing behavior until they succeeded; (3) learners continually interacted with their peers and engaged in Reading behavior when their interactions ended.

We then adjusted the residual table based on the dimensions of the Anxiety Group and discovered that the significant sequences for $p < .05$ were Test→Test ($z = 17.82$), Test→Reading ($z = 4.90$), Reading→Reading ($z = 3.12$), Interaction→Interaction ($z = 17.56$) and Game→Game ($z = 16.65$). This group's learning behavioral patterns chart is shown in Figure5. The learning behaviors of the Anxiety Group exhibited the following characteristics: (1) performing multiple Tests indicated that learners had completed all the tests; (2) after completing the pretest, learners started and continued to Reading; and (3) upon the completion of Test and Reading, learners would keep the Game playing behavior until they succeeded, while also Interacting repeatedly with peers.

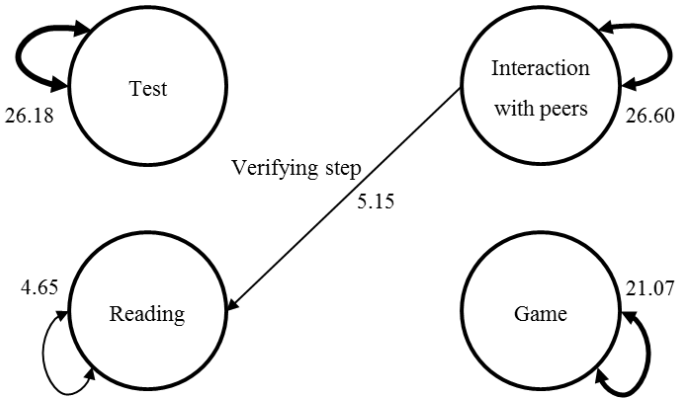

Figure 4. The dimensional behavioral patterns chart of the Flow Group (*Note.* The thickness of the lines represents the closeness of sequential relations)

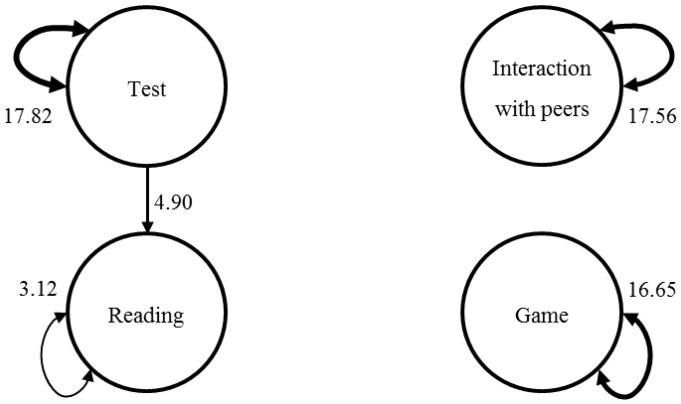

Figure 5. The dimensional behavioral patterns chart of the Anxiety Group (*Note.* The thickness of the lines represents the closeness of the sequential relations)

Finally, we adjusted the residual table based on the dimensions of the Boredom Group, and discovered that the significant sequences for $p < .05$ were Test→Test ($z = 13.89$), Test→Reading ($z = 3.14$), Reading→Reading ($z = 7.24$), Interaction→Interaction ($z = 3.10$) and Game→Game ($z = 12.80$). This group's learning behavioral patterns chart is shown in Figure 6. Their dimension behavior eventually returned to the Test dimension, indicating that the Boredom Group had completed all the tests in the study. The learning behaviors of the Boredom Group exhibited the following characteristics: (1) learners preferred repeated Reading behavior after the pretest; and (2) upon completion of the Test and Reading, learners would keep the Game playing behavior until they succeeded, while also Interacting repeatedly with peers. Thus, their behaviors were similar to the behaviors of the Anxiety Group.

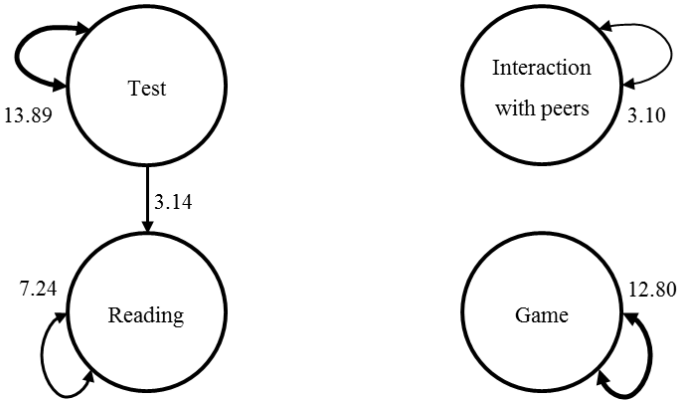

Figure 6. The dimensional behavioral patterns chart of the Boredom Group (*Note.* The thickness of the lines represents the closeness of the sequential relations)

Learning achievement in different flow states

We first used one-way ANOVA to examine whether different flow groups had significant differences in their average scores on the pre-test on phishing knowledge about social sites. Based on the application of Levene's test, $p = .21$ was taken to mean that the assumption of homogeneity of variance was not rejected and that subsequent analysis could be performed. The ANOVA results showed that the pre-test scores of all the flow groups did not reach significance ($F = 1.21$, $p = .30$), indicating no significant difference in the prior knowledge of the three groups; therefore, the possibility of prior knowledge affecting learning achievement in the post-test could be ruled out, and subsequent analysis could proceed.

The results of the paired *t*-test are shown in Table 2. The overall pre- and post-test results on phishing knowledge about social sites reached significance ($t = 3.02$, $p = .03$). Among the groups, however, the Flow Group did not reach significance in the pre-test or the post-test ($t = 1.28$, $p = .21$); the Anxiety Group reached significance on both tests ($t = 3.36$, $p < .01$); and the Boredom Group did not reach significance on either test ($t = 0.79$, $p = .44$). In short, the anti-phishing game-based learning materials significantly improved the learning achievement of the Anxiety Group, while the other two group did not see any significant improvement in their learning achievement.

Table 2. Paired-samples *t*-test of various flow state groups' anti-phishing learning achievements

Groups	Pre-test		Post-test				
	M	*SD*	*M*	*SD*	*t*	*p*	Cohen's *d*
Flow	47.25	15.33	49.67	14.95	1.28	.21	.54
Anxiety	43.59	10.87	52.03	13.37	3.36	< .01	.33
Boredom	49.72	15.58	52.50	12.86	0.79	.44	.47
Total	46.59	14.25	50.82	14.12	3.02	.03	.35

Note. The minimum anti-phishing achievement test score was 5, the maximum was 100, and the range was 95.

Discussion

Flow experience and learning behavioral patterns

This study's results for learning behavioral patterns are similar to those of Liu et al. (2011), which proposed that learners tend to learn from their mistakes. After a failed game, the Flow Group might engage in the behavior of discussing the results with peers, followed by the Reading behavior, and would continue to repeat these behaviors until they succeeded in the learning task. In other words, the Flow Group not only engaged in independent learning but also sought assistance from peers (Hou & Li, 2014). However, the difference between our study and previous studies is that the learners in the Flow Group would verify the information by reading the materials again after discussing and interacting with peers. This may have been due to the different designs of the game-based learning environments. Liu et al. (2011) adopted a collaborative simulation game, while the current study incorporated a task-challenge style, helping learners promote a behavioral strategy of collaborating with others and reading/verifying materials. We infer that after discussing and interacting with peers, learners in the Flow Group would verify the outcomes of the discussion using the learning materials before they proceeded with the game, and that this is what made their learning more effective (Inal & Çağıltay, 2007). The Anxiety Group also sought help from peers after a failed game and kept repeating this behavior until they succeeded. We infer that learners in the Anxiety Group also tended to turn to reading materials and peers for solutions, but lacked the step of reading and verifying what they had learned from the discussions; instead, they simply continued playing the game (and thus had higher frequency of Game behavior compared to the Flow Group). As a result of this process of repeated trial and failure and the learning behaviors of overestimating the learners' levels of understanding due to the lack of opportunity to internalize the knowledge (Csíkszentmihályi, 2000), this group experienced more anxiety than the others. Finally, the Boredom Group relied less on the reading materials and interaction with peers, tending instead to try the challenges repeatedly until they succeeded, again similar to the findings of Liu et al. (2011). Although Hou (2013) suggested that learners with less prior knowledge lack the confidence to interact with peers, the flow experience of the three groups in our study did not show significant differences in prior knowledge, ruling out this interpretation. Instead, it may be that this group's level of prior knowledge and skill far exceeded the difficulty level of the tasks, leading to the feeling of boredom and making it difficult for them to focus on the activities (Csíkszentmihályi, 2000).

The influence of flow experience on anti-phishing game-based learning achievement

As for post-test learning achievement, only the Anxiety Group showed that the anti-phishing game-based learning materials were effective in improving anti-phishing knowledge in relation to social sites. This result is contrary to past results, which have proposed that the flow state should lead to positive learning achievement (Choi et al., 2007; Hou & Li, 2014; Pearce et al., 2005; Skadberg & Kimmel, 2004). With regard to the Flow Group, based on learning behavioral patterns, we infer that the reading behavior of this group was insignificant before the game, leaving the participants in this group with insufficient anti-phishing knowledge and ability to solve the game tasks. Instead, this group completed the games through peer assistance and re-reading, leading them not to perform well on the post-test in the absence of assistance. Although the Anxiety Group had read the learning materials before the game and substantially acquired the anti-phishing knowledge provided, this knowledge remained insufficient for them to complete the tasks without interacting with peers to strengthen their skills. Although the Anxiety Group lacked the behavior of verification after interaction and reading, leading them to require more time to complete the tasks, they were able to obtain relatively good learning achievement when allowed to read the materials comprehensively and engage in repeated practice. Finally, the materials read by the Boredom Group before the game were sufficient for them to complete the tasks, and they felt bored by the (putative) challenges of the lesson, lacked peer interaction, and were unable to fully focus on the activities. As a result, they showed no significant improvement in their learning achievement, a result congruent with the views proposed by Csíkszentmihályi (2000).

In terms of learning efficiency, the Flow Group enjoyed the games, and viewed their skills to be in equilibrium with the level of difficulty of the challenges (Kiili, 2005; Liu et al., 2011); they sought to accomplish the game tasks using suitable methods. Although the Flow Group's incidence of Game behavior was slightly lower than that of the Anxiety and Boredom Groups, the combination of interaction and reading was an effective learning model. The results of our study are similar to those of past studies that have proposed that flow experience can help learners focus and maintain their motivation to reach their goals (Inal & Çağıltay, 2007), thereby leading to more effective learning (Hoffman & Novak, 1996; Hou & Li, 2014).

Conclusion, limitations, and recommendations for future study

The purpose of this study was to examine the differences in learning behavioral patterns and learning achievement among learners with different flow experiences. The results showed that learners can acquire anti-phishing knowledge through trial and error via a repeated gaming behavioral pattern. Leaners in the Flow Group might engage in the behavior of discussing with peers and verifying the outcomes of the discussion; the Anxiety Group tended to turn to reading materials and peers for solutions, but lacked the step of reading and verifying what they had learned; the Boredom Group relied less on reading materials and interaction with peers, tending to try the challenges repeatedly until they succeeded. It is suggested that future educators and researchers on anti-phishing education appropriately increase the level of difficulty of games used and design learning materials with flexible difficulty based on learners' flow states.

In terms of study limitations, flow was measured using only two questions in this study; thus, various factors potentially impacting flow experience were not considered. Due to insufficient flow scale matching, the age groups of our research subjects in this study, and the relatively short duration of the experiment, flow state in this study only focused on the skill-challenge balance measured on one occasion among students aged 9-12. To fully understand flow state, the learners' flow precondition, state, and outcomes need to be measured (Fang et al., 2013). Pearce et al. (2005) also argued that the complex changes of flow state have to be measured continuously throughout the learning process through questions concerning skill and challenge. Therefore, we suggest that future studies may consider measuring flow experience before and during activities so as to better understand changes in learners' flow states, in order to understand better how changes in flow affect learning behavior. Furthermore, although the materials of this study did lead to learning achievement, the learning content could still be improved to make the lesson more interesting and enhance learning motivation, for example by making the game tasks more challenging or more dynamic to stimulate the learning motivation and flow experience (Hung et al., 2014; Hung et al., 2015).

With regard to game-based learning, we suggest that future educators offer learning questions and guide learners to interact with their peers; further, they can encourage learners to verify information as well as to improve the involvement of learners experiencing boredom by getting them to help others, thereby helping them to form the flow experience from a new angle. Whether for the development of game-based learning materials or the delivery of related lessons and courses, learning content should allow learners to better enjoy reading the

materials and challenging themselves by playing the games, as well as to adjust the difficulty of games in a timely way according to flow state, so as to maintain learners' flow experience and help them engage in activities with greater learning efficiency and effectiveness, which should in turn enhance the educational value of the game-based learning materials used.

Acknowledgements

This research was supported by the Ministry of Science and Technology in Taiwan through Grant numbers MOST 104-2511-S-009-008-MY3, MOST 103-2511-S-009-008-MY2, NSC 101-2511-S-009-010-MY3, and NSC 100-2511-S-009-012. The authors would like to thank the students who participated in this study and acknowledge the contributions of Shian-Shyong Tseng, Sunny S. J. Lin, and Chao-Hsiu Chen who supported this research study and provided valuable comments.

References

Anti-Phishing Working Group. (2013). *APWG phishing trends reports*. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_Q4_2012.pdf

Arachchilage, N. A. G., & Love, S. (2013). A Game design framework for avoiding phishing attacks. *Computers in Human Behavior, 29*(3), 706-714. doi:10.1016/j.chb.2012.12.018

Bakeman, R., & Gottman, J. M. (1997). *Observing interaction: An Introduction to sequential analysis* (2nd ed.). New York, NY: Cambridge University Press.

Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2011). The Socialbot network: When bots socialize for fame and money. In *Proceedings of the 27th Annual Computer Security Applications Conference* (pp. 93-102). New York, NY: ACM.

Choi, D. H., Kim, J., & Kim, S. H. (2007). ERP training with a web-based electronic learning system: The Flow theory perspective. *International Journal of Human-Computer Studies, 65*(3), 223-243.

Csíkszentmihályi, M. (1975). *Beyond boredom and anxiety.* San Francisco, CA: Jossey-Bass.

Csíkszentmihályi, M. (2000). *Beyond boredom and anxiety: Experiencing flow in work and play* (25th Anniversary ed.). San Francisco, CA: Jossey-Bass.

Ebel, R. L., & Frisbie, D. A. (1986). *Essentials of educational measurement* (4th ed.). Englewood Cliffs, NJ: Prentice Hall.

Fang, X., Zhang, J., & Chan, S. S. (2013). Development of an instrument for studying flow in computer game play. *International Journal of Human-Computer Interaction, 29*(7), 456-470.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: Threats and solutions. *Communications Surveys & Tutorials, IEEE, 16*(4), 2019-2036.

Fossi, M., Turner, D., Johnson, E., Mack, T., Adams, T., Blackbird, J., Entwisle, S., Graveland, B., McKinney, D., & Mulcahy, J. (2013). *Internet Security Threat Report 2013*. Mountain View, CA: Symantec Corporation.

Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., & Zhao, B. Y. (2010). Detecting and characterizing social spam campaigns. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement* (pp. 35-47). New York, NY: ACM.

Harper, B. (2014). *The Sky is not falling: Teens still active on Facebook.* Retrieved from http://www.socialbakers.com/blog/2090-the-sky-is-not-falling-teens-still-active-on-facebook

Hoffman, D. L., & Novak, T. P. (1996). Marketing in hypermedia computer-mediated environments: Conceptual foundations. *Journal of marketing, 60*(3), 50-68.

Hou, H.-T. (2012a). Analyzing the learning process of an online role-playing discussion activity. *Educational Technology & Society, 15*(1), 211-222.

Hou, H.-T. (2012b). Exploring the behavioral patterns of learners in an educational massively multiple online role-playing game (MMORPG). *Computers & Education, 58*(4), 1225-1233. doi:10.1016/j.compedu.2011.11.015

Hou, H.-T. (2013). Analyzing the behavioral differences between students of different genders, prior knowledge and learning performance with an educational MMORPG: A Longitudinal case study in an elementary school. *British Journal of Educational Technology, 44*(3), E85-E89. doi:10.1111/j.1467-8535.2012.01367.x

Hou, H.-T., & Li, M.-C. (2014). Evaluating multiple aspects of a digital educational problem-solving-based adventure game. *Computers in Human Behavior, 30*, 29-38. doi:10.1016/j.chb.2013.07.052

Hung, C.-Y., Kuo, F.-O., Sun, J. C.-Y., & Yu, P.-T. (2014). An Interactive game approach for improving students' learning performance in multi-touch game-based learning. *IEEE Transactions on Learning Technologies, 7*(1), 31-37. doi:10.1109/TLT.2013.2294806

Hung, C.-Y., Sun, J. C.-Y., & Yu, P.-T. (2015). The Benefits of a challenge: Student motivation and flow experience in tablet-PC-game-based learning. *Interactive Learning Environments, 23*(2), 172-190.

Inal, Y., & Çağıltay, K. (2007). Flow experiences of children in an interactive social game environment. *British Journal of Educational Technology, 38*(3), 455-464.

Internet World Stats. (2014). *Internet usage statistics. The Internet big picture: World Internet users and populations stats*. Retrieved from http://www.internetworldstats.com/stats.htm

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & information technology, 32*(6), 584-593.

Kiili, K. (2005). Content creation challenges and flow experience in educational games: The IT-emperor case. *The Internet and higher education, 8*(3), 183-198. doi:10.1016/j.iheduc.2005.06.001

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A Real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (pp. 3). New York, NY: ACM.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007a). Protecting people from phishing: The Design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 905-914). New York, NY: ACM.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007b). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 70-81). New York, NY: ACM.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology, 10*(2), 7. doi:10.1145/1754393.1754396

Liu, C.-C., Cheng, Y.-B., & Huang, C.-W. (2011). The Effect of simulation games on the learning of computational problem solving. *Computers & Education, 57*(3), 1907-1918. doi:10.1016/j.compedu.2011.04.002

Livingstone, S., & Haddon, L. (2009). EU kids online. *Zeitschrift Für Psychologie/Journal of Psychology, 217*(4), 236-239.

Massimini, F., & Carli, M. (1988). The Systematic assessment of flow in daily experience. In M. C. Csikszentmihalyi & I. Selega (Eds.), *Optimal experience: Psychological studies of flow in consciousness* (pp. 266-287). New York, NY: Cambridge University Press.

Mayer, R. E. (1992). *Thinking, problem solving, cognition* (2nd ed.). New York, NY: W. H. Freeman and Company.

Novak, T. P., Hoffman, D. L., & Yung, Y.-F. (1998, March). *Modeling the structure of the flow experience among web users.* Paper presented at the INFORMS Marketing Science and the Internet Mini-Conference, Boston, MA.

Nunnally, J. C. (1967). *Psychometric theory* (1st ed.). New York, NY: McGraw-Hill.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). New York, NY: McGraw-Hill.

Pearce, J. M., Ainley, M., & Howard, S. (2005). The Ebb and flow of online learning. *Computers in Human Behavior, 21*(5), 745-771. doi:10.1016/j.chb.2004.02.019

Quilliam, E. T., Rifon, N. J., & Larose, R. (2006). Protecting household online privacy: Who is the first line of defense? In D. Grewal, M. Levy & R. Krishnan (Eds.), *Enhancing Knowledge Development in Marketing* (pp. 286-287). Chicago, IL: American Marketing Association.

Robila, S. A., & Ragucci, J. W. (2006). *Don't be a phish: Steps in user education*. In *ACM SIGCSE Bulletin* (Vol. 38, No. 3, pp. 237-241). New York, NY: ACM.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, month). *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions.* Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: The Design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382). New York, NY: ACM.

Skadberg, Y. X., & Kimmel, J. R. (2004). Visitors' flow experience while browsing a web site: Its measurement, contributing factors and consequences. *Computers in Human Behavior, 20*(3), 403-422. doi:10.1016/S0747-5632(03)00050-5

Sweetser, P., & Wyeth, P. (2005). Game flow: A Model for evaluating player enjoyment in games. *Computers in Entertainment, 3*(3), 1-24.

Tsai, F.-H., Yu, K.-C., & Hsiao, H.-S. (2007, August). *Designing constructivist learning environment in online game.* Paper presented at the Digital Game and Intelligent Toy Enhanced Learning, Jhongli, Taiwan.

Webster, J., Trevino, L. K., & Ryan, L. (1993). The Dimensionality and correlates of flow in human-computer interactions. *Computers in Human Behavior, 9*(4), 411-426.

Wirth, C. B., Rifon, N. J., LaRose, R., & Lewis, M. L. (2007, May). *Promoting teenage online safety with an i-safety intervention: Enhancing self-efficacy and protective behaviors.* Paper presented at the Annual Meeting of the International Communication, Canada.

Wishart, J. M., Oades, C., & Morris, M. (2007). Using online role play to teach internet safety awareness. *Computers & Education, 48*(3), 460-473.

Yang, C. C., Tseng, S. S., Lee, T. J., Weng, J. F., & Chen, K. (2012, July). Building an anti-phishing game to enhance network security literacy learning. In *IEEE 12th International Conference on Advanced Learning Technologies* (pp. 121-123). IEEE. doi:10.1109/ICALT.2012.174

Appendix 1. Test questions on phishing in social network sites

	Items
True or False Questions	
T	1. After being added into a shopping group, it is correct to select "Report Group" in the top-right corner of the group's page and then select the reason "This is junk email or fraud" and "This has caused inconvenience to me."
T	2. It is correct to regularly select the "Setting" icon in the top-right corner of Facebook, execute the setting function, enter into the "Account Privacy" settings page, and select "Applications" to remove unused programs.
F	3. To report unlawful Facebook shopping groups, one may call the reporting line 0800-016587, the main line 02-22150711, or send a fax to 02-22142627; one may also write to No. 66, Anfeng Road, Xindian District, New Taipei City 23156, or send an email directly to liao@tipo.gov.tw.
F	4. When logging into Facebook, directly inputting the password (in the sequence of first character, second character…) could prevent Trojan horse programs from being imbedded into computers to record the users' passwords.
F	5. It is best to ignore the situation when you discover that your account has been continuously inviting others to join a shopping group.
T	6. When using Google Chrome as your browser, it is correct to select "≡ " → "Tools" → "Extensions" (you may type chrome://extensions/ directly) to regularly check, deactivate, and remove the "Chrome Service Pack" application.
T	7. When using Mozilla Firefox as your browser, it is correct to select "Tools" → "Extensions" (or use the keyboard shortcut Ctrl + Shift + A) and select "Extensions" to regularly check, deactivate, and remove the "Mozilla Service Pack" application.
T	8. Entering into the "Advertisement" setting page in account settings, and changing the settings for "Third-party Sites" and "Advertisement and Friends" to "Limit to my friends" ensures that when you "Like" any advertisements in the future, it will not become a channel for advertising among your friends.
F	9. When you see an instant notification from Facebook showing that '"You have been tagged in a YouTube Video Link "Adobe Flash Click!!"', it means there is a required update and you should open the link without worrying.
T	10. Setting security codes on Facebook is one of the most effective methods to defend against phishing.
Multiple Choice Questions (MCQs)	
D	1. How do you activate a two-stage verification? Please arrange the steps in sequence: 1. Select setting 2. Account security 3. Account setting 4. Log in authorization 5. Check "require safety pin, allow me to access my account from an unknown browser". A 12345 B 13452 C 23145 D 13245
A	2. How do you recover your account within five minutes? Please arrange the steps in sequence: 1. Log into the website http://www.facebook.com/hacked that was jointly developed by Facebook and the Crime Investigation Bureau (CIB) 2. Select "My account has been hacked" and enter the user's account details, followed by an account detail confirmation 3. Enter the user's existing or past passwords 4. Reset the password and increase passwords' complexity 5. Set a new security question and recover account access. A 12345 B 12435 C 14325 D 12543
C	3. Attackers use rewards or prizes to invite users to join dubious events, or fill in personal information to steal their information. Which of the following phishing tactics on social networking sites is the aforementioned tactic? A Manual sharing of virus attack B Dubious "Like" phishing attack C Dubious reward phishing attack

		D Virus copy phishing attack
A	4.	When attackers tempt users into clicking on links to certain content or “Like”, a different action immediately takes place in the background. Which of the following is an example of this kind of phishing tactic? A Dubious “Like” phishing attack B Dubious reward phishing attack C Manual sharing of virus attack D Dubious browser phishing attack
C	5.	Attackers create false news or interesting clips to tempt friends into clicking/selecting them, and collects their personal information. Which of the following is an example of this kind of phishing tactic? A Dubious “Like” phishing attack B Dubious reward phishing attack C Manual sharing of virus attack D Dubious browser phishing attack
B	6.	Attackers usually use vouchers as rewards and invite users to their URLs to attach malicious “JavaScript” codes for activating the fraud mechanism. Which of the following is an example of this kind of phishing tactic? A Dubious “Like” phishing attack B Virus copy phishing attack C Manual sharing of virus attack D Dubious browser phishing attack
D	7.	Attackers trick users into downloading malicious browsers, which then reasonably expand in user’s computers, stealing sensitive personal information during the process. Which of the following is an example of this kind of phishing tactic? A Dubious “Like” phishing attack B Dubious reward phishing attack C Manual sharing of virus attack D Dubious browser phishing attack
A	8.	A frame is superimposed onto a dubious video player, once a user clicks on the video or “Like”, the fraud mechanism is activated immediately to collect the user’s information. Which of the following is an example of this kind of phishing tactic? A Dubious “Like” phishing attack B Dubious reward phishing attack C Manual sharing of virus attack D Dubious browser phishing attack
D	9.	Which one of the following is “NOT” a method for defending against phishing tactics on social networking sites? A Switch to non-sequential key-in of password during log in B The best way is to reinstall the computer when you found yourself continuously inviting others to shopping groups C Set up security codes D Cancel log in notification

Appendix 2. Game-based learning behavioral coding scheme

Dimensions	Coding	Behavior	Definition
Reading	R	Reading course learning	Select the "Course learning—learn about social sites attack methods" page to read.
	r	Reading course learning	Select the "Course learning—guard against social sites attack methods" page to read.
	E	Reading real-life practice	Select the "Real-life practice—learn about social sites attack methods" page to read.
	e	Reading real-life practice	Select the "Real-life practice—guard against social sites attack methods" page to read.
Interaction with peers	C	View leaderboard	Select the "Leaderboard" page and view the challenge scores of other learners.
	M	View message	Select the "Forum."
	m	Post question message	Select the "Forum" and add comments or post questions.
Game	G	Challenge games	Select the "Game" page.
	Y	Successful challenge	Select the "Game" page and win the challenge.
	N	Failed challenge	Select the "Game" page but fail the challenge.
Test	S	Take the pre-test	Select the "Pre-test" page and take the test.
	s	Take the post-test	Select the "Post-test" page and take the test.
	F	Take the flow test	Select the "Flow test" page and take the test.