Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 12 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i12.53199

PAPER

# Phishing Awareness through Game-Based Learning: A Mobile-Responsive Web Application for Middle School Learners

Thanakorn Uiphanit[1] (✉), Thatsanan Chutosri[2], Natcha Wattanaprapa[1], Wannarat Bunchongkien[1], Phachaya Chiewchan[1], Nipon Nachin[2]

[1]Sunandha Rajabhat University, Bangkok, Thailand

[2]Alphasec Co. Ltd, Bangkok, Thailand

thanakorn.ui@ssru.ac.th

## ABSTRACT

This study aimed to design a phishing-focused learning approach for middle school learners using a game-based educational format. The objective of this project is to (a) study and develop an educational game to enhance knowledge about phishing emails, (b) compare the academic results before and after learning, and (c) evaluate the acceptability of the educational game to enhance knowledge about phishing emails. The sample group used in this study was 130 from seventh-grade students in School A, Nonthaburi Province, Thailand. To create a game-based learning model focused on phishing emails, the researchers opted for a spot-the-difference game format. The game leveraged the fact that learners were already acquainted with the game's rules and had prior experience playing it. Furthermore, the game is web-based, enabling learners to engage with it at their convenience, regardless of location or time. The research instruments were (a) a phishing-awareness educational game, (b) pre- and post-assessment tools to evaluate knowledge gain, and (c) a questionnaire measuring students' acceptance of game-integrated instruction. The study's results indicated a high level of learner approval for the phishing-focused instructional model that employed gamified techniques. This acceptance was evident in terms of both the perceived ease of use and the convenience associated with the learning process. Additionally, learners reported significant benefits derived from engaging with the game, including various elements that effectively supported and enhanced their learning outcomes related to phishing emails, resulting in a marked improvement compared to their prior knowledge.

## KEYWORDS

educational game, phishing, mail phishing

Uiphanit, T., Chutosri, T., Wattanaprapa, N., Bunchongkien, W., Chiewchan, P., Nachin, N. (2025). Phishing Awareness through Game-Based Learning: A Mobile-Responsive Web Application for Middle School Learners. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(12), pp. 55–67. https://doi.org/10.3991/ijim.v19i12.53199

Article submitted 2024-11-06. Revision uploaded 2025-04-28. Final acceptance 2025-04-30.

## 1 INTRODUCTION

Phishing is a widespread cyber risk that critically affects individuals, businesses, and the broader community. This form of attack leverages social engineering tactics to establish a false sense of credibility, thereby manipulating victims into complying with the attackers' objectives. Given that phishing requires minimal investment while yielding substantial returns, the incidence of such illegal attacks has escalated significantly. In 2023, phishing attacks conducted via mobile devices surged by 85%, while 82% of phishing attempts were executed through email platforms [1], [17], [25]. Email phishing is a variant of phishing in which malicious actors disseminate fraudulent emails, purporting to originate from trusted entities, with the intent of deceiving recipients into divulging sensitive information or performing actions desired by the attackers. This type of attack is typically indiscriminate, targeting a broad audience through mass email distribution. Common examples include emails that appear to be from financial institutions, prompting recipients to click a link to verify their account details. The link, in turn, redirects victims to a counterfeit website designed to capture their login credentials. [12] In the second quarter of 2024, a report by the Anti-Phishing Working Group (APWG) indicates that phishing emails will adopt a new scam technique. This approach involves using a distinctive email subject line or mirroring the subject line of a legitimate marketing campaign to increase the likelihood of deceiving recipients [14], [32].

Seventh grade students, usually aged 12 to 13, begin using email for various school-related activities, such as attending online classes, accessing lessons, and participating in academic enrichment programs. Consequently, raising awareness and equipping students to handle the threat of phishing emails is crucial.

However, traditional lecture-based training in the classroom is often insufficient to fully engage students and stimulate their interest in learning about these threats [14], [23].

Numerous researchers and educators have also designed and developed educational games aimed at enhancing learning about phishing in various formats. This includes the development of various kinds of games [6], [8], [24] such as mobile game development (Phish Phinder, PHISHGEM) [9], [10], [20] learning-based platform simulation (CyberPhishing) [16], board games (Smells Phishy) [18], gaming quiz [19], and role-playing games [22].

Incorporating a digital game-based learning model to educate students about phishing emails can significantly improve the learning environment and foster a positive attitude towards learning. In addition to acquiring knowledge, learners will experience enjoyment, enhancing their engagement with the material. This approach also promotes positive interactions between learners and the games, as well as among learners themselves as they collaborate and learn through gameplay [1], [2], [3], [4], [5], [6], [7], [11], [26], [27].

In this study, the researchers designed and developed an educational game based on digital game-based learning (DGBL), mobile learning (m-learning), and Game-flow to improve knowledge about phishing emails, structured as a "spot-the-difference" game involving both images and text. This format was chosen due to its familiarity among most learners. The details are as follows: [6], [15], [26], [27].

- **Delivering a good learning experience using games:** The games used will be engaging and appealing so that students can continue learning through them during the learning period, fostering a desire for ongoing education [2], [4], [7], [31].

- **Game-flow:** Encouraging students to develop a desire to learn by designing content and activities that match their skill levels [2], [4], [7].
- **Creating collaborative learning using games:** While the students play the game, they can exchange information with each other to accomplish missions [2], [11].
- **Data Feedback:** Providing guided learning information during game-based learning helps learners effectively acquire and retain the correct content [7].

Moreover, the game does not require installation on devices, as it can be accessed via a website, providing the convenience of learning anytime and anywhere. The game's content and narrative immerse learners in the role of cyber detectives, adding an engaging storyline to the educational experience [28]. The game is divided into two sections: the lesson section, which focuses on identifying irregularities in email subjects, text, images, and sources; and the game section. The design of images, graphics, colors, and music has been carefully chosen to suit the learners' age group. Additionally, the game's difficulty levels are tailored to match the learners' observational abilities and language proficiency, ensuring an appropriate and effective learning experience [21], [28], [29], [32], [33].

## 2 OBJECTIVE

- To study and develop an educational game to enhance knowledge about phishing emails.
- To compare learners' academic performance before and after playing the educational game.
- To evaluate the acceptance of the implementation of an educational game to enhance knowledge about phishing emails.

## 3 HYPOTHESIS

Students who learned with educational games to enhance their knowledge about phishing emails had higher learning achievement than before learning with games.

## 4 RESEARCH FRAMEWORK

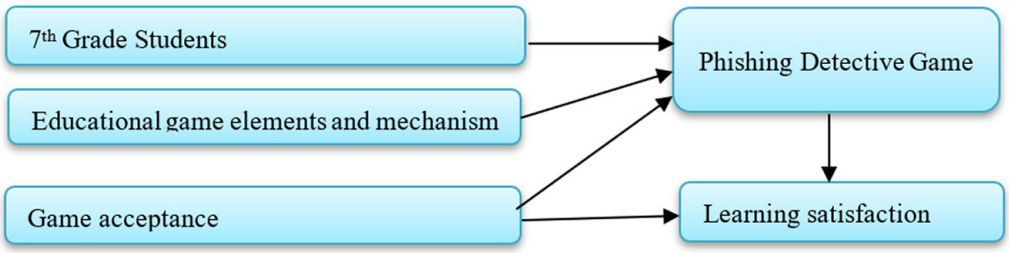


**Fig. 1.** The research framework for developing a mobile-responsive web application for middle school learners

# 5 RESEARCH METHODOLOGY

## 5.1 Research design

This study aimed to promote phishing email awareness and improve learning outcomes among seventh-grade students by utilizing a spot-the-difference game that incorporated both images and text elements. The research methodology was based on the ADDIE framework, encompassing five sequential stages: 1) Analysis, 2) Design, 3) Development, 4) Implementation, and 5) Evaluation. Each phase was systematically applied to ensure the game's effectiveness and relevance to the learning objectives.

The research proposal was considered, and agreed to implementation of the proposal of this study by the Suan Sunandha Rajabhat University Ethics Committee (Certificate number: COE.2-108/2025). The study adhered to ethical standards based on the 1964 Declaration of Helsinki, including all relevant later revisions.

Before the experiment commenced, consent forms were completed by all student participants, and parental authorization was acquired to maintain ethical standards and safeguard minors' rights.

**Analysis.** The research team collected data and examined students' awareness and learning behaviors related to phishing emails among seventh-grade students. This analysis aimed to identify appropriate game types and formats that align with students' learning preferences, informed by existing research on phishing games and the principles of digital game-based learning.

The Phishing Mail Detective game developed by the research team was distinct from other phishing awareness games. The game was designed to enable students to independently understand and learn through the following features:

- **Clear instructional design:** The game includes clearly defined steps, allowing students to easily read and follow the instructions.
- **Cross-device accessibility:** The game can be played via any device with a web browser, requiring no installation.
- **Improved engagement and comprehension:** The game helps learners more easily grasp the concept of phishing and improves their learning response through active engagement.

**Design.** The analysis revealed that most students commonly engage in gameplay during their free time after school, with a specific interest in spot-the-difference games involving images and text. Based on these preferences, the research team developed a game that conveys phishing email concepts through this familiar format.

To enhance learner engagement, the game incorporates key features of effective educational games, including visually appealing graphics, age-appropriate content, and a consistent alignment with learning objectives. Additionally, well-structured rules and progressively challenging levels were implemented to maintain students' interest and promote continuous learning throughout gameplay.

**Development.** Considering that the target learners are between 12 and 13 years old, the researchers designed the game using bright, engaging colors and a storyline featuring cartoon characters. In the game, learners assume the role of detectives

working alongside the "Cyborg" Cyber Police to investigate whether specific emails contain phishing content.

To support diverse language needs, the game incorporates both Thai and English text. Ambient background music was intentionally selected to foster a calm and focused learning atmosphere, as it emphasizes soothing tones that promote concentration during gameplay.

The game's difficulty levels were carefully aligned with the learners' cognitive development and educational stage. In order to assess how well the game performed, as well as the overall game-based learning model, a questionnaire was administered to three experts: one in game design and development, one in cybersecurity, and one in educational assessment and evaluation.

**Implementation.** The researchers first administered a pre-test to the students, followed by a lesson on phishing emails delivered through the educational game. This instructional intervention was conducted with a sample of 130 students.

**Evaluation.** After the sample group completed the gameplay session, the researchers administered a questionnaire to assess the learners' acceptance of the phishing email learning experience. The collected data were then analyzed to evaluate the overall effectiveness of the game-based learning model.

## 5.2 Research sample

In this study, School A had a total of 325 seventh-grade students. A screening questionnaire was distributed to all students to identify those who were unfamiliar with phishing emails. Based on the results, a purposive sample of 130 students was selected to participate in the study.

## 5.3 Research tools

In this study, the research team created an educational game designed to enhance students' understanding of phishing emails. Pre- and post-assessments were conducted to measure students' knowledge before and after engaging with the game. Additionally, the researchers employed an acceptance questionnaire to evaluate students' perceptions of learning through the game-based approach.

**Phishing detective game.** The researchers designed and developed a web-based game, accessible through a browser, with educational content that learners are encouraged to read and understand before beginning gameplay. The game follows a spot-the-difference format, focusing on phishing detection within images and text, with content available in both Thai and English.

Players must scrutinize the text or images in emails to spot differences, helping to determine whether an email is a phishing attempt. If a learner suspects an email is phishing, they can press a green button to flag it. If they believe an email is legitimate, they need not press the button. Each email presents unique errors and observable clues that vary in complexity, designed to progressively challenge learners and maintain engagement. The game also features ambient background music to create an immersive and conducive learning atmosphere [13]. The following sections provide details of an example game screen.


**Fig. 2.** The enter student name screen

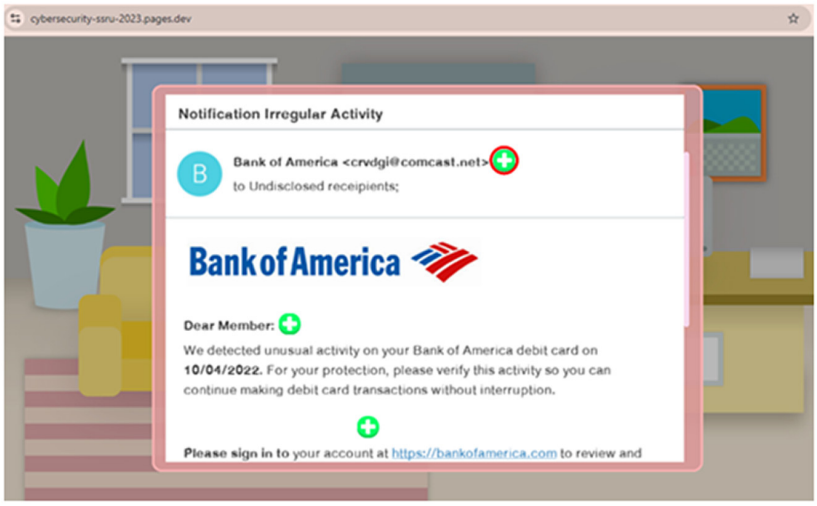


**Fig. 3.** Display showing a selection of message suspected of being phishing email

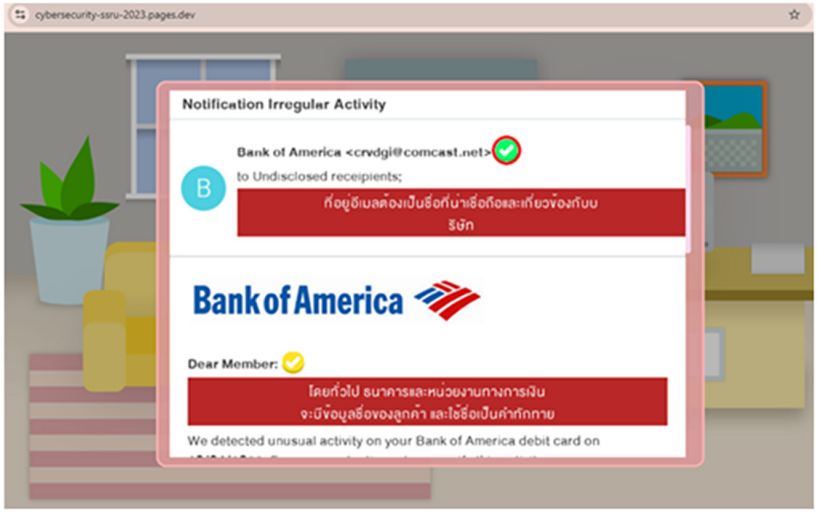


**Fig. 4.** The answer screen displayed after the student has played through each level


**Fig. 5.** The correct answer screen is shown in a green bar

**Pre- and post-test.** To measure learning achievement, the researchers created a paired set of assessments—one administered before and one after the intervention, this test covers mail phishing content with 20 multiple-choice questions, each offering four options, from which students must select the correct answer, considering the difficulty level of each question.

**Survey on acceptance of educational games to enhance knowledge about phishing emails.** To evaluate the acceptance of the educational game designed to enhance knowledge about phishing emails, the researchers developed a questionnaire utilizing a 5-point Likert scale. The scale ranged from 1 ("Totally disagree") to 5 ("Totally agree"), assessing learners' perceptions across multiple dimensions of game-based learning.

The rating levels were categorized according to the scale shown below [30]:

4.21–5.00 = Strongly agree
3.41–4.20 = Moderately agree
2.61–3.40 = Neutral
1.81–2.60 = Moderately disagree
1.00–1.80 = Strongly disagree

The gap between maximum and minimum scores was calculated as 4 (5–1), and each interpretation level was assigned a range of 0.8 points.

## 6 FINDINGS

The researchers tested the hypothesis that "students who learned through educational games would demonstrate higher learning achievement regarding phishing emails compared to their performance before the intervention." A paired-samples t-test was utilized to examine the outcomes of both pre- and post-assessments. The findings derived from this analysis are shown in Table 1.

**Table 1.** Summary of learning achievement test results analyzed via independent t-test

| Test | N | Scores | Total Scores | Mean | S.D. | D | S.D.D | t | Sig.(1-Tailed) |
|---|---|---|---|---|---|---|---|---|---|
| Pre-test | 130 | 30 | 2899 | 22.30 | 3.96 | 6.04 | 4.16 | 14.43* | 0.0000 |
| Post-test | 130 | 30 | 3585 | 27.58 | 1.46 | | | | |

As shown in Table 1, students achieved an average pre-test score of 22.30 and an average post-test score of 27.58. The mean difference of 6.04 points, with a p-value of 0.0000, indicates a statistically significant improvement in learning achievement. These findings suggest indicating that the educational game produced a substantial a beneficial effect on learners' ability to recognize and understand phishing emails.

**Table 2.** Learners' acceptance of game-based learning

| No | Question | Mean | S.D. | Interpreted |
|---|---|---|---|---|
| **Ease of use** | | | | |
| 1 | Learners do not need to install the game because it can be played via the web | 4.70 | 0.52 | Strongly agree |
| 2 | The game can be processed quickly | 4.67 | 0.51 | Strongly agree |
| 3 | The order of the content within the game is appropriate | 4.60 | 0.58 | Strongly agree |
| 4 | Learners can learn through games continuously, anytime, anywhere | 4.74 | 0.46 | Strongly agree |
| | **Average** | **4.68** | **0.52** | **Strongly agree** |
| **Usefulness** | | | | |
| 6 | The content of the game is consistent with the learning objectives | 4.57 | 0.54 | Strongly agree |
| 7 | The experiences gained from learning through games can be applied in daily life | 4.67 | 0.49 | Strongly agree |
| 8 | Learning through games enhances imagination and critical thinking. | 4.69 | 0.50 | Strongly agree |
| 9 | Games can meet the learning needs of learners | 4.59 | 0.57 | Strongly agree |
| | **Average** | **4.63** | **0.53** | **Strongly agree** |
| **Education game elements** | | | | |
| 10 | The gameplay is entertaining | 4.52 | 0.63 | Strongly agree |
| 11 | Images and graphics used are enjoyable | 4.55 | 0.65 | Strongly agree |
| 12 | The format and content of the game are appropriate for learners | 4.59 | 0.55 | Strongly agree |
| 13 | The difficulty level in the game is appropriate | 4.45 | 0.64 | Strongly agree |
| 14 | The music used in the game is appropriate | 4.49 | 0.61 | Strongly agree |
| 15 | The language used in the game is accurate and clear | 4.37 | 0.79 | Strongly agree |
| | **Average** | **4.50** | **0.65** | **Strongly agree** |

According to the data presented in Table 2, learners perceived employing educational game-based methods for learning about phishing emails as highly accessible and user-friendly. This positive perception was largely attributed to the game's web-based nature, which eliminated the need for installation and allowed learners to engage with the content anytime and anywhere. Additionally, the game's fast processing speed contributed to a responsive and seamless learning experience.

Learners also indicated that the game facilitated a better understanding of content structure and learning objectives. Beyond convenience, they noted that the game enhanced their imagination, encouraged logical and analytical thinking, and provided knowledge that could be applied to real-life scenarios—highlighting the practical relevance of game-based learning.

Regarding the design components, the most influential factors contributing to learners' acceptance were the game's overall structure, its compelling visual design, and the level of enjoyment experienced during gameplay. Other contributing elements included the appropriateness of the game's difficulty, the immersive background music, and the clarity of language used throughout the game—all of which played a role in shaping learners' engagement and positive reception of the learning tool.

## 7 DISCUSSION

The findings of this study demonstrate that Phishing Mail Detective is a highly suitable educational tool for teaching phishing awareness to seventh-grade students. Its familiar spot-the-difference format, intuitive interface, and simple game mechanics allowed learners to engage with the content immediately, without the need for prior instruction. Moreover, the game's web-based accessibility enabled students to interact with the learning material conveniently from any device and location [11], [12].

Beyond the significant improvement in post-assessment scores, the game received the highest acceptance ratings across three dimensions: instructional design, perceived usefulness, and ease of use. These results suggest that web-based games, which do not require installation and are device-independent, are particularly effective in supporting diverse learning environments, including resource-limited rural schools [6], [15], [31], [33].

Students valued the game's interactivity and immersive elements. The spot-the-difference design closely mirrors familiar game experiences, enabling immediate engagement. Content alignment with instructional objectives also enhanced learners' imaginative and critical thinking skills. Many learners reported being capable of utilizing the knowledge gained acquired through gameplay into real-world situations.

The educational game also integrated motivational components that further supported learning, including:

- Role-playing as a cyber detective
- Realistic phishing scenarios
- Immediate feedback via answer screens and scoring
- Ambient music to enhance focus
- Language-based clues (e.g., grammatical errors or suspicious links)

These features contributed to developing learners' observational skills and overall understanding of phishing tactics.

The results align with previous studies on phishing education games—such as Phishing Phinder, Smells Phishy, Cyber-Phishing, and PHISHGEM—which also emphasize the importance of interactivity, accessibility, and adaptability in digital game-based learning formats [9], [10], [16], [18], [20], [28].

## 8 CONCLUSIONS

The findings of this study suggest that Phishing Mail Detective is an effective and accessible educational game for enhancing phishing awareness among middle

school students. Its simple gameplay mechanics, device-independent accessibility, and web-based design make it well-suited for a variety of learning environments—including those with limited technological infrastructure.

The game's positive reception by students further supports its potential scalability and adaptability. The framework used in this study could be extended to cover other areas of cybersecurity education. However, future adaptations should consider key contextual factors such as the school's technological resources, curriculum focus, and the learners' prior knowledge and cognitive development to ensure maximum educational impact.

## 9 LIMITATION

There are restrictions on using the Thai language for communication within the game, which may hinder the understanding of the email content. This makes it challenging to differentiate between students' emails within the game.

Therefore, subsequent studies might necessitate the assistance of Thai language experts to ensure that the material appropriately matches the students' proficiency level in Thai language proficiency.

## 10 SUGGESTION

In the future research, we should evaluate the long-term results. To assess long-term knowledge retention, a method can be implemented to verify achievements each semester. Additionally, have the effectiveness and acceptability of other educational tools been compared to educational games to determine if there are significant differences.

## 11 REFERENCES

[1] K. A. Aqeel Alzoubi, "The effectiveness of the application of game-based e-learning on academic achievement in mathematics for students in Jordan," *International Journal of Engineering Pedagogy (iJEP)*, vol. 13, no. 6, pp. 64–75, 2023. https://doi.org/10.3991/ijep.v13i6.41961

[2] H. K. Abd El-Sattar, "A new learning theory-based framework for combining flow state with game elements to promote engagement and learning in serious games," *Information Sciences Letters*, vol. 12, no. 6, pp. 2663–2677, 2023. https://digitalcommons.aaru.edu.jo/cgi/viewcontent.cgi?article=1977&context=isl

[3] A. Khan, H. F. Ahmad, and M. M. Malik, "Use of digital game-based learning and gamification in secondary school science: The effect on student engagement, learning and gender difference," *Education and Information Technologies*, vol. 22, pp. 2767–2804, 2017. https://doi.org/10.1007/s10639-017-9622-1

[4] A. All, E. P. N. Castellar, and J. Van Looy, "Assessing the effectiveness of digital game-based learning: Best practices," *Computers & Education*, vol. 92–93, pp. 90–103, 2015. https://doi.org/10.1016/j.compedu.2015.10.007

[5] A. Steinmaurer, J. Pirker, and C. Gütl, "sCool–Game-based learning in computer science class: A case study in secondary education," *International Journal of Engineering Pedagogy (iJEP)*, vol. 9, no. 2, pp. 35–50, 2019. https://doi.org/10.3991/ijep.v9i2.9942

[6] C. J. Huizenga, T. G. Ten Dam, J. M. Voogt, and F. W. Admiraal, "Teacher perceptions of the value of game-based learning in secondary education," *Computers & Education*, vol. 110, pp. 105–115, 2017. https://doi.org/10.1016/j.compedu.2017.03.008

[7] S. Erhel and E. Jamet, "Digital game-based learning: Impact of instructions and feedback on motivation and learning effectiveness," *Computers & Education*, vol. 67, pp. 156–167, 2013. https://doi.org/10.1016/j.compedu.2013.02.019

[8] G. Jayakrishnan, V. Banahatti, and S. Lodha, "PickMail: A serious game for email phishing awareness training," in *Usable Security and Privacy (USEC) Symposium*, 2022. https://doi.org/10.14722/usec.2022.23059

[9] G. Misra, G. A. N. Arachchilage, and S. Berkovsky, "Phish phinder: A game design approach to enhance user confidence in mitigating phishing attacks," *arXiv preprint arXiv:1710.06064*, 2017. https://doi.org/10.48550/arXiv.1710.06064

[10] G. A. N. Arachchilage, S. Love, and C. Maple, "Can a mobile game teach computer users to thwart phishing attacks?" *International Journal for Infonomics (IJI)*, vol. 6, nos. 2/4, 2015. https://doi.org/10.20533/iji.1742.4712.2013.0083

[11] H. Gharbaoui, K. Mansouri, and F. Poirier, "Improving student engagement and success in computer programming courses through social learning in online environments," *International Journal of Engineering Pedagogy (iJEP)*, vol. 14, no. 6, pp. 54–68, 2024. https://doi.org/10.3991/ijep.v14i6.48705

[12] H. Yousif, K. Al-saedi, and M. D. Al-Hassani, "Mobile phishing websites detection and prevention using data mining techniques," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 13, no. 10, pp. 205–213, 2019. https://doi.org/10.3991/ijim.v13i10.10797

[13] I. Leuchter and G. Kurtz, "Effects of instructions, assistance, narrative, competition, challenge, and age on performances in digital learning games," *International Journal of Advanced Corporate Learning (iJAC)*, vol. 15, no. 2, pp. 16–33, 2022. https://doi.org/10.3991/ijac.v15i2.30867

[14] J. Andrić, D. Oreški, and T. Kišasondi, "Analysis of phishing attacks against students," in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2016, pp. 1423–1429. https://doi.org/10.1109/MIPRO.2016.7522363

[15] J. Bourgonjon, F. De Grove, C. De Smet, J. Van Looy, R. Soetaert, and M. Valcke, "Acceptance of game-based learning by secondary school teachers," *Computers & Education*, vol. 67, pp. 21–35, 2013. https://doi.org/10.1016/j.compedu.2013.02.010

[16] L. M. Hale, F. R. Gamble, and P. Gamble, "CyberPhishing: A game-based platform for phishing awareness testing," in *2015 48th Hawaii International Conference on System Sciences*, 2015, pp. 5260–5269. https://doi.org/10.1109/HICSS.2015.670

[17] M. Almseidin, A. Zuraiq, M. Al-Kasassbeh, and N. Alnidami, "Phishing detection based on machine learning and feature selection methods," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 13, no. 12, pp. 171–183, 2019. https://doi.org/10.3991/ijim.v13i12.11411

[18] M. Baslyman and S. Chiasson, "'Smells phishy?' An educational game about online phishing scams," in *2016 APWG Symposium on Electronic Crime Research (eCrime)*, 2016, pp. 1–11. https://doi.org/10.1109/ECRIME.2016.7487946

[19] M. L. Podila *et al.*, "Practice-oriented smartphone security exercises for developing cybersecurity mindset in high school students," in *2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 2020, pp. 303–310. https://doi.org/10.1109/TALE48869.2020.9368440

[20] O. C. Tinubu, J. O. Falana, O. E. Oluwumi, S. A. Sodiya, and A. S. Rufai, "PHISHGEM: A mobile game-based learning for phishing awareness," *Journal of Cyber Security Technology*, vol. 7, no. 3, pp. 134–153, 2023. https://doi.org/10.1080/23742917.2023.2167276

[21] P. Kingsuwankul, P. Bhattarakosol, P. Liangyoo, T. Uiphanit, P. Cheevavet, and P. Preepremvilas, "Gaming application development to promote cultural tourism in Bangnoi floating market in Samutsongkram," in *Proceedings of the 8th International Conference on Informatics, Environment, Energy and Applications*, 2019, pp. 248–252. https://doi.org/10.1145/3323716.3323751

[22] R. Fatima, A. Yasin, L. Liu, and J. Wang, "How persuasive is a phishing email? A phishing game for phishing awareness," *Journal of Computer Security*, vol. 27, no. 6, pp. 581–612, 2019. https://doi.org/10.3233/JCS-181253

[23] S. Das, C. Nippert-Eng, and J. L. Camp, "Evaluating user susceptibility to phishing attacks," *Information & Computer Security*, vol. 30, no. 1, pp. 1–18, 2022. https://doi.org/10.1108/ICS-12-2020-0204

[24] S. Sheng *et al.*, "Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish," in *Proceedings of the 3rd Symposium on Usable Privacy and Security*, 2007, pp. 88–99. https://doi.org/10.1145/1280680.1280692

[25] Softdebut, "Revealing the most shocking statistics! Phishing can hurt you more easily than you think," *Know the Hidden Dangers in the Digital World*, 2023. https://www.softdebut.com/blog/phishing-scams-digital-world-risks

[26] S. Papadakis, "Evaluating a game-development approach to teach introductory programming concepts in secondary education," *International Journal of Technology Enhanced Learning*, vol. 12, no. 2, pp. 127–145, 2020. https://doi.org/10.1504/IJTEL.2020.106282

[27] S. Papadakis, A. M. Trampas, A. K. Barianos, M. Kalogiannakis, and N. Vidakis, "Evaluating the learning process: The 'ThimelEdu' educational game case study," in *Proceedings of the 12th International Conference on Computer Supported Education (CSEDU 2020)*, 2020, vol. 2, pp. 290–298. https://doi.org/10.5220/0009379902900298

[28] T. Chutosri, T. Uipanit, P. Kingsuwankul, M. Opanapan, N. Preechapongcharoen, and T. Suthiapa, "The development of gaming application to facilitate resource center," in *Proceedings of the 8th International Conference on Informatics, Environment, Energy and Applications*, 2019, pp. 73–77. https://doi.org/10.1145/3323716.3323749

[29] T. Uiphanit, K. Suanpong, and P. Bhattarakosol, "A short survey for Thai teenager's attitudes towards game-play learning," *Research Gate*, 2017. https://www.researchgate.net/publication/334451245

[30] T. Uiphanit, P. Bhattarakosol, K. Suanpong, S. Iamsupasit, and C. Wongwan, "Chibumons: A positive effect on game to undergraduate students," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 15, no. 1, pp. 222–230, 2020. https://doi.org/10.3991/ijet.v15i01.11502

[31] J. Tay, Y. M. Goh, S. Safiena, and H. Bound, "Designing digital game-based learning for professional upskilling: A systematic literature review," *Computers & Education*, vol. 184, pp. 1–15, 2022. https://doi.org/10.1016/j.compedu.2022.104518

[32] The Anti-Phishing Working Group, "Phishing activity trends report 2nd Quarter 2024," 2024. https://apwg.org/trendsreports/

[33] V. H. Carvalho, T. Martins, F. Soares, and M. Araújo, "Total challenge: A serious game for stimulating cognitive abilities," *International Journal of Advanced Corporate Learning (iJAC)*, vol. 9, no. 1, pp. 4–11, 2016. https://doi.org/10.3991/ijac.v9i1.4903

## 12 AUTHORS

**Asst. Prof. Dr. Thanakorn Uiphanit** is currently a Lecturer in the Department of Digital Innovation and Content Management, Faculty of Science and Technology, Suan Sunandha Rajabhat University, Bangkok, Thailand (E-mail: thanakorn.ui@ssru.ac.th).

**Thatsanan Chutosri** is currently a Lecturer in the Department of Digital Innovation and Content Management, Faculty of Science and Technology, Suan Sunandha Rajabhat University, Bangkok, Thailand (E-mail: thatsanan.ch@ssru.ac.th).

**Natcha Wattanaprapa** is currently a Lecturer in the Department of Digital Innovation and Content Management, Faculty of Science and Technology, Suan Sunandha Rajabhat University, Bangkok, Thailand (E-mail: natcha.wa@ssru.ac.th).

**Wannarat Bunchongkien** is currently a Lecturer in the Department of Digital Innovation and Content Management, Faculty of Science and Technology, Suan Sunandha Rajabhat University, Bangkok, Thailand (E-mail: wannarat.bu@ssru.ac.th).

**Phachaya Chiewchan** is currently a Lecturer in the Department of Digital Innovation and Content Management, Faculty of Science and Technology, Suan Sunandha Rajabhat University, Bangkok, Thailand (E-mail: phachaya.ch@ssru.ac.th).

**Dr. Nipon Nachin** is currently a Chief Executive Officer, ALPHASEC Co. Ltd, Bangkok, Thailand (E-mail: nipon@alphasec.co.th).