

How Can Mechanics Stimulate Behaviour, Motivation, and Engagement Levels in Learning and Training Applications?

Phillip Benachour and Carina Chang

School of Computing and Communications, Lancaster University, UK

p.benachour@lancaster.ac.uk

carinachangyy@gmail.com

Abstract: This aim of this paper is to report on a preliminary research study investigating a quiz-based cyber awareness game-based application and its impact on consumers' knowledge, awareness, and behaviour regarding e-commerce fraud and scams. A pilot inter-group experiment involving N=46 participants was conducted to gauge users' attitudes, behaviour and motivation towards protection from e-commerce fraud and online scams. Participants chose between a traditional quiz (control group = 16) and a quiz-style role-playing game (treatment group = 30). The effectiveness of the game application was evaluated using the risk behaviour diagnosis (RBD) methodology. Results of the experiment show that interest in games, e-commerce usage frequency, and fear of victimisation are the key motivators for the treatment group to improve their awareness of e-commerce fraud and scam prevention. From a design perspective, calibrating and balancing game mechanics is essential to maintaining user motivation and engagement. The design of the application focused on four key techniques: flow, meaningful choices, incentives, and task duration. This work in progress paper discusses and reflects on how these techniques were utilised in the design process of the features cards (i.e. Tutorial cards, Shield cards, Shield Cards) of the gamified application; and how its associated rewards were effective for learner motivation and overall game experience. Based on an additional pilot study, feedback from the treatment group (N=30) on the game's mechanics showed that 86.7% of the players felt that the feature cards offered them sufficient freedom to progress during the game. Further, 33.3% of the players found the choices afforded were meaningful, and 46.7% of the players viewed the choices given as quite meaningful. The user study results and proposed balanced mechanics techniques can provide insights to broader applications designs related to micro-credentials and gamified applications for professional training. Based on research into learner engagement, we explore how flow, meaningful choices, incentives, and task duration can be applied to stimulate behaviour, motivation, and engagement levels.

Keywords: Game-based learning, Cyber hygiene, Adult Learning theory, Risk behaviour theory

1. Background and Research Motivation

Cyber-enabled fraud and scam incidents pose major global cybercrime concerns. The UK Finance reported £485 million losses from authorized pushed payment ("APP") fraud in 2022 and £239 million in the first half of 2023 (Fitchratings.com, 2024). In tackling the problem of e-commerce fraud and scams, the burden is often placed on the organisations (e.g. banks, mobile app developers, social media companies, cloud services provider) (Psr.org.uk, 2023). Additionally, the attention is also focused on technological enhancements (e.g. enhancing authentication and encryption technologies used in mobile payment systems) (Liu, Wang and Peng, 2020). However, no system control and application design can be flawless or immune to vulnerabilities exploitations. Research shows that humans can be considered as one of the weakest links in the cybersecurity chain (Zwilling et al., 2020). For this reason, cybersecurity awareness campaigns and cybersecurity training are widely recommended (UK Finance, 2022). These approaches have been adopted by many governments. However, the present approaches are in-sufficient; partially due to the lack of engagement during traditional cybersecurity training or that the individuals find the training to be overly time-consuming (Australian Competition and Consumer Commission, 2023). Information overload is also problematic with the existing methods in improving awareness (Tang, 2024). The above reveals the inadequacy in the current measures against e-commerce fraud and scams. Consequently, there is an urgent need to explore alternative solutions to safeguard consumers and organisations.

The aim of this study is to examine whether game-based-learning and gamified learning applications as an approach, can increase consumers' awareness and knowledge on e-commerce fraud and scams and subsequently encourage behavioural change. The user study results and proposed balanced mechanics techniques could provide insights to broader applications designs for professional training. Based on research into learner engagement, we explore how flow, meaningful choices, incentives, and task duration can be applied to stimulate behaviour, motivation, and engagement levels. Previous research has shown that gamification has emerged as a natural complement to microlearning, given their shared emphasis on engagement and learner motivation (Malamed, 2012). Gamification can be integrated effectively to enhance microlearning by adding motivational mechanics, such as rewards, challenges, elements that promote sustained learning (Sailer and Homner, 2019). In addition, the provision of immediate and timely feedback is a

key mechanism for gamification to learner engagement (Näsi, Danielsson and Kaakinen, 2021). Several studies have demonstrated that learners retain more information and remain more engaged when they receive prompt responses to their actions during a learning activity. According to Sailer and Homner, immediate feedback allows learners to quickly recognize and correct mistakes, contributing to improved learning outcomes and sustained motivation.

2. Game Prototype

To satisfy the game mechanics and the four balancing techniques, the scenarios created are based on a narrative that focusses on a shopping challenge within an organization (i.e. Elephant Impact) in preparation for their staff summer party. Players are given a fixed character (i.e. Lauren) who must contest with fictitious colleagues from other departments in a shopping challenge. The winner will be decided based on whether the player emerges as the champion by purchasing the greatest number of items from the party's shopping lists. The players can earn money (credits) by learning acquiring knowledge on identifying “threats” relating to e-commerce fraud and scams. Players can use “shields” to *charge-back* their resources when required and a “tutorial” to reinforce their learning.

The three main deck cards shown in Figure 1 are used to connect the four balancing techniques described. Figure 2 and Figure 3 show the expanded versions of the “threat” and “shield” deck cards respectively. Players can earn points in exchange for additional lives by learning new protective measures against e-commerce fraud and scams. Players must earn sufficient credit and pass the quiz challenge correctly before they can purchase any items on their allocated shopping list. If they fail the quiz challenge, they lose credit or a life. The game narrative is based on a visual interactive dialogue. To win the game, a player must complete all three stages of the story.



Figure 1: Card action decks used in the game



Figure 2: Threat information deck example



Figure 3: Shield information deck example

In addition to the threat, shield and tutorial decks, a player is presented with a “secret mission” (see Figure 4) as an additional option to encourage players to learn and explore more within the game. For instance, a secret mission is placed within Stage 2’s Tutorial Deck. It is triggered when the More button is selected. Another secret mission is placed in Stage 3’s Shield Deck. The player will only discover this mission if he or she continues to explore more Shield tips by clicking on button number 6. There is no identifiable pattern where the secret missions are placed, to preserve the surprise element. Special sound effect was also added to bolster the mystical feel.



Figure 4: Secret mission example

3. Research Design and Data Collection Methods

It was shown that consumers who are at a higher risk of falling for e-commerce fraud and scams have an age range of 18-54 years old (Fitchratings.com, 2024). As a result, the pilot study target audience were selected from this age group. A mixed-methods survey collected both quantitative and qualitative data. A total of 30 participants (N=30) completed the questionnaire. Ethical approval was granted by the academic department and university. To adjust to word limitations of this paper, we present the quantitative subset of our user feedback, which was converted into numerical data via a 5-point Likert scale (see Figures 5–7). Participants from a wide range of nationalities and backgrounds were recruited and surveyed online over a 2–3-week period. The corresponding qualitative results will be presented at the main session to offer additional insights.

The questionnaire evaluates participants' post-game experience. It collected data about play duration, usability, enjoyment, and perceived learning. Further, it examined the motivational value of specific game mechanics, including credit rewards, chargeback points, and the perceived educational importance of the “threat”, “shield”, and “tutorial” feature cards. The questionnaire also explores player agency, favourite and frustrating aspects of the game, repetition, and suggested game-play improvements. Overall, the questionnaire is designed to capture both quantitative indicators of usability and perceived learning, and qualitative feedback to inform future game refinement.

4. Results and Evaluation

4.1 Game Experience

Figure 5 presents the overall game experience feedback results. The game demonstrates highly engaging gameplay as educational tool, with 90% of players learning anti-fraud tips. However, usability and some

engagement gaps remain. Additionally, male players found it easier to navigate (4.2/5 vs 3.8/5), while the overall "fun" rating was moderate (3.6/5), indicating that game mechanics require refinement.

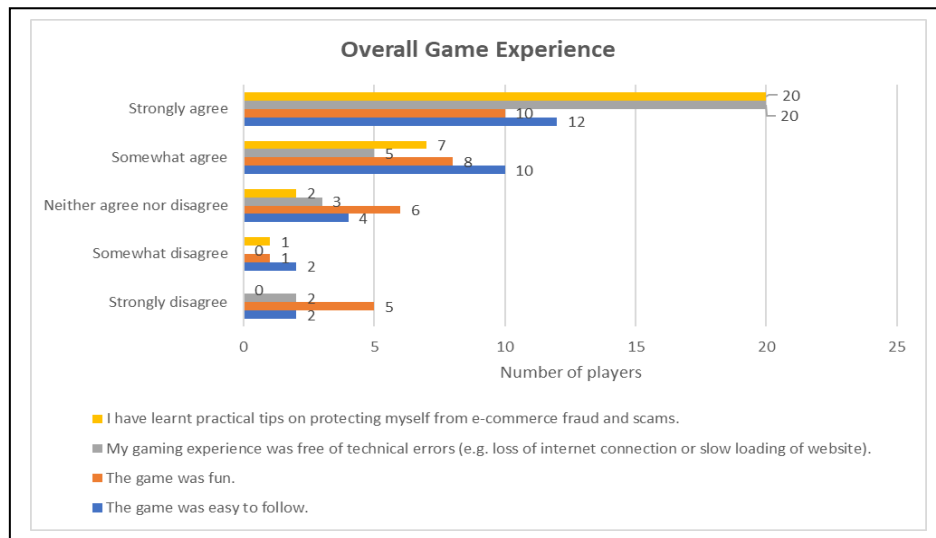


Figure 5: Overall game users game experience

4.2 Game Element and Learning

The positive feedback on the feature cards: threat, shield, tutorial, demonstrates that aligning the specific in-game rewards with learning objectives coupled with flow, meaningful choices, incentives, and task duration as game mechanics balancing techniques engages players effectively and promotes educational outcomes.

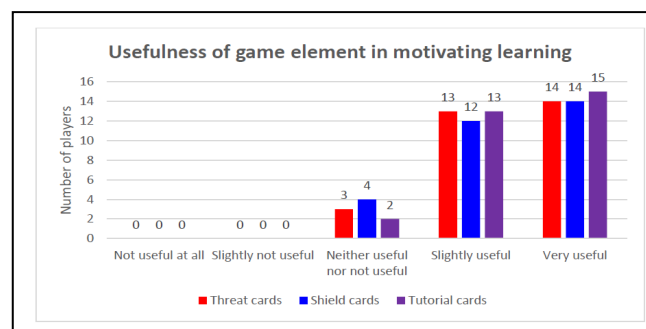


Figure 6: Usefulness of game elements in motivating learning

Participants found "threat" and "tutorial" cards most helpful for learning, while "shield" cards were least important. This discrepancy stems from the game's incentives: players prioritized cards that directly helped them gather credits for their shopping lists, and lost interest in "shield" cards once minimum requirements were met. Immediate qualitative feedback after each quiz question enabled players to verify and correct their fraud prevention knowledge, making it more effective than passive reading. It is worth noting that Players soon discovered that "threat" and "tutorial" cards provide the feedback and credit needed to reach their goal.

Player perception of tutorial cards was split, with ratings influenced by the interaction between user interface layout and pedagogical engagement. While the right-side positioning caused some users to disregard the cards due to left-to-right reading habits, others valued them highly for their interactive, "mini-game" style content that aligned with adult learning principles. The full research analysis is available for review.

Player opinions on the value of "tutorial" cards were split. Their importance was rated lowest by 15 players, while 10 rated them highest. This split is influenced by two main factors: screen layout, and interactive design. For screen layout, the "tutorial" cards were placed to the right of the "threat" and "shield" cards. While the right-side positioning caused some users to disregard the cards due to left-to-right reading habits (players often selected and purchased the necessary items first, losing interest in the tutorial cards by the time they reached them), others valued the "tutorial" cards highly for their interactive, "micro-game" style content that aligned with adult learning principles. For interactive design, the "tutorial" cards acted as engaging "mini

games" with real-life context. This interactivity and real-world alignment engaged one-third of the players, making the cards highly valued by that group.

4.3 Game Mechanics

Players were asked to provide feedback on the game mechanics affecting freedom, meaningful choices, flow, and perception of game-length (shown in Figure 7). Most players, 86.7%, reported high levels of freedom to progress using the feature cards, but the game's choice mechanics were perceived as lacking significance due to a feedback mechanism that revealed correct answers. To enhance meaningful play decision-making and increase challenge, implementing a reward mechanism for initial attempts or costs for viewing solutions is recommended. This might be more attractive to players who prefer a cost-associated variant, instead of getting direct answers.

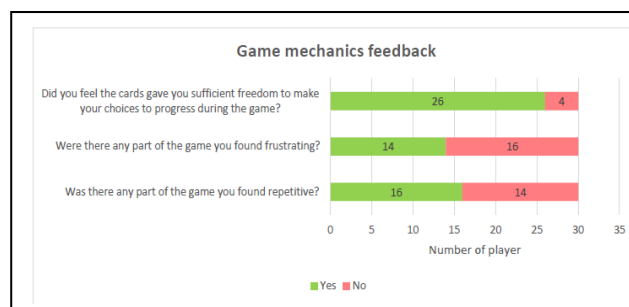


Figure 7: Game mechanic's feedback

5. Discussion

While most quantitative results and their analysis show that some game mechanics require further improvements, most of the participants found all feature cards to be very useful. This demonstrates that the gaming features tied to the learning objectives were well received and were instrumental in maintaining gameplay *flow*. However, limitations related to *meaningful choices* have been observed. There appears to be less incentive for players to harvest chargeback points using the "shield" deck. Players have realized quickly that they can collect sufficient credit using the "threat" and "tutorial" cards and reach their goal. This could be influenced by the game's incentive structure (to acquire most items from the shopping list). There could be a disparity when designing to balance *meaningful choices* *v* *incentives*. Further investigation is required to adjust meaningful play and avoid the game becoming more predictable.

In summary, there are clear areas to adjust and improve to attain a balance of the mechanics. Given the incentives associated with behaviour change, maintaining user engagement is key as well as task and game duration. Given the conducted pilot study, the aim is to run a longitudinal study to improve balance adjustments, particularly between *meaningful choices* *v* *incentives*.

References

- Australian Competition and Consumer Commission (2023). ACCC calls for united front as scammers steal over \$3bn from Australians. [online] [www.accc.gov.au](https://www.accc.gov.au/media-release/accc-calls-for-united-front-as-scammers-steal-over-3bn-from-australians). Available at: <https://www.accc.gov.au/media-release/accc-calls-for-united-front-as-scammers-steal-over-3bn-from-australians>.
- Fitchratings.com. (2024). Available at: <https://www.fitchratings.com/research/banks/fraud-reimbursement-costs-are-likely-to-rise-for-uk-banks-18-01-2024>.
- Malamed, C. (2012). Book Review: 'The Gamification of Learning and Instruction: Game-Based Methods and Strategies For Training And Education' by Karl Kapp. *eLearn*, 2012(5), p.3. doi:<https://doi.org/10.1145/2207270.2211316>.
- Näsi, M., Danielsson, P. and Kaakinen, M. (2021). Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*. doi:<https://doi.org/10.1007/s10610-021-09497-0>.
- Liu, W., Wang, X. and Peng, W. (2020). State of the Art: Secure Mobile Payment. *IEEE Access*, 8, pp.13898–13914. doi:<https://doi.org/10.1109/access.2019.2963480>.
- Psr.org.uk. (2023). CP22/4: Authorised push payment (APP) scams: Requiring reimbursement. [online] Available at: <https://www.psr.org.uk/publications/consultations/cp22-4-app-scams-requiring-reimbursement/>
- Sailer, M. and Homner, L. (2019). The Gamification of Learning: a Meta-analysis. *Educational Psychology Review*, [online] 32(1), pp.77–112. doi:<https://doi.org/10.1007/s10648-019-09498-w>.

- Tang, L. (2024). Scam cases in Singapore jumped almost 50% in 2023; most victims fell for job, e-commerce cons. [online] CNA. Available at: <https://www.channelnewsasia.com/singapore/scams-2023-increase-50-percent-job-e-commerce-measures-4128051>.
- UK Finance (2022). *The definitive overview of payment industry fraud in 2022*. [online] Available at: https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf.
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, [online] 62(1), pp.1–16. doi:<https://doi.org/10.1080/08874417.2020.1712269>.