PROPOSAL FOR A SERIOUS GAME ON THE THEME OF PERSONAL INFORMATION

Rin Kokubo and Jun Iio
Faculty of Global Informatics, Chuo University
1-18 Ichigaya-tamachi, Shinjuku-ku, Tokyo 162-8478, Japan

ABSTRACT

With the advent of the Internet, our society has evolved into a place where personal information can be easily shared and collected. To explore people's attitudes towards this reality, we developed an interactive online game to analyze these attitudes and promote digital literacy. We conducted a survey with 36 university students using this game. This paper provides an overview of the game, details the experiment, and discusses the findings.

KEYWORDS

Serious game, Personal information, Privacy, Gamification

1. INTRODUCTION

With the widespread use of information and communication networks, along with the accelerated expansion of information processing capabilities, the handling of vast amounts of personal information has become a reality. However, this has also amplified concerns over the potential leakage and misuse of privacy-related information. Advances in search technology have further complicated matters, as even fragmented pieces of information available publicly on the Internet can be pieced together with other data to increase the probability of identifying individuals. These issues underscore the crucial need for privacy protection in the digital era.

Therefore, we sought to investigate people's awareness and understanding of privacy issues. Instead of utilizing a traditional questionnaire, we developed an interactive game centered around personal data. By leveraging this engaging format, our goal was to stimulate individual involvement in privacy issues based on their personal experiences and enhance their overall digital literacy on the topic.

2. GAME STRUCTURE AND RULES

In the development of games centered around personal information, incorporating the viewpoints of those who might exploit such information is crucial. Games uniquely offer role-playing experiences that aren't typically encountered in day-to-day life. Thus, we designed a game format in which participants, acting as either the holders of personal information (defenders) or those attempting to exploit it (attackers), engage in competition.

The attacker is given three cards, each depicting a different scenario of information exploitation, from which they choose one. Conversely, the defender possesses five cards, each assigned a set score corresponding to the card chosen by the attacker. Without knowing the content of the attacker's selected card, the defender must decide on three cards to reveal. This arrangement mirrors real-world scenarios where a potential offender cannot fully anticipate the details of their prospective offense; in our game, the information is unveiled under conditions where the opponent doesn't know the specifics of the selected card.

The attacker's score is computed as the total points of the three cards passed on by the defender, while the defender's score is calculated as the sum of the points from the two remaining cards in their hand.

An overview of the game is depicted in Figure 1.

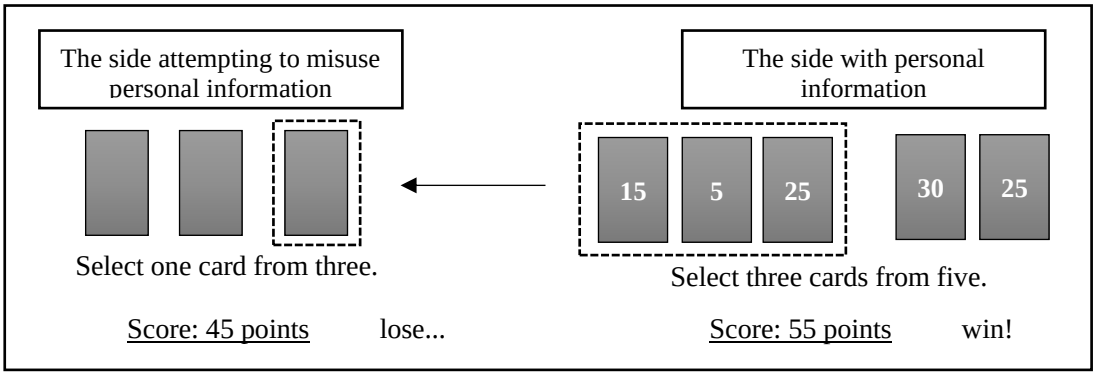

Figure 1. Game rule

3. OVERVIEW OF THE GAME SYSTEM

This section presents the game's system architecture and flowchart. Our game was developed as a web application, enabling online player interaction, and streamlined data collection.

Figure 2 provides a schematic representation of the system's architecture. The database meticulously captures all player decisions and the resulting game outcomes.

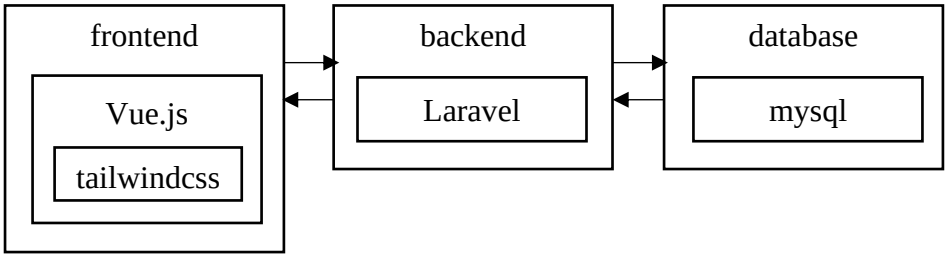

Figure 2. System configuration

The gameplay sequence is depicted in the flowchart provided (refer to Figure 3). Participants have the option to assume roles as either attackers or defenders.

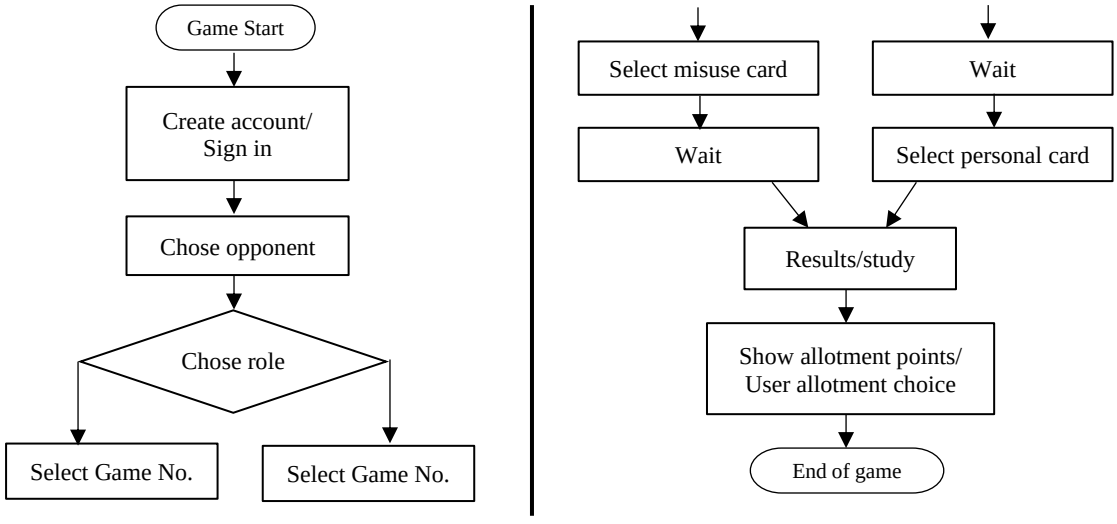

Figure 3. Game progression chart

4. OUTLINE OF EXPERIMENTS AND ANALYSIS OF RESULTS

This section delineates the conducted experiments and the ensuing analysis of the outcomes. Our experimental findings are further contextualized with comparisons to public opinion surveys concerning personal information, as provided by the Japanese government.

4.1 Outline of Experiments

We conducted two experiments: an initial trial in June 2022 with 12 students, and a subsequent one in December with 24 participants. Data was collected from 24 games in the first trial and 72 in the second. Prior to and following the experiments, participants completed a questionnaire on information literacy and game experience.

4.2 Analysis of Results

Table 1 summarizes the results of 93 valid matches from the first and second experiments. (Three games were excluded due to system issues rendering the results invalid.)

Table 1. Win rage by role

Role	Win	Lose	Draw	Win Rate
Attacker	67	21	5	0.72
Defender	21	67	5	0.23

The results indicate a higher winning rate for the attackers, as anticipated given their advantage of acquiring more cards towards the end.

Subsequently, we evaluated players' reluctance to share various personal information by analyzing the percentage of players unwilling to disclose each piece.

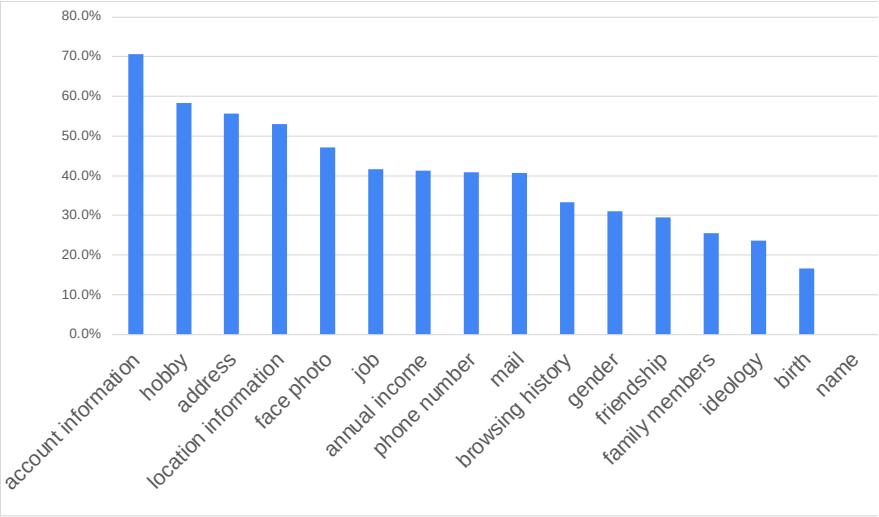

Figure 4. Percentage of players who did not want others to know

Figure 4 presents the types of personal information that players were most reluctant to share, ranked from most to least private: account information, hobbies, and addresses. On the other hand, participants were more comfortable with sharing information such as their names, dates of birth, and ideologies.

4.3 Comparison of Public Opinion Polls and The Results of The Experiment

In 2006, a public opinion survey conducted by the Japanese government (Cabinet Office of Japan, 2006) yielded results somewhat like our study. The survey found that 88.7% of respondents were most unwilling to disclose account and credit card numbers, making it the most guarded piece of personal information. Coming second was annual income, property status, and tax payments (74.2%), followed by photographs of faces (53.3%).

A noteworthy divergence between the government survey and our study concerns the data on hobbies. In our survey, hobbies emerged as the second most protected category of information among college student participants, which was an unexpected outcome. Although knowing an individual's hobbies can increase the chances of falling prey to crimes such as phishing scams and fraudulent websites, our data suggested that the high level of reluctance to share hobbies was not necessarily driven by crime-related fears. Rather, many individuals consider their hobbies to be a private matter.

5. RELATED WORK

Antonaci et al. (2017), Sailer et al. (2020), and Oroszi (2020) have all demonstrated the efficacy of gamification in education and security awareness, highlighting its role in enhancing IT literacy, student engagement, learning outcomes, and user security awareness.

Liz-Domínguez et al. (2020) and Smiderle et al. (2020) both explored the impact of gamification in educational contexts. While the former used gamification to collect data to improve education, the latter showed the effects of gamification varied according to students' personality traits. Differently, our study implements gamification to assess attitudes towards personal information, in addition to providing literacy education.

6. CONCLUSIONS

While there is no legislation categorizing hobbies as personal information, societal perceptions may not align with current regulations. With advancements in technology, one's hobbies can now be discerned from search histories, social media analytics, purchase records, and behavioral patterns. These developments warrant a reassessment of what constitutes personal information in the digital age. Although our study focused on Japanese university students, we plan to broaden the scope to include international and multi-generational participants, leveraging the global and cross-generational appeal of online gaming. This study also lays the foundation for a novel game-based awareness survey methodology, positioning the game as a competitive card-style activity.

REFERENCES

Antonaci, A., Klemke, R., Stracke, C. M., Specht, M., Spatafora, M., and Stefanova, K. (2017). Gamification to Empower Information Security Education. *In P. Tuomi, & A. Perttula (Eds.), Proceedings of the 1st International GamiFIN Conference (Vol. 1857, pp. 32-38). CEUR Workshop Proceedings (CEUR-WS.org)*

Cabinet Office of Japan (2006). Public Opinion Poll on Personal Information Protection. (in Japanese)

Liz-Domínguez. M., Caeiro-Rodríguez. M., Llamas-Nistal. M., and Mikic-Fonte. F. (2022). Exploring the Synergies between Gamification and Data Collection in Higher Education. *Learning Analytics Summer Institute Spain (LASI Spain)* 2022.

Oroszi. E. D., (2020). Using Gamification to Improve the Security Awareness of Users: The Security Awareness Escape Room. *ISACA Journal,* Volume 4, 2020.

Sailer, M. and Homner. L. (2020). The Gamification of Learning: a Meta-analysis. *Educational Psychology Review* 32, 77-112.

Smiderle, R., Rigo, S. J., Marques, L. B., Coelho, J. A. P. M., and Jaques., P. A. (2020). The impact of gamification on students' learning, engagement and behavior based on their personality traits. *Smart Learning Environments* volume 7, Article number: 3