Gamification Software to educate against Cyber Addiction and Digital Threats

1st Alexander Rangel V.
Mathematics
Universidad del Norte
Barranquilla, Colombia
alexanderrangel@uninorte.edu.co
Rol: *Project Manager*

2nd Jose Peña C.
Systems engineering
Universidad del Norte
Barranquilla, Colombia
pjosed@uninorte.edu.co
Rol: *UI Manager*

3rd Alejandro Cuello N.
Systems engineering
Universidad del Norte
Barranquilla, Colombia
mcalejandro@uninorte.edu.co
Rol: *Design Director*

4rd Ana Meza G.
Mathematics
Universidad del Norte
Barranquilla, Colombia
mezaana@uninorte.edu.co
Rol: *Documentation Manager*

5rd Julian Castro C.
Mathematics
Universidad del Norte
Barranquilla, Colombia
cjcalvo@unionrte.edu.co
Rol: *Test Manager*

Final project on object-oriented programming (NRC 2139) and data structure I (NRC 2145).
Department of Systems Engineering

DOI: 10.1109/JPHOT.2009.XXXXXXX
1943-0655/$25.00 ©2009 IEEE

Abstract: This project addresses the growing need to educate teenagers on digital security practices and emotional well-being through an interactive video game inspired by the style of ”My Talking Tom.” In the game, the protagonist is a cat who faces various situations in different scenarios, tackling key topics such as spoofing, phishing, and cyber addiction. Players must help the cat make appropriate decisions to maintain its self-esteem bar, which ranges from 0 to 100. A low score indicates sadness, an intermediate score reflects neutrality, and a high score represents happiness. Unlike traditional games, there are no absolute right or wrong answers; each option has a level of suitability that impacts the character's emotional stability. The methodology included designing realistic scenarios and adaptive scoring response options. The results indicate that teenagers develop greater awareness of digital risks and how to address them. In conclusion, this video game has the potential to serve as an effective and engaging educational tool to promote safe practices in the digital environment. (Results and conclusion are missing.)

1. Introduction

In today's digital era, teenagers are constantly exposed to the dangers of cyberspace, such as spoofing, phishing, and cyber addiction—issues that affect both their online security and emotional well-being. Despite the relevance of these topics, many young people lack the necessary education to identify and react appropriately to these risks, which can negatively impact their personal development and self-esteem. This project proposes the development of an interactive video game that, through a playful and accessible format, seeks to raise awareness among teenagers about the importance of digital security and emotional health management.

The video game presents an everyday scenario where players must help a character, a cat similar to ”My Talking Tom,” face situations related to digital risks in different settings. During

gameplay, the cat interacts with the player, whose mission is to guide it in making decisions that will affect its self-esteem bar, reflecting its emotional stability. Response options vary in suitability, encouraging players to think critically about the best way to handle the problems. This design provides a flexible and realistic approach tailored to situations teenagers may encounter in their daily lives.

The primary objective of this project is to create an interactive learning tool that promotes cybersecurity practices and emotional self-management in a digital context. By using game design methodologies oriented toward education and adaptive decision-making development, this game offers an educational experience that could be integrated into school programs to foster informed and responsible digital citizenship among young people.

2. Related Work

This project explores topics such as cybercrimes and cybersecurity, particularly in the context of an educational video game aimed at raising awareness of online risks, including phishing, identity theft, cyber addiction, and the responsible use of Information, Communication, and Relationship Technologies (ICRT). A relevant study validated a cybercrime awareness scale among university students, highlighting factors like phishing, spamming, antivirus effectiveness, and online bullying (Ramírez et al., 2022). A 20-item questionnaire was applied to 372 students, revealing difficulties in identifying fraudulent sites and a lack of familiarity with data protection practices. Engineering students demonstrated greater awareness compared to other faculties, likely due to their technical training and familiarity with cybersecurity topics. The scale's high reliability (Cronbach's alpha of 0.892) makes it useful for measuring and improving preparedness against cyber threats.

Regarding identity theft, another study addressed this issue on social media, where cybercriminals use phishing techniques to steal credentials through fraudulent emails (INCIBE, 2023; Harán, 2020). The importance of implementing two-step authentication was emphasized, as studies by Google and Microsoft showed that it can block up to 99

The relationship between identity theft and phishing was investigated in another study, which described how both methods are used together to commit financial fraud or damage victims' reputations (Pedrero Zornoza, 2020). To delve deeper into the issue, laws and jurisprudence on unauthorized system access and disclosure of secrets were reviewed. The study concluded that the lack of security measures, such as two-step authentication, facilitates these crimes and highlighted the need for reforms in the Penal Code to address identity theft in digital environments.

On the other hand, a project related to cyber addiction and other digital risks used the Service-Learning (SL) methodology with secondary school students to raise awareness about cyberbullying, grooming, and sexting. Fourth-year students trained their first-year peers using collaborative materials, increasing awareness of cyber addiction and promoting the responsible use of ICRT. The evaluation phase showed significant improvements in students' perceptions of digital risks and the importance of healthy leisure options.

These studies and projects underscore the importance of addressing cybercrimes and digital security comprehensively, proposing education, security measures, and legislative reforms as pillars for protection in the online environment.

3. Methodology

3.1. Technological Proposal

This report presents a technological proposal for developing an interactive game addressing relevant issues like cyber addiction, phishing, and spoofing. The goal of the game is to raise players' awareness of these problems through the story of a cat whose happiness depends on the player's decisions in various situations.

3.2. Functional Requirements

- **Cat's Mood:** The cat has a happiness level influenced by the player's decisions.
- **Player Interaction:** The player selects from various options in five different situations, affecting the cat's happiness.
- **Final Evaluation:** After five rounds, the game determines if the cat has maintained a good mood and awards points based on the player's score.
- **Save Progress:** Players can enter their names and save their progress for future game sessions.
- **Leaderboard:** A section displays a leaderboard based on players' scores.

3.3. Non-Functional Requirements

- **Functionality:** The game offers various responses and their corresponding consequences on the cat's state.
- **Usability:** The interface is user-friendly and easy to navigate, enabling players of all ages to interact effortlessly.
- **Support:** A mechanism allows players to save games and retrieve information easily.
- **Error Handling:** User inputs are validated, such as empty name fields or invalid names.

3.4. Class Diagram

The class diagram illustrating the structure and relationships between the game's entities is presented below:

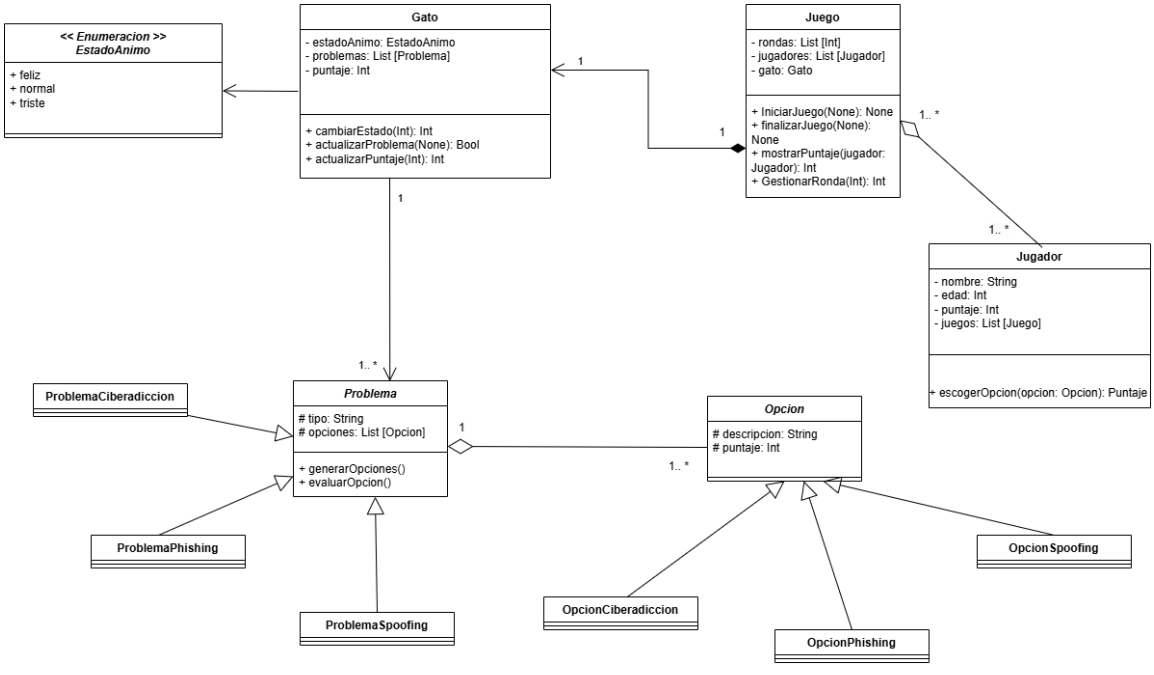

Fig. 1. Class Diagram of the Game.

3.5. Language and Platform

The game was developed in Java using NetBeans as the Integrated Development Environment (IDE). Java was chosen for its portability, robustness, and extensive support community. NetBeans facilitated coding, debugging, and creating an attractive graphical interface.

4. Results

In this section, evidence of the functionality of the developed software, the use of data structures, performance indicators, and a usability test conducted with users to evaluate the interface and overall gameplay experience are presented.

4.1. Functionality Evidence

Fig. 2. Main menu of the game.

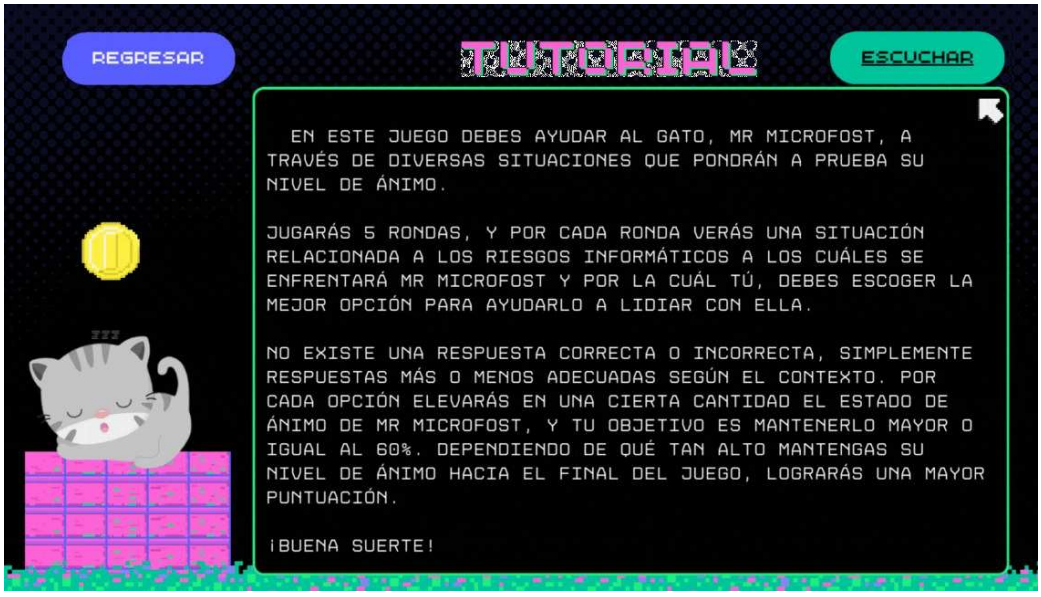

Fig. 3. Game tutorial.

Fig. 4. Gameplay of *Guide to Microfost*.

4.2. Usability Test

To evaluate the user experience, a usability test was conducted based on the guidelines from Maze and the Nielsen Norman Group:

4.2.1. Test Setup

A group of 20 teenagers aged between 13 and 18 years was selected. The participants played five rounds of the game and subsequently completed a survey.

4.2.2. Evaluated Metrics

- **Task success rate:** 91% of participants successfully completed all five rounds of the game.
- **Error rate:** Less than 30% of users experienced difficulties navigating the interface.
- **Satisfaction level:** On a scale from 1 to 5, the game achieved an average satisfaction score of 4.3.

4.2.3. Key Findings

Participants appreciated the simple yet appealing interface and found the scenarios realistic and relevant to their daily lives. Some improvement suggestions included adding customization options and expanding the available scenarios.

4.3. Summary of Results

The results demonstrate that the video game meets its functional and educational objectives, successfully capturing user attention and raising awareness about digital risks and emotional health. The usability test confirmed that the interface is intuitive and the game mechanics are engaging. However, to enhance the experience, it is recommended to expand the content and add new features in future versions.

5. Conclusions

The development of the video game has provided an interactive and educational approach to cybersecurity and emotional health topics for teenagers, meeting the functional and non-functional requirements outlined in the initial proposal. The results demonstrate that the project has the

potential to positively impact teenagers' awareness of cyberspace risks and promote responsible digital citizenship. Below are the main points of analysis:

Meeting the Requirements

- The video game implements a gameplay mechanic that allows for evaluating the impact of the player's decisions on the cat's emotional state, fulfilling the defined functional requirements, such as the mood bar, scenario interaction, and score ranking.
- The interface and gameplay are accessible and user-friendly, ensuring a pleasant experience for players of various skill levels.
- Additional functionalities, such as the narrated tutorial and the ability to save progress, make the game inclusive and adaptable to different contexts.

Impact on the Target Area

- **Cybersecurity Education:** The game provides an innovative medium to raise awareness among teenagers about critical topics such as phishing, spoofing, and cyber addiction, helping them identify and respond appropriately to these issues.
- **Emotional Reflection:** The game's mechanics encourage responsible decision-making by linking choices to the character's emotional stability, which can strengthen players' emotional self-management skills.

Identified Limitations

- **Content Scope:** The scenarios presented in the game may be limited compared to the diversity of digital risks that teenagers face in their daily lives.
- **Technological Dependency:** Access to the game is restricted to those with the necessary devices, which could limit its impact in communities with reduced access to technology.

Future Improvements

- **Expanding Scenarios:** Include more situations related to cybersecurity and emotional health, such as managing time on social media or handling online conflicts.
- **Game Customization:** Implement the possibility of customizing the cat or the environment, which could enhance player immersion.
- **Data Analysis:** Incorporate an analytics system to measure the educational effectiveness of the game based on player behavior and decisions.
- **Multiplatform Availability:** Develop versions of the game for mobile devices and web browsers, expanding its reach.

In conclusion, *"Guide to Microfost"* represents an innovative and promising tool for educating teenagers about cybersecurity and emotional health in a digital context. While the project meets the initial objectives, future improvements and content expansion could further enhance its long-term impact in the educational field.

References

1 Cobacango, M. J., Cedeño, V. P., & Tinoco, M. G. (2019). La ciberadicción en la conducta de los estudiantes. Revista Atlante: Cuadernos de Educación y Desarrollo, 11763, 1-13. https://www.eumed.net/rev/atlante/2019/07/ciberadiccion-estudiantes.zip

2 Díaz-López, A., Maquilón, J. J., & Mirete, A. B. (2020). Uso desadaptativo de las TIC en adolescentes: Perfiles, supervisión y estrés tecnológico. Revista Científica de Educomunicación, (64), 29-38. https://dialnet.unirioja.es/servlet/articulo?codigo=7486697

3 Harán, J. M. (2019, mayo 21). Doble factor de autenticación: la solución más efectiva para prevenir el secuestro de cuentas. WeLiveSecurity.

https://www.welivesecurity.com/la-es/2019/05/21/doble-factor-autenticacion-solucion-seguridad-mas-efectiva/

4 Harán, J. M. (2020, marzo 11). El 99,9% de las cuentas vulneradas no utilizan doble factor de autenticación. WeLiveSecurity. https://www.welivesecurity.com/la-es/2020/03/11/mayoria-cuentas-vulneradas-no-utilizan-doble-factor-autenticacion/

5 INCIBE. (2023, abril 4). Suplantación y robo de identidad en las redes sociales, un riesgo para las empresas. INCIBE. https://www.incibe.es/empresas/blog/suplantacion-y-robo-identidad-las-redes-sociales-riesgo-las-empresas

6 MJA, M. d. J. (2024, febrero 14). ¿Cómo me doy cuenta si un perfil es falso en Facebook? Argentina.gob.ar. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-detecto-un-perfil-falso

7 Pedrero Zornoza, J. (2020). Suplantación de identidad. Trabajo Fin de Grado, Universidad Miguel Hernández de Elche, Facultad de Ciencias Jurídicas y Sociales. https://dspace.umh.es/handle/11000/27041

8 Ramírez Asís, E. H., Norabuena Figueroa, R. P., Toledo Quiñones, R. E., & Henostroza Márquez Mázmela, P. R. (2022). Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú. Revista Científica General José María Córdova, 20(37), 209-224. https://doi.org/10.21830/19006586.791