Gamification as a Tool for Elevating Password Strength Awareness

Miloš Kostić[1,*], Igor Saveljić[1]

[1]Faculty of Information Technology, Belgrade Metropolitan University, Tadeuša Košćuška 63, 11000 Belgrade, Serbia

Abstract

In modern society, where users are confronted with the necessity of managing an ever-growing number of personal profiles and accounts, low password security awareness remains a significant vulnerability in cybersecurity. Despite the existence of numerous tools designed for password safekeeping, educating users and broadening their knowledge of password strength and related cybersecurity risks cannot be understated. The popularity of gamification as an educational technique for overcoming challenges in different domains, mostly related to the lack of motivation and attention, has grown in recent years. This paper explores the concept of a two-dimensional game in which players face specific challenges aimed at replacing existing weak passwords with new, stronger ones, while avoiding the loss of access to various platforms. Time constraints and simulated cyber-attacks enhance the learning process and underscore the importance of the analyzed topic.

Keywords

Gamification, Security awareness, Games-based learning, Human-centered cybersecurity

1. Introduction

In the digital age, our society increasingly relies on the Internet for various aspects of our lives, from banking to e-commerce. Transactions conducted online often require the exchange of personal information, such as home addresses and credit card details. Within this digital landscape, passwords continue to serve as the primary authentication mechanism for accessing online services. Ensuring users remain secure while using passwords is of paramount importance. This paper seeks to address the critical need to enhance security awareness and promote better password practices through the implementation of gamification techniques.

Importance of raising password strength awareness and concept of gamification and its application within the context of the learning environment will be explored within this paper. Additionally, an concept overview of a two-dimensional game ("Lockedout") in which players face specific challenges aimed at replacing existing weak passwords with new, stronger ones, while avoiding the loss of access to various platforms will be presented.

2. Importance of password strength awareness

The Internet presents numerous potential risks when browsing the web, such as interacting with malicious websites and domains, using inadequately constructed and weak passwords, responding to phishing emails and messages etc. These risks can place users in dangerous situations [1]. Various methods have been employed to raise user security awareness during online transactions. With the prevalence of password-related vulnerabilities, research efforts have predominantly concentrated on the creation and enhancement of security awareness tools aimed at fortifying password security.

Users often grapple with the creation and retention of strong, secure passwords, leading to various studies aimed at addressing this issue [2, 3, 4]. Experience has revealed that the prevalent method of incorporating password meters into password creation forms can frequently create a false sense of security. This is often attributed to the shortcomings in many of the available password meter algorithms, which may incorrectly label weak or poorly defined passwords as strong [5, 6]. Research suggests that additional factors should be considered when using password meters, such as user perceptions of account importance, as opposed to solely relying on the feedback provided by the meter. It becomes evident that password meters alone may not be sufficient in raising awareness and encouraging the creation of secure passwords.

Persuasive messages intended to instill fear by outlining the possible consequences of non-compliance have also been investigated as a means to boost security awareness. By educating end-users on the importance of pass-

BISEC'23: 14th International Conference on Business Information Security, November 24, 2023, Niš, Serbia

*Corresponding author.

milos.kostic@metropolitan.ac.rs (M. Kostić); igor.saveljic@metropolitan.ac.rs (I. Saveljić)

0009-0005-0912-9518 (M. Kostić); 0000-0002-0707-5174 (I. Saveljić)

word strength and heightening their awareness of associated risks, this approach has proven effective in motivating users to craft more robust passwords.

Despite ongoing efforts, issues with password hygiene persist, highlighting the necessity for more effective ways to convey password security information to users.

3. Gaminfication

Gamification is often described as the application of game design principles in non-gaming contexts [6, 7]. However, it encompasses more than just incorporating elements from games. It encompasses the infusion of game thinking into non-game scenarios, involving elements such as: player control, rewards, progress mechanics, collaborative problem-solving, storytelling, and even competition. At its core, gamification seeks to motivate individuals to change their behavior, primarily through enhanced engagement and motivation.

Research and recent studies have unveiled numerous instances where competitive elements successfully encouraged participants to change their behavior [6, 8]. The inclusion of competitive and cooperative elements in non-game contexts exemplifies the integration of gamification. Such gamified contexts provide a safe environment for participants to practice and hone their skills under pressure, fostering an environment of controlled learning and adaptation. Despite the growing popularity of digital or online gamified environments, gamification can also be seamlessly incorporated into tabletop contexts, using elements from card games or board games.

Studies consistently indicate a preference for gamified environments over their non-gamified counterparts among participants. The advantages of increased engagement, motivation, and skill development make gamification an attractive proposition for cybersecurity education and awareness. Nevertheless, a detailed investigation into the precise application of gamification within existing cybersecurity awareness contexts remains an underexplored area.

4. “Lockedout” – Game concept

"Lockedout" is a 2D pixel art time challenge game designed to educate players about prevalent cybersecurity risks and underscore the critical importance of password strength. It embraces a pixelated aesthetic reminiscent of video games from the 1980s and 1990s, deliberately chosen to infuse a sense of charm and playfulness into the overall gaming experience.

The game’s title (Figure 1.), "Lockedout," is a wordplay carefully selected to convey the concept of being virtually locked out due to password-related issues.

Figure 1: Current game title/logo design.

Figure 2: Password change UI.

4.1. Game Structure

In terms of UI/UX elements, "Lockedout" will revolve around the visible borders of a computer monitor, featuring a fictional operating system (OS) hosting five simulated computer applications. Additionally, an OS Guard, akin to antivirus software, will facilitate player interactions within the game and provide essential narrative elements and guidance (Figure 2.). Each of the computer applications will possess its own interface, complete with predefined content, and will serve as representations of significant daily activities necessitating robust password protection:

- Email communication
- Socializing with friends
- Online shopping
- Engaging with social media
- Managing bank account and transactions

A fully operational password checker, featuring a password strength indicator and corrective notifications, will serve as a key gameplay mechanic. The flow of gameplay will be regulated by a predefined scenario and relevant timers.

An imaginary hacker or hacker group will also be featured in the narrative; however, they will not be directly portrayed within the game.

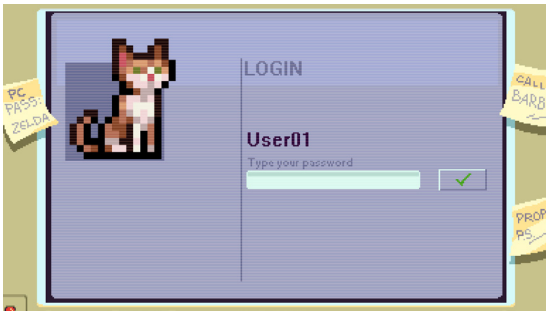

Figure 3: OS Login screen.

Figure 5: MyPasswords.txt document preview.

Figure 4: Desktop.

Figure 6: "Chat" app UI.

4.2. Gameplay scenario

First element of player-game interaction represents an old computer monitor with an operating system login window (Figure 3). Several sticky notes are scattered across the monitor frame, with login and password carelessly written on them. Player needs to use these written credentials in order to access the system.

Upon entering the desktop, the player encounters a file named "MyPasswords.txt" and five distinct computer application icons on the taskbar: "Email," "Bank," "Chat," "Social," and "Shopping" (Figure 4.)

At this stage,, player can access the text document, or see the interface of each application and read predefined content. The text document (Figure 4) holds passwords for each application, shockingly weak and representative of statistically some of the most commonly used passwords in the world:

- Email: "123456"
- Bank: "password123"
- Chat: "letmein"
- Social: "qwerty"
- Shopping: "shopping123"

Upon a short interval, a visual and audio notification triggers within the "Chat" app (Figure 5), revealing a message from a friend inquiring about recent data breaches in their city. As the player begins to respond to the message (or when a short timer elapses due to player inactivity), they are abruptly logged out of the chat application.

An OS Guard notification then appears, warning the player of an ongoing cyberattack (Figure 6) and prompting them to change their password to protect their account. Subsequent pop-ups follow, indicating attacks on other applications, heightening tension.

Each app screen displays a red timer, reflecting the time remaining for the player to enter their old password and generate a new, robust one. Timer durations are based on the application's importance, with the bank application's timer set to the shortest duration, emphasizing its critical nature. The chat and social media apps enjoy slightly longer timers.

In addition to time constraints, the player faces a limited number of password change attempts, with each password required to be unique and meet predefined strength criteria. Throughout this phase of the game, OS Guard occasionally provides essential feedback and tips on password strength, and the password check window informs the player of unsuccessful attempts, specifying the contributing factors.

If the timer expires on an application or if the player accumulates too many failed attempts to change a password, the hacker takes control of the app account, en-

Figure 7: Guard prompt when system is under cyberattack.

gaging in malicious activities such as sending phishing emails, creating compromising posts, or initiating friend requests.

The primary objective of the game is to safeguard as many accounts as possible. Successfully changing all passwords with strength and uniqueness enables the player to defeat the hacker's attempts and receive a congratulatory victory screen. Conversely, the game concludes with a loss if the player loses access to the "Bank" app or if two or more other accounts are compromised.

Following either a win or a loss, an epilogue provides a summary of best practices for password security. It further explains why the passwords in the initial textual document were weak. Players are granted the option to delve deeper into password security through links to additional resources or tutorials.

4.3. Educational and informative aspects

The game's narrative seamlessly integrates educational content into the player's journey, resulting in an engaging and immersive learning experience. It ensures that players develop a nuanced understanding of the risks associated with weak passwords, highlighting poor practices such as storing login data in easily accessible locations like sticky notes or files on the computer desktop.

"Lockedout" offers in-game tutorials and pop-up tips to educate players on password strength, complexity, and the significance of unique passwords. Real-time feedback on password strength, accompanied by explanations of the criteria for robust passwords, enhances the learning process.

After each playthrough, an informative summary reinforces the importance of sound password practices, providing practical guidance. Furthermore, a dedicated section invites players to delve deeper into the subject, offering supplementary resources to expand their knowledge.

To ensure that game is accessible to players with various levels of gaming and technical experience, potentially different difficulty levels will be implemented to cater to beginners and more advanced users.

5. Conclusion and future work

The gamification of password security education, exemplified by "Lockedout: Password Defense," marks a significant innovation in the realm of digital security instruction. Password security is an indispensable facet of modern life, and yet, conventional methods of education in this domain often fall short in terms of engagement and efficacy. By embracing gamification, this chapter has demonstrated the potential to transcend these limitations and foster a more interactive, enjoyable, and impactful learning experience.

"Lockedout" reinforces the significance of strong and unique passwords while actively promoting good practices and awareness. This approach is not only informative but also enjoyable, creating a transformative learning experience. "Lockedout" should represent a small step toward enhancing password security education. Its gamification principles will provide an innovative path for teaching users about the importance of strong passwords, making the educational journey more engaging and, ultimately, more effective.

Future work considers completion and refinement of all required graphics and audio elements. The game will be developed in the Unity engine, utilizing the C# programming language. This development phase includes the implementation and customization of the password-checking algorithm. Additionally, extensive testing and optimization procedures will be conducted to ensure a seamless and robust gaming experience.

Acknowledgment

This paper was supported by the Blockchain Technology Laboratory at Belgrade Metropolitan University, Belgrade, Serbia.

References

[1] L. A. Shepherd, J. Archibald, R. I. Ferguson, Perception of risky security behaviour by users: Survey of current approaches, in: Human Aspects of Information Security, Privacy, and Trust: First International Conference, HAS 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013. Proceedings 1, Springer, 2013, pp. 176–185.

[2] S. L. Pfleeger, D. D. Caputo, Leveraging behavioral science to mitigate cyber security risk, Computers & security 31 (2012) 597–611.

[3] S. Cohen, W. Nutt, Y. Sagiv, Deciding equivalences among conjunctive aggregate queries, Journal of the ACM (JACM) 54 (2007) 5–es.
[4] J. M. Stanton, K. R. Stam, P. Mastrangelo, J. Jolton, Analysis of end user security behaviors, Computers & security 24 (2005) 124–133.
[5] X. D. C. D. Carnavalet, M. Mannan, A large-scale evaluation of high-impact password strength meters, ACM Transactions on Information and System Security (TISSEC) 18 (2015) 1–32.
[6] S. Scholefield, L. A. Shepherd, Gamification techniques for raising cyber security awareness, in: HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21, Springer, 2019, pp. 191–203.
[7] G. Fink, D. Best, D. Manz, V. Popovsky, B. Endicott-Popovsky, Gamification for measuring cyber security situational awareness, in: Foundations of Augmented Cognition: 7th International Conference, AC 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013. Proceedings 7, Springer, 2013, pp. 656–665.
[8] I. Rieff, Systematically applying gamification to cyber security awareness trainings, 2018.