Roby on a Mission: Promoting Awareness and Adoption of Password Managers Through Public Security User Interfaces

Doruntina Murtezaj
doruntina.murtezaj@unibw.de
University of the Bundeswehr Munich / LMU Munich
Munich, Germany

Jovana Dinic
jovana.dinic@campus.lmu.de
LMU Munich
Munich, Germany

Viktorija Paneva
viktorija.paneva@ifi.lmu.de
LMU Munich
Munich, Germany

Florian Alt
florian.alt@ifi.lmu.de
LMU Munich / University of the Bundeswehr Munich
Munich, Germany

Abstract

Public Security User Interfaces (PSUIs) are a relative new approach to increasing cybersecurity awareness and promoting secure behavior in public and semi-public spaces. Unlike traditional methods such as emails or mobile apps, PSUIs use dynamic content and interactive elements to engage users in real time and promote proactive security measures. This paper explores the design and implementation of a previously introduced concept of PSUIs through a use case, driving awareness and adoption of password managers. Drawing insights from a pilot study (N=5) and a main study (N=25), we identify a set of implications for designing PSUIs that prioritize engagement strategies, actionable outcomes, accessibility and inclusivity, and normalizing mistakes. Key challenges include content adaptation, audience dynamics, and privacy. By bridging the gap between public engagement and cybersecurity education, this work lays the foundation for future research and practical implementation of PSUIs as a tool to foster secure digital habits.

CCS Concepts

• **Security and Privacy → Human and societal aspects of security and privacy**; • **Human-centered computing** → *Human-computer interaction.*

Keywords

Public Security User Interfaces, Cybersecurity awareness, Password manager, Gamification in security education

ACM Reference Format:
Doruntina Murtezaj, Jovana Dinic, Viktorija Paneva, and Florian Alt. 2025. Roby on a Mission: Promoting Awareness and Adoption of Password Managers Through Public Security User Interfaces. In *24th International Conference on Mobile and Ubiquitous Multimedia (MUM '25), December 01–04, 2025, Enna, Italy.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3771882.3771905

MUM '25, Enna, Italy

ACM ISBN 979-8-4007-2015-4/25/12
https://doi.org/10.1145/3771882.3771905

1 Introduction

Public Security User Interfaces (PSUIs) are any type of interface positioned in shared, non-personal areas that offers information or the opportunity to interact with security-related topics [33]. They have been proposed as a promising approach for use in public and semi-public spaces – for instance, through interactive public displays – to promote cybersecurity awareness and encourage secure behavior. Public displays can serve as dynamic educational tools that use interactivity and contextual cues to raise cybersecurity awareness among diverse audiences. By embedding engaging content in everyday environments, they can make security concepts more accessible, encourage reflection, and promote safer digital behaviors in a non-intrusive manner. Over the past decade, there has been increasing attention to interactive public displays for various applications, ranging from community engagement to education [11]. However, their potential for addressing pressing cybersecurity issues remains underexplored.

The challenge of fostering secure behavior is rooted in the complexity of behavioral change. As Sasse et al.'s [42] Security Learning Curve emphasizes, behavior change occurs progressively through stages of knowledge acquisition, concordance, self-efficacy, implementation, and embedding. By delivering tailored security content in real-time and incorporating interactive elements, Public Security User Interfaces can support users at each stage of the behavioral learning curve. Public displays, with their ability to engage users in real time, offer unique opportunities to support users across these stages by delivering contextually relevant security information and encouraging active participation. Furthermore, studies have shown that gamified interventions can increase user motivation and retention in learning environments [46]. By incorporating gamification elements into software applications further enhances engagement and learning. When applied to Public Security User Interfaces, we can transform abstract cybersecurity concepts into interactive and memorable experiences.

As the need for effective security measures grows, designing user-friendly interfaces for public display applications becomes crucial. To address this challenge, we investigate the following research question:

RQ: What are the learnings and the challenges in designing interactive Public Security User Interfaces for promoting password manager adoption?

We investigate the challenges and opportunities for designing PSUIs through a use case. More specifically, we first built a prototype and then implemented, *Roby's Password Mission*, an interactive quiz to promote password manager adoption using a gamified experience. Insights from a pilot study and a main study inform implications for design and reveal lessons learned for improving their usability, engagement, and accessibility.

Contribution Statement. Our contributions to the emerging PSUI field are twofold: (1) We *design, implement and evaluate a functional PSUI application* aimed at urgent security concerns. The application draws on prior research and user feedback, yielding concrete insights into structuring security content in public and semi-public settings. (2) We derive broader *implications for future PSUIs* and identify open questions for future research.

2 Related Work

This chapter reviews existing research on how users engage with security interfaces, the factors driving behavior change in cybersecurity, and the role of gamification in enhancing security education and promoting secure behavior. It further discusses password managers and the challenges surrounding their adoption, which form the central focus of our application.

Interacting with Public Security User Interfaces. Public interfaces can surpass traditional awareness methods (e.g., email campaigns, workplace training, or social media) by providing location-specific content at moments of spontaneous engagement [3, 5]. They eliminate the need for personal devices or apps, so users can view and interact with security information seamlessly without seeking it out. These displays also deliver real-time updates, reach wider audiences (including those not active on digital platforms), and integrate non-disruptively with everyday environments, allowing users to absorb essential security content without interrupting their usual routines. Behavioral models, such as the Audience Funnel [32], outline progressive levels of engagement with public displays – from mere awareness (i.e., *passing by*) to *active* interaction. Such models offer a structured lens through which PSUIs can be designed, ensuring content is suitable for both casual passersby and highly motivated users. Group interactions, especially in shared environments such as workplaces or educational institutions, can further support learning and participation, as individuals often encourage each other to explore the display [31]. Early research on interactive public displays primarily addressed single-user scenarios, such as Hermes door displays [7]. Still, subsequent work recognized the value of communal settings (e.g., hallways, break rooms), which can foster engagement among co-located groups [10]. Mid-2000s innovations, including GroupCast [30] and CoCollage [13], highlighted how such displays can spark social interaction—an opportunity that PSUIs could leverage to prompt collective dialogue around security topics. Large-scale deployments, including the UBI-hotspot network in Oulu, Finland [19], demonstrated the ability of public displays to foster long-term community engagement, a concept relevant to security-focused networks in organizations. Public interfaces offer distinct advantages over traditional methods like email campaigns, including spontaneous engagement, real-time updates, and the ability to provide contextually relevant information without requiring additional devices or apps [3, 5]. Drawing from strategies in advertising and public campaigns, PSUIs can leverage techniques such as emotional appeal and targeted messaging to effectively promote cybersecurity awareness and secure behavior.

Factors Influencing Behavioral Change in Cybersecurity. Behavior change involves modifying actions, routines, and habits to achieve specific outcomes [20]. In cybersecurity, this process is influenced by cognitive, social, and environmental factors. Research in Human-Computer Interaction (HCI) aims to understand why users engage in certain behaviors and design interventions to support shifts toward more secure practices. The process typically begins with awareness, driven by personal motivations, external pressures, or an understanding of the consequences of current actions. Educational tools and social influences may facilitate this awareness. However, awareness alone is insufficient; motivation, either intrinsic (from personal goals and values) or extrinsic (from rewards or social expectations) is crucial. According to Fogg's Behavior Model [15], motivation is necessary but insufficient without the ability to act, which depends on having the required skills, knowledge, and resources. Interventions like gamification and nudges have been explored to make adopting new behaviors more intuitive and less intimidating [39, 41]. Public displays may provide information and encouragement for security-related behavior change. However, achieving such change is challenging, often requiring strong internal motivation and being influenced by the behavior and expectations of others [28]. While a comprehensive discussion of behavior change is beyond the scope of this paper, a framework by Sasse et al. [42] highlights factors necessary for supporting security-related behavior change in organizational settings. Their security learning curve theory emphasizes the importance of aiding employees in adopting secure routines. The curve consists of five stages individuals need to navigate to effectively adopt and maintain secure practices, including (1) *Concordance*, (2) *Self-efficacy*, (3) *Implementation*, (4) *Embedding*, and (5) *Secure Behavior.*

The Role of Gamification in Security Awareness Training. Gamification uses game design elements to improve motivation and behavior change [46]. Koivisto et al. [24] have demonstrated its effectiveness in areas such as health, education, and crowdsourcing. In security education, gamification has evolved as a prominent approach to address challenges related to human error and user engagement. Existing work on gamified security education includes both serious games and gamified systems [26, 45, 48–50]. Serious games, characterized by structured narratives and goal-oriented gameplay, dominate in this area. König et al. [25] developed GHOST, a turn-based game that simulates real-world security challenges, leading to measurable improvements in security behaviors such as screen locking and USB security. Similarly, Schreuders et al. [44] proposed a game-based system involving points, tasks, and feedback mechanisms to teach computer security to undergraduate students. Scalability remains a challenge as immersive experiences often require significant resources and are difficult to scale for large groups [17, 37, 47]. The lack of standardized methods in gamified security education has also been noted. Katsantonis et al. [23] propose a concept map for effective design that emphasizes the integration of pedagogical and technological elements.

Password Manager Adoption: Behavioral Patterns and Challenges. Despite their security advantages, password managers (PMs) face significant adoption hurdles due to usability challenges and user behavior. Designing an intuitive interface remains complex, as developers must balance transparency with unobtrusiveness, while ensuring users trust the system's operations [8]. Many users remain unaware of PMs or perceive them as unnecessary, continuing to rely on insecure practices like password memorization and reuse [35, 36, 38].

The adoption process can be understood through migration theory, which identifies push factors (dissatisfaction with current methods), pull factors (PM benefits like convenience and security), and mooring factors (barriers like setup complexity) [2]. While frustration with insecure practices motivates some users to switch, others resist due to perceived risks, such as reliance on a master password or technical difficulties with autofill and cross-device synchronization [21]. User behavior further complicates adoption, with many employing multiple PMs as backups due to concerns about data loss or sync failures [36]. Additionally, advanced features like password generation and security audits are frequently underused because of usability issues, such as difficulty entering complex passwords or overwhelming alert systems [29, 38].

Password reuse remains prevalent, with users recycling approximately 60% of their credentials, often prioritizing convenience over security despite understanding the risks [16]. Behavioral inertia also plays a role, as many users prefer familiar but insecure methods, such as writing passwords on paper, rather than adapting to new tools [29, 38]. Older adults, in particular, exhibit reluctance due to distrust in cloud storage and a preference for physical recordkeeping, though family recommendations and security assurances can encourage adoption [40].

Technical limitations further hinder PM adoption. Cloud-based solutions depend on internet connectivity, while device-integrated PMs often lack cross-platform compatibility [38]. In enterprise settings, setup complexity and subscription costs deter smaller organizations, despite the potential benefits [12]. Strict password policies can also backfire, increasing IT burdens and reducing productivity, suggesting a need for systems that align with human cognitive constraints [9]. To improve adoption, PMs must address usability flaws, enhance feedback mechanisms, and simplify integration into users' existing workflows. By balancing security with accessibility, developers can encourage wider acceptance and more effective use of password management tools.

Summary Existing literature underscores the potential of public displays to promote awareness and behavioral change but falls short in addressing cybersecurity-specific challenges. Similarly, while gamification has shown promise in improving user engagement with cybersecurity topics, its application to PSUIs is yet to be explored. This paper addresses these gaps by developing and evaluating a PSUI designed specifically for cybersecurity education.

3 Methodology

To explore the practical application of PSUIs, we implemented a prototype display application designed to promote awareness and adoption of password managers. Our methodology follows a human-centered design approach involving iterative prototyping, feedback collection, and preliminary evaluation.

The development process was informed by prior conceptual work on PSUIs [33] and guided by principles from behavioral psychology and human-computer interaction [1, 34]. The prototype was designed around principles of persuasive design [14] and gamified learning [18], using narrative storytelling, immediate feedback, and progress visualization to engage users and promote reflection on password management practices.

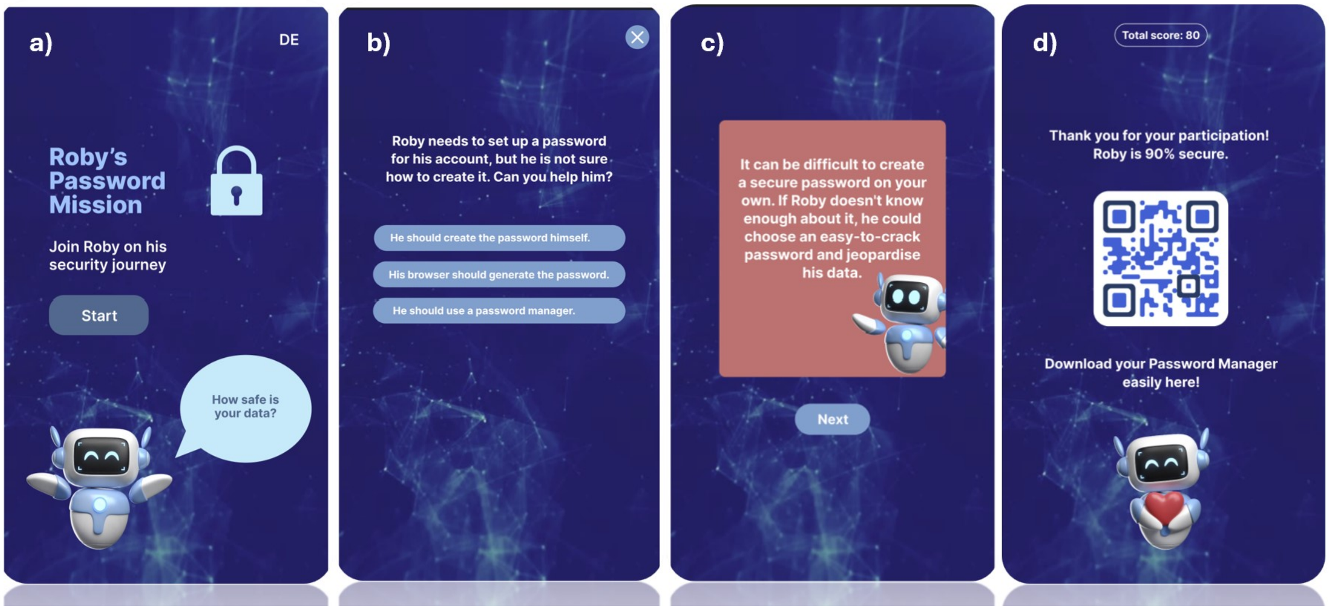
We first defined learning objectives aligned with key stages of the *Security Learning Curve*: knowledge acquisition, concordance, self-efficacy, and habit formation. Based on these goals, we designed an interactive quiz-based application, tailored for use on large touch-enabled public displays. Following the implementation, we conducted a pre-study to gather early feedback on usability, engagement, and the app's perceived educational value. The collected insights were used to refine the design for the next iteration and the main user study.

3.1 App Walkthrough: Roby's Password Mission

The main purpose of this use case is to promote awareness about cybersecurity, specifically password managers, through PSUIs. The quiz-based application aims to educate users on the importance of secure password behavior, the general functionality of a password manager and motivate them to integrate password managers into their daily lives.

As the interface is designed for a public display, its primary goal is to capture user attention. The introduction page (see Figure 1-a) includes the quiz's name, a short description, and an indicator that the screen is interactive, featuring a touch icon. To enhance user engagement, animations are used for the background and a jumping robot, an avatar whose journey the user follows throughout the quiz. Users can also change the interface's language. The robot presents cybersecurity facts through speech bubbles, designed to further capture the user's attention. The robot is designed to appear friendly and inviting. The quiz name, *Roby's Password Mission* and the touch-screen indicator, conveys that the display is interactive and related to passwords. The visuals are tailored to the cybersecurity theme, using primarily blue and white tones to create a modern and technical aesthetic.

During the quiz, users get to know Roby's story and assist him with password-related challenges. The quiz comprises six questions (see Appendix A). An example question is: *"Roby needs to set up a password for his account, but he is not sure how to create it. Can you help him?"* (see Figure 1-b). After each question, the user receives feedback on their chosen option (see Figure 1-c). There are no right or wrong answers, however, the security level of each choice is reflected in the answer button's color red, yellow, or green, and users earn 5, 10, or 15 points accordingly. This encourages them to reflect on their own cybersecurity behavior and realize that some methods they use may not be as secure as they previously thought. The feedback includes a description, an updated mood for Roby's avatar, and a visual or animation aligned with the feedback. For instance, Roby may display a smiling face and a heart when the most secure option is selected, while a sad or worried face appears for


a)
DE
Roby's Password Mission
Start
How safe is your data?
b)
He should create the password himself.
His browser should generate the password.
He should use a password manager.
c)
Next
d)
Total score: 80

Join Roby on his security journey

Roby needs to set up a password for his account, but he is not sure how to create it. Can you help him?

It can be difficult to create a secure password on your own. If Roby doesn't know enough about it, he could choose an easy-to-crack password and jeopardise his data.

Thank you for your participation! Roby is 90% secure.

Download your Password Manager easily here!

Figure 1: Screenshots of *Roby's Password Mission* illustrating the main stages of user interaction. (a) The welcome screen, which introduces the quiz and invites users to participate. (b) An example quiz question, where users assess a password-related scenario. (c) The feedback screen, providing immediate textual and visual feedback on the user's response using color-coded indicators. (d) The final screen, displaying the user's total score and encouraging further engagement with password managers.

less secure choices. Visuals include animated clocks showing how quickly different passwords can be cracked. For the most secure answers, celebratory confetti is displayed to provide positive and rewarding feedback. After completing all the questions, the end page thanks the user for helping Roby, shows a final score and a QR code to download the Bitwarden password manager (see Figure 1-d).

The application is designed to encourage users who are unfamiliar with password managers to consider using one and increase their awareness of cybersecurity.

3.2 Implementation

The app was developed in Kotlin for the Android platform and designed to operate seamlessly on a large public display. It follows a modular structure that separates visual presentation, interaction flow, and content management. Animated elements and short narrative sequences introduce users to the quiz and guide them through the experience. To support bilingual interaction, all content can dynamically switch between English and German. User interactions, including responses and completion times, were locally recorded to enable later analysis of engagement and learning outcomes. The app was deployed via an Android environment emulated on Windows hardware, ensuring touch functionality and stable performance during field use. Refinements were made during testing to optimize responsiveness and visual quality for the large-screen format.

3.3 Study Design

To evaluate user engagement and the app's usability, we conducted a two-phase study, consisting of a pilot study followed by a main study. Insights from the pilot study informed improvements for the final version tested in the main study, following an iterative user-centered design approach. Both studies primarily employed qualitative methods, to gain a more in-depth understanding of participants' interactions with the PSUI, their perceptions of usability and engagement, and their prior knowledge and motivation related to password security. The main study also incorporated quantitative measures to complement the qualitative findings.

Data Collection. In both studies, participants provided informed consent before participation. Each session began with spontaneous interaction with the public display, followed by a short semi-structured interview. The pilot study focused on observing participants using the application and collecting qualitative feedback on its usability, visual design, engagement potential, and perceived educational value. The main study followed a similar procedure, but also included an online questionnaire that gathered data on participants' password habits, perceptions of the quiz, and standardized usability and user experience scales, i.e., the System Usability Scale (SUS) [6], and the User Experience Questionnaire (UEQ) [27].

Data Analysis. The interview transcripts from both studies were analyzed in MAXQDA[1] using a deductive content analysis approach. Two researchers were responsible for the coding process. An initial codebook was developed based on the predefined interview question categories (e.g., engagement, design, feedback, motivation), which served as the analytical framework. During coding, the researchers iteratively refined this framework by adding inductive subcodes to capture emerging themes that were not fully represented by the initial structure. Coding was conducted in two rounds: an initial coding round to identify relevant segments and

[1] https://www.maxqda.com/ (Last accessed: 18.10.2025)

a second round to consolidate themes, ensure consistency, and resolve any ambiguities through discussion between the coders.

For the main study, the quantitative data from the SUS, UEQ, and Likert-scale questions were analyzed using descriptive statistics (mean, median, and standard deviation).

4 Pilot Study

The pilot study served as a preliminary evaluation to gather feedback on the app's design, functionality, and educational value, with the goal of identifying areas for improvement.

Procedure. The study was conducted in a controlled university lab environment, simulating the use of the app on a public display. Beforehand, participants got informed about the study and filled out a consent form for participating, agreeing to audio recording of their verbal responses during the interview. The study was scheduled in 30-minute slots. Each participant first provided demographic information and then interacted with the display at their own pace. No specific requirements or additional guidance were imposed to simulate spontaneous interaction with a public display. At the end of the session, participants were asked to reflect on their overall experience with the display application and provide feedback by answering the pilot study interview questions (see Appendix B), including suggestions for improvement. This feedback, combined with observations during the study, provided insights into user interaction patterns and design refinements for future iterations of the PSUI.

Apparatus. The collected data was primarily qualitative and consisted of audio-recorded verbal responses provided during the interview phase. The interview recordings were transcribed to ensure accurate and detailed analysis. The collected qualitative data was analyzed using open coding in MAXQDA.

Participants and Recruitment. The pilot study (N=5) involved three participants aged 18 to 25 and two aged 26 to 33. Four participants identified as women and one as a man. Educational backgrounds included high school diplomas, bachelor's degrees, and first state examination. Fields of study and professions varied, encompassing media informatics, computer science, teaching, engineering, and electrical engineering. Most participants were students, while one worked as a hardware developer. Participants were recruited through a user study channel on the university's communication networks and through referrals from friends.

Findings. From the analysis of the interview transcripts, five main categories emerged. *Engagement and Accessibility* examines participants' willingness to approach the display in different scenarios and their suggestions for improving its design. *Visual Design and Usability* focuses on the app's layout and visual elements, evaluating how well they support interaction in a public display setting. *Content Clarity and Quiz Flow* assesses the understandability of the content, the structure and pacing of the quiz, the language switch option, and overall quiz length. *Educational Value and User Impact* investigates whether the quiz introduced new ideas, encouraged reflection, or influenced participants' thinking about password security. Finally, *User Feedback and Improvement Suggestions* gathers insights on the quiz's perceived difficulty and suggestions for enhancing the overall experience. Insights from the pilot study informed the following design improvements, which are mapped to the identified categories:

Engagement and Accessibility – Participants reported that, in busy environments, they sometimes did not notice the display. We therefore added an initial on-screen prompt (e.g. a brief animation and *Tap to Begin* call-out) to draw attention and invite interaction in a variety of contexts.

Visual Design and Usability – The lack of real-time feedback made the quiz feel flat. We introduced a points system plus color-coded visual cues (aligned with our blue-and-white cybersecurity theme) to reinforce correct answers and guide users through each question.

Content Clarity and Quiz Flow – To reduce confusion about quiz length and language, we combined an explicit progress bar with a more intuitive language-switch control (flags/abbreviations). This ensures users know how many questions remain and can immediately see how to change language.

Educational Value and User Impact – Many participants said they were motivated to take action only while still engaged. We therefore added a QR code at the end that links directly to the Bitwarden[2] password-manager download page, turning momentary interest into concrete follow-up.

User Feedback and Improvement Suggestions – Several users found some questions either too trivial or too obscure. In response, we calibrated difficulty by adding brief contextual hints for harder items and removing overly simplistic ones—balancing challenge with clear learning outcomes.

5 Main Study

In the main user study, we tested the improved version of the PSUI application, refined based on insights from the pilot study. The pilot study helped refine the interaction flow and visual design based on early user impressions. The main study builds on these insights and provides a deeper look into how participants perceived the content, interacted with the system in a public setting, and reflected on their own password habits.

Procedure. The main study was conducted during a public outreach event held at a European university, where various research projects were showcased to visitors across multiple floors and classrooms. The event lasted approximately 3.5 hours, and the interactive display was set up in one of the rooms.

Apparatus. The main study was conducted in person using a public display located in the university environment (see Figure 2). The display was situated in a high-traffic area during an event, allowing for natural interaction in a realistic setting. The interactive application was deployed on a large touchscreen display.

First, participants took part in a short, semi-structured interview to provide qualitative feedback on their experience. The interviews included questions about the experience with the app, content, visual design and general feedback (Appendix C.1). These interviews were conducted on-site immediately after the interaction.

[2] https://bitwarden.com (Last accessed: 20.01.2025)

The interviews lasted approximately 5–7 minutes and were audio-recorded with participants' consent for subsequent transcription and analysis.

Subsequently, participants completed an online survey. The survey consisted of five categories: General Behavior, Password Managers, Quiz Questions, and Evaluation of the App. Additionally, they filled out the SUS and the UEQ questionnaires. The full list of questions is provided in Appendix C.2.

Participants and Recruitment. Out of the 25 survey participants, 16 were between the ages of 18 and 25, and 9 were between 26 and 35. Fourteen participants identified as women, and eleven as men. In terms of educational background, 9 participants held a bachelor's degree, 8 had completed high school or lower, and 5 had a master's degree. The 3 remaining participants held qualifications such as a PhD, Higher Education Certificate, or first state examination. Twenty-one participants were students, and seven were employed. Sixteen participants studied computer science, while the others came from fields such as sociology and cultural studies, teaching, or electrical engineering. Participants were visitors who approached the display voluntarily and were subsequently invited to take part in the study. Before participating, they were informed about the study's purpose and procedure and provided their consent. This study was approved by the institutional ethical review board, ensuring adherence to all relevant ethical guidelines.

Limitations. This study also highlights opportunities for further development. The display was not yet fully accessible, suggesting that future versions could integrate sound features such as text-to-speech or audio prompts to attract bypassers. The presence of the researchers may have influenced participant behavior, which could be addressed through longer-term deployments in naturalistic settings. While the number of participants provided a solid basis for exploratory insights, expanding the sample would help strengthen the generalizability of the findings. In addition, technical aspects offer room for improvement: the current app does not yet support simultaneous multi-user interaction.

6 Results

We present the findings of the main study evaluating *Roby's Password Mission* within the context of promoting secure behavior using PSUIs. We first outline participants' existing password practices and attitudes toward password managers to contextualize the PSUI's focus. We then report quantitative findings on usability, engagement, and perceived educational impact, followed by qualitative insights from the post-study interviews.

6.1 Password Practices and Password Manager Adoption

This subsection summarizes participants' existing password habits, experiences, and attitudes toward password managers, establishing a behavioral baseline for evaluating the PSUI.

Account Numbers and Password Memory. Participants reported having a considerable number of online accounts. Six participants (24%) indicated they had between 11 and 25 accounts. This was followed by 10 participants (40%) who reported having between 26 and 50 accounts. Three participants (12%) stated they had between 51 and 100 accounts, while five participants (20%) reported having more than 100 accounts.

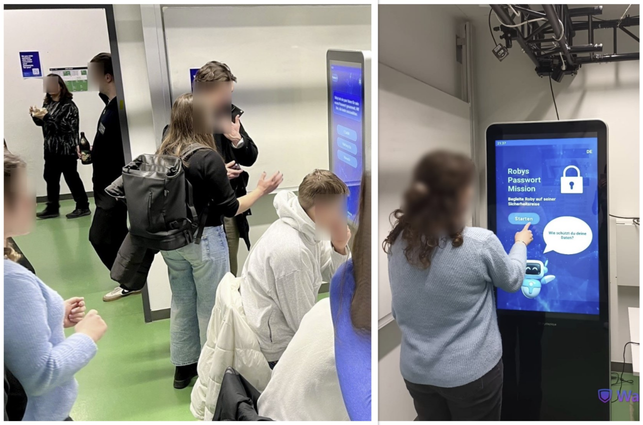


Figure 2: Participants interacting with the display application during the main study, conducted as part of the Open Lab Day at a European university. Visitors were invited to try out the application and take part in the study. Their interactions were observed and feedback was gathered through surveys and interviews.

In terms of password memory, 10 participants (40%) stated they sometimes forget their passwords, while 6 participants (24%) reported forgetting them often, and 2 participants (8%) very often. In contrast, 4 participants (16%) indicated they rarely forget their passwords. Additionally, 2 participants noted that they rely on password managers and therefore do not need to memorize passwords. One participant stored their passwords in an online notes application, and another was unsure of their method.

Password Reset Frequency and Concern About Hacking. Participants reported varying frequencies of password resets. Seven participants (28%) stated they reset their passwords rarely, while 11 participants (44%) did so sometimes. Three participants (12%) reset their passwords often, and two participants (8%) reported resetting them very often. Some participants clarified they only reset credentials for important accounts periodically.

Participants' concern regarding account hacking was assessed on a 5-point Likert scale (1 = not at all concerned, 5 = very concerned). Responses showed a moderate to high level of concern (M = 3.52, Mdn = 4, SD = 1.10). No participants selected the lowest level of concern. Six participants (24%) selected level 2, again six (24%) chose level 3, seven (28%) selected level 4, while six (24%) reported the highest level of concern (5).

Understanding and Perception of Strong Passwords. Participants generally showed awareness of password best practices, citing strategies such as using long strings with a mix of characters and avoiding password reuse. Nonetheless, some participants emphasized memorability or character variety over overall complexity. When asked to rate the strength of their own passwords on a 5-point Likert scale (1 = very weak, 5 = very strong), responses varied: 2 participants (8%) selected 1, 5 (20%) selected 2, 6 (24%) selected 3, 8 (32%) selected 4, and 4 participants (16%) chose 5. The average perceived password strength was M = 3.08, with a median of Mdn = 3 and a standard deviation of SD = 1.19.

Difficulty Creating and Managing Passwords. Participants were asked to indicate how frequently they experience difficulty both in creating and managing secure passwords, using a 5-point Likert scale (1 = never, 5 = always). In terms of creating secure passwords, 5 participants (20%) selected 1, 6 (24%) chose 2, 4 (16%) selected 3, 8 (32%) selected 4, and 2 (8%) a 5 (M = 2.84, Mdn = 3, SD = 1.29).

Responses regarding the difficulty of managing passwords showed that 3 participants (12%) reported no difficulty at all (1), 8 participants (32%) rated it as low difficulty (2), 9 participants (36%) indicated moderate difficulty (3), 1 participant (4%) selected 4, and 4 participants (16%) reported the highest level of difficulty (5). The mean reported difficulty was M = 2.80, with a median of Mdn = 3, and a standard deviation of SD = 1.20.

Awareness and Use of Password Managers. Most participants, 24 out of 25 (96%) were aware of password managers. A total of 15 participants (60%) reported using one. Reasons for adoption primarily centered on convenience: 13 mentioned autofill, 12 liked not having to remember passwords, and 11 appreciated centralized storage of credentials. Other advantages included quicker logins (10), cross-device access (10), and synchronization (8). Security-related reasons included password generation (8), improved overall security (7), and data protection (4).

Reasons for Non-use and Future Intention. Among the 10 participants who did not currently use a password manager, three reported using the same passwords across accounts, while two expressed a general distrust in password managers. Two participants found them too complicated, and another two indicated satisfaction with their existing password management strategies. One participant preferred to memorize passwords as a way to ensure access.

Despite these reservations, 9 out of the 10 non-users expressed openness to adopting a password manager in the future. Their motivations included improved security (7), easier management (6), multi-device access (4), strong password generation (3), and time-saving potential (3). One participant stated they were unlikely to adopt a password manager, citing trust issues and a preference for reusing a few passwords.

6.2 Quantitative Evaluation of the PSUI

Building on the behavioral context above, we analyzed how participants perceived and interacted with *Roby's Password Mission* in terms of clarity, engagement, and motivational impact.

Quiz Clarity, Usefulness, and User Experience. Participants evaluated the quiz experience across several dimensions using 5-point Likert scales. When asked whether the questions of the quiz were clear (1 = strongly disagree, 5 = strongly agree), 24 out of 25 participants (96%) responded with agreement or strong agreement, indicating high clarity of the content (Mdn = 5). All participants (100%) agreed or strongly agreed that the feedback on the answers was clear (Mdn = 5), and 20 participants (80%) similarly agreed that the feedback was useful (Mdn = 4).

Participants also rated the difficulty level of the quiz on a scale from 1 (very easy) to 5 (very difficult). The vast majority, 23 participants (92%), rated it as either very easy or easy, indicating that the quiz was broadly accessible (Mdn = 2). With respect to quiz length, participants rated it on a scale from 1 (very short) to 5 (very long). Thirteen participants (52%) considered the quiz to be very short or too short, while 9 participants (36%) rated it as "just right" (Mdn = 2). These results highlight opportunities to extend the content while preserving clarity and ease of use.

Satisfaction with the quiz experience was high. When asked "How satisfied are you with the application overall?" (1 = very dissatisfied, 5 = very satisfied), 22 participants (88%) reported being satisfied or very satisfied (Mdn = 4). Visual elements also contributed positively to the user experience: 24 participants (96%) expressed satisfaction with the animations used in the quiz (Mdn = 5).

Perceived Potential for Behavior Change. A majority, 20 out of 25 participants (80%), believed the application could motivate people to take action (Mdn = 4). Additionally, 17 participants (68%) stated they would recommend the application to others (Mdn = 4). Roby's story and challenges were relatable for 15 participants (60%), with median value 4, while 13 (52%) found it helpful for understanding data protection (Mdn = 4). Thirteen participants (52%) reported that they reflected on their own password-related behaviors due to the quiz (Mdn = 4). When asked if they had learned new information, 60% reported that the quiz primarily reinforced existing knowledge, while 7 participants (28%) stated they learned something new about password security practices (Mdn = 2).

System Usability (SUS). The mean SUS score across participants was 83.1 (Mdn = 85, SD = 8.21), placing it in the "good" usability range [4]. The respective SUS scores for each participant are presented in Figure 3.

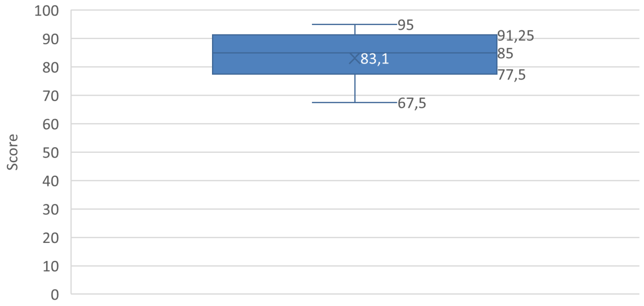


Figure 3: Boxplot of System Usability Scale (SUS) scores obtained from participants after interacting with the PSUI application. The median SUS score was 85, with an interquartile range of 77.5–91.25, and an overall mean score of 83.1—indicating usability in the *good* range.

User Experience Questionnaire (UEQ). User experience was assessed using UEQ, which evaluates six dimensions: attractiveness, perspicuity, efficiency, dependability, stimulation, and novelty. The scores across these dimensions were consistently high, with attractiveness rated at 2.17 (Mdn = 2.17, SD = 0.58), perspicuity at 2.48

(Mdn = 2.50, SD = 0.55), efficiency at 1.79 (Mdn = 2.00, SD = 0.82), dependability at 1.58 (Mdn = 1.50, SD = 0.71), stimulation at 1.69 (Mdn = 1.75, SD = 0.89), and novelty at 0.85 (Mdn = 1.00, SD = 0.90).

To better interpret these results, we compared them against established UEQ benchmarks, which categorise outcomes as "excellent," "good," "above average," "below average," or "bad" based on a large dataset of prior studies [43]. In this context, the application was rated "excellent" in the dimensions of attractiveness, perspicuity, efficiency, and stimulation. Dependability achieved a "good" rating, while novelty was considered "above average".

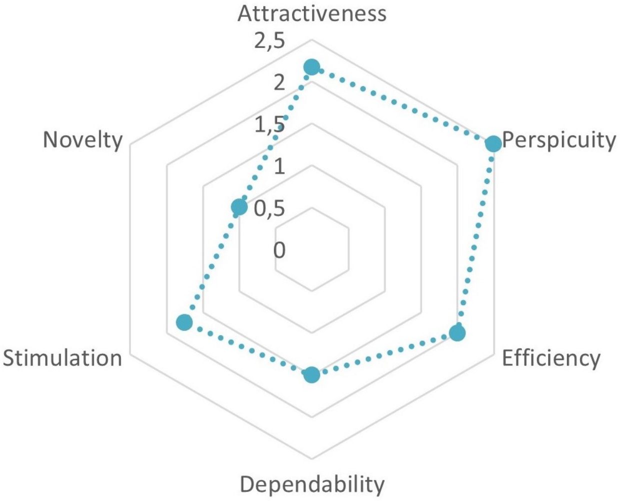


Figure 4: User Experience Questionnaire (UEQ) results across six dimensions: attractiveness, perspicuity, efficiency, dependability, stimulation, and novelty. The highest scores were achieved in attractiveness and perspicuity, both rated as *excellent*, while novelty scored lower but still within the *above average* benchmark range.

6.3 Post-Study Interviews

This section presents a qualitative analysis of 23 post-study interviews (2 participants did not complete the interview, only the surveys) conducted after participants interacted with the public display application. The interviews provided insights into motivations, user experience, and suggestions for improvement.

Reasons for Approaching the Display. Participants cited several reasons for approaching the display. The most frequently mentioned was the visually appealing and modern design, characterized by vibrant colors, a clean layout, and inviting imagery. The animated robot mascot, Roby, stood out as a major attraction. Participants described it as friendly, engaging, and approachable. Many were drawn to its jumping and waving motions, which made the display feel alive. The interface design also supported engagement. Participants noted that the "Start" button was prominently placed and intuitive, encouraging them to begin the quiz. Additionally, social dynamics played a role: seeing peers already interacting with the display sparked curiosity and motivated others to join.

Clarity of Instructions. Most participants reported that the interaction flow was clear and intuitive. However, some usability issues emerged. A few participants experienced confusion when approaching while it was showing the end screen, which lacked a visible prompt for restarting the quiz. Two participants also did not initially understand the purpose of the quiz but picked it up as they progressed. One participant began the experience in the default language and did not immediately notice the option to switch to English.

Quiz Understanding and Description. All interview participants were able to clearly articulate the purpose of the application: to assist the character Roby while simultaneously reinforcing knowledge about password security, with a particular focus on the use of password managers. Many appreciated the approach of combining entertainment with education, describing it as a fun way to test or reinforce what they already knew.

Participant Reflections on Interaction and Design. Participants offered a range of feedback on their interaction with the PSUI display, summarized in Table 1. Overall, they highlighted the engaging format, clear layout, and enjoyable design elements as key strengths. The animated mascot, gamified elements, and clear navigation contributed to a sense of ease and enjoyment during use.

In addition to these positive aspects, participants suggested minor adjustments to improve usability and accessibility. These included suggestions to better accommodate users of different heights, shorten animations, allow skipping content, and strengthen the behavioral impact of the feedback.

Motivation to Complete the Quiz. All participants completed the quiz, citing a combination of motivating factors that sustained their engagement. These included animated feedback, visual elements, and the presence of a clear progress indicator. In addition, many participants also expressed genuine curiosity about the content and a desire to assist the character Roby. The concise and manageable format of the quiz further supported completion sustained attention and completion.

QR Code Usage and Bitwarden Download. At the end of the quiz, participants were presented with a QR code linking to the Bitwarden password manager, accompanied by matching promotional posters placed nearby. QR tracking data indicated that seven scans came directly from the display and one from the posters. Despite this engagement, only one participant proceeded to download the application.

Participants cited several reasons for not scanning the code, including time constraints, not noticing the QR code, or preferring desktop password management. Additionally, some participants were already using a password manager and therefore did not feel the need to explore an alternative tool.

Likelihood of Returning to the Display. Participants were asked how likely they would be to return to the display if they had not completed the quiz on their first attempt, using a 5-point Likert scale (1 = not likely, 5 = very likely). Out of the 23 participants that took part in this phase, 2 (8.7%) selected 1, 3 (13.0%) selected 2, 6 (26.1%) chose 3, 9 (39.1%) selected 4, and 3 (13.0%) rated their likelihood as 5. The average likelihood score across participants was

Table 1: Summary of qualitative feedback from participants on their interaction with the PSUI display. Themes include engagement, interface design, visuals, and impact, with both positive observations and areas for refinement.

Category	Positive Feedback	Suggested Improvements
Engagement	Fun, interesting, and engaging.	Stronger arguments needed to promote the value of password managers.
Design & Layout	Large, clearly positioned buttons; intuitive navigation.	"Next" button too low for taller users; interface felt conservative or slow.
Animations & Visuals	Smooth animations; mascot enhanced interaction; gamified elements (e.g., points).	Animations perceived as too long; resolution could be improved; skip button suggested.
Impact	Helped users test and reinforce existing knowledge.	Correct answers did not always translate into a stronger intention to adopt a password manager; stronger impact desired.

M = 3.34, Mdn = 4.0, SD = 1.13. Several participants noted that they would be more inclined to return if the display were situated in a convenient location or if the quiz featured additional levels or new content. Others, however, perceived the experience as "complete" after one interaction and did not see the need to revisit.

Design's Fit with the Security Theme. Most participants felt the design aligned well with the theme of password security. However, two individuals commented that the aesthetic seemed somewhat generic and could apply to a broader range of topics.

Further Suggestions for Application Improvement. Participants proposed several enhancements to extend the application's educational reach and effectiveness. Key ideas included developing a web-based version to reach more users, adding short pre-quiz educational animations, enabling clickable explanations for correct and incorrect answers, visualizing how password managers work to foster understanding and trust, offering high-contrast and accessibility modes, and introducing more advanced levels or gamified challenges to encourage repeated engagement. Overall, these suggestions highlight a strong interest in more personalized and accessible learning experiences.

7 Lessons Learned from Designing and Evaluating PSUIs

The results of the main study highlight the feasibility and potential of PSUIs for promoting awareness of cybersecurity topics – in this case, promoting the adoption of password managers. Participants showed high engagement with *Roby's Password Mission*, reporting high usability and positive user experience, and expressing motivation to improve their security practices, although actual behavioral follow-through remained limited. These findings demonstrate that PSUIs can effectively capture attention and stimulate reflection through short, gamified interactions; however, sustaining long-term behavioral change requires further investigation.

Our findings complement prior gamified cybersecurity interventions, such as *PASDJO* [45] and *Passworld* [22] by exploring gamified learning and engagement with cybersecurity topics in public and semi-public spaces. Whereas previous approaches relied on planned, device-based participation, *Roby's Password Mission* demonstrates that similar motivational cues, such as, narrative framing, visual feedback, and scoring, can effectively engage spontaneous users in shared physical environments, albeit with some limitations in learning depth. These results position PSUIs as a promising reinforcement layer within broader, multi-channel cybersecurity awareness strategies. Next, we discuss the key findings in relation to engagement, impact, usability, and adoption barriers, each followed by a direct implication for future PSUI design, and directions for future work.

7.1 Engagement and Interaction

The study confirmed that dynamic visuals, gamified interactions, and relatable narratives are key drivers of user engagement in PSUIs. The animated mascot Roby and the interactive quiz format were particularly effective in attracting attention and sustaining interaction, while the gamified elements, particularly the scoring system and visual feedback, were cited as motivating factors for completing the quiz. Social dynamics also played a role, as individuals were more inclined to engage when others were already interacting with the display, highlighting the potential of PSUIs to spark curiosity and collective participation in public settings.

Participants often engaged with the display during brief idle moments, suggesting that PSUIs may be most effective when strategically placed in locations such as bus stops, train stations, or university cafeterias – settings where users are usually more receptive to short, low-effort interactions. Considering the situational context and dwell time is therefore crucial for realistic adoption of PSUIs beyond controlled study conditions.

While the format encouraged completion, several participants remarked that the experience felt "one-off" and lacked incentive for repeat interactions, indicating a need to design PSUIs with evolving content or progressive challenges to sustain engagement over time.

Implication: PSUIs should leverage appealing animations, real-time feedback, and clear progress indicators to encourage deeper engagement and comprehension of security concepts.

Future RQ: How can PSUIs be designed to encourage repeated engagement or integrate with longitudinal campaigns to reinforce secure behavior over time?

7.2 Educational Value and Behavior Change

Participants generally felt the quiz reinforced known information rather than introducing novel concepts. Nonetheless, many reflected on their security habits and acknowledged the potential of the app to drive action. The clarity of both the quiz content and the feedback was consistently praised, suggesting that the PSUI succeeded in its educational objectives.

However, a notable gap emerged between intention and behavior. While 80% believed the app could encourage change, and over half reported reflecting on their own practices, only a small number took direct action, such as scanning the QR code or downloading the suggested password manager. This outcome highlights a broader challenge in cybersecurity education: awareness does not automatically translate into action.

Implication: PSUIs should explore a variety of low-friction mechanisms for follow-up actions, such as contextual reminders, email summaries, or links to further resources, in order to support sustained behavior change beyond the initial interaction.

Future RQ: What nudging strategies or incentives can be embedded in PSUIs to better support concrete behavioral change?

7.3 Usability and User Experience

The PSUI scored highly in usability (SUS) and most UX dimensions (UEQ), indicating a well-received interface. Nonetheless, minor usability issues were noted, such as the placement of interface elements being less accessible to taller users, and occasional confusion about how to restart the quiz after reaching the end screen. Participants also offered some suggestions for improvement, including adding accessibility features (such as high-contrast and screen-reader modes), the ability to skip or shorten animations, and the inclusion of more varied and customizable content.

Implication: Designers should ensure PSUIs are optimized for diverse user preferences and contexts, incorporating personalization options, accessibility settings (e.g., high contrast mode, alternative navigation), and content modularity to support multiple engagement styles.

Future RQ: How can PSUIs be designed to dynamically adapt to individual user needs and preferences while maintaining clarity and simplicity?

8 Conclusion

This paper presents an implementation and evaluation of Public Security User Interfaces (PSUIs), on the use case of promoting password manager adoption. Through the design and deployment of *Roby's Password Mission*, an interactive and gamified public display application, we showed how PSUIs can effectively engage users, foster reflection, and support the adoption of password managers.

Our findings indicate that PSUIs, when thoughtfully designed with engaging visuals, contextual relevance, and clear feedback mechanisms, have the potential to educate and motivate users. The system was well received, as reflected in both usability and user experience metrics, and it sparked meaningful reflection among participants regarding their own cybersecurity practices. However, our results also underscore a gap between awareness and action. While participants acknowledged the educational value of the system and expressed intent to adopt password managers, actual follow-up, such as scanning the provided QR code, remained limited. This points to a key challenge for future PSUIs: sustaining user engagement beyond the initial interaction and prompting real-world action.

In response, we propose several design implications and outline future research questions focused on enhancing long-term engagement, supporting diverse user needs, and fostering more sustained security-related behavior changes. While this study provides valuable initial insights into PSUI implementation, future work should include longitudinal studies to assess long-term impact and effectiveness. Looking ahead, we see significant potential to further enhance PSUIs with technologies, such as adaptive content delivery and AI. This could enable more personalized, emotionally aware, and context-sensitive learning experiences, unlocking new possibilities for promoting secure digital practices in public spaces.

Acknowledgments

This research is part of the *Voice of Wisdom* project and received funding from dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU.

References

[1] Icek Ajzen. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 50, 2 (1991), 179–211. doi:10.1016/0749-5978(91)90020-T Theories of Cognitive Self-Regulation.

[2] Nora Alkaldi and Karen Renaud. 2022. MIGRANT: Modeling Smartphone Password Manager Adoption using Migration Theory. *SIGMIS Database* 53, 2 (April 2022), 63–95. doi:10.1145/3533692.3533698

[3] Florian Alt, Stefan Schneegaß, Albrecht Schmidt, Jörg Müller, and Nemanja Memarovic. 2012. How to evaluate public displays. In *Proceedings of the 2012 International Symposium on Pervasive Displays* (Porto, Portugal) *(PerDis '12)*. Association for Computing Machinery, New York, NY, USA, Article 17, 6 pages. doi:10.1145/2307798.2307815

[4] Aaron Bangor, Philip T. Kortum, and James T. Miller and. 2008. An Empirical Evaluation of the System Usability Scale. *International Journal of Human–Computer Interaction* 24, 6 (2008), 574–594. doi:10.1080/10447310802205776

[5] Harry Brignull and Yvonne Rogers. 2003. Enticing People to Interact with Large Public Displays in Public Spaces. In *IFIP TC13 International Conference on Human-Computer Interaction*. https://api.semanticscholar.org/CorpusID:45271459

[6] John Brooke et al. 1996. SUS-A quick and dirty usability scale. *Usability evaluation in industry* 189, 194 (1996), 4–7.

[7] Keith Cheverst, Alan Dix, Dan Fitton, Adrian Friday, and Mark Rouncefield. 2003. Exploring the Utility of Remote Messaging and Situated Office Door Displays. In *Human-Computer Interaction with Mobile Devices and Services*, Luca Chittaro (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 336–341. doi:10.1007/978-3-540-45233-1_24

[8] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle. 2006. A Usability Study and Critique of Two Password Managers. In *15th USENIX Security Symposium (USENIX Security 06)*. USENIX Association, Vancouver, B.C. Canada. https://www.usenix.org/conference/15th-usenix-security-symposium/usability-study-and-critique-two-password-managers

[9] Yee-Yin Choong. 2014. A Cognitive-Behavioral Framework of User Password Management Lifecycle. In *Human Aspects of Information Security, Privacy, and Trust*, Theo Tryfonas and Ioannis Askoxylakis (Eds.). Springer International Publishing, Cham, 127–137. doi:10.1007/978-3-319-07620-1_12

[10] Elizabeth Churchill, Les Nelson, Laurent Denoue, Paul Murphy, and Jonathan Helfman. 2003. *The Plasma Poster Network*. Springer Netherlands, Dordrecht, 233–260. doi:10.1007/978-94-017-2813-3_10

[11] Nigel Davies, Sarah Clinch, and Florian Alt. 2014. *Pervasive Displays: Understanding the Future of Digital Signage* (1 ed.). Springer Nature Switzerland AG, Cham. XIII + 114 pages. doi:10.1007/978-3-031-02484-9

[12] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does my password go up to eleven? the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 2379–2388. doi:10.1145/2470654.

2481329

[13] Shelly D. Farnham, Joseph F. McCarthy, Yagnesh Patel, Sameer Ahuja, Daniel Norman, William R. Hazlewood, and Josh Lind. 2009. Measuring the impact of third place attachment on the adoption of a place-based community technology. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA) *(CHI '09)*. Association for Computing Machinery, New York, NY, USA, 2153–2156. doi:10.1145/1518701.1519028

[14] B.J. Fogg. 2003. *Persuasive Technology: Using Computers to Change What We Think and Do.* Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[15] Brian J Fogg. 2009. A behavior model for persuasive design. In *Proceedings of the 4th international Conference on Persuasive Technology.* 1–7. https://api.semanticscholar.org/CorpusID:1659386

[16] Xianyi Gao, Yulong Yang, Can Liu, Christos Mitropoulos, Janne Lindqvist, and Antti Oulasvirta. 2018. Forgetting of Passwords: Ecological Theory and Data. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 221–238. https://www.usenix.org/conference/usenixsecurity18/presentation/gao-xianyi

[17] Lukas Hafner, Florian Wutz, Daniela Pöhn, and Wolfgang Hommel. 2023. TASEP: A Collaborative Social Engineering Tabletop Role-Playing Game to Prevent Successful Social Engineering Attacks. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (Benevento, Italy) *(ARES '23)*. Association for Computing Machinery, New York, NY, USA, Article 67, 10 pages. doi:10.1145/3600160.3605005

[18] Juho Hamari, Jonna Koivisto, and Harri Sarsa. 2014. Does Gamification Work? – A Literature Review of Empirical Studies on Gamification. In *2014 47th Hawaii International Conference on System Sciences.* 3025–3034. doi:10.1109/HICSS.2014.377

[19] Tommi Heikkinen, Tomas Lindén, Timo Ojala, Hannu Kukka, Marko Jurmu, and Simo Hosio. 2010. Lessons Learned from the Deployment and Maintenance of UBI-Hotspots. In *2010 4th International Conference on Multimedia and Ubiquitous Engineering.* 1–6. doi:10.1109/MUE.2010.5575054

[20] Jonas Hielscher, Annette Kluge, Uta Menges, and M. Angela Sasse. 2022. "Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting. In *Proceedings of the 2021 New Security Paradigms Workshop* (Virtual Event, USA) *(NSPW '21)*. Association for Computing Machinery, New York, NY, USA, 108–122. doi:10.1145/3498891.3498902

[21] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one can hack my mind": comparing expert and non-expert security practices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 327–346.

[22] Gokul Chettoor Jayakrishnan, Gangadhara Reddy Sirigireddy, Sukanya Vaddepalli, Vijayanand Banahatti, Sachin Premsukh Lodha, and Sankalp Suneel Pandit. 2020. Passworld: A Serious Game to Promote Password Awareness and Diversity in an Enterprise. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 1–18. https://www.usenix.org/conference/soups2020/presentation/jayakrishnan

[23] Menelaos N. Katsantonis, Panayotis Fouliras, and Ioannis Mavridis. 2017. Conceptualization of Game Based Approaches for Learning and Training on Cyber Security. In *Proceedings of the 21st Pan-Hellenic Conference on Informatics* (Larissa, Greece) *(PCI '17)*. Association for Computing Machinery, New York, NY, USA, Article 36, 2 pages. doi:10.1145/3139367.3139415

[24] Jonna Koivisto and Juho Hamari. 2019. The rise of motivational information systems: A review of gamification research. *International Journal of Information Management* 45 (2019), 191–210. doi:10.1016/j.ijinfomgt.2018.10.013

[25] Johannes A. König and Martin R. Wolf. 2018. GHOST: An Evaluated Competence Developing Game for Cybersecurity Awareness Training. *International Journal on Advances in Security* 11, 3 & 4 (2018), 274–287. http://www.iariajournals.org/security/ Published under agreement with IARIA.

[26] Srishti Kulshrestha, Sarthak Agrawal, Devottam Gaurav, Manmohan Chaturvedi, Subodh Sharma, and Ranjan Bose. 2021. Development and Validation of Serious Games for Teaching Cybersecurity. In *Serious Games*, Bobbie Fletcher, Minhua Ma, Stefan Göbel, Jannicke Baalsrud Hauge, and Tim Marsh (Eds.). Springer International Publishing, Cham, 247–262. doi:10.1007/978-3-030-88272-3_18

[27] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and Evaluation of a User Experience Questionnaire. In *HCI and Usability for Education and Work*, Andreas Holzinger (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 63–76. doi:10.1007/978-3-540-89350-9_6

[28] Linda Little, Pam Briggs, and Lynne Coventry. 2005. Public space systems: designing for privacy? *Int. J. Hum.-Comput. Stud.* 63, 1–2 (July 2005), 254–268. doi:10.1016/j.ijhcs.2005.04.018

[29] Peter Mayer, Collins W. Munyendo, Michelle L. Mazurek, and Adam J. Aviv. 2022. Why Users (Don't) Use Password Managers at a Large Educational Institution. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 1849–1866. https://www.usenix.org/conference/usenixsecurity22/presentation/mayer

[30] Joseph F. McCarthy. 2002. Using Public Displays to Create Conversation Opportunities. In *Workshop on Public, Community, and Situated Displays at CSCW 2002.* ACM, New Orleans, LA, USA, 1–7. https://www.researchgate.net/publication/228622325_Using_public_displays_to_create_conversation_opportunities

[31] Nemanja Memarovic, Marc Langheinrich, Florian Alt, Ivan Elhart, Simo Hosio, and Elisa Rubegni. 2012. Using public displays to stimulate passive engagement, active engagement, and discovery in public spaces. In *Proceedings of the Media Architecture Biennale Conference: Participation* (Aarhus, Denmark) *(MAB '12)*. Association for Computing Machinery, New York, NY, USA, 55–64. doi:10.1145/2421076.2421086

[32] Jörg Müller, Florian Alt, Daniel Michelis, and Albrecht Schmidt. 2010. Requirements and design space for interactive public displays. In *Proceedings of the 18th ACM International Conference on Multimedia* (Firenze, Italy) *(MM '10)*. Association for Computing Machinery, New York, NY, USA, 1285–1294. doi:10.1145/1873951.1874203

[33] Doruntina Murtezaj, Viktorija Paneva, Verena Distler, and Florian Alt. 2025. Public Security User Interfaces: Supporting Spontaneous Engagement with IT Security. In *Proceedings of the New Security Paradigms Workshop (NSPW '24)*. Association for Computing Machinery, New York, NY, USA, 56–70. doi:10.1145/3703465.3703470

[34] Donald A. Norman. 2013. *The Design of Everyday Things.* Basic Books, New York, NY, USA. https://www.basicbooks.com/titles/don-norman/the-design-of-everyday-things/9780465072996/ Originally published as *The Psychology of Everyday Things* (1988).

[35] Gilbert Notoatmodjo and Clark Thomborson. 2009. Passwords and perceptions. In *Proceedings of the Seventh Australasian Conference on Information Security - Volume 98* (Wellington, New Zealand) *(AISC '09)*. Australian Computer Society, Inc., AUS, 71–78.

[36] Sean Oesch, Scott Ruoti, James Simmons, and Anuj Gautam. 2022. "It Basically Started Using Me:" An Observational Study of Password Manager Usage. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 33, 23 pages. doi:10.1145/3491102.3517534

[37] Eszter Diána Oroszi. 2019. Security awareness escape room - a possible new method in improving security awareness of users. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. 1–4. doi:10.1109/CyberSA.2019.8899715

[38] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 319–338. https://www.usenix.org/conference/soups2019/presentation/pearman

[39] Eyal Peer, Alisa Frik, Conor Gilsenan, and Serge Egelman. 2024. "Protect Me Tomorrow": Commitment Nudges to Remedy Compromised Passwords. *ACM Trans. Comput.-Hum. Interact.* 31, 5, Article 59 (Nov. 2024), 25 pages. doi:10.1145/3689038

[40] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2021. Why Older Adults (Don't) Use Password Managers. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 73–90. https://www.usenix.org/conference/usenixsecurity21/presentation/ray

[41] Przemysław Rodwald. 2019. Using gamification and fear appeal instead of password strength meters to increase password entropy. *Maritime Technical Journal* 217, 2 (2019), 17–33.

[42] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2023. Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours. In *Computer Security. ESORICS 2022 International Workshops.* Springer International Publishing, Cham, 248–265. doi:10.1007/978-3-031-25460-4_14

[43] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. 2017. Construction of a Benchmark for the User Experience Questionnaire (UEQ). *International Journal of Interactive Multimedia and Artificial Intelligence* 4, 4 (2017), 40 – 44. doi:10.25968/opus-3397

[44] Z. Cliffe Schreuders and Emlyn Butterfield. 2016. Gamification for Teaching and Learning Computer Security in Higher Education. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. USENIX Association, Austin, TX. https://www.usenix.org/conference/ase16/workshop-program/presentation/schreuders

[45] Tobias Seitz and Heinrich Hussmann. 2017. PASDJO: quantifying password strength perceptions with an online game. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction* (Brisbane, Queensland, Australia) *(OzCHI '17)*. Association for Computing Machinery, New York, NY, USA, 117–125. doi:10.1145/3152771.3152784

[46] Karzan Hussein Sharif and Siddeeq Y. Ameen. 2020. A Review of Security Awareness Approaches With Special Emphasis on Gamification. *2020 International Conference on Advanced Science and Engineering (ICOASE)* (2020), 151–156. https://api.semanticscholar.org/CorpusID:235308063

[47] Silvestro V. Veneruso, Lauren S. Ferro, Andrea Marrella, Massimo Mecella, and Tiziana Catarci. 2020. CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues. In *Proceedings of the 2020 International Conference on Advanced Visual Interfaces* (Salerno, Italy) *(AVI '20)*. Association for Computing Machinery, New York, NY, USA, Article 13, 8 pages. doi:10.1145/

3399715.3399860

[48] Vasaka Visoottiviseth, Atit Phungphat, Nuntapob Puttawong, Pamanut Chantaraumporn, and Jason Haga. 2018. Lord of Secure: the Virtual Reality Game for Educating Network Security. In *2018 Seventh ICT International Student Project Conference (ICT-ISPC)*. 1–6. doi:10.1109/ICT-ISPC.2018.8523947

[49] Nima Zargham, Mehrdad Bahrini, Georg Volkmar, Dirk Wenig, Karsten Sohr, and Rainer Malaka. 2019. What Could Go Wrong? Raising Mobile Privacy and Security Awareness Through a Decision-Making Game. In *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts* (Barcelona, Spain) *(CHI PLAY '19 Extended Abstracts)*. Association for Computing Machinery, New York, NY, USA, 805–812. doi:10.1145/3341215.3356273

[50] Leah Zhang-Kennedy, Robert Biddle, and Sonia Chiasson. 2017. Secure comics: an interactive comic series for improving cyber security and privacy. In *Proceedings of the 31st British Computer Society Human Computer Interaction Conference* (Sunderland, UK) *(HCI '17)*. BCS Learning & Development Ltd., Swindon, GBR, Article 65, 3 pages. doi:10.14236/ewic/HCI2017.65

A Quiz Questions

(1) Roby has to set up a password for his account, but he is not sure how to create it. Could you help him?
  - He should create the password himself.
  - His browser should generate the password.
  - He should use a password manager.

(2) Roby has collected a few ideas for his new password. Help him choose the best one.
  - 123456
  - f&M3#p12k
  - S0mm3r

(3) Roby already has a password for another account. Should he reuse the same password for this one?
  - Yes
  - No

(4) Roby does not want to forget the new password he has created. What is the best way to store it?
  - He should memorize it.
  - He should write it down.
  - He should store it in a password manager.
  - He should save it in the browser.

(5) Roby is not quite sure what a password manager does. Let us explain it to him. It is a software...
  - that securely stores your passwords in encrypted form.
  - that creates strong passwords for you.
  - that automatically fills in your passwords.
  - that performs all three of the above functions.

(6) Roby is considering starting to use a password manager. Should he do it?
  - Yes
  - No

B Pilot Study

B.1 Interview Questions

Engagement and Approachability

(1) How likely is it that you would approach the display and try it out?
  - if you were by yourself
  - if you were with someone
  - if you are in a waiting situation
  - if you are in a rush

(2) What features or design elements would make the app more eye-catching or engaging for people passing by?

Visual Appeal and Usability

(1) How well do you think the app's layout (buttons, images, text) fits for a public display?
(2) How effective were the visuals? Are there any specific visuals you would improve or change?
(3) Would you be interested in audio effects to enhance the experience? If so, what type of audio would you suggest?

Content Clarity and Quiz Flow

(1) What did you think about the clarity and intuitiveness of the instructions during the quiz?
(2) How easy was it to find and use the language change option?
(3) What features or elements, if any, do you feel were missing from the app?
(4) How did you feel about the overall length of the quiz?

Educational Value and Impact

(1) How well did the quiz balance between being educational and entertaining?
(2) How relatable did you find the questions?
(3) Did the quiz introduce new concepts regarding password security that you hadn't considered before?
(4) Did any of the quiz questions feel repetitive?
(5) Were the answer options clear and easy to understand?

Feedback and Suggestions

(1) Did you feel like the app provided useful and clear feedback after each question?
(2) Did the quiz motivate you to think about your own behavior regarding security? Can you think of ways to make the quiz even more impactful on this topic?
(3) How would you describe the difficulty level of the quiz? Did it feel too complicated, too simple, or just right?
(4) Is there any additional feedback or suggestions you have to improve the app, especially for public use?

C Main Study

C.1 Interview Questions

General

(1) What has made you approach the display?
(2) Did you know what to do from the very beginning? (*yes / no*)
(3) Can you tell me what the application was about?
(4) How would you describe your experience interacting with the display?

Content

(1) Did you finish the quiz? (*yes / no*)
(2) **If yes:**
  - What has made you stay until the end?
  - Did you download the suggested app?

(3) **If no:**

- What could be done differently to make you stay until the end?

(4) How likely is it that you would come back to the quiz if you weren't able to finish it the first time?
(Scale 1–5, with 1 being not likely and 5 being very likely)

(5) How can we improve the approachability of the application by improving design features?

Visual Design

(1) What do you think about the design of the application (colors, fonts, icons, layout)? What would you change?

(2) Did you find the font size, buttons, and icons easy to interact with? Were they appropriately sized and placed?

(3) Do you feel that the design of the application aligns with its purpose? Why or why not?

Feedback

(1) Do you have any suggestions for improving the usability, design, or content of the application?

C.2 Survey Questions

General Behavior

(1) How many online accounts do you approximately have?
- Less than 10
- 11–25
- 26–50
- 51–100
- More than 100
- I'm not sure

(2) How often do you forget your passwords?
- Never
- Rarely
- Sometimes
- Often
- Very often
- I'm not sure
- Other: ____________________

(3) How often do you need to reset your passwords?
- Never
- Rarely
- Sometimes
- Often
- Very often
- I'm not sure
- Other: ____________________

(4) How concerned are you about your important accounts being hacked?
Likert scale: 1 (Not at all concerned) – 5 (Very concerned)

(5) What is a strong password in your opinion?

(6) How would you rate the overall strength of your passwords?
Likert scale: 1 (Very weak) – 5 (Very strong)

(7) How often do you face difficulties creating secure passwords?
Likert scale: 1 (Never) – 5 (Always)

(8) How often do you face difficulties managing passwords?
Likert scale: 1 (Never) – 5 (Always)

Password Manager

(1) Do you know what a password manager is?
- Yes
- No
- I don't know

(2) Do you currently use one?
- Yes
- No

(3) Why are you using a password manager? (Select all that apply)
- Trust
- Better password security
- Data protection through encryption
- Autofill function
- I don't need to remember passwords
- It saves time when logging in
- It generates secure passwords
- It manages all passwords in one place
- Access passwords on multiple devices
- Syncs across platforms
- Other: ____________________

(4) Why aren't you using a password manager? (Select all that apply)
- I don't know what it is
- I don't know how it works
- I don't trust it
- I'm afraid of security risks (hacking, breaches)
- I prefer to store passwords offline
- I find it too complicated to use
- I already have a system that works
- I use the same passwords
- Other: ____________________

(5) Would you consider using a password manager?
- Yes
- No

(6) Why would you want to use a password manager? (Select all that apply)
- Stronger passwords
- Better security
- Protecting accounts from being hacked
- Easier password management
- Saves time logging in
- Syncs across multiple devices
- Other: ____________________

(7) Why wouldn't you want to use a password manager? (Select all that apply)
- I don't trust password managers
- I'm afraid of hacking or breaches
- I already have my own system
- I use the same few passwords
- I find them difficult to use
- I don't want to rely on an external tool
- Other: ____________________

Quiz Questions

(1) The questions of the quiz were clear.
Likert scale: 1 (Strongly disagree) – 5 (Strongly agree)
(2) The feedback on the answers was clear.
Likert scale: 1 (Strongly disagree) – 5 (Strongly agree)
(3) The feedback on the answers was useful.
Likert scale: 1 (Strongly disagree) – 5 (Strongly agree)
(4) How would you rate the difficulty level of the quiz?
Likert scale: 1 (Very easy) – 5 (Very difficult)
(5) How would you rate the overall length of the quiz?
Likert scale: 1 (Very short) – 5 (Very long)

Evaluation of the App

(1) How satisfied are you with the application overall?
Likert scale: 1 (Very dissatisfied) – 5 (Very satisfied)
(2) How satisfied are you with the animations of the quiz?
Likert scale: 1 (Very dissatisfied) – 5 (Very satisfied)
(3) I could relate to Roby's story and his issues.
Likert scale: 1 (Strongly disagree) – 5 (Strongly agree)
(4) I learned new information regarding password security I didn't know before.
Likert scale: 1 (Strongly disagree) – 5 (Strongly agree)
(5) The quiz made me think about my own behavior regarding password managers.
Likert scale: 1 (Strongly disagree) – 5 (Strongly agree)
(6) The quiz helped me understand how to protect my data.
Likert scale: 1 (Strongly disagree) – 5 (Strongly agree)
(7) The application could motivate people to take actions.
Likert scale: 1 (Strongly disagree) – 5 (Strongly agree)
(8) How likely are you to recommend this application to others?
Likert scale: 1 (Very unlikely) – 5 (Very likely)

System Usability Scale (SUS)

Likert scale: 1 (Strongly disagree) – 5 (Strongly agree)

(1) I think that I would like to use this system frequently.
(2) I found the system unnecessarily complex.
(3) I thought the system was easy to use.
(4) I think that I would need the support of a technical person to be able to use this system.
(5) I found the various functions in this system were well integrated.
(6) I thought there was too much inconsistency in this system.
(7) I would imagine that most people would learn to use this system very quickly.
(8) I found the system very cumbersome to use.
(9) I felt very confident using the system.
(10) I needed to learn a lot of things before I could get going with this system.

User Experience Questionnaire (UEQ)

For each pair below, mark your response on a 7-point semantic differential scale.

annoying 1 2 3 4 5 6 7 enjoyable
not understandable 1 2 3 4 5 6 7 understandable
creative 1 2 3 4 5 6 7 dull
easy to learn 1 2 3 4 5 6 7 difficult to learn
valuable 1 2 3 4 5 6 7 inferior
boring 1 2 3 4 5 6 7 exciting
not interesting 1 2 3 4 5 6 7 interesting
unpredictable 1 2 3 4 5 6 7 predictable
fast 1 2 3 4 5 6 7 slow
inventive 1 2 3 4 5 6 7 conventional
obstructive 1 2 3 4 5 6 7 supportive
good 1 2 3 4 5 6 7 bad
complicated 1 2 3 4 5 6 7 easy
unlikable 1 2 3 4 5 6 7 pleasing
usual 1 2 3 4 5 6 7 leading edge
unpleasant 1 2 3 4 5 6 7 pleasant
secure 1 2 3 4 5 6 7 not secure
motivating 1 2 3 4 5 6 7 demotivating
meets expectations 1 2 3 4 5 6 7 does not meet expectations
inefficient 1 2 3 4 5 6 7 efficient
clear 1 2 3 4 5 6 7 confusing
impractical 1 2 3 4 5 6 7 practical
organized 1 2 3 4 5 6 7 cluttered
attractive 1 2 3 4 5 6 7 unattractive
friendly 1 2 3 4 5 6 7 unfriendly
conservative 1 2 3 4 5 6 7 innovative