Catch the Phish: A Gamified Public Display to Encourage Anti-Phishing Behaviors

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

Xuanyu Zhou
LMU Munich
Munich, Germany
Xuanyu.Zhou@campus.lmu.de

Florian Bemmann
LMU Munich
Munich, Germany
University of Mannheim
Mannheim, Germany
florian.bemmann@ifi.lmu.de

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

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

Abstract

Phishing remains one of the most persistent cybersecurity threats, largely because awareness alone rarely translates into secure behavior. This paper explores how users can be supported in moving from cognitive understanding to actionable and sustained phishing awareness. We present and evaluate *Catch the Phish*, a gamified public display system that embeds interactive phishing scenarios into everyday environments to provide an engaging, low-barrier learning experience. In a five-day field study (N = 35), we examined three factors: (1) Task complexity – how varying difficulty levels affect detection accuracy and perceived time sufficiency; (2) Feedback mechanisms – how error prompts, emotional cues, and corrective indicators shape learning and engagement; and (3) Contextual factors – how social and environmental conditions influence interaction with cybersecurity content in public spaces. Quantitative data and qualitative interviews reveal high usability, positive engagement, and heightened phishing awareness. The findings offer design implications for integrating gamification and public displays into cybersecurity education to foster behavior change in open, ambient learning contexts.

CCS Concepts

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

Keywords

Interactive Public Displays, Usable Security, Phishing, Public Security User Interfaces, Gamification

PerDis '26, Munich, Germany
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2513-5/26/03
https://doi.org/10.1145/3797993.3798005

ACM Reference Format:
Doruntina Murtezaj, Xuanyu Zhou, Florian Bemmann, Viktorija Paneva, and Florian Alt. 2026. Catch the Phish: A Gamified Public Display to Encourage Anti-Phishing Behaviors. In *International Conference on Pervasive Displays (PerDis '26), March 16–18, 2026, Munich, Germany.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3797993.3798005

1 Introduction

Phishing remains one of the most persistent and evolving forms of social engineering, exploiting emotions such as trust, fear, and urgency to deceive users into revealing sensitive information, including credentials or financial data [37]. Unlike spam, which is mostly unsolicited yet harmless, phishing actively manipulates human decision-making. According to Verizon's 2025 Data Breach Investigations Report[1], nearly 60% of breaches involve the human element, with phishing among the most prevalent tactics. The emergence of AI-generated phishing content has further intensified the threat, as synthetically produced emails have doubled in frequency in the recent years [17]. The Anti-Phishing Working Group (APWG)[2] recorded nearly one million incidents in the fourth quarter of 2024 alone, with Software as a Service (SaaS) and webmail services being the most frequently targeted sectors.

Phishing campaigns vary in sophistication. Mass phishing typically relies on brand impersonation, urgency cues, and deceptive links to reach a broad audience [2]. Spear phishing, by contrast, targets specific individuals using personal or professional details to enhance credibility [14]. More advanced variants such as whale phishing and business email compromise (BEC) target executives or financial departments, causing severe financial and reputational harm [4].

Despite extensive awareness efforts, users often remain vulnerable to phishing because of limited attention, low engagement with training materials, and the difficulty of translating abstract knowledge into practical, moment-to-moment judgments [21]. Gamification offers a promising approach to overcome these barriers by

[1] https://www.verizon.com/dbir, last accessed 23.10.2025
[2] https://apwg.org/globalphishingsurvey/, last accessed 23.10.2025

transforming learning into an interactive and rewarding experience [16]. Through immediate feedback and experiential learning, users can safely explore deceptive scenarios, reflect on mistakes, and reinforce decision-making strategies. Integrating such gamified approaches into public displays further expands their reach. Public displays attract passers-by and invite spontaneous interaction through the so-called *honeypot effect* [24], creating a low-barrier setting for informal security learning in everyday contexts.

Building on this intersection of gamification, public displays, and cybersecurity, our work is informed by the concept of Public Security User Interfaces (PSUIs) [26], interactive walk-up public kiosks designed to support engagement with cybersecurity-related content. While prior work primarily introduces PSUIs as a conceptual design space, our work empirically investigates how such interfaces support learning and engagement with cybersecurity topics in-the-wild.

Conceptually, this work investigates how interactive public displays can foster security-relevant decision-making through feedback-driven engagement. The public display prototype, called *Catch the Phish*, serves as a medium to examine this idea. The system presents phishing detection tasks with different difficulty levels, immediate feedback, and supportive hints, designed for casual walk-up interaction. Rather than focusing only on awareness, it targets the transition from recognition to confident and informed action, which is a key step toward sustaining secure behavior. We therefore address the following research question:

RQ: How can a gamified public display support users' phishing detection performance and engagement in everyday public settings?

Contribution Statement. Our contributions are threefold: 1) *design and implementation of Catch the Phish*, a gamified interactive public display that embeds phishing detection tasks into everyday public spaces, supporting spontaneous, low-barrier engagement with cybersecurity learning; 2) *empirical insights from an in-the-wild field study* (N = 35) examining user performance and engagement during walk-up interactions; and 3) *design implications* for gamified PSUIs, highlighting how public displays can support engagement with cybersecurity topics in open, time-constrained public settings.

2 Related Work

To show the research gap that our paper fills, we present in this section existing research on phishing attacks, the use of gamification in cybersecurity training, and the role of public displays in influencing behavioral change.

2.1 Understanding Phishing and User Vulnerability

Understanding why users fall victim to phishing requires analyzing not only external deception strategies but also underlying psychological mechanisms. Phishing remains one of the most pervasive forms of cybercrime, not because of technical sophistication, but because it exploits predictable patterns of human cognition through social engineering and persuasion techniques [6, 12, 19, 29]. A large body of literature demonstrates that phishing emails are strategically designed around key psychological triggers intended to manipulate users' decisions. Koddebusch [19] identifies four dominant persuasive tactics: authority, urgency, personal incentive, and threat or fear cues. These tactics pressure recipients into impulsive, unreflective responses, leading to information disclosure or unsafe actions. Emotional manipulation amplifies phishing's impact, particularly during collective crises, such as the COVID-19 pandemic [30]. Emotionally charged messages significantly increased susceptibility by appealing to fear and urgency. These findings underscore that emotional priming can compromise rational decision-making, emphasizing the need for adaptive, context-aware educational interventions.

Phishing also succeeds by leveraging cognitive shortcuts, or heuristics, that users employ under time pressure or cognitive load [30, 36]. Instead of applying analytical reasoning, users often judge an email's legitimacy based on superficial cues such as sender familiarity, professional layout, or brand logos. These insights suggest that raising technical awareness alone is insufficient; users must also understand how cognitive biases can be exploited. Furthermore, the presented characteristics of phishing attacks show that phishing requires *preventive* countermeasures, as in-situ measures might not reach the user (c.f. unreflective processing, exploitation of pressure [19, 30]).

Individual traits play a significant role in phishing vulnerability. Factors such as risk tolerance, impulsivity, and technological literacy influence users' likelihood of deception [1]. Abroshan et al. [1] showed that users with high risk-taking tendencies were markedly more prone to phishing. Demographic and contextual influences are also relevant: cultural background, emotional stability, and prior experience shape users' responses to phishing [18]. Younger users tend to respond more to socially engineered lures [33], while more experienced users show higher resistance.

An effective countermeasure against deceptive contents is inoculation - an approach from the learning sciences that subsumes educational measures that make people aware of potential deceptive techniques *before* they are exposed to it. That motivates educational tools in public spaces, such as public-display-based games, to reach a variety of people. Cognitive aspects are currently mostly addressed through security trainings [3]. Due to the high effort of participation, they unfortunately do not reach many people at scale. Furthermore, research has shown that cybersecurity education requires reminders, i.e., needs to be repeated after certain amounts of time [7].

2.2 Gamification in Cybersecurity Training

Gamification, the application of game mechanics in non-game contexts, has become a popular method for improving engagement and learning in cybersecurity. Gamification introduces elements such as points, badges, leaderboards, and progress indicators to make learning more engaging [16]. Its theoretical grounding lies in Self-Determination Theory (SDT) [13], which posits that intrinsic motivation arises when autonomy, competence, and relatedness are satisfied. Effective gamified systems thus provide meaningful choices, achievable goals, and social comparison opportunities that support internalized motivation and sustained engagement.

Several systems demonstrate the utility of gamification for phishing awareness. *Anti-Phishing Phil* [35] and *School of Phish* [20] use simulated phishing scenarios, real-time feedback, and reward mechanisms to train users in a safe, interactive environment. These systems promote active learning and allow users to learn from mistakes without real-world consequences, helping to develop durable recognition skills [34].

In educational contexts, Domínguez et al. [15] found that gamified online learning environments improved engagement and practical task performance but were less effective for theoretical knowledge retention. These findings suggest that gamification is particularly suited for procedural and experiential learning, reinforcing its relevance for cybersecurity training that relies on scenario-based interaction.

While gamification holds promise, it also presents challenges. Overreliance on extrinsic rewards, such as badges or points, can undermine intrinsic motivation [16]. Privacy concerns may also arise when behavioral data are tracked for feedback or ranking [11, 32]. Additionally, novelty effects may fade over time if challenges become repetitive or lack depth [11, 27]. Therefore, maintaining user engagement requires balancing reward structures with meaningful learning experiences and adaptive content design.

2.3 Public Displays and Behavior Change

Public displays have emerged as an effective medium for communicating information and shaping user behavior. This section discusses their background, behavioral mechanisms, educational integration, and representative examples.

Advances in display technology and connectivity enabled the proliferation of interactive public screens in everyday settings [28]. Unlike personal devices, public displays can reach diverse audiences in contexts where users are not actively seeking information, such as campuses, libraries, and transportation hubs. Their ambient visibility enables spontaneous engagement and awareness formation. Research on public display interaction identifies five progressive stages—pass-by, attention, exploration, engagement, and participation [25]. To achieve deep engagement, systems must first attract attention, then sustain curiosity through responsive interactivity. Modern public displays leverage multimodal input (touch, voice, gaze) and real-time responsiveness, making them well-suited for influencing attitudes and behaviors [28].

Public displays can incorporate behavioral design strategies such as nudges and real-time feedback to promote security awareness. For instance, displaying messages that highlight how many peers have changed their passwords leverages social conformity to drive action [5]. Timely and visual nudges embedded in daily routines tend to be most effective [10]. However, nudges alone may have limited long-term impact unless reinforced by broader system-level design [34]. Contextualized real-time feedback—such as localized alerts about phishing incidents—helps users connect abstract risks with concrete preventive actions [5, 34].

The *Security Learning Curve* model describes secure behavior formation as a progression through stages: awareness, understanding, willingness, self-efficacy, implementation, and habituation [26, 34]. Most training interventions focus only on early stages such as knowledge transfer, neglecting later stages of reinforcement and habit formation. PSUIs [26] can support all stages by delivering context-relevant information, guiding users toward actionable steps, and reinforcing behavioral commitments through reminders and rewards, thus enabling situated, ongoing engagement that fosters both reflection and habit formation in public contexts. The FunSquare project [24], though not security-focused, provides empirical evidence of how interactive public displays can engage communities through localized, social content. By transforming passive observation into active participation, such systems demonstrate mechanisms transferable to digital security education—fostering awareness, reflection, and dialogue in everyday spaces.

2.4 Research Gap

Past research has shown that cybersecurity, especially attacks that exploit user unknowingness, requires more user education about such techniques. Public displays, therefore, are a promising medium: They reach people without requiring their active interest in the topic, and can be placed to meet people in opportune moments. They usually show repeated exposure, which is necessary in order to keep phishing awareness stable [7]. However, so far, little is known about gamified public displays that promote phishing awareness in practice. With our in-the-wild deployment and field study, we provide insights on the effectiveness and acceptance of public displays for cybersecurity education, and identify design implications for future research in that area.

3 Study Design

The study employed a two-phase approach: a pilot study in a controlled laboratory setting and a main study conducted as an open deployment on a public display in a university atrium. The pilot study was used to refine the system and interaction flow, and the main study was a field study, exploring how people engaged with the system in a natural environment.

The artifact developed for this work is an interactive phishing training system presented on a touchscreen-based public display. The system allows users to examine email examples of varying difficulty, identify suspicious elements, request hints, and receive immediate feedback. This arrangement supports the observation of both performance outcomes, such as the correct identification of phishing cues, and subjective responses, such as confidence and engagement.

3.1 System Design

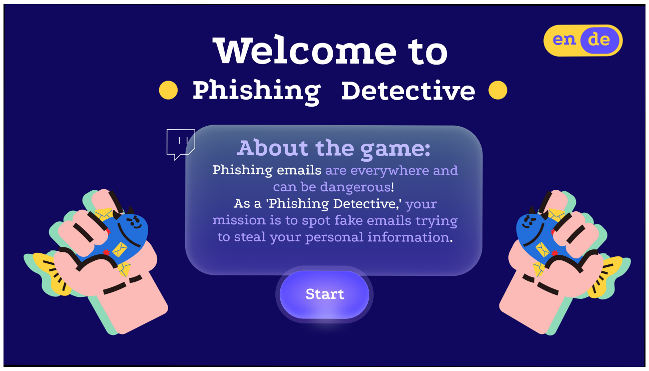
The system presents short phishing detection tasks that encourage users to examine email content, make a decision, and learn from immediate feedback. The design supports brief, casual interactions and aims to strengthen attention to phishing cues and confidence in recognizing them. The learning experience consists of three interconnected components:

- **Phishing Scenario Presentation:** Email examples illustrate common phishing cues such as misleading sender information, linguistic inconsistencies, and suspicious links or attachments. Scenarios are based on familiar contexts to support recognition.
- **Decision and Interaction:** Users decide whether an email is legitimate or suspicious. A countdown timer limits inspection time, while an optional hint feature provides selective guidance.

- **Feedback and Reflection:** Each decision triggers immediate visual feedback. Incorrect choices highlight relevant indicators. A final summary supports brief reflection and encourages replay.

3.2 Implementation

The development process began with prototyping in Figma[3], where visual elements (color scheme, icon style, layout, transitions) were defined. The interactive version was then implemented in Unity. The homepage was designed with strong visual appeal: contrasting colors, bold typography, and a detective-theme framing (*Phishing Detective*) to create a sense of challenge while reducing the impression of formal training. Figure 1 shows the start screen with its prominent "Start" button and thematic visuals.



Welcome to Phishing Detective

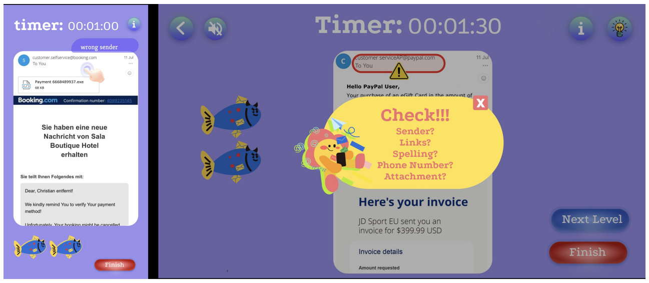
About the game:

Phishing emails are everywhere and can be dangerous!

As a 'Phishing Detective,' your mission is to spot fake emails trying to steal your personal information.

Figure 1: Homepage of the phishing game, using a detective theme to attract and motivate users.

After pressing "Start," users viewed introduction screens explaining phishing indicators (e.g., suspicious senders, spelling errors, strange links). Participants encountered phishing email examples across different difficulty levels during the session. A countdown timer limited inspection time, and hints could be requested when needed. The interface also provided navigation, mute, and exit controls. Feedback overlays rewarded correct identifications with fish icons and displayed encouraging text for errors. Participants could continue to the next task or exit at any point.



timer: 00:01:00

wrong sender

customer.selfservice@booking.com
To You
11 Jul

Payment 6668489937.exe
68 KB

Booking.com Confirmation number: 4089235145

Sie haben eine neue Nachricht von Sala Boutique Hotel erhalten

Sie teilt Ihnen Folgendes mit:

Dear, Christian entfernt!

We kindly remind You to verify Your payment method!

Unfortunately, Your booking might be cancelled

Timer: 00:01:30

customer serviceAP@paypal.com
To You
11 Jul

Hello PayPal User,

Your purchase of an eGift Card in the amount of

Check!!!
Sender?
Links?
Spelling?
Phone Number?
Attachment?

Here's your invoice

JD Sport EU sent you an invoice for $399.99 USD

Invoice details

Amount requested

Figure 2: Comparison of phishing detection screens: (pilot version left) with direct hint and no exit button; (revised version right) with guiding feedback overlay and an exit option. Note: The setup was initially tested on a vertical screen and later deployed on a horizontal screen.

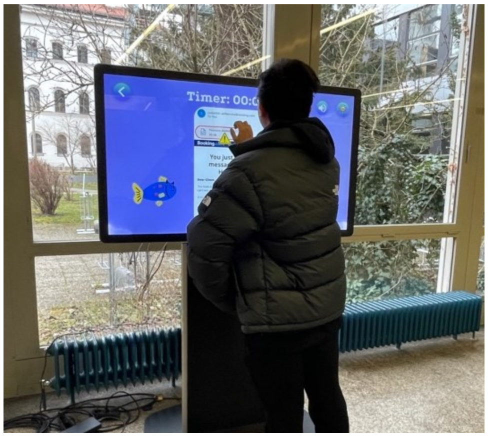


Figure 3: A participant interacting with the display during the main study.

3.3 Pilot Study

The pilot study took place in a controlled laboratory setting with five student participants, recruited through personal contacts and friends. Participation was voluntary and not compensated. Each participant completed the phishing detection task and then joined a short interview focusing on clarity, pacing, and the usefulness of the feedback (see Appendix A). The feedback informed several refinements to the system. The task duration was extended from 60 to 90 seconds, the hint feature was revised to provide brief textual cues, and visual feedback was adjusted to be clearer and more supportive (see Figure 2). In addition, an instruction screen and an exit option were introduced to improve transparency and user control before proceeding to the main deployment.

3.4 Main Study

The main study was conducted as an open five-day deployment in a university atrium. The location provided steady foot traffic and allowed the observation of walk-up interaction in a natural public setting. Participation was voluntary and unprompted: passers-by could approach the display, explore the task, and complete a short questionnaire afterward (Figure 3). The interaction and questionnaire together took approximately five to seven minutes, and participants who completed both received a small snack as appreciation. During the deployment, 35 participants completed the full study flow (phishing detection task and questionnaire), and no early terminations were logged. The system offered three difficulty levels (easy, medium, hard), and to maintain low interaction barriers typical for public displays, participants self-selected one level per session. This resulted in a between-subjects allocation with uneven group sizes that reflected walk-up behavior rather than controlled assignment. Accordingly, we report descriptive statistics rather than inferential comparisons between difficulty levels.

3.4.1 Data Collection Methods. Data collection combined interaction logs, questionnaire responses, and brief post-task reflections to capture both detection performance and user experience. Data collection focused on usability, user experience, engagement, and task

[3] https://www.figma.com/, last accessed 25.02.2025.

performance. After completing the interaction with the display, participants filled out a questionnaire consisting of both standardized and custom measures including (see Appendix B):

Usability. The System Usability Scale (SUS) [9] assessed perceived ease of use, learnability, and overall usability.

User Experience. Selected items from the User Experience Questionnaire (UEQ) [22] captured impressions of clarity, attractiveness, and interaction quality.

Engagement and Perceived Learning. Custom Likert-scale items assessed satisfaction, perceived improvement in phishing awareness, confidence in identifying suspicious cues, and willingness to engage with similar training formats. These items were adapted from prior work on situated cybersecurity learning [23].

Performance Measures. The system logged accuracy, hint usage, and interaction time for each task.

3.4.2 Data Analysis. Quantitative data from the questionnaire and system logs were analyzed using descriptive statistics. Qualitative responses were examined using a reflexive thematic analysis approach [8], using MAXQDA[4]. Two researchers conducted an initial coding pass, grouped codes into themes, and refined them through iterative review. The analysis focused on recurring experiences related to engagement, clarity of feedback, and perceived learning.

3.4.3 Participants. The main study included 35 participants. Of these, 54.3% identified as female and 45.7% as male. Most participants were between 18 and 25 years old (91.4%), with a smaller group aged 26 to 35 (8.6%). In terms of education, 65.7% reported holding or pursuing a bachelor's degree, 17.1% a master's degree or higher, 14.3% a high-school diploma or equivalent, and 2.9% a doctoral degree. Participants represented a range of academic fields, including Mathematics and Physics (29.4%), Computer Science (20.6%), Business and Economics (17.6%), Arts and Humanities (8.8%), Law (5.9%), Health Sciences (2.9%), and Engineering (2.9%), with 11.8% choosing not to specify their field.

3.5 Ethics and Data Protection

All participants received informed consent instructions prior to participation. They were briefed on the study's purpose, data handling procedures, and privacy protections. Data were anonymized and analyzed solely for academic purposes, ensuring that no personal information was disclosed. The study was carefully designed in line with our federal and university's data protection regulations, and approved by the local ethics committee.

4 Results

This section reports the empirical findings based on participants' in-the-wild interactions with the system. We structure the results around three dimensions aligned with our research focus: phishing detection performance, confidence in phishing judgments, and engagement in public display contexts.

4.1 Supporting Phishing Detection Performance

Phishing detection performance was measured as the percentage of correctly classified email examples. This metric reflects how effectively participants identified suspicious cues during the interaction.

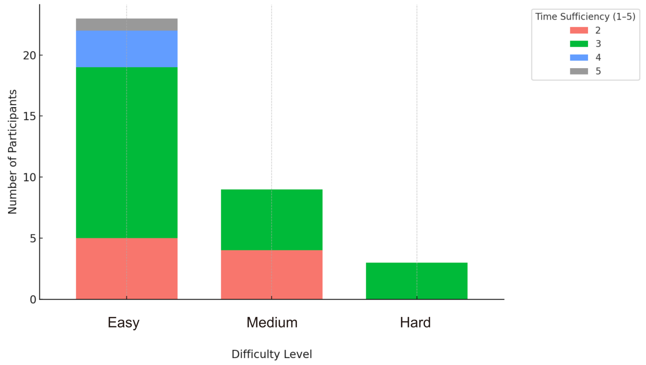


Figure 4: Perceived time sufficiency across starting difficulty levels.

After completing the tasks participants also rated whether the available time felt sufficient, providing insight into how time pressure influenced their decision-making process.

Participants engaged with phishing examples at different difficulty levels. As shown in Table 1, average accuracy decreased as difficulty increased: easy 70.29%, medium 68.89%, and hard 66.67%. The variability in performance was higher for more difficult tasks, with larger standard deviations at medium and hard levels. The number of participants completing each difficulty level differed (easy n=23, medium n=9, hard n=3), which should be considered when interpreting the results, particularly for the hard level.

Table 1: Detection accuracy, variability, and sample size by starting difficulty.

Difficulty	Mean Accuracy (%)	SD (%)	n
Easy	70.29	21.88	23
Medium	68.89	30.18	9
Hard	66.67	33.33	3

Perceived time sufficiency was rated on a 5-point Likert scale (1 = very insufficient, 5 = very sufficient). As illustrated in Figure 4, participants in the easy condition tended to report that the available time was mostly sufficient. Responses in the medium condition shifted toward lower sufficiency ratings, indicating increased time pressure. For the few participants who engaged with the hard condition, responses centered around a neutral assessment of sufficiency. Overall, perceived time sufficiency decreased as task difficulty increased. Given the small and uneven group sizes, particularly for the hard condition, we report trends descriptively rather than computing subgroup medians. Participants generally found the interaction easy to understand and did not report difficulties navigating the interface. The overall SUS score was 76.6 (SD = 14.1), which indicates good perceived usability.

4.2 Building Confidence in Phishing Judgments

Most participants reported that the game supported their ability to recognize phishing cues. In total, 97.2% rated the game as *Helpful* or *Very helpful* for identifying suspicious emails, and one participant selected a neutral response. Participants also reported increased

[4] https://www.maxqda.com/ (Last accessed: 15.01.2026)

caution when handling emails afterward: 45.7% described themselves as *Very cautious*, 40.0% as *More cautious*, and 11.4% as *Slightly more cautious*, while one participant reported no change.

Regarding anticipated future behavior, 45.7% expected a significant effect on how they evaluate email content, and 34.3% anticipated a moderate effect. In terms of retention, 45.7% indicated they were *Very likely* to remember the cues highlighted in the game, 34.3% *Likely*, and 14.3% *Extremely likely*, with one participant indicating lower likelihood. Overall, more than 80% expected their future confidence in identifying phishing attempts to improve.

Mean scores from the UEQ were above 4.0 for *Attractiveness*, *Perspicuity*, *Efficiency*, *Dependability*, and *Stimulation* (see Figure 5). *Attractiveness* received the highest rating (M = 4.39, SD = 0.52), suggesting that participants found the interaction appealing. *Novelty* received the lowest rating (M = 3.71, SD = 0.77), indicating more varied perceptions of how new or distinctive the experience felt.

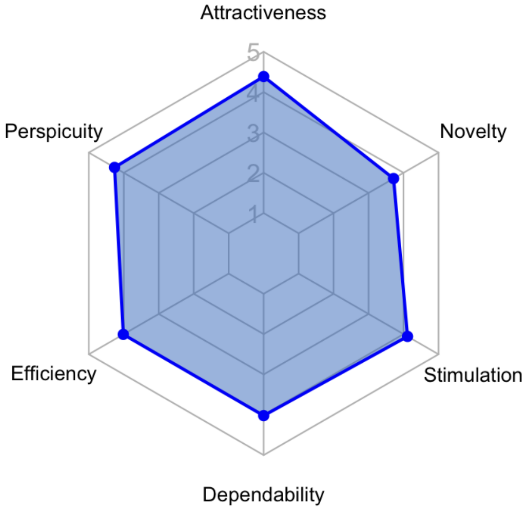


Figure 5: Overview of participant ratings on the User Experience Questionnaire.

4.3 Fostering Engagement in Public Display Contexts

As summarized in Figure 6, 68.6% of participants reported that they usually pay attention to content shown on public displays, compared to 20.0% who do not. A majority (65.7%) considered public screens to be effective for raising cybersecurity awareness, and only 5.7% viewed them as ineffective. Gamification for security-related topics was viewed as feasible by 74.3%, with no participants selecting *not feasible*. Willingness to engage with such games in public settings was more mixed: 54.3% indicated they would be willing to play, 34.3% were neutral, and 11.4% were unwilling.

To assess sustained engagement, participants were asked whether they felt tired or lost interest during the interaction. Most participants (65.7%) reported no fatigue or loss of interest. Smaller proportions reported slight (14.3%) or moderate (11.4%) fatigue, while 8.6% were neutral. No participants indicated complete disengagement.

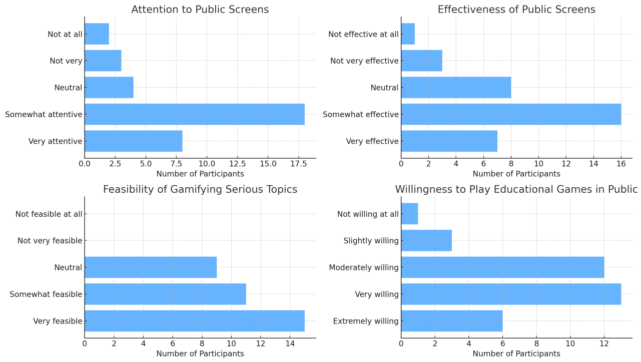


Figure 6: Acceptance of public displays and gamification across four items: attention to public display content, perceived effectiveness for cybersecurity awareness, feasibility of gamification for security topics, and willingness to engage with the game in public.

4.4 Qualitative Insights

Overall impressions. The open-ended responses centered on usability, feedback, and emotional engagement. Most participants expressed positive evaluations. Frequently mentioned descriptors included *helpful*, *interesting*, and *easy to use*. As one participant noted, *"The presentation of the system's goals is pretty clear"* (P27), while another emphasized the smooth interaction, *"The display responded well and was easy to follow"* (P19). Most users began interacting only after observing others do so, indicating the effect of social presence. Emotional responses varied during play. Some participants showed brief frustration or nervousness when errors occurred under time pressure, while correct identifications often elicited positive reactions. A noticeable portion (n=13) did not spend much time on the final summary screen, suggesting that brief public interactions may limit attention to end-of-session educational messaging.

Immediate feedback supported learning. Participants highlighted the role of clear corrective feedback and optional guidance in understanding phishing cues. For example, *"The error box made me notice what I missed"* (P2) and *"The hint helped me understand what to look for next time"* (P13). Beyond indicating correctness, feedback also appeared to scaffold phishing cue recognition: several participants described changes in their strategies after repeated exposure, such as *"checking the sender more carefully"* (P25) or *"looking at the link first"* (P3). This suggests that error-based feedback may encourage novices to adopt more systematic inspection behaviors. A small subset requested stronger visual emphasis or longer display duration for feedback, indicating that salience is important under time pressure.

Visual elements influenced engagement. Animated scoring and playful elements were described as engaging, for instance, *"The fish-catching animation is fun and keeps attention"* (P12). A few participants cautioned that highly playful visuals may reduce perceived realism (P17, P32). These responses indicate that gamified visual elements supported affective engagement during brief interactions, while also revealing a potential tension between playfulness and perceived seriousness for security-related content. Participants also mentioned that immediate rewards (e.g., catching the fish) created a sense of progress and satisfaction, suggesting that lightweight reward mechanics may help maintain attention in public display contexts.

Opportunities for refinement. Participants suggested minor adjustments, including a clearer timer display and additional guidance for first-time users. A small number mentioned that feedback could occasionally feel abrupt or difficult to interpret. These comments highlight the importance of onboarding and clarity in walk-up interactions: without prior instructions or contextual support, participants relied entirely on interface cues to make sense of the task. Suggestions such as clearer initial tutorials, more visible timers, and improved feedback transitions point to concrete design considerations for future deployments. Some participants also requested more informative end-of-session summaries, implying that reflection may not occur naturally unless explicitly supported in fast-paced public settings.

5 Discussion

Our findings suggest that brief, walk-up interactions with a gamified PSUI can support early stages of phishing awareness and decision confidence. At the same time, the situational and immediate nature of these learning outcomes highlights both the potential and the limitations of short-form security interventions in public settings.

5.1 Phishing Detection Performance

Detection accuracy was measured directly through task performance. As expected, accuracy declined slightly as the scenarios became more complex. This pattern aligns with prior work showing that phishing detection depends both on cue recognition and the cognitive resources available during evaluation [30, 36]. Similar to scaffolded training tools such as Anti-Phishing Phil [35], users benefited from beginning with simpler examples before encountering more subtle cues. While this reflects the intended design of increasing difficulty rather than a cognitive difference between users, it shows that even relatively simple phishing cues are not consistently recognized. Participants also reported that the available time felt more limited as difficulty increased, suggesting that time pressure influenced how closely they inspected email elements. These observations highlight the need for scaffolding when introducing more subtle phishing cues, especially in short public interactions. Participants' responses in the post-interaction questionnaire indicated increased confidence and greater caution when evaluating emails afterward. This suggests that immediate feedback and exposure to phishing cues can support early reflection and awareness formation, even within a short interaction window.

Implication 1: PSUIs should be evaluated not only by immediate detection accuracy, but by their ability to **support early reflection** and **confidence formation** under time and attention constraints.

5.2 Role of Feedback and Visual Engagement

Participants emphasized the importance of clear and immediate feedback. Error highlighting and selective hints helped them understand why an email was suspicious, without revealing answers outright. This reflects findings from security training research showing that supportive feedback can promote reflection without removing challenge [31, 38]. Our results extend this insight to a public display context, where feedback must be immediate and easy to interpret during short interactions. Animated visual elements contributed to engagement, although a few participants noted that highly playful visuals may reduce perceived seriousness. This indicates a design balance: feedback should be noticeable and engaging, but not distract from the security relevance of the task.

Implication 2: Immediate feedback should support **error interpretation rather than answer resolution**, while visual elements should remain **engaging without diminishing the perceived seriousness** of the security task.

5.3 Interaction in Public Space

Field observations showed that while many passers-by noticed the display, only a subset initiated interaction, and some began only after seeing others interact. This corresponds with prior work on public display engagement, which highlights the influence of social presence and visibility on participation decisions [24, 25]. Similar to the PSUI design considerations [26], our deployment shows that brief situated encounters can still support awareness formation and onboarding cues may encourage first steps. Several users spent little time on the final summary screen, indicating that reflective or explanatory information may need to be integrated earlier in the interaction rather than at the end. Public settings therefore require concise, in-flow learning moments rather than extended after-task explanations.

Implication 3: While social proof can encourage initial interaction with the PSUI, brief engagement norms in walk-up settings limit dwell time, suggesting that **reflection should be embedded within the interaction flow** rather than deferred to the end.

5.4 Limitations

The participant sample consisted mainly of young adults in a university setting, limiting generalizability to other populations and contexts. As a walk-up field deployment, the study introduced natural self-selection bias and constrained interaction time, which may have reduced the richness of qualitative responses and prevented longer reflection. Due to the brief, single-session nature of the deployment, we measured only immediate performance and perceived learning effects; sustained engagement, and transfer to real email behavior remain open questions. Future work should examine follow-up performance over time, explore adaptive difficulty progression, and evaluate deployments in more diverse public environments and demographic groups.

6 Conclusion

This study investigates how a gamified public display can support phishing awareness in everyday environments. Building on the Security Learning Curve and the goals of Public Security User Interfaces (PSUIs), the system was designed to enable short, walk-up interactions in which users examine email content, make classification decisions, and receive immediate feedback. The open deployment allowed the observation of in-situ engagement, showing that users were able to recognize phishing cues and reported increased caution when evaluating emails. Participants described the interaction as usable and engaging, and highlighted immediate feedback and hint-based guidance as particularly helpful. Field observations also indicated that attention and interest can be sustained in public contexts when the interaction remains brief, visually clear, and self-explanatory. These insights suggest that concise and interactive training formats can support initial stages of security awareness without requiring prior motivation or extended time commitment. Taken together, the results indicate that public displays may complement more formal cybersecurity training by embedding accessible learning opportunities into everyday routines. Gamified walk-up interactions have the potential to reach wider audiences and to encourage early awareness in contexts where traditional training would not normally be encountered.

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] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. 2021. Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access* 9 (2021), 44928–44949. doi:10.1109/ACCESS.2021.3066383

[2] Bhupendra Acharya, Dario Lazzaro, Efrén López-Morales, Adam Oest, Muhammad Saad, Antonio Emanuele Cinà, Lea Schönherr, and Thorsten Holz. 2024. The imitation game: exploring brand impersonation attacks on social media platforms. In *Proceedings of the 33rd USENIX Conference on Security Symposium* (Philadelphia, PA, USA) *(SEC '24)*. USENIX Association, USA, Article 248, 18 pages.

[3] Luca Allodi, Tzouliano Chotza, Ekaterina Panina, and Nicola Zannone. 2019. The need for new antiphishing measures against spear-phishing attacks. *IEEE Security & Privacy* 18, 2 (2019), 23–34.

[4] Amirah M Almutairi, Boojoong Kang, and Nawfal AL Hashimy. 2025. Business Email Compromise: A Comprehensive Taxonomy for Detection and Prevention. In *Proceedings of the 2024 7th International Conference on Information Science and Systems (ICISS '24)*. Association for Computing Machinery, New York, NY, USA, 49–54. doi:10.1145/3700706.3700714

[5] 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 (PerDis '12)*. Association for Computing Machinery, New York, NY, USA, Article 17, 6 pages. doi:10.1145/2307798.2307815

[6] Brandon Atkins and Wilson Huang. 2013. A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences* 1 (2013), 23–32. doi:10.4236/jss.2013.13004

[7] Benjamin Berens, Katerina Dimitrova, Mattia Mossano, and Melanie Volkamer. 2022. Phishing awareness and education–When to best remind. In *Workshop on Usable Security and Privacy (USEC)*. Network and Distributed System Security (NDSS) Symposium.

[8] Virginia Braun and Victoria Clarke. 2019. Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health* 11, 4 (2019), 589–597. arXiv:https://doi.org/10.1080/2159676X.2019.1628806 doi:10.1080/2159676X.2019.1628806

[9] John Brooke. 1996. Sus: A "quick and dirty" usability scale. *Usability Evaluation In Industry* (June 1996), 207–212. doi:10.1201/9781498710411-35

[10] Paolo Buono, Giuseppe Desolda, Francesco Greco, and Antonio Piccinno. 2023. Let warnings interrupt the interaction and explain: designing and evaluating phishing email warnings. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23)*. Association for Computing Machinery, New York, NY, USA, Article 197, 6 pages. doi:10.1145/3544549.3585802

[11] Brian Burke. 2014. *Gamify: How Gamification Motivates People to Do Extraordinary Things* (1st ed.). Routledge. doi:10.4324/9781315230344

[12] Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, and Robert G. Rittenhouse. 2016. Phishing Attacks and Defenses. *International Journal of Security and Its Applications* 10, 1 (2016), 247–256. doi:10.14257/ijsia.2016.10.1.23

[13] Edward L Deci and Richard M Ryan. 1980. Self-determination theory: When mind mediates behavior. *The Journal of mind and Behavior* (1980), 33–43.

[14] Verena Distler. 2023. The Influence of Context on Response to Spear-Phishing Attacks: an In-Situ Deception Study. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 619, 18 pages. doi:10.1145/3544548.3581170

[15] Adrián Domínguez, Joseba Saenz-de Navarrete, Luis de Marcos, Luis Fernández-Sanz, Carmen Pagés, and José-Javier Martínez-Herráiz. 2013. Gamifying learning experiences: Practical implications and outcomes. *Computers & Education* 63 (2013), 380–392. doi:10.1016/j.compedu.2012.12.020

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

[17] Raja Jabir, John Le, and Chau Nguyen. 2025. Phishing Attacks in the Age of Generative Artificial Intelligence: A Systematic Review of Human Factors. *AI* 6, 8 (2025). doi:10.3390/ai6080174

[18] Alexandros Kavvadias and Theodore Kotsilieris. 2025. Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review. *Applied Sciences* 15, 4 (2025), 2236. doi:10.3390/app15042236

[19] Michael Koddebusch. 2022. Exposing the Phish: The Effect of Persuasion Techniques in Phishing E-Mails. In *Proceedings of the 23rd Annual International Conference on Digital Government Research (dg.o '22)*. Association for Computing Machinery, New York, NY, USA, 78–87. doi:10.1145/3543434.3543476

[20] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 3, 1–12. doi:10.1145/1572532.1572536

[21] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)* 10, 2, Article 7 (May 2010), 7:1–7:31 pages. doi:10.1145/1754393.1754396

[22] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and evaluation of A user experience questionnaire. *Lecture Notes in Computer Science* (2008), 63–76. doi:10.1007/978-3-540-89350-9_6

[23] Ioana Andreea Marin, Pavlo Burda, Nicola Zannone, and Luca Allodi. 2023. The Influence of Human Factors on the Intention to Report Phishing Emails. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 620, 18 pages. doi:10.1145/3544548.3580985

[24] 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 (MAB '12)*. Association for Computing Machinery, New York, NY, USA, 55–64. doi:10.1145/2421076.2421086

[25] 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 (MM '10)*. Association for Computing Machinery, New York, NY, USA, 1285–1294. doi:10.1145/1873951.1874203

[26] 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

[27] Tatsuo Nakajima and Vili Lehdonvirta. 2013. Designing Motivation Using Persuasive Ambient Mirrors. *Personal and Ubiquitous Computing* 17, 1 (Jan. 2013), 107–126. doi:10.1007/s00779-011-0469-y

[28] Timo Ojala, Vassilis Kostakos, Hannu Kukka, Tommi Heikkinen, Tomas Linden, Marko Jurmu, Simo Hosio, Fabio Kruger, and Daniele Zanni. 2012. Multipurpose Interactive Public Displays in the Wild: Three Years Later. *Computer* 45, 5 (May 2012), 42–49. doi:10.1109/MC.2012.115

[29] Kathryn Parsons, Marcus Butavicius, Paul Delfabbro, and Meredith Lillie. 2019. Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies* 128 (2019), 17–26. doi:10.1016/j.ijhcs.2019.02.007

[30] Pooja Patel, Dawn M. Sarno, Joanna E. Lewis, Mindy Shoss, Mark B. Neider, and Corey J. Bohil. 2019. Perceptual representation of spam and phishing emails. *Applied Cognitive Psychology* 33, 6 (2019), 1296–1304. doi:10.1002/acp.3594

[31] Jan L. Plass, Steffi Heidig, Elizabeth O. Hayward, Bruce D. Homer, and Enjoon Um. 2014. Emotional design in multimedia learning: Effects of shape and color on affect and learning. *Learning and Instruction* 29 (2014), 128–140. doi:10.1016/j.learninstruc.2013.02.006

[32] Byron Reeves and J Leighton Read. 2009. *Total engagement: How games and virtual worlds are changing the way people work and businesses compete.* Harvard Business Press.

[33] Dawn M Sarno, Maggie W Harris, and Jeffrey Black. 2023. Which phish is captured in the net? Understanding phishing susceptibility and individual differences. *Applied Cognitive Psychology* 37, 4 (2023), 789–803. doi:10.1002/acp.4075

[34] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2022. Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours. In *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 13782)*. Springer, Berlin, Heidelberg, 248–265. doi:10.1007/978-3-031-25460-4_14

[35] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security (SOUPS '07)*. Association for Computing Machinery, New York, NY, USA, 88–99. doi:10.1145/1280680.1280692

[36] Frank Stajano and Paul Wilson. 2011. Understanding scam victims: seven principles for systems security. *Commun. ACM* 54, 3 (2011), 70–75. doi:10.1145/1897852.1897872

[37] Ioannis Stylianou, Panagiotis Bountakas, Apostolis Zarras, and Christos Xenakis. 2025. Suspicious minds: Psychological techniques correlated with online phishing attacks. *Computers in Human Behavior Reports* 19 (2025), 100694. doi:10.1016/j.chbr.2025.100694

[38] Eunjoon Um, Jan L Plass, Elizabeth O Hayward, Bruce D Homer, et al. 2012. Emotional design in multimedia learning. *Journal of educational psychology* 104, 2 (2012), 485.

A Pilot Study Questionnaire

1. Basic Information

(1) What types of email do you use most? (Select all that apply)
- Work email
- School email
- Personal email
- I don't use email
- Other: ____________________

(2) Have you ever received a phishing email?
- Yes
- No
- Not sure

(3) How much experience do you have with recognizing phishing emails?
- 1 - No experience at all
- 2 - Very little experience
- 3 - Some experience
- 4 - Quite a bit of experience
- 5 - Very experienced

(4) Have you received any formal training on phishing email detection?
- Yes (Please specify: ____________________)
- No

2. Interest in Game-based Learning

(1) Have you ever used a game to learn something?
- Yes
- No
- Not sure

(2) How interested are you in learning cybersecurity through interactive games?
- 1 - Not interested at all
- 2 - Slightly interested
- 3 - Neutral
- 4 - Interested
- 5 - Extremely interested

(3) If interested, what motivates you the most to engage with an educational game? (Select all that apply)
- Learning new skills
- Competing with others
- Gaining rewards or points
- Fun and entertainment
- Other: ____________________

(4) Besides interactive games, which forms of cybersecurity education are you interested in? (Select all that apply)
- Video tutorials
- Workshops or lectures
- Written materials
- In-person guidance or mentoring
- Other: ____________________

3. Game Functionality and Design

(1) What type of feedback mechanism do you find most helpful in detecting phishing emails?
- Immediate error notifications
- Summary report after the game
- Sound effects
- Comparison with real examples
- Other: ____________________

(2) Which elements of the game do you find most engaging? (Select all that apply)
- Visual design
- Rewards or incentives
- Game interactivity
- Immediate feedback
- Challenge level
- Educational content
- Other: ____________________

(3) How long should each game session ideally last?
- Less than 1 minutes
- 1–3 minutes
- 3–6 minutes
- More than 6 minutes

(4) How important is the scoring system (e.g., points, levels) to your engagement?
- Not important at all
- Slightly important
- Neutral
- Important
- Very important

(5) Would a leaderboard or comparison with other players make the game more engaging?
- Yes
- No

- Not sure

(6) Do you prefer levels with progressive difficulty or the ability to choose difficulty upfront?
- Progressive difficulty
- Choose difficulty upfront
- No preference

4. Expectations and Feedback

4.1 What do you expect from a phishing email detection game? (Select all that apply)
- Help me learn how to identify phishing emails
- Provide realistic case simulations
- Increase my cybersecurity awareness
- Offer challenges and rewards
- Other: ____________________

4.2 How would you rate the difficulty of the game?
- 1: Too easy
- 2: Slightly easy
- 3: Just right
- 4: Slightly hard
- 5: Too hard
- I cannot assess yet

4.3 What do you find most challenging in phishing email detection? (Select all that apply)
- Recognizing suspicious senders
- Identifying malicious links
- Spotting spelling or grammar errors
- Detecting suspicious attachments
- Other: ____________________

4.4 After playing this game, how confident do you feel about detecting phishing emails?
- 1: Not confident at all
- 2: Slightly confident
- 3: Neutral
- 4: Confident
- 5: Very confident

B Main Study Questionnaire

Part 1: Interview

I. General

(1) How would you describe your experience interacting with the display?

(2) Can you summarize the main purpose of the application in your own words?

(3) How easy or difficult was it to understand the purpose of the game?
- Very Easy
- Easy
- Neutral
- Difficult
- Very Difficult

(4) What specific improvements could make the first interaction more intuitive? ____________________

II. 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?
- Yes
- No

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

III. Content & Feedback

(1) What specific aspects of the game content did you find most engaging, and how did they enhance your experience?

(2) What type of feedback during gameplay impacted you most significantly, and why was it impactful?

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

Part 2: Survey

I. Overall Satisfaction

(1) How satisfied are you with the application overall?
- Very Satisfied
- Satisfied
- Neutral
- Unsatisfied
- Very Unsatisfied

(2) Do you think the application could motivate people to take action against phishing attacks?
- Yes
- No
- I don't know

(3) How likely are you to recommend this application to others?
- Very Likely
- Likely
- Neutral
- Unlikely
- Very Unlikely

II. Game Effectiveness in Phishing Awareness

(1) Do you think the game helped you identify phishing emails?
- Not helpful at all
- Not helpful
- Neutral
- Helpful
- Very helpful

(2) After playing this game, how cautious will you be about phishing emails in daily life?
- No cautious at all
- Not very cautious
- Neutral
- Somewhat cautious
- Very cautious

(3) Has the game changed the way you handle phishing emails?
- No change
- Slightly changed
- Moderately changed
- Significantly changed
- Completely changed

III. Educational & Long-Term Impact

(1) How likely are you to remember the knowledge gained from the game after 6 months?
- Not at all likely
- Slightly likely
- Moderately likely
- Very likely
- Extremely likely

(2) After 6 months, how do you expect your confidence in identifying phishing emails to change?
- Decreased significantly
- Slightly decreased
- No change
- Slightly increased
- Increased significantly

(3) How important is cybersecurity to you?
- Not important at all
- Not very important
- Neutral
- Somewhat important
- Very important

IV. Gamification & Public Display

(1) How feasible do you think gamifying serious topics is?
- Not feasible at all
- Not very feasible
- Neutral
- Somewhat feasible
- Very feasible

(2) Do you usually pay attention to content displayed on public screens?
- Not attentive at all
- Not very attentive
- Neutral
- Somewhat attentive
- Very attentive

(3) How effective do you think public display content is for cybersecurity awareness?
- Not effective at all
- Not very effective
- Neutral
- Somewhat effective
- Very effective

V. Interest in Content Format

(1) How willing are you to play educational games in public settings?
- Not willing at all
- Slightly willing
- Moderately willing
- Very willing
- Extremely willing

(2) If you are not willing, what is the main reason?
- Privacy concerns
- Social anxiety
- Lack of interest
- Other: ____________________________

(3) Did you feel tired or lose interest at any point during the game?
- Not at all
- Slightly
- Neutral
- Somewhat
- Completely

(4) If yes, please explain: ____________________________

3. 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.

4. 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

5. Personal Information

(1) What is your age group?
- 18–25
- 26–35
- 36–45
- 46–55
- 56 and above
- Prefer not to answer

(2) What is your gender?
- Male
- Female
- Other

(3) What is your highest degree or level of school you have completed?
- High school or below
- Bachelor's degree or equivalent
- Master's degree or above
- PhD
- Other: ____________________________

(4) What is your current employment status?
- Student
- Employed
- Self-employed
- Unemployed
- Retired
- Other: ____________________________

(5) What is your field of study?
- Computer Science
- Health Sciences
- Mathematics / Physics
- Psychology
- Other: ____________________________