Public Security User Interfaces

Supporting Spontaneous Engagement with IT Security

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

Viktorija Paneva
viktorija.paneva@unibw.de
University of the Bundeswehr Munich
Munich, Germany

Verena Distler
verena.distler@aalto.fi
Aalto University
Espoo, Finland
University of the Bundeswehr Munich
Munich, Germany

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

ABSTRACT

We introduce the concept of *Public Security User Interfaces* as an innovative approach to enhancing cybersecurity awareness and promoting security behavior change among users in public spaces. We envision these interfaces as dynamic platforms that leverage interactive elements and contextual cues to deliver timely security information and guidance to users. We identify four key objectives: raising awareness, triggering actions, providing control, and sparking conversation. Drawing upon Sasse et al.'s Security Learning Curve, we outline the stages for supporting users in adopting new security-related routines into habits, encompassing knowledge, concordance, self-efficacy, implementation, embedding, and secure behavior. Insights from research on public displays and spontaneous interactions inform the design of public security user interfaces tailored to different environments and user groups. Furthermore, we propose research questions pertaining to stakeholders, content, user interface design, and effects on users and discuss challenges as well as limitations. Introducing public security user interfaces to bridge the gap between cybersecurity experts and lay users sets the stage for future research and development in this emerging field.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Usability in security and privacy**;

KEYWORDS

Security User Interfaces, Privacy Awareness, Public Displays, Behaviour Change

ACM Reference Format:

Doruntina Murtezaj, Viktorija Paneva, Verena Distler, and Florian Alt. 2024. Public Security User Interfaces: Supporting Spontaneous Engagement with IT Security. In *New Security Paradigms Workshop (NSPW '24), September 16–19, 2024, Bedford, PA, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3703465.3703470

NSPW '24, September 16–19, 2024, Bedford, PA, USA

ACM ISBN 979-8-4007-1128-2/24/09
https://doi.org/10.1145/3703465.3703470

1 INTRODUCTION

We introduce the notion of *Public Security User Interfaces* and propose their exploration as a novel paradigm in security research. Public user interfaces have received considerable attention from the Human-Computer Interaction community for their ability to support spontaneous, low-friction engagement [18]. Think about a large display in a museum or shopping mall providing access to an exhibition or store directory. Users can plan their visit without needing to pull out the phone of their pocket and install an app first, but it is available and easy to use as users are willing to engage.

To date, we see few such public user interfaces being applied in security contexts despite many of their properties being a seemingly good fit with users' security behavior: for example, users generally do not actively engage with security, while personal devices (smartphones, laptops) require users to access security resources (pull) actively, public user interfaces can proactively deliver security content (push) [18]; moreover, public user interfaces can be (and often already are) deployed in settings in which users are open to engage, such as in a waiting situation, while commuting, or when willing to be educated [6]; and they can easily deliver value to multiple users, leveraging group dynamics [45].

The increased prevalence of cyber threats requires innovative approaches to public security awareness. This paper advocates the establishment of a public security user interface for providing information and encouraging behavior change on security-related topics. The novelty of this approach lies in its potential to reach diverse populations in different public sectors and thus improve overall cyber resilience. Unlike traditional methods, such as static posters or individual notifications, public interfaces provide dynamic, real-time information that can adapt to the context and needs of the audience. For example, during peak hours, when there is a high footfall, the interface can display brief, impactful messages to raise awareness quickly. During quieter times, it can provide more detailed guidance and instructions. The public interface can integrate with existing security systems, such as surveillance and emergency alerts, to provide both physical and digital security updates. For instance, during a cybersecurity threat, the interface can instantly

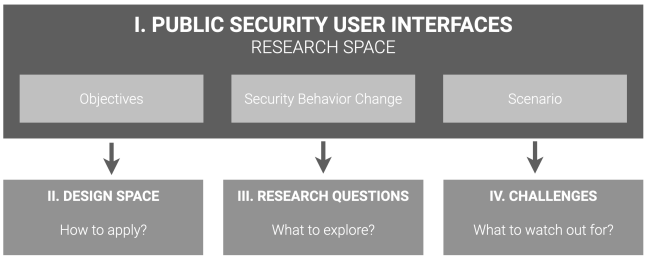


Figure 1: Our paper is centered around a research space for public security user interfaces, demonstrating how security behavior change can be supported using such interfaces. Then, we sketch a design space to guide researchers and practitioners aiming to create and deploy them. Furthermore, we show that many still open research questions exist in the context of the proposed paradigm. Our work is complemented by reflecting on challenges researchers and practitioners may encounter as they explore public security user interfaces.

broadcast alerts and guidance on protecting personal information while coordinating with physical security measures if needed.

Those properties of public user interfaces suggest an unexplored potential to address many open challenges in security research. Such user interfaces can raise awareness of security issues in which users are open to learning about them; they can spark discussion about security among a group of users in front of the display, thus supporting security becoming an integral part of their daily interactions; or they can trigger immediate actions in opportune moments and even provide active control over a security mechanism.

We provide a motivating scenario before briefly introducing related research. Afterwards, we lay out the concept of public security user interfaces in more detail, demonstrating the potential for supporting the habituation of secure user behavior and showcasing how the research space supports this novel class of security user interfaces. Then, we sketch a design space (for those interested in building public security user interfaces), list research questions (for those interested in exploring the concept in more depth) and finally discuss several challenges of this novel paradigm (see Figure 1).

2 DEFINITION AND MOTIVATING SCENARIO

We define a *Public Security User Interface* as any type of interface positioned in shared, non-personal areas that offers information or the opportunity to interact with security-related topics.

Consider the following scenario: Kim, a student at Crestwood University, begins her day with a visit to the university library. As she walks through the park adjacent to the library, she notices a prominent public display showcasing educational information and campus news. The display catches her eye with a screenshot of a suspicious phishing email circulated earlier that morning. Intrigued, she reads the accompanying information about cybersecurity best practices. Kim makes a mental note to stay vigilant about emails.

Kim decides to take a break in the afternoon after attending classes and studying in the library. She heads to the city's main square, where a popular takeaway coffee station is located. A public

Figure 2: Illustrative Scenarios for Public Security User Interfaces. (a) The public security user interface alerts students of potential tailgating situations, prompting proactive security actions. (b) Students are informed about an email phishing attack, promoting awareness and sparking discussion around cyber threats. Images generated with DALL-E 3.

display nearby shows current news updates and community messages. Today, it highlights practical tips for identifying phishing emails, which Kim finds relevant and timely given the morning's display at the park. Additionally, the display includes a segment on the importance of secure entry points. While waiting for her coffee, she discusses the importance of cybersecurity awareness on campus with Steven, a fellow student from her classes.

Later, Kim heads to the access-protected laboratory, where she conducts her research. The lab has valuable equipment and sensitive data, and entry is restricted to authorized personnel only. As Kim approaches the lab's entrance, she recalls the morning's lesson about tailgating and the importance of secure entry points. The lab's access system requires swiping her university ID card, which is monitored by security cameras to prevent unauthorized access.

As she swipes her card, the system detects someone closely following behind her (see Figure 2–left) and automatically prompts the person to provide their ID as well, highlighting the dangers of tailgating. The individual turns out to be Dr. Anderson, one of the leading researchers in her department. Dr. Anderson appreciates the system's vigilance and explains to Kim how such measures help prevent tailgating. They discuss the importance of maintaining strict access controls to safeguard their research projects from potential threats.

After settling in the lab, Kim runs into John (see Figure 2–right), an exceptional student known for his knowledge of cybersecurity. They talk about their day, and John mentions how he spotted the phishing email earlier via the university's distribution mail system. He credits the university's proactive cybersecurity measures, which he often reads about on the public displays around campus. They discuss strategies for secure online behavior, including the use of password managers and careful scrutiny of email links.

3 BACKGROUND AND RELATED WORK

We introduce research relevant to the proposed paradigm, specifically, interaction in public spaces and the security learning curve.

3.1 Interaction in Public Space

Research on interactive technology for deployment in public spaces began in the 1990s when small LCD displays became available. The

first applications were interactive door signs, cf. the Hermes door displays [13] for office doors and the RoomWizzard for meeting rooms [46]. As displays grew in size, the focus shifted towards communal areas in the workplace, where screens were used to publish news stories [34] or share photos [30]. Soon thereafter, researchers reflected on more suitable locations, identifying kitchens, foyers, and hallways as places where users would likely engage [15]. Furthermore, displays allowing users to post content (e.g., CommuntyWall [29]) were explored. The observation that many people engaged with such displays motivate their potential for security.

Another aspect attracting researchers' attention at that time was *targeting content* towards users and their interests. One example was the Aware Community Portal [52] at MIT. This capability is highly relevant in security as well, as users strongly differ in their interest in the topic and their prior knowledge.

In the mid-2000s, research on interactive technology in public spaces started to focus on *promoting social interaction*. For example, the GroupCast system [40] was specifically designed to spark conversations among colleagues. Similarly, systems like Sparks [14] and Ticket2Talk [41] were designed to encourage conversations at conferences. CoCollage [25] was deployed in a community-oriented cafe to support awareness and face-to-face interaction. We believe that, similarly, public displays can be used to make users talk about security topics.

The late 2000s saw larger, *long-living deployments* of displays, like the UBI-hostpot network, consisting of 12 displays installed across the city of Oulu, Finland [33]. Similarly, the e-Campus system deployed several displays across the campus of Lancaster University for many years [27]. Communities established themselves around those displays, which we envision to happen also around security-oriented networks installed in organizations.

The research community explored different *(future) applications* supported by deploying technology in public space relevant to the proposed paradigm. For example, Davies et al. [20] proposed using public displays to support behavior change (e.g., increasing fitness among school children through a walk-to-school program), seeking support in emergency situations, and providing personalized information. While cybersecurity was not a major focus of research during that time, its potential becomes apparent when we consider situations like phishing attacks aimed at multiple employees, where targeted education of individuals about cybersecurity and providing support as people try to habituate cybersecurity behavior would be very beneficial.

In the 2010s, much research has explored how *user engagement* with public user interfaces can be measured and supported. To this end, researchers created several behavioral models. Those can be used during the design and setup to guide users from becoming mere passersby to people interacting, as well as to measure the displays' effectiveness. Mueller et al. [44] present the audience funnel, which builds upon the Public Interaction Flow Model [10] and focuses on observable audience behavior. It consists of several interaction phases: passing by, viewing and reacting, subtle interaction, direct interaction, multiple interactions, and follow-up actions. Between the different phases, certain thresholds exist that need to be overcome to enter the next phase. To overcome the first threshold and transition from 'passing by' to 'viewing and reacting', the passerby's attention must be captured. To overcome the second threshold and move on to 'subtle interaction', the onlooker's curiosity must be piqued. Subsequent thresholds can be overcome by motivation. The strength of this model is that it can be used to calculate conversion rates and thus provide a measure of success for public display content or applications.

Interactions with public security user interfaces are typically spontaneous, opportunistic, and voluntary. Individuals need to be aware of the interfaces and their interactivity. They may potentially require convincing from the system itself to engage with them [44]. People gathered in front of the public security interface would naturally collaborate and discuss the content displayed [12]. The type of interaction between the user interface and an individual or group can vary depending on the environment. In environments such as companies or educational institutions (universities or schools), where individuals know each other, group formation tends to occur more quickly than in public environments with strangers [42]. This insight could be used in the system's design to increase acceptance. Insights from the advertising industry offer valuable strategies for maximizing public engagement with public security interfaces. Techniques such as targeted messaging, emotional appeal, and visual design can enhance public interest and engagement. Governmental campaigns, like military recruitment drives or public health initiatives, demonstrate effective ways of communicating complex topics in an accessible, appealing manner. Applying these methods can help make cybersecurity topics, such as privacy and secure behavior, more relatable to the public.

While traditional methods such as email campaigns, workplace online training, and social media are effective for disseminating information, there are unique advantages to using public interfaces:

Spontaneous Situations and Pushed Information Public interfaces engage users in spontaneous situations by pushing information directly to them, eliminating the need for users to actively seek out or pull information [5, 10].

Immediate Visibility and Contextual Relevance Public interfaces can provide contextually relevant information tailored to the specific location and situation, making the interaction more impactful.

Non-Disruptive Interaction Public interfaces allow the dissemination of information without disrupting the users.

No Need for Additional Devices or Apps Users do not need to take out their phones or install any apps to receive information from public displays. This convenience is a significant advantage over other methods, making information accessible and immediate.

Real-Time Updates and Broad Reach Public interfaces can reach a broader audience, including those who might not be engaged with digital communication channels.

3.2 Security-Related Behavior Change

Public displays might lend themselves to providing information and encouragement to change security-related behaviors. Behavior change is notoriously challenging and often depends on strong internal motivation from the person changing their behavior and routines. The behavior of an individual can be significantly affected by the presence of others. The actions and expectations of those

around them can strongly dictate an individual's response to various situations [38]. While a general discussion of behavior change is out of scope for the present paper, we want to highlight a recent framework summarizing security-related behavior change in organizational settings. To support employees in adopting new security-related routines, Sasse et al. [51] presented the security learning curve, a theory describing the factors required to support employees in behavior change.

The security learning curve consists of 9 stages, out of which traditional security measures in the form of security awareness education and training usually only cover the basic four. Beyond ensuring secure behavior is feasible (i.e., security policies can be followed and do not noticeably reduce productivity), those stages include sensitizing (what is the risk?), understanding (why is it a risk?), and information (how can the risk be mitigated?).

The following stages are particularly interesting, as they usually receive much less attention upon implementing measures and can be supported through public security user interfaces.

Concordance refers to users committing to a certain behavior and supporting them in doing so. It is known from other areas (e.g., health and well-being) that behavior change is only likely to happen as users really do want to change behavior. Here, it is particularly important to capture cases in which, despite users' general willingness, they do not succeed. For example, change usually requires time, but users will find excuses for not even trying if such time is not provided.

Self-efficacy refers to users having confidence in their ability to succeed. Several approaches exist to achieve this. Most importantly, self-efficacy increases as users have a positive experience (mastery experience) or observe others succeed with similar skills (vicarious experience) [7].

Implementation entails removing triggers to the old insecure behavior to avoid people falling back into existing routines.

Embedding refers to repeating the new, secure behavior to become automated. This includes applying techniques, such as intentional forgetting, by getting rid of stimuli (sensory, routine-related, space/time-related) hinting at old behavior.

Secure behavior has finally become routine. In this stage, rewards can be considered for those who have managed the transition (and sanctions for those who won't).

3.3 Summary

Our review suggests a strong potential at the intersection of research on interaction in public space and IT security-related behavior change. Prior research has shown that making users engage with public displays is challenging, and so is making users engage with security. We believe that through the combination of knowledge from both fields, more effective security user interfaces can be built that make security an integral part of users' everyday lives.

4 A RESEARCH SPACE FOR PUBLIC SECURITY USER INTERFACES

In the following, we sketch a research space for public security user interfaces structured along two dimensions, illustrated in Figure 3. Firstly, we will introduce four *objectives* of human-centered security research that we believe can particularly benefit from public interfaces. Secondly, we reflect on the *stages of the security learning curve* that public security user interfaces can support.

4.1 Objectives

We see the particular strength of public security user interfaces in four objectives. We do not consider this a comprehensive list of what can possibly be achieved by those interfaces, but they illustrate how such interfaces can support security research.

4.1.1 Creating Awareness. An inherent challenge in security is that users are often unaware of how their behavior puts them at risk [49]. Many reasons exist for this. Threats in the digital world are often difficult to perceive, attack vectors are complex and challenging to understand, and users struggle to assess how likely threats are.

One example is password reuse. Users generally understand the risk of attackers guessing simple passwords. In response, they often create complex, stronger passwords. However, because these are harder to remember, they end up reusing the same passwords across several accounts [17]. This poses a more difficult-to-understand risk for users, so-called credential stuffing attacks, resulting from a lack of awareness of how attackers exploit password-reuse behavior. As database breaches, attackers use bots to try out the credentials obtained on many websites, and as a result, each account protected with the same credentials is at risk.

Making users aware of such issues or addressing misconceptions is challenging as users are unlikely to look for such information actively. At the same time, public interfaces can deliver such knowledge in opportune moments (e.g., when users are in a waiting situation or other situations in which they are killing time).

Creating awareness does not come without challenges. Information needs to be *conveyed concisely*. Today, explanations are often textual, but reading text is very often unengaging. Public security interfaces can address this by using different kinds of media (for example, videos or sketches that explain a security-related topic in an entertaining yet understandable way. Another challenge is considering *user's prior knowledge*. For example, explaining to a user that checking the URL in an email could help identify a phishing email only makes sense after the user understands what a URL is and what the term 'phishing' relates to. This can be addressed in multiple ways. One approach could be to find a way of monitoring users' state of knowledge. However, this would require identifying users in front of the interface. Another approach would be to identify challenges in understanding certain terminology from physiological data. For example, eye gaze data has been shown to reveal situations in which users struggle to understand text, in particular terms unknown to them [50].

4.1.2 Triggering Actions. Another objective is to trigger security-related actions, making users perform a security task. One example could be installing security updates (for the operating system, the browser, or other software). A common challenge with this is that requests for updates often interfere with users' work, i.e., they are usually requested to perform the update when this would require interrupting what they are currently doing [54]. Furthermore, judging the importance of performing the update is often difficult.

Public security user interfaces can support such security actions in several ways. Firstly, users often encounter them when they are

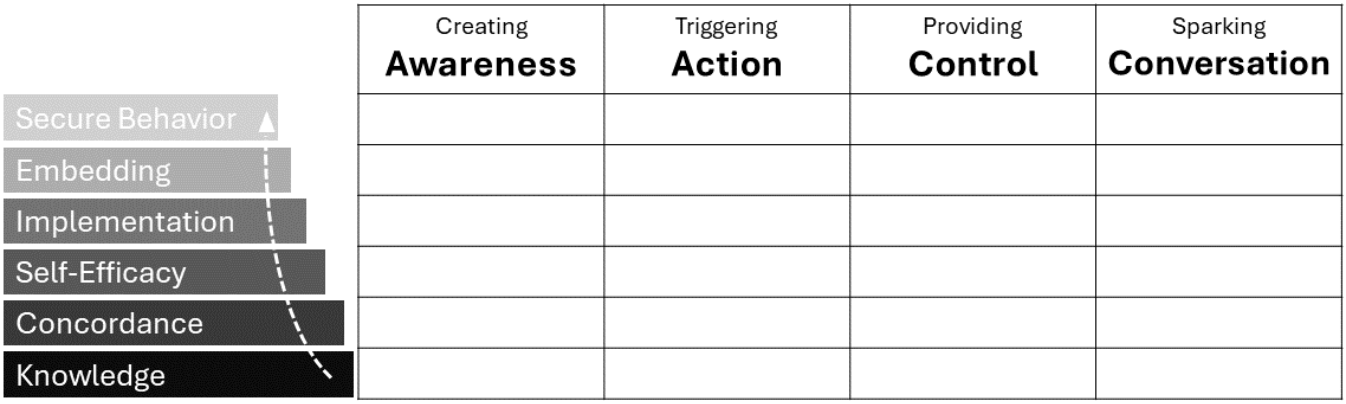


Figure 3: Research Space of Public Security User Interfaces along two dimensions: Objectives and Stages of the Security Learning Curve. This conceptual framework can guide the design, implementation, and evaluation of public security user interfaces by providing a structured approach to address key objectives along the different stages of the security learning curve.

not actively performing a task using their computer. As a result, this encounter provides an opportune moment to approach users with the suggestion to now perform the security task. For example, as a public security user interface makes users aware of the need for an update at the coffee machine, they could dedicate the first 3 minutes after returning to their work desk for the update. Another opportunity is to provide a reason for the requested update. Often, security updates result from discovering a weakness in the software (e.g., a zero-day exploit). In this case, providing users with some background information could serve as an additional motivating factor. Finally, it might be possible to monitor actions on an organizational level and use this information as a nudge to trigger action. Consider a public user interface conveying the percentage of employees that have already taken a certain action (for example, using email encryption, installing the latest security update, etc.).

Again, this objective comes with challenges. It is an open question of how to achieve high conversion rates resulting from the need to *switch the device* (e.g., perceiving the trigger on a display at the coffee machine but then performing the action on the working desk). Users might quickly *forget* about the intention after their return. Research could look into mechanisms that support such conversions. Researchers might also look at particularly suitable actions. For example, performing a security task for/on the smartphone might lead to high conversion rates. Consider a display in a subway station that suggests a security task that can be performed during the five minutes before the next train arrives.

4.1.3 Providing Control. Closely related to the previous objective, public security user interfaces can be designed not just to trigger actions but to enable users to perform certain security tasks directly using the interface. For example, the public interface might provide a means to initiate an update at the workplace through a simple click on the screen. Or, the user might be able to lock their desktop from the public interface if they have not done so.

A challenge might be that such control mechanisms could be *complex to implement*. For example, triggering a remote action would require identifying the user, e.g., through swiping a badge.

4.1.4 Sparking Conversation. Finally, a powerful objective is supporting cybersecurity discussion. While humans often report on security-related incidents from the real world (e.g., having been pickpocketed during a short weekend trip or burglars having broken into the neighbor's house), cybersecurity is rarely the topic of daily conversations [2]. Public security user interfaces can provide conversation starters, for example, in the form of thought-provoking or fun facts in situations where groups of people are near the interface. As a result, cybersecurity can be supported by becoming a more integral part of everyday life, leading to a generally higher level of awareness, knowledge, and willingness to engage.

4.2 Stages in the Learning Curve

We explain how the different stages[1] in the security learning curve can benefit from using public security user interfaces, thus supporting the aforementioned objectives. To recap, the objective of the security learning curve is to support secure behavior habituation.

4.2.1 Knowledge. The basis for the habituation of secure behavior is that users understand the reasons and need for such behavior. Traditionally, employees are often required to perform security tasks (e.g., participating in cyberawareness training) without much reasoning for why this is done beyond the very general argument that the company needs to protect itself from cyberattacks. With public security user interfaces, a much more detailed picture of why certain behavior is helpful and how specifically it reduces the risk of attacks can be drawn. This is highly motivating and likely increases users' willingness to engage in certain security behavior, even though it creates additional effort for them [1]. Again, we see the strength of public security user interfaces in their ability to provide such knowledge in opportune moments and deliver such knowledge in a push manner (as opposed to users being required to actively look for such information, which they usually only do as they are required to, e.g., being asked to look at training material and having to take a quiz/exam on it afterwards).

4.2.2 Concordance. Prescribing behavior is much less likely to result in sustained behavior change than cases in which users commit to changing their behavior [51]. Think about eating healthier or

[1]We subsume the first four stages of the original security learning curve under knowledge, as explanations of the risk and how to protect oneself are closely related.

exercising more: if prescribed by a doctor, it is unlikely that users will really change their behavior unless they want to [21].

Security behavior change is much more likely to happen as users commit to this change. Yet, it is currently an open question as to how this can be supported. Public security user interfaces can here provide means to increase their willingness to commit, remind them about this commitment, and, very importantly, to also provide them an opportunity to critically reflect on their progress and take action in cases in which they do not succeed.

A public security user interface could propose a certain behavior to focus on for some weeks and make people sign up to change their behavior. It could then provide reminders about the behavior, propose strategies of how to best implement it, and provide a mechanism that allows users to track their progress and point out reasons for which they do or do not succeed.

4.2.3 Self-Efficacy. Even when people know how to complete an action, they often do not put their knowledge into practice. One reason is that people's judgment of their capabilities (self-efficacy) affects their motivation and behavior [7].

Public security user interfaces could create so-called vicarious experiences by conveying the success of others: the number of current password manager users within the company or department could be displayed to motivate users also to start using it.

The challenge hereby is creating those vicarious experiences with as little effort as possible required by the user. The question here is how successful behavior can be automatically assessed and conveyed in an easy-to-understand and motivating manner.

4.2.4 Implementation. Secure behavior often requires effort to implement it. This can involve various steps, such as installing security software, setting up authentication mechanisms, or configuring privacy settings. Public security user interfaces can streamline the implementation process by providing clear and easy-to-follow instructions, step-by-step guides, and automated tools where possible, guiding and supporting users in adopting secure behaviors.

4.2.5 Embedding. Once secure behaviors are implemented, it is important to ensure they become integrated into daily routines and the organization's or community's culture. Embedding security practices into existing workflows and processes helps reinforce their importance and ensures long-term adherence. Public security user interfaces can support embedding by promoting continuous reinforcement of security principles through reminders, notifications, and integration with other tools and systems already in place. Fostering a culture of accountability and recognition for security-conscious behavior can further enhance embedding efforts.

4.2.6 Secure Behavior. As secure behavior has become routine, mechanisms can be implemented to reward successful behavior change and motivate others to do the same (e.g., establishing a 'cybersecurity champion' network [3]). Public security interfaces can support rewarding, for example, by conveying employees or departments that were successful in implementing the behavior.

4.3 Using the Research Space

Consider a company that wants to introduce a password manager for voluntary use by the employees. We discuss how, for this use case, public security user interfaces can support the process and increase employee uptake and adoption.

The organization 'WillSicher' is about to introduce a password manager. Hereby, the organization seeks to make passwords more usable and secure for their employees. Security is thought to be enhanced by (1) making users choose stronger passwords and not reuse passwords, primarily through the integrated password generator; (2) supporting users in getting rid of their previously created weak passwords; and (3) using the password managers to fill in password fields to prevent phishing. Usability is thought to be increased by eliminating the need for users to come up with and remember strong passwords and speeding up the authentication process through passwords being entered automatically. To support this process uptake and use by their employees, the introduction is accompanied by deploying public security user interfaces.

In the initial step, the organization seeks to raise awareness and create an understanding of what a password manager is useful for, pointing out the advantages to the user. In the initial step, the organization raises awareness of the password manager's purpose and advantages for users. At the same time, users' misconceptions and concerns are being addressed. To this end, displays deployed in public areas of the organization provide brief videos and comics introducing the password manager. These are easy and quick to perceive by employees as they cue for lunch, have a break, or wait for the elevator. The videos explain the common issues with easy-to-remember passwords and the reuse of passwords. Furthermore, it explains the password manager as the equivalent of a list of login names and passwords locked away in a safe. After providing these fundamentals, in the following weeks, it also points out some more specific features, such as the availability of the password manager for different devices and applications, the ability to automatically generate passwords, and how using the password manager to fill out password forms automatically protects users from phishing attacks. Steven realizes that the password manager has become a prominent topic among employees and sparked curiosity towards its release.

A week later, the availability of the password manager is announced via different communication channels, among them the public screens. The displays allow employees to have the link to download the password manager sent to their company email address by simply swiping the organization badge at the NFC reader next to the display. Along with the link, employees are asked whether they want to actively commit to using the password manager and receive active support (illustrated in Figure 4). Initially hesitant, Steven reads on the displays that already about 40% of the organization's employees had already committed to using the password manager. 'Cannot hurt to try it!', he thinks. Swiping his badge, the display shows him a brief and concise description of what he is committing to: first, he would get all his passwords entered into the password manager; second, he would, every time he signs up, use the password manager to generate a strong password and store it; third he would use the password manager each time he authenticates; and fourth, over time, he would update all his weak passwords. The display asks Steven to confirm with his signature and then sends the link to an online platform to Steven's email address. The platform provides additional information on the different steps, and Steven can ask questions if he gets stuck.

His colleague Laura sees him as he signs up. They have a brief chat, and as a result, Laura decides to sign up. 'Bet I will have all my passwords in the password manager faster than you!' Before they leave, the display suggests a strategy to get their passwords entered into the password manager, specifically suggesting setting two hours of working time aside for this task.

Two days later, Linda, responsible for in-organization mail delivery, walks up to Steven's desk and hands him over a small package. 'I know what it is', she says with a smile. 'It's a super cute get-rid-of-your-old-passwords squirrel with a small integrated display, my colleague also got one and put it on her desk. Whenever you access a website for which you are still using a password you should not, it will remind you to change it using your password manager. You can simply tip on its head, and your browser will take you to the site where you can update your password. I think they do it with a browser plugin.' 'That's a cool idea - don't you also want one?' 'I just signed up this morning', Linda replies. 'Can't wait to get it.'

Two days later, as Steven stands in the coffee kitchen, he notices a message on the display prompting him about his progress with transferring his passwords. 'I've got too much on my plate right now,' he thinks. Then, he spots a button on the display labeled 'Struggling to transfer your passwords?' Intrigued, he clicks it. The display presents a form, asking Steven to explain why he's encountering difficulties. 'Too much work, don't find time' he types. His colleague Mark observes him. 'I also wrote a message last week. I switched to the Brave browser recently, and the password manager is unavailable for it. I got a reply just the other day that the plugin is now available, so I installed it right away'.

At the team meeting two days later, Stevens's manager announces that the planned strategy meeting for Friday was called off. 'Everybody seems excited about the password manager but struggles initially to find the time to set it up. We discussed this with the CIO. Each team manager agreed to provide time for this explicitly. Let's get all our password managers up and running Friday!'

In Appendix A, we populate the table in Figure 3, illustrating how the objectives are targeted with the use of the public security user interface along the security learning curve for this scenario.

4.4 Summary

We laid out the proposed concept and used the scenario to demonstrate how a security measure in an organization as a semi-public place could benefit from it. In the following, we focus on how practitioners and researchers can benefit from and contribute to this novel line of research. In Section 5, we will sketch a design space, demonstrating how practitioners and researchers can design public security interfaces. In Section 6, we will provide some starting points for future research in this area. Section 7 reflects on some challenges we encountered while engaging with this novel concept.

5 DESIGN SPACE

We sketch a design space for public security interfaces aimed to guide designers and practitioners as they conceptualize and implement future applications. Design spaces not only provide a structured approach and a common vocabulary to compare and discuss different interface designs but also facilitate communication among

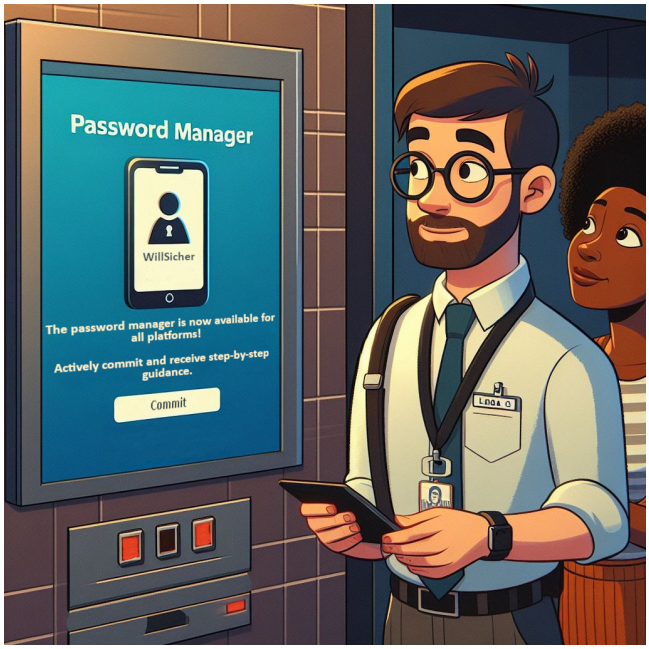


Figure 4: Public Security User Interface Supporting Password Manager Adoption. The interface facilitates adopting a password manager within an organization by guiding employees with information and interactive features (e.g., active commitment and support). Image generated with DALL-E 3.

diverse stakeholders such as security experts, developers, and end-users. Similar frameworks have proven useful in various domains of HCI research, e.g., public displays [44] and Automotive UIs [32, 35] as well as in privacy research, for example, the design of privacy notices [53]. Drawing upon them, we identify the following key dimensions of our design space of public security user interfaces: user, content, interaction, technology, and context (see Figure 5). By envisioning public security user interfaces as dynamic, interactive tools that use contextual information, we seek to push the boundaries of current thinking and challenge traditional security models. While the design space is not exhaustive and remains to evolve alongside the technology and the research area itself, it provides a foundation for collaboration and informed decision-making in the design of public security user interfaces.

5.1 User

With regard to the user, we distinguish the mode (i.e. whether the display is for use by a single or multiple users) and the relationshiop between the user interacting as well as the bystanders.

User Mode Depending on the purpose, size, and context, public security user interfaces can be actively used by one person exclusively (*single user*) or by several persons (*multi-user*).

Bystander Public security user interfaces can be designed to not only support active users but also bystanders. Previous research indicates that people are more inclined to talk about privacy and security with people in their social circle [28]. Hence, the design might differ based on the relationship between user(s) and bystanders (*acquaintances* or *strangers*).

User	User Mode	Single User			Multiple Users	
	Bystander	Acquaintances			Strangers	
Content	Medium	Text	Image	Audio	Video	Other
	Adaptability	Demographics	Location	Time	Event-based	Other
Interaction	Input Modality	Touch	Gesture	Gaze	Speech	
	Output Modality	Visual	Auditory	Haptic/Tactile	Olfactory	
	Initiation	User		System		
Technology	Display Properties	Size	Resolution	Brightness	Other	
	Device	Touchscreen	Projector	Tabletop	Tangible	Other
	Connectivity	E-mail	App	Notification	Printout	Other
Context	Environment	Workplace	Public Transport	Public Spaces	Other	

Figure 5: Design Space of Public Security User Interfaces

To ensure inclusivity, these interfaces must be designed to accommodate users with diverse abilities, including those with visual, auditory, or cognitive impairments. The specific medium for delivering content to users will be discussed further in the next section.

5.2 Content

Regarding the content, we distinguish the medium on which it is displayed as well as whether and if so, how the content is adapted.

5.2.1 Medium. Public security user interfaces can use *text* to convey important security messages, guidelines, and instructions to users, that they can read at their own pace. *Images* such as diagrams, infographics, and illustrations can enhance understanding and retention of security-related information. The content could also include engaging *videos*, *comics* [37], and *games* [16, 39] to capture users' attention while illustrating security concepts, demonstrating security procedures, or showcasing real-world scenarios. *Audio* elements can complement visual information, provide auditory alerts for security notifications, and enhance display accessibility.

5.2.2 Adaptability. The content on the public security user interface can be adapted according to the user *demographics*, encompassing factors such as occupation, age, familiarity with security topics etc., to enhance its effectiveness. Moreover, the content can be tailored to the *location* where the interface is deployed (e.g., providing information about tailgating at main entrances), and the *time* (e.g., prompting employees to log off before leaving the workplace during lunchtime). *Event-based* adaptability enables responses to situational factors or security threats, such as an ongoing phishing attack. To ensure accuracy and relevance, public security user interfaces require a dedicated content management system to oversee regular updates and prevent misinformation. A verification process for content creation and dissemination would help maintain consistency across platforms.

5.3 Interaction

Interactive user interfaces differ from non-interactive counterparts primarily in the level of participation they invoke from viewers. Interactive screens allow users to actively engage with the content by touching, gesturing, or using other interactive input methods. In contrast, on non-interactive screens, the content is displayed statically without any interaction with the user being possible. Viewers of non-interactive screens usually passively absorb the information displayed without actively engaging with it. According to Veenstra et al. [55] the introduction of interactive features has a significant impact on audience engagement with public user interfaces.

In considering the design of these interfaces, it is essential to address the principles of persuasive design. While nudging users towards better security practices can be beneficial, we must differentiate approaches from overly persuasive techniques that may exploit psychological vulnerabilities [26]. Careful consideration should be given to how we measure user engagement and ensure that the methods align with the best interests of users, promoting genuine understanding and adoption of security practices.

5.3.1 Input Modality. Public security user interfaces can integrate various input modalities to enhance user interaction and control [6]. *Touch* lets users directly interact with the interface by tapping, swiping, or pinching on touch-sensitive screens, facilitating intuitive navigation and control. *Gestures* provide an alternative input modality, allowing users to control the interface through hand movements or gestures, such as waving or pointing, to trigger actions or navigate security features. *Gaze* interaction allows users to interact with the interface using eye movements or gaze direction. By tracking the user's gaze, the interface can detect where the user is looking and respond accordingly, enabling hands-free interaction [36]. *Speech* interaction can be integrated into public security user interfaces, enabling users to interact with the interface using voice commands or spoken input to perform tasks, retrieve information, or initiate security actions.

5.3.2 Output Modality. Public security user interfaces can employ various output modalities to convey information or provide feedback to users. *Visual* output displays information through graphical elements, text, and icons, offering users visual cues and feedback. *Haptic/tactile* output involves tactile feedback, such as vibrations or tactile patterns, to alert users to security events or notifications, enhancing their awareness through touch sensation. *Auditory* output utilizes sound cues, tones, or spoken messages to deliver alerts and notifications. *Olfactory* output, although less common, could potentially be used to convey certain security-related cues, alert users, or promote secure behavior using scents [23].

5.3.3 Initiation. The user or the system can initiate the interaction with the public security user interface [4]. *User-initiated* interfaces require users to actively initiate the interaction, typically through explicit input such as tapping on a screen, speaking a command, or performing a gesture [56]. For example, a public user interface in a shopping center might offer interactive quizzes or games to educate users about security best practices, with users having to touch the display to start the interaction. In contrast, *system-initiated* interfaces trigger interaction autonomously based on predefined conditions or events, prompting users to engage without direct user input. For instance, a public security user interface in a museum might periodically change its content or display animations to attract the attention of passersby, encouraging them to interact, or it might show content upon users approaching (potentially even personalized in case the public user interface can identify the user in front of it).

5.4 Technology

A variety of technologies can serve as the basis for public security user interfaces. We distinguish display properties, devices, and means for users to connect to the public security user interface.

5.4.1 Display Properties. The *size* of graphical elements within security user interfaces influences their prominence and visibility. By strategically displaying important security indicators in larger sizes, designers can effectively draw users' attention and emphasise their significance. Varying the size of graphical elements allows for the creation of a visual hierarchy, guiding users' focus towards key security information. Furthermore, the *resolution* of the display determines the clarity and detail of the content presented, with higher resolutions allowing for sharper images and text. *Brightness* plays and important role in ensuring visibility and legibility of the content, especially in different lighting conditions.

5.4.2 Device. Public security user interfaces could be implemented using different devices. *(Touch) Screens* can be attached to walls or integrated into stands. The advantage is that the technology is widely available at low prices. They support different means of interaction, the most popular being touch capability, which is mostly integrated with the screen. *Projectors* are suitable for larger surfaces and allow for interfaces that can be widely viewed, approaching various people. *Tabletops*, that is, tables with an integrated display, often using touch functionality, are often found in education-centric environments, such as museums or schools. People can gather around the table, creating a need to make content perceivable from different perspectives while supporting settings well-suited for collaboration. Devices can also be *tangibles*, for example, small objects for placement on tables [22]. These can come with integrated sensing and actuation technology. Their advantage is that they are usually good at capturing attention, and they can serve as reminders. An example is the squirrel from the motivating scenario that served as a mascot for the password manager campaign. Finally, public security interfaces can be *wearables*. A well-known example from research is the BubbleBadge [24], a badge users can wear attached to their shirts and which can show short text messages. It could serve as a conversation starter or identify users as willing to help others with security tasks.

5.4.3 Connectivity. Enabling connectivity is important for extending the support of public security user interfaces beyond the immediate engagement with the interface itself. By allowing connectivity with other devices in users' ecosystems, the interaction can seamlessly transition to the user's private device, where security tasks can be executed. For instance, *e-mail* connectivity can facilitate the distribution of security updates and notifications directly to users' email accounts, ensuring widespread dissemination. *In-app* tutorials can offer comprehensive guidance for users requiring detailed instructions, empowering them to adopt security best practices at their own pace, whether they are on the go or have spare time. *Alerts* and *notifications* can promptly notify users of suspicious activities or breaches, or serve as proactive reminders to take recommended security actions. Additionally, *printout* functionality can enable users to generate hard copies of security-related documents for offline reference or sharing, ensuring seamless communication and engagement.

5.5 Context

Public security user interface can be situated in different environments and it may change over time. This can affect its visibility and, therefore, its effectiveness at attracting user engagement. The proximity of screens to the main trajectory in public spaces correlates strongly with user activity [48]. Screens in darker areas attract more attention due to their brightness, which leads to higher engagement. The effectiveness of outdoor displays is influenced by sunlight, which varies depending on the position, location, and time of day of the public user interface. Large user interfaces reach a captive audience, especially on escalators and in elevators, while grabbing the attention of those around them. The goals and success metrics for public security interfaces vary between corporate and public spaces. In public settings, success may be gauged by community engagement or awareness metrics, while in corporate environments, compliance and adherence to specific security protocols may serve as indicators.

5.5.1 Environment. In *workplace* environments, public security user interfaces can communicate important security protocols, procedures, and measures to employees. Positioned strategically in common areas like lobbies and break rooms, these interfaces provide real-time updates on potential cyber threats, security breaches, and contact information for IT security personnel. They also raise awareness of cybersecurity best practices and policies to prevent

data breaches, phishing attacks, and unauthorized access to sensitive data, ensuring that employees remain informed to protect the organization's assets and data. *Transportation hubs* like train stations, bus terminals, and airports can also benefit from public security user interfaces. These interfaces may inform travelers about common cyber threats, such as vulnerabilities in wireless networks or fraudulent ticketing websites, while also guiding practicing safe online behavior, e.g., when using a public WiFi or mobile devices during their journey. In *public spaces*, such as municipal buildings, government offices, and healthcare facilities, public security interfaces can promote cybersecurity awareness and community resilience. They can offer information about local cyber threats affecting residents, businesses, and government services, along with resources for reporting incidents or seeking assistance from experts. Furthermore, they can offer updates on events and initiatives introducing new technology to protect users and their digital environment. Moreover, public user interfaces can serve as educational tools in museums and educational institutions by offering information on security-related topics. They can inform visitors of security measures to safeguard digital exhibits, educational resources, and personal data. These interfaces may clarify existing security protocols, such as encryption methods, password policies, and secure data storage practices, and serve as channels for sharing information regarding cybersecurity workshops or training sessions available to visitors and staff. Positioned near entrances, exhibition areas and information desks, the interface can promote a culture of secure digital interaction in their educational context.

6 RESEARCH QUESTIONS

While the prior section was mainly meant as a starting point for designing public security user interfaces, the following section identifies interesting directions for future research in this area.

6.1 Stakeholders

Different stakeholders are involved as public security user interfaces are designed. These include, apart from users and bystanders (research questions for them are identified below), the place owner (i.e., the stakeholder on whose premises the interface is being deployed), the display provider (who is setting up/maintaining the display hardware), the application provider (the entity providing the software running on the public security user interface), and the content provider (might be the same as the application provider).

Place and Display Owners. In the sketched examples, the place and display owners (e.g., an organization) were directly interested in the public security user interface. This might not always be the case. Consider a bus stop or train station where large screens are deployed that are owned and operated by the transit authorities. The motivation to grant access to security content is less clear in this case. Here, interesting questions evolve around business models and value proposition for such settings, as well as the question of how the impact of such public security interfaces can be measured.

Furthermore, cases exist where place and display owners are different entities. Think about an office building with multiple companies, where one of the companies wants to install its own display in the lobby or elevator. How can place owners be motivated to grant access to those locations?

Application and Content Providers. Regarding applications and content, interesting questions emerge about maintenance, content creation, delivery, and moderation. About *maintenance*, the question is how to ensure the display and application are up and running and how to deal with operating system, software, and content updates.

Another interesting question is *scheduling* within and across applications. In some cases, security-related content/applications might be interlaced with other types of content. This becomes particularly interesting as the content is being targeted. What should be displayed if users with different knowledge or types of target behavior are in front of the display?

Another challenge is that of *content generation and curation*. To be engaging, novel content needs to be provided constantly. To be effective, information needs to be populated quickly. Think about cases in which employers are to be informed about a wave of phishing emails. Questions are: Who should be responsible for curating the content displayed on public security interfaces? Should it be sourced from security experts, crowdsourced from users, or a collaborative effort? If the latter, what workflows and supporting digital tools (e.g., content management systems, community forums, or specialized collaboration software tailored to security contexts) need to be set in place to ensure effective collaboration and content curation? If the content is user-generated/crowd-sourced, questions arise about how the effort to get such information on the display can be realized with as little effort as possible. In this case, content moderation is also important (who verifies the content for correctness and appropriateness? [31]).

6.2 Content

Independent of who is responsible for the content, many questions revolve around the selection, adaptation, and targeting of content.

Content Selection Criteria. What criteria should be employed to evaluate and select content for public security user interfaces? Key considerations may include factors like relevance to the target audience, accuracy of the security information, clarity, timeliness, and potential to engage users.

Content Adaptation. How can content be dynamically adapted based on contextual factors such as location, time of day, and user activity? What algorithms and mechanisms can be employed to ensure timely and relevant content delivery (potentially) based on real-time contextual data?

Content Personalization. How can user preferences, demographics, and past interactions be effectively captured and utilized to maximize the effectiveness of the interface? How can different presentation formats and multimodal interactive elements accommodate user needs and learning styles? How can the content personalization algorithms evolve over time to accommodate changes in user behavior, knowledge, and experience?

6.3 User Interface Design

While the design space above provides design options, many questions remain about how the user interfaces should be designed.

Conveying What Users Can/Should Do. What strategies can be used to effectively communicate security-related actions and recommendations to users in a concise, clear and accessible manner? How can interactive elements (tooltips, walkthroughs, and tutorials) be integrated into the interface to provide step-by-step guidance? What approaches can be taken to simplify complex security concepts and terminology for users of diverse technical literacy?

Targeting Opportune Moments. How can the timing of security interventions be optimized to coincide with moments of increased user attention and receptiveness? What scheduling algorithms and behavioral triggers can be used to identify optimal intervention windows? What sensors and data sources can be integrated into the public interface to capture real-time environmental cues and user behaviors? How can the collected sensor data (ambient light, noise, motion) be interpreted to infer user availability and receptiveness?

6.4 Effects on Users

Despite a compelling vision, the effects of the proposed user interfaces on users are still unclear but subject to interesting research. Helping users change their behavior through public interfaces is an important step towards solving many cybersecurity challenges. However, it is equally important to recognize that certain security measures need to be implemented privately, such as using multifactor authentication (MFA) to access sensitive systems or regularly updating personal devices and backing up important data. In addition, social constraints, such as the fear of being judged for applying or not applying strict security measures can influence security decisions. A comprehensive security strategy should consider both public interfaces and private measures, taking into account the broader societal context.

Short-Term vs. Long-Term Effects. Future studies could explore the short-term and long-term impact of the engagement and interaction with public security user interfaces on user sentiment, awareness, behavior, and overall receptiveness around security topics and discussions. Do users employ and follow up on suggested actions? What factors influence the adoption of the recommended security measures and foster sustainable behavioral change over time?

User Feedback and Sustained User Engagement. What mechanisms can be implemented to collect user feedback after interacting with the security interface? What strategies can ensure ongoing user engagement beyond the initial encounter? What incentives or motivational factors drive users to follow up on proposed or agreed-upon security actions? How can the interface continually reinforce security awareness and adherence to best practices? How can user interest in security topics be maintained in the long term?

User Perception. The users' perception can greatly influence engagement, trust, and adoption of security measures. Key considerations include understanding users' experience, ensuring usability in real-world environments, balancing perceived benefits and risks, and fostering community engagement, outreach, and learning. Are users comfortable with interacting with security-related content in public settings? Are the interfaces easy and intuitive to navigate? Are there barriers to accessing or comprehending content? How can public security user interfaces be designed to maximize benefits, such as increased awareness and empowerment, while minimizing risks, such as privacy concerns or information overload? Can public security user interfaces serve as a catalyst for dialog and engagement in security-related activities among community members?

7 CHALLENGES

The proposed security paradigm creates several challenges relevant to practitioners and researchers alike. In the following we discuss these challenges grouped into privacy, security, acceptance, and governance and investment.

7.1 Privacy

Personalized information and interactive user interface customization in public settings raise privacy concerns. One risk is *information disclosure*, where displaying personalized data on public screens could allow unauthorized individuals to access personal (potentially sensitive) information, compromising individuals' privacy. For example, as the display provides strategies to get rid of re-used passwords, this might suggest to bystanders that the person in front of the display is still reusing passwords.

Additionally, the lack of context in personalized content shown on public security user interfaces can lead to misinterpretation or incorrect assumptions by viewers, a phenomenon known as *decontextualization* [47]. Imagine a public display at a university that issues a cybersecurity alert stating *'University currently targeted by phishing attack!'* Without additional context, such as who has so far been affected, the type of phishing emails/the pretext used, or specific preventative measures students and staff should take, recipients of the information could either overreact by avoiding all university emails or underreact by not taking precautions.

Furthermore, while interactive customization enhances user engagement, it also raises concerns about the *privacy of shared or accessed information during interactions*. The visibility of personalized information to a wide audience increases the risk of privacy breaches and unauthorized access. Implementing privacy-preserving measures, such as the opportunity to transfer some content to the personal phone for perception, can help mitigate these risks and maintain user trust and acceptance of interactive security user interfaces in public settings. One effective example of such a measure is TouchProjector [8], which allows users to interact with remote screens via their mobile devices. Closely related is using visual markers to display personalized information on a user's smartphone [9]. This method secures the data and adheres to privacy standards by limiting access to personal information to the device owner.

For *identifying returning users*, public security user interfaces employ various methods, including implicit and explicit techniques. Implicit identification methods like face recognition and Bluetooth rely on biometric or technological characteristics to identify users in public spaces. Face recognition technology analyzes facial features captured by cameras to match them against stored profiles. Similarly, Bluetooth detects and recognizes users' mobile devices or wearables near the interface without requiring active user participation in the identification process [19]. In contrast, explicit identification methods, like tokens, involve using physical devices that users must present to the interface. Tokens, such as smart

cards or RFID tags, contain unique identifying information that the interface reads to identify the user.

Striking a balance between providing relevant content and protecting user privacy is crucial. To protect users' privacy, personalized content on public displays should be managed by authorized entities and based on user consent. This means that only authorized entities or systems should control what is displayed to ensure that no sensitive data is displayed without the explicit consent of users. This approach aligns with our objective to avoid sensitive information sharing in public spaces.

7.2 Security

Public interfaces may become targets for malicious actors seeking to disseminate misleading information, posing risks to user data and system integrity. Public user interfaces connected to networks are susceptible to security vulnerabilities, necessitating regular security assessments, software updates, and intrusion detection systems to identify and mitigate potential threats. Maintaining the security of public displays is essential, including regular patching, content updates, and physical security checks. Prolonged exposure of unattended digital displays can pose risks if left unmonitored, necessitating robust management protocols to maintain device integrity. Furthermore, Denial of Service (DoS) attacks threaten the availability and reliability of interactive interfaces, highlighting the importance of implementing measures such as rate limiting and traffic filtering [11]. Our paper suggests that user interfaces designed to influence user behavior can contribute to enhance security outcomes. Nevertheless, we recognize that relying on user behavior alone is not enough. Effective security also requires robust back-end measures. For example, ensuring that passwords are properly salted and hashed can reduce the risk of credential stuffing attacks. Salting a password involves adding a unique, random string of characters to each password before it is hashed, which is the process of converting the password into a fixed-size string of characters that appears random. This makes it much harder for attackers to crack the passwords, even if they obtain the hashed versions. Therefore, a holistic approach that combines both user-oriented and technical solutions is essential for optimal security. Physical security measures, including securing display hardware and controlling access to control systems, are also important to prevent physical tampering or theft.

7.3 Acceptance

While public displays could support spontaneous engagement with security topics, they also hold the risk of low acceptance or even negative reactions in certain cases. For instance, a person might feel shame if the interface displays information that seems personalized to them and that is not socially desirable. Public interfaces have been used for public shaming, for instance, when jaywalkers' faces are shown on large screens to deter jaywalking [43]. Even if unintentional, security information could also be perceived as shameful if it is perceived to relate to the person in front of the public interface. For instance, when an interface changes the message at the precise moment when somebody comes in sight and provides information that is perceived as obvious, the person might think that they were categorized as somebody with little IT security knowledge and feel put down in front of others. It is important for public interfaces to avoid such impressions or to even categorize people based on, for instance, age group and display information that could be stigmatizing. While these displays can foster group-based accountability, they must avoid inadvertently encouraging behaviors like public shaming or unnecessary self-policing. Acceptance aspects might also depend on culture, which has different conventions.

7.4 Governance and Investment

One crucial aspect of deploying displays in public spaces is the management and funding of these initiatives. In a public sphere, the deployment and maintenance of public interfaces would likely fall under the purview of local government agencies or public safety departments. Therefore, this approach necessitates public governance and investment. It is essential to consider whether the public would support such expenditures and how these interfaces could deliver tangible benefits to justify the investment. Public displays enable dynamic, interactive, and real-time content that engages users and adapts to changing security needs, making them a worthwhile investment. One challenge is maintaining the relevance of security information, as overly specific advice may quickly become outdated while general tips lack actionable value. Employing a system to dynamically adjust content based on real-time events or prevalent security concerns could bridge this gap. Engaging with community stakeholders and conducting pilot projects could provide valuable insights into public opinion and the practical impacts of public interfaces. In addition, partnerships with private entities or collaboration between the public and private sectors could provide alternative funding mechanisms that reduce the financial burden on public resources while increasing public security and awareness.

8 CONCLUSION

Public Security User Interfaces are a promising way to contribute to cybersecurity awareness and behavior change in the public space. By integrating interactive features, real-time updates and contextual relevance, these interfaces have the potential to engage users, stimulate discussion and empower individuals to make informed security decisions. Through various scenarios, we illustrate how public security user interfaces can facilitate knowledge sharing, incident response, and the cultivation of a security-conscious culture.

The main contributions of our paper include: (1) Identifying four key objectives of Public Security User Interfaces: raising awareness, triggering actions, providing control, and sparking conversation; (2) outlining a framework based on Sasse et al.'s Security Learning Curve [51] on how Public Security User Interfaces can support users in adopting new security-related routines into habits; (3) drawing a design space for Public Security User Interfaces to facilitate conceptualisation and implementation; and (4) proposing research questions pertaining to stakeholders, content, user interface design, and effects on users.

Public Security User Interfaces have the potential to transform passive bystanders into active participants in protecting digital assets and personal data. Empirical research findings demonstrating the value of such public interfaces can provide compelling support for such efforts. Gamification elements, such as interactive quizzes

or security challenges, can increase user engagement by encouraging active participation. Pilot studies in controlled environments, could further assess the impact of gamification on user motivation and learning outcomes. This is an important direction for future research in this area. Further research is also essential to refine design principles and explore scalability in different public environments.

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] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.

[2] Shahid Alam. 2022. Cybersecurity: Past, present and future. *arXiv preprint arXiv:2207.01227* (2022).

[3] Moneer Alshaikh. 2020. Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security* 98 (2020), 102003. https://doi.org/10.1016/j.cose.2020.102003

[4] Florian Alt, Jörg Müller, and Albrecht Schmidt. 2012. Advertising on Public Display Networks. *IEEE Computer* 45, 5 (may 2012), 50–56. https://doi.org/10.1109/MC.2012.150

[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*. 1–6.

[6] Florian Alt, Alireza Sahami Shirazi, Thomas Kubitza, and Albrecht Schmidt. 2013. Interaction techniques for creating and exchanging content with public displays. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 1709–1718. https://doi.org/10.1145/2470654.2466226 alt2013chi.

[7] Albert Bandura. 1982. Self-Efficacy Mechanism in Human Agency. *American Psychologist* (1982), 26.

[8] Sebastian Boring, Dominikus Baur, Andreas Butz, Sean Gustafson, and Patrick Baudisch. 2010. Touch projector: mobile interaction through video. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 2287–2296. https://doi.org/10.1145/1753326.1753671

[9] Sebastian Boring, Marko Jurmu, and Andreas Butz. 2009. Scroll, tilt or move it: using mobile phones to continuously control pointers on large public displays. In *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7* (Melbourne, Australia) *(OZCHI '09)*. Association for Computing Machinery, New York, NY, USA, 161–168. https://doi.org/10.1145/1738826.1738853

[10] Harry Brignull and Yvonne Rogers. 2003. Enticing people to interact with large public displays in public spaces.. In *Interact*, Vol. 3. 17–24.

[11] Han Cao, Patrick Olivier, and Daniel Jackson. 2008. Enhancing Privacy in Public Spaces Through Crossmodal Displays. *Soc. Sci. Comput. Rev.* 26, 1 (feb 2008), 87–102. https://doi.org/10.1177/0894439307307696

[12] Lei Chen, Hai-Ning Liang, Jialin Wang, Yuanying Qu, and Yong Yue. 2021. On the use of large interactive displays to support collaborative engagement and visual exploratory tasks. *Sensors* 21, 24 (2021), 8403.

[13] Keith Cheverst, Daniel Fitton, Alan Dix, and Mark Rouncefield. 2002. Exploring Situated Interaction with Ubiquitous Office Door Displays. In *Public, Community and Situated Displays (Workshop at CSCW 2002)*. New Orleans, LA, USA.

[14] Andrea Chew, Vincent Leclerc, Sajid Sadi, Aaron Tang, and Hiroshi Ishii. 2005. SPARKS. In *Extended Abstracts on Human Factors in Computing Systems* (Portland, OR, USA) *(CHI '05)*. ACM, New York, NY, USA, 1276–1279.

[15] Elizabeth F. Churchill, Les Nelson, Laurent Denoue, and Andreas Girgensohn. 2003. The Plasma Poster Network: Posting Multimedia Content in Public Places. In *Proceedings of the 9th IFIP TC13 International Conference on Human-Computer Interaction* (Zurich, Switzerland) *(INTERACT '03)*. IOS Press.

[16] Merijke Coenraad, Anthony Pellicone, Diane Jass Ketelhut, Michel Cukier, Jan Plane, and David Weintrop. 2020. Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. *Simulation & Gaming* 51, 5 (2020), 586–611. https://doi.org/10.1177/1046878120933312 arXiv:https://doi.org/10.1177/1046878120933312

[17] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The tangled web of password reuse.. In *NDSS*, Vol. 14. 23–26.

[18] Nigel Davies, Sarah Clinch, and Florian Alt. 2014. *Pervasive Displays - Understanding the Future of Digital Signage*. Morgan and Claypool Publishers. http://www.florian-alt.org/unibw/wp-content/publications/davies2014synthesis.pdf

[19] Nigel Davies, Adrian Friday, Peter Newman, Sarah Rutlidge, and Oliver Storz. 2009. Using bluetooth device names to support interaction in smart environments. In *Proceedings of the 7th international conference on Mobile systems, applications, and services*. 151–164.

[20] Nigel Davies, Marc Langheinrich, Rui Jose, and Albrecht Schmidt. 2012. Open display networks: A communications medium for the 21st century. *Computer* 45, 5 (2012), 58–64.

[21] Edward L Deci and Richard M Ryan. 2008. Self-determination theory: A macrotheory of human motivation, development, and health. *Canadian psychology/Psychologie canadienne* 49, 3 (2008), 182.

[22] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Human-Computer Interaction Conference* (Aarhus, Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 74, 13 pages. https://doi.org/10.1145/3546155.3546640

[23] Dmitrijs Dmitrenko, Emanuela Maggioni, Giada Brianza, Brittany E Holthausen, Bruce N Walker, and Marianna Obrist. 2020. Caroma therapy: pleasant scents promote safer driving, better mood, and improved well-being in angry drivers. In *Proceedings of the 2020 chi conference on human factors in computing systems*. 1–13. https://doi.org/10.1145/3313831.3376176

[24] Jennica Falk and Staffan Björk. 1999. The BubbleBadge: a wearable public display. In *CHI'99 extended abstracts on Human factors in computing systems*. 318–319.

[25] 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*. 2153–2156.

[26] Brian J Fogg. 2002. Persuasive technology: using computers to change what we think and do. *Ubiquity* 2002, December (2002), 2.

[27] Adrian Friday, Nigel Davies, and Christos Efstratiou. 2012. Reflections on Long-Term Experiments with Public Displays. *Computer, IEEE* 45, 5 (May 2012), 34–41.

[28] Nina Gerber and Karola Marky. 2022. The Nerd Factor: The Potential of S&P Adepts to Serve as a Social Resource in the User's Quest for More Secure and Privacy-Preserving Behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 57–76.

[29] Antonietta Grasso, Martin Muehlenbrock, Frederic Roull, and Dave Snowdon. 2003. Supporting Communities of Practice With Large Screen Displays. In *Public and Situated Displays – Social and Interactional Aspects of Shared Display Technologies*, Kenton O'Hara, Mark Perry, Elizabeth Churchill, and Daniel M. Russel (Eds.). Kluwer, 261–282.

[30] Saul Greenberg. 1999. Designing Computers As Public Artifacts. In *International Journal of Design Computing: Special Issue on Design Computing on the Net (DCNet '99)*.

[31] Miriam Greis, Florian Alt, Niels Henze, and Nemanja Memarovic. 2014. I Can Wait a Minute: Uncovering the Optimal Delay Time for Pre-moderated User-generated Content on Public Displays. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 1435–1438. https://doi.org/10.1145/2556288.2557186

[32] Renate Haeuslschmid, Bastian Pfleging, and Florian Alt. 2016. A Design Space to Support the Development of Windshield Applications for the Car. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5076–5091. https://doi.org/10.1145/2858036.2858336

[33] 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 *Proceedings of the 4th International Conference on Multimedia and Ubiquitous Engineering* (Cebu, Philippines) *(MUE '10)*. 6 pages.

[34] Stephanie Houde, Rachel Bellamy, and Laureen Leahy. 1998. In Search of Design Principles for Tools and Practices to Support Communication within a Learning Community. *SIGCHI Bulletin* 30, 2 (April 1998), 113–118.

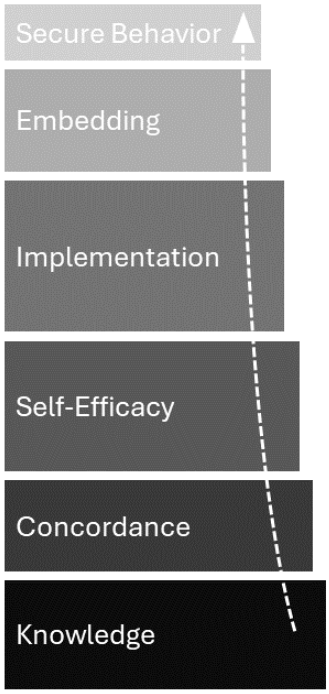
[35] Dagmar Kern and Albrecht Schmidt. 2009. Design space for driver-based automotive user interfaces. In *Proceedings of the 1st International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (Essen, Germany) *(AutomotiveUI '09)*. Association for Computing Machinery, New York, NY, USA, 3–10. https://doi.org/10.1145/1620509.1620511

[36] Mohamed Khamis, Florian Alt, and Andreas Bulling. 2016. Challenges and design space of gaze-enabled public displays. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* (Heidelberg, Germany) *(UbiComp '16)*. Association for Computing Machinery, New York, NY, USA, 1736–1745. https://doi.org/10.1145/2968219.2968342

[37] Sonia Chiasson Leah Zhang-Kennedy and Robert Biddle. 2016. The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity. *International Journal of Human–Computer Interaction* 32, 3 (2016), 215–257. https://doi.org/10.1080/10447318.2016.1136177 arXiv:https://doi.org/10.1080/10447318.2016.1136177

[38] Linda Little, Pam Briggs, and Lynne Coventry. 2005. Public space systems: Designing for privacy? *International journal of human-computer studies* 63, 1-2 (2005), 254–268.
[39] Sana Maqsood and Sonia Chiasson. 2021. Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Trans. Priv. Secur.* 24, 4, Article 28 (sep 2021), 37 pages. https://doi.org/10.1145/3469821
[40] Joseph F. McCarthy. 2002. Using Public Displays to Create Conversation Opportunities. In *Public, Community and Situated Displays (Workshop at CSCW 2002)*. New Orleans, LA, USA.
[41] Joseph F. McCarthy, David W. McDonald, Suzanne Soroczak, David H. Nguyen, and Al M. Rashid. 2004. Augmenting the Social Space of an Academic Conference. In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*. ACM, New York, NY, USA, 39–48.
[42] 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. https://doi.org/10.1145/2421076.2421086
[43] Paul Mozur. 2018. Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras. *The New York Times* (July 2018). https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html
[44] Jörg Müller, Florian Alt, Daniel Michelis, and Albrecht Schmidt. 2010. Requirements and Design Space for Interactive Public Displays. In *Proceedings of the International Conference on Multimedia* (Firenze, Italy) *(MM'10)*. ACM, New York, NY, USA, 1285–1294. https://doi.org/10.1145/1873951.1874203
[45] Andrea Nutsi and Michael Koch. 2015. Multi-User Usability Guidelines for Interactive Wall Display Applications. In *Proceedings of the 4th International Symposium on Pervasive Displays* (Saarbruecken, Germany) *(PerDis '15)*. Association for Computing Machinery, New York, NY, USA, 233–234. https://doi.org/10.1145/2757710.2776798
[46] Kenton O'Hara, Mark Perry, and Simon Lewis. 2003. Situated Web Signs and the Ordering of Social Action. In *Public and Situated Displays – Social and Interactional Aspects of Shared Display Technologies*, Kenton O'Hara, Mark Perry, Elizabeth Churchill, and Daniel M. Russel (Eds.). Kluwer, 105–140.
[47] Morin Ostkamp, Christian Kray, and Gernot Bauer. 2015. Towards a privacy threat model for public displays. In *Proceedings of the 7th ACM SIGCHI Symposium on Engineering Interactive Computing Systems* (Duisburg, Germany) *(EICS '15)*. Association for Computing Machinery, New York, NY, USA, 286–291. https://doi.org/10.1145/2774225.2775072
[48] Callum Parker, Martin Tomitsch, and Judy Kay. 2018. Does the Public Still Look at Public Displays? A Field Observation of Public Displays in the Wild. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 73 (jul 2018), 24 pages. https://doi.org/10.1145/3214276
[49] Karen Renaud and Wendy Goucher. 2014. The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. In *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2*. Springer, 361–372.
[50] Sheikh Radiah Rahim Rivu, Yasmeen Abdrabou, Yomna Abdelrahman, Ken Pfeuffer, Dagmar Kern, Cornelia Neuert, Daniel Buschek, and Florian Alt. 2021. Did you Understand this? Leveraging Gaze Behavior to Assess Questionnaire Comprehension. In *Proceedings of the 2021 ACM Symposium on Eye Tracking Research & Applications* (Stuttgart, Germany) *(COGAIN '21)*. Association for Computing Machinery, New York, NY, USA, 5 pages. https://doi.org/10.1145/3448018.3458018
[51] M Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2022. Rebooting it security awareness–how organisations can encourage and sustain secure behaviours. In *European Symposium on Research in Computer Security*. Springer, 248–265.
[52] Nitin Sawhney, Sean Wheeler, and Chris Schmandt. 2001. Aware community portals: Shared information appliances for transitional spaces. *Personal and Ubiquitous Computing* 5 (2001), 66–70.
[53] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Eleventh symposium on usable privacy and security (SOUPS 2015)*. 1–17.
[54] Kami Vaniea and Yasmeen Rashidi. 2016. Tales of software updates: The process of updating software. In *Proceedings of the 2016 chi conference on human factors in computing systems*. 3215–3226.
[55] Mettina Veenstra, Niels Wouters, Marije Kanis, Stephan Brandenburg, Kevin Raa, Bart Wigger, and Andrew Vande Moere. 2015. Should Public Displays be Interactive? Evaluating the Impact of Interactivity on Audience Engagement. https://doi.org/10.1145/2757710.2757727
[56] Robert Walter, Gilles Bailly, and Jörg Müller. 2013. StrikeAPose: revealing mid-air gestures on public displays. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 841–850. https://doi.org/10.1145/2470654.2470774

A ACHIEVING SECURITY OBJECTIVES USING PUBLIC SECURITY USER INTERFACES: EXAMPLE



Creating **Awareness**	Triggering **Action**	Providing **Control**	Sparking **Conversation**
		Follow-up prompts with additional support and feedback collection.	Exchanging solutions on common issues, e.g., using the password manager on a new browser. Creating a security culture by providing the employees dedicated time slots to perform the security actions.
		Step-by-step guidance, tutorials and links to additional resources.	
	Information about the percentage of employees already using the password manager.		A colleague motivated by seeing someone they know signing up for the password manager.
	An active commitment prompt.	A download link automatically sent to the user's work email.	
Engaging visual content introducing the password manager and its features.			

Figure 6: We illustrate how the objectives identified along the different stages of the security learning curve can be achieved through the use of a public security user interface, using the introduction of a new password manager in an organization (Section 4.3) as an example scenario.