Enhancing the Experience of Security and Privacy Warnings with Smell, Taste, and Temperature

DANIELA NAPOLI and SONIA CHIASSON, Carleton University, Canada

Cybersecurity and privacy warnings are often ignored by users, and previous work has considered improvements to their visual design, such as attention to symbols, colours, and text used. Despite these improvements, users continue to bypass warnings and are exposed to security and privacy threats, thus indicating that further work is needed. Continuing to hone visual aspects of warnings may not suffice. Visual warnings are problematic for users of emerging display-less technology, people who cannot use their sight to engage with interfaces, and users whose visual attention is elsewhere. In this position paper, we discuss the opportunities for using smell, taste, and temperature feedback to enhance the experience of security warnings. Using our previous work on temperature warnings as a case study, we outline unique challenges relating to adopting such feedback for warnings and propose areas of considerations when implementing thermal interactions within security and privacy context.

ACM Reference Format:

Daniela Napoli and Sonia Chiasson. 2021. Enhancing the Experience of Security and Privacy Warnings with Smell, Taste, and Temperature. In *CHI '21: CHI Conference on Human Factors in Computing Systems, May 08–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Cybersecurity and privacy information is delivered primarily via visual means (i.e., on a device screen). We contend that non-visual feedback can either augment or replace visual techniques for communicating security information to users. Our research investigates many non-visual alternatives, but we specifically consider the potential of smell, taste, and temperature in this position paper. We focus on the challenges from two use cases: communicating security and privacy information to users of display-less technology and to users with visual impairments. As an example, we discuss our work on thermal TLS warnings and describe the unique design challenges arising from communicating browser security via temperature feedback.

Researchers have explored many different ways of improving the usability of security warnings. To attract users' attention and guide them towards secure actions, dynamic skins [6], full-page warnings [7], and jiggling or colour-changing warnings [4] have been implemented. Persuasive textual content has been used to articulate threats meaningfully to help users understand their actions and encourage safer options [8]. However, despite this progress, users continue to bypass warnings [14] and are at risk. Further, users have become fatigued by traditional browser-based warnings [3], and as a result, can become desensitized to these critical indicators.

It is also important to note that these traditionally visual warnings have not served everyone. Users with visual impairments, whether due to temporary or permanent effects, such as screen-glare or disability, are at a disadvantage while assessing their state of security and privacy [1, 2] with current visualizations. Security cues that provide more than visual information can better integrate usability and accessibility principles and serve as more equitable solutions.

Manuscript submitted to ACM

Additionally, smart home devices such as virtual assistants, smart appliances, and smart locks are becoming increasingly popular. These devices can have also security problems but the lack of displays on these devices makes it difficult for users to monitor their devices and prevent potential security breaches.

To address these issues, visual warnings may integrate audio cues on their own or as supplemental signals to gain users' attention. While useful, audio warnings also have drawbacks. Used individually, audio cues would also exclude some portion of the population who are unable to hear either due to physical impairments or environmental circumstances. Audio cues may also draw attention from nearby individuals, which could be disruptive or could lead to privacy violations for the user.

2 NON-VISUAL WARNINGS

Instead of visual (or auditory) interactions, we are currently exploring how security warnings could engage users' other bodily senses to deliver security or privacy messages. Smell, taste, and temperature interactions have been explored in HCI but are not often considered within usable security literature. Below, we discuss these feedback modalities and their potential advantages for security and privacy communication.

Smell. Maggioni et al. [10] map out four key considerations of smell-based interaction that we find helpful in our conceptualizing our designs: (i) *chemical* aspects relating to choosing scents and scent intensity; (ii) *emotional* aspects relating to recognition and hedonic effects of scents; (iii) *spatial* aspects relating to the space where diffusion occurs and its effects on activity within said space; and (iv) *temporal* aspects relating to timing, duration, frequency, and habituation to scent stimuli.

Thus far, our exploration of olfactory designs have considered the distributed nature and nuances in privacy concerns related to using smart home devices [15]. Smell-based interaction could be particularly helpful for users managing the security of their network connected lightbulbs, thermostats, and other home appliances. For example, smart home devices often serve a group of people rather than a single person. This characteristic poses a number of challenges relating to respecting the privacy concerns of various family members and guests [16]. Typically, security-related information about smart home devices is delivered via an accompanying smartphone application (e.g., downloaded by the primary user). The scale of smell-based communication provides opportunities for delivering notifications to any user within range, thus minimizing the need to rely on the primary user or their smartphone.

Taste. Taste experiences similarly offer opportunity for rich emotional and temporal interactions. Here, we consider Obrist et al.'s [13] framework highlighting three main themes in taste experiences, including: (i) *temporality* or the growth and decline of experiencing flavours; (ii) *affective reactions* which refers to the pleasure and displeasure of taste experiences, and (iii) *embodiment* and mouth-feel, or physical sensations, resulting from taste simulations.

The tendency of affective reactions to taste-based stimuli seems particularly useful for security warning contexts. Often, users are uncertain about their current state of security or how to appropriately protect their security and privacy when interacting with technology. This is a particularly relevant problem for users with visual disabilities with limited means of evaluating an interface [1, 11]. We explore whether taste-based stimuli can convey the urgency of warnings, or offer users the confidence to engage with secure scenarios.

Novice website users often rely on the "look and feel" of interfaces when deciding what protective actions, if any, are required [5]. This notion can refer to the perceived professionalism of a website or warning, but can also refer to instinctual reactions to an interface. We consider whether users' instinctual approaches to security could be complemented with taste-based warnings. For example, could phishing warnings be supplemented with bitter/unpleasant or umami/confusing flavours to elicit uneasy feelings [13] and discourage users from proceeding to a predatory website?

Temperature. Thermal-based experiences have been extensively explored in HCI literature. A key challenge with temperature interactions is the ambiguous nature of thermal perception. To approach this challenge, and others relating to thermal experience, Wilson et al. [17] propose a set of design guidelines focused on commonalities relating to thermal perception. A particularly relevant common perception for our research is that *heat can convey risk-related status*.

Some usable security work has begun to explore the application of thermal notifications within website security contexts. Wilson, Maxwell and Just [19] explored users' associations between temperature and states of security. In their study, higher temperatures were most often associated with insecure websites because participants tended to associate higher temperatures with offline heat-related dangers.

Like taste-based affective reactions, thermal feedback can be used to encourage or discourage users from engaging with technology depending on security assessments. Our approach to thermal feedback for security warnings is described below.

3 CASE STUDY: NO-VIZ THERMAL

We have built a notification system [12] for communicating website TLS certificate data, describing whether a website uses encrypted communication. This is conveyed to users via thermal feedback as a supplement to traditional browser warnings. Our objectives were to encourage users to consider the security of websites and improve users' accuracy and confidence in detecting secure websites. Our evaluation of the thermal prototype has thus far been limited by the COVID-19 pandemic; however, we discuss some design challenges that we faced, in hopes of engaging other researchers in discussion.

Residual Heat. The first major issue pertains to a lack of warning reliability. When heat is being used to communicate potential security risks, the thermal conductor may not have enough time to cool down when switching from an insecure website to a secure website. In this circumstance, users may feel residual heat which can be perceived as a thermal warning for a website that does not actually pose as a threat (i.e., a false positive). Additionally, if the thermal conductor is consistently warm due to residual heat, this could lead users to perceive the system's assessment of the website as flawed or untrustworthy.

Users are less likely to bypass warnings they trust [14] and, conversely, may ignore a thermal indicator if they experience residual heat or false positives. Thus, our first design challenge is: *how do we ensure thermal conductors are consistent in use cases where a user may be faced with a quick succession threats and non-threats?*

Threat Association. Users tend to associate simulated high temperatures with real life physical dangers such as stove-tops or fires [19]. Based on what we know about users' security mental models [5], it remains unclear whether users can clearly link thermal stimulation with digital dangers such as phishing, malware, or network threats without additional explanation. Furthermore there may be opportunity to confuse device warmth with physical malfunction.

Our next design challenge is: *how do we make clear associations between conducted heat and the specific security or privacy issues users face?* This may be particularly difficult in scenarios where users interact with a mix of threatening and non-threatening websites simultaneously (i.e., multiple tabs open, or viewing in split-screen).

Comfort and Detection. Warm stimuli can effectively arouse attention [18, 20], yet due individual variance in people's heat sensitivity, thermal notifications may not be consistently comfortable for users. Furthermore, a number of factors can significantly alter the perception of thermal notifications, including ambient temperature, the presence of clothing [9], or neurological disorders affecting sensitivity.

This leaves us with the following challenge: *how do we accommodate users' individual heat detection abilities to effectively communicate warnings?* We note that the critical nature of security or privacy warnings mean that miscommunication can have significant impact on users.

4 CONCLUDING REMARKS

We intend to continue exploring non-visual security and privacy warnings. Through this workshop, we hope to engage with others in discussing the unique opportunities and challenges provided by smell, taste, and temperature feedback. We will continue our research and explore the potential and limitations of these modalities within the context of identifying security threats in a timely, reliable, and consistent manner.

REFERENCES

[1] A. Abdolrahmani and R. Kuber. 2016. Should I Trust It When I Cannot See It? Credibility Assessment for Blind Web Users. In *Proceedings of the 18th International ACM SIGACCESS Conference on Computers and Accessibility.* 191–199.

[2] T. Ahmed, R. Hoyle, K. Connelly, D. Crandall, and A. Kapadia. 2015. Privacy concerns and behaviors of people with visual impairments. In *Conference on Human Factors in Computing Systems (CHI).* ACM, 3523–3532.

[3] D. Akhawe and A. P. Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *Security Symposium.* USENIX, 257–272.

[4] B. B. Anderson, C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance. 2015. How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study. In *Conference on Human Factors in Computing Systems (CHI).* ACM, 2883–2892.

[5] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. 2011. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security and Privacy* 9, 2 (2011), 18–26.

[6] R. Dhamija, J. D. Tygar, and M. Hearst. 2006. Why Phishing Works. In *Conference on Human Factors in Computing Systems (CHI).* 581–590.

[7] S. Egelman, L. F. Cranor, and J. Hong. 2008. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Conference on Human Factors in Computing Systems (CHI).*

[8] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. 2015. *Improving SSL Warnings: Comprehension and Adherence.*

[9] M. Halvey, G. Wilson, Y. Vazquez-Alvarez, S. A. Brewster, and S. A. Hughes. 2011. The Effect of Clothing on Thermal Feedback Perception. In *Proceedings of the 13th International Conference on Multimodal Interfaces.* 217–220.

[10] E. Maggioni, R. Cobden, D.s Dmitrenko, K. Hornbæk, and M. Obrist. 2020. SMELL SPACE: Mapping out the Olfactory Design Space for Novel Interactions. *ACM Trans. Comput.-Hum. Interact.* 27, 5 (2020).

[11] D. Napoli. 2018. *Accessible and Usable Security: Exploring Visually Impaired Users' Online Security and Privacy Strategies.* Master's thesis. Carleton University.

[12] D. Napoli, S. N. Chaparro, S. Chiasson, and E. Stobert. 2020. Something Doesn't Feel Right: Using Thermal Warnings to Improve User Security Awareness. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020).*

[13] M. Obrist, R. Comber, S. Subramanian, B. Piqueras-Fiszman, C. Velasco, and C. Spence. 2014. Temporal, Affective, and Embodied Characteristics of Taste Experiences: A Framework for Design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* 2853–2862.

[14] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman. 2018. *An Experience Sampling Study of User Reactions to Browser Warnings in the Field.* 1–13.

[15] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor. [n.d.]. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015).*

[16] B. Ur, J. Jung, and S. Schechter. 2014. Intruders versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing.* 129–139.

[17] G. Wilson, G. Davidson, and S. A. Brewster. 2015. *In the Heat of the Moment: Subjective Interpretations of Thermal Feedback During Interaction.* 2063–2072.

[18] G. Wilson, D. Dobrev, and S. A. Brewster. 2016. *Hot Under the Collar: Mapping Thermal Feedback to Dimensional Models of Emotion.* 4838–4849.

[19] G. Wilson, H. Maxwell, and M. Just. 2017. Everything's Cool: Extending Security Warnings with Thermal Feedback. In *Conference on Human Factors in Computing Systems (Extended Abstracts).* 2232–2239.

[20] K. Zhu, S. Perrault, T. Chen, S. Cai, and R. Lalintha Peiris. 2019. A sense of ice and fire: Exploring thermal feedback with multiple thermoelectric-cooling elements on a smart ring. *International Journal of Human-Computer Studies* (2019).