Emokey: Tangible Online Authentication Interface for Novice Users in a Low-resourced Community

Saebom April Kwon
School of Information
University of Michigan
saebom@umich.edu

Chetan Keshav
School of Information
University of Michigan
kchetan@umich.edu

Florian Schuab
School of Information
University of Michigan
fschaub@umich.edu

Tawanna Dillahunt
School of Information
University of Michigan
tdillahu@umich.edu

Abstract

Despite the steady increase of Internet accessibility and utilization, novice users in low-resourced communities who are mostly older adults are falling behind in understanding and being aware of appropriate actions in securing user information. We present Emokey, a proof-of-concept online authentication interface for users with low digital literacy. Our design stems from observations and interviews with adult users in an under-connected community in the Southeastern Michigan area, and the finding that users favor physical, visible metaphors for security and usability. Our initial evaluation suggests that our participants prefer emojis and a familiar physical metaphor and the 3D tangible interface and on-screen interface had positive responses for their learnability and utility. We plan to further evaluate and refine our designs and investigate users' notions of online security.

Author Keywords

Online authentication, tangible security, digital literacy; novice tech users.

ACM Classification Keywords

H.5.0 [Information interfaces and presentation (e.g., HCI)]: General

INTRODUCTION

While protecting personal information online is a key digital literacy skill [5, 23], novice tech users in low-resource communities fall into a ’digitally-not-ready’ group [7], accounting for 14% of the U.S. population, particularly among older, less educated, and less affluent populations [6, 19]. In spite of the drastically increasing Internet penetration rate in the U.S., these individuals have lower levels of Internet access and educational resources, and are often more vulnerable to more negative events regarding personal information shared online such as compromise of their email accounts or stalking [15]. As a result of these vulnerabilities, they voluntarily limit their Internet use and information sharing [11, 21].

It is crucial to understand authentic user behaviors and requirements to reduce user workload in designing secure authentication systems. However, providing security often conflicts with user mental models and actions [4, 18]. The mental model approach, which externalizes users’ world view and the way they understand a system should work, can provide insights for designers and facilitate user awareness of security actions [9, 22]. We explore the familiarity of physical object metaphors as a potential authentication support for novice tech users.

With the design of Emokey, a proof-of-concept online authentication interface for novice tech users, we explore tangible metaphors as a potential solution to manage online accounts for novice users. We introduce a PIN-based authentication scheme and online password managing method, present our design process, and our preliminary user evaluation results. We aim to further assess whether tangible metaphors in security design can result in better comprehension, and utility/attractiveness.

RELATED WORK

Novice Tech Users in Low-Resource Communities

In low-resource communities in the U.S., the scarcity of support for digital literacy of minority groups is fueled by the limited infrastructure of technological access, training, and social environments [6, 16]. While users are willing to utilize new technologies for practical information [2] or communication [24], novice users in low-resource communities face difficulties understanding technologies due to a lack of general literacy, motivation, and social support. There are several distinct characteristics of novice users compared to higher-literacy users: higher rate of reusing the same passwords than higher-literacy users, less concern about Internet security [17, 20]. Understanding appropriate designs and authentication schemes for these emerging users is both needed and timely.

Security Mental Models of Novice Tech Users

Mental models have been widely leveraged in security system design to communicate users’ authentic cognitive structure for decision making and behavior [12]. Previous research finds that novice users have fuzzier mental models about the the Internet, networks, and online flow of information than expert users [9]. Even though the models might not be completely correct, building inner mental models can promote risk communication and security-related actions [22]. To mitigate the gap, Camp et al. constructed five security mental models that support non-expert users to understand different security concepts [1]. For instance, a medical mental model of the Internet might emphasize an ecosystem that myriad of users co-exist as an interdependent environment against one-to-many viruses and mass-hacking. Physical metaphors, on the other hand, might emphasize how locks or fences necessitate individual awareness and responsibilities, facilitating the security actions of users.

Total	19	
Gender	Men	9
	Women	10
Age	Median	50
	Range	19-76
Race	African American	18
	Caucasian	1
Edu. Level	Less than High School	4
	High School	9
	College or More	6

Table 1: Participant demographics

Security with Tangible Metaphors for Novice Tech Users
Tangible metaphors are promising to help users construct concrete mental models by externalizing design elements [8]. There are several indications that novice tech users prefer 'visible' and familiar metaphors when adopting and evaluating new technologies [3]. Kang et al. also show that novices rely more on physical components such as hardware parts for explaining the Internet as they are more concrete, perceivable components, while experts consider multiple layers of networks and organizational stakeholders [9]. Similarly, a recent study on people's understanding of 'privacy' generated more visible or tangible metaphors such as locks and physical barriers from non-expert users [13]. More recently, Payne et al.'s study [14] shows both the usability benefits and challenges of token- or object-based authentication. However, we have not found any studies regarding the physical mental models applied in real design concepts for novice tech users, who are likely to benefit from such metaphors.

OBSERVATIONS & INTERVIEWS

Participants
We recruited participants in Southeastern Michigan, a region reported to have lower home Internet access than other cities in the U.S. [16]. We began investigating this community by conducting a series of on-site observations of technology training events hosted by a non-profit organization in October and November 2018. Next, we interviewed 15 tech users (7 women & 8 men, median age = 53) in the organization and a technology learning center in a local public library. Considering the limited access to online recruitment media, we recruited participants at the library with the help of librarians. 14 out of 15 participants were African Americans, and most of them were older adults; 1 in their 20s, 1 in 30s, 5 in 40s, and 8 in 50s or older.

Data Collection
The design process was grounded in several iterations of observation and interviews. In the first-round interviews, we focused on their technology use and challenges in managing their web accounts. We found that the most participants had an entry level understanding of the Internet and had trouble on effectively managing their online accounts; the participants were not fluent in typing on smartphone keypads, and unfamiliar with basic Internet functionalities such as downloading files. We asked follow-up questions on their security requirements and included a sketch activity for designing a better password managing method. We transcribed audio-recorded interviews and kept typed notes after each observation session and interview. We inductively analyzed the data using affinity diagramming to identify major themes. The participants' drawings were also categorized and analyzed to inform the design.

EMOKEY DESIGN

Emokey is a proof-of-concept emoji-based combination lock interface (see Figures 1, 2) for tech users who are not familiar with online authentication and basic computer skills such as typing. Emokey aims to improve usability in web user authentication by leveraging familiar design affordances, and providing visual cues to support users awareness of online security. We found from the interviews that familiarity plays a significant role in managing passwords; most of the participants had utilized paper password manager templates and did not show strong interest in utilizing online password managers due to the extra learning burden and their limited technology use. To provide both a familiar and security-related metaphor for users who voluntarily limit their technology use, Emokey applies a combination-type lock shape for easy learnability and resemblance with a PIN-based password system.

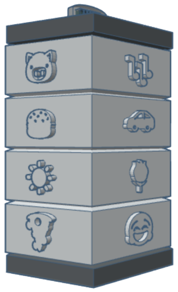
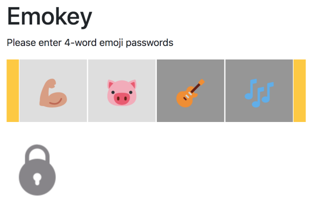


Figure 1: 3D modeled Emokey device can be connected to a digital device and work as a physical lock with preset passwords with four emojis

Furthermore, Emokey is emoji-based rather than PIN or text-based and the pictorial cues provide a level of simplicity that doesn't exist with PINs or text. A recent study suggests that emoji-based passwords can provide a larger password space and better memorability compared to numerical PINs [10]. While Emokey design focuses on easy comprehension and strong perceived utility and appeal, its tangible shapes might create trade-offs in objective security and vulnerability to shoulder-surfing attacks.

PRELIMINARY FINDINGS

While our evaluation is on-going, we present initial responses from evaluative interviews with four participants (2 women & 2 men; median age = 43), mainly focusing on comprehension and perceived utility and attractiveness of both the 3D-printed device and on-screen web design prototypes (Figure 2) on the Windows Chrome page. For each participant, we tested the interfaces with the wizard-of-oz task of setting up and matching a 4-emoji password.



Emokey

Please enter 4-word emoji passwords

Figure 2: Emokey screen version

Comprehension

We found that the visual cues and the shape of the device interface was favored for comprehension. While it was not a controlled setting, all users succeeded in setting and logging in with the setup 4-emoji passwords without an error. Also, the participants mentioned no issue understanding emojis or the shape of the device. Meanwhile, compared to the tangible device, the vertical scroll interaction on the on-screen interface was not intuitive for users. This could be a downside of the design compared to a keypad interface as vertical scrolling might not be as efficient as interacting with the PIN input.

Perceived utility/attractiveness

While we have not assessed the objective security and memorability of the design, we received some participant comments on its practicality and attractiveness. Overall, the participants indicated a strong willingness to use the websites with emoji-based passwords than other PIN-based schemes. All participants mentioned that they leveraged stories and favorable objects to recall the password, which was also found in Kraus et al.'s study [10]. *"It is kind of refreshing to the brain. It is kind of taking a break and I am enjoying these emojis."* (Female, age 43) Furthermore, one participant mentioned that emojis can reduce user burden that often occurs in high-stress situations such as recovering their passwords or forced change of their passwords. Finally, we received mixed opinions on the 3D tangible interface. All participants appreciated the reduction of on-screen interaction, however, they also pointed out the burden of carrying a physical device.

CONCLUSION AND NEXT STEPS

In this abstract, we present the preliminary findings of our efforts to design an online authentication system for novice tech users with lower levels of digital literacy and security awareness in a community that is under-connected to the Internet. We contributed designs based on multiple rounds of observation and interviews. Results from our initial evaluation show that our target users found emojis and the visual intuitiveness of the interface preferable than existing PIN-based passwords. However, a 3D tangible interface was not strongly favored than an on-screen web interface due to inefficiency.

The next step is to conduct additional user evaluations of the device design compared to the screen-based variant, and existing PIN-based passwords for assessing efficiency and utility. We will refine the 3D and 2D web interface and further explore the reasoning behind users' preference and the potential of applying tangible metaphors in security system design.

REFERENCES

1. L Jean Camp. 2009. Mental models of privacy and security. *IEEE Technology and society magazine* 28, 3 (2009), 37–46.

2. Tawanna R Dillahunt, Nishan Bose, Suleman Diwan, and Asha Chen-Phang. 2016. Designing for disadvantaged job seekers: Insights from early investigations. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. ACM, 905–910.

3. Tawanna R Dillahunt, Vaishnav Kameswaran, Linfeng Li, and Tanya Rosenblat. 2017. Uncovering the values and constraints of real-time ridesharing for low-resource populations. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2757–2769.

4. Steve Dodier-Lazaro, R Abu-Salma, I Becker, and MA Sasse. 2017. From paternalistic to user-centred security: Putting users first with value-sensitive design. In *CHI 2017 Workshop on Values in Computing*. Values In Computing.

5. Anusca Ferrari. 2013. DIGCOMP: A framework for developing and understanding digital competence in Europe. (2013).

6. Eszter Hargittai. 2010. Digital na (t) ives? Variation in internet skills and uses among members of the "net generation". *Sociological inquiry* 80, 1 (2010), 92–113.

7. John B Horrigan. 2016. Digital Readiness Gaps. (Feb 2016). `http://www.pewinternet.org/2016/09/20/digital-readiness-gaps/`

8. Hilary Hutchinson, Wendy Mackay, Bo Westerlund, Benjamin B Bederson, Allison Druin, Catherine Plaisant, Michel Beaudouin-Lafon, Stéphane Conversy, Helen Evans, Heiko Hansen, and others. 2003. Technology probes: inspiring design for and with families. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 17–24.

9. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "my data just goes everywhere": user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association Berkeley, CA, 39–52.

10. Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, and Sebastian Möller. 2017. On the use of emojis in mobile authentication. In *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 265–280.

11. Mary Madden. 2017. Privacy, security, and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity. *Data & Society, Sep* (2017).

12. Donald A Norman. 2014. Some observations on mental models. In *Mental models*. Psychology Press, 15–22.

13. Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies* 2018, 4 (2018), 5–32.

14. Jeunese Payne, Graeme Jenkinson, Frank Stajano, M Angela Sasse, and Max Spencer. 2016. Responsibility and tangible security: Towards a theory of user acceptance of security tokens. *arXiv preprint arXiv:1605.03478* (2016).

15. Lee Rainie, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish. 2013. Anonymity, privacy, and security online. *Pew Research Center* 5 (2013).

16. Bianca Reisdorf, Keith Hampton, Laleah Fernandez, and William H Dutton. 2018. Broadband to the neighborhood: Digital divides in detroit. *Available at SSRN 3103457* (2018).

17. Caitlin Rinn, Kathryn Summers, Emily Rhodes, Joël Virothaisakun, and Dana Chisnell. 2015. Password creation strategies across high-and low-literacy web users. In *Proceedings of the 78th ASIS&T Annual Meeting: Information Science with Impact: Research in and for the Community*. American Society for Information Science, 52.

18. M Angela Sasse and Ivan Flechais. 2005. Usable security: Why do we need it? How do we get it? O'Reilly.

19. Kathryn Summers, Noel Alton, Anna Haraseyko, and Rachel Sherard. 2018. Bridging the Digital Divide: One Smartphone at a Time. In *International Conference of Design, User Experience, and Usability*. Springer, 653–672.

20. Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining security and privacy research in developing regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. ACM, 25.

21. Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True: The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 176.

22. Rick Wash and Emilee Rader. 2011. Influencing mental models of security: a research agenda. In *Proceedings of the 2011 New Security Paradigms Workshop*. ACM, 57–66.

23. Mark Wilson and Joan Hash. 2003. Building an information technology security awareness and training program. *NIST Special publication* 800, 50 (2003), 1–39.

24. Sarita Yardi and Amy Bruckman. 2012. Income, race, and class: exploring socioeconomic differences in family technology use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3041–3050.