

Designing Digital Literacy and Security Trainings for Latinx Immigrants in the United States

Sylvia Simioni¹, Allan Martell¹, Allison McDonald², Abraham Mhaidli¹,
Tamy Guberek¹, Kentaro Toyama¹, and Florian Schaub^{1,2}

¹School of Information
University of Michigan
Ann Arbor, MI, USA

²Computer Science & Engineering
University of Michigan
Ann Arbor, MI, USA

{ssimioni, allanmar, amcdon, mhaidli, tamyg, toyama, fschaub} @umich.edu

MOTIVATION

We previously conducted a study about digital privacy practices among undocumented Latinx immigrants in the United States [5]. Through this work, we learned about strategies and challenges of this community in mitigating risks of deportation, discrimination, and family disruption. Prior research [3, 4] shows that digital security trainings can help mitigate the risks of vulnerable communities; we thus designed a Spanish-language digital literacy and security training to equip Latinx immigrants with strategies to protect their privacy when using technology. By holding this training in Spanish, we aimed to close the gap with regard to the limited resources available in their native language.

CONSIDERATIONS FOR DESIGN

We offer three considerations when designing trainings for undocumented individuals and the larger Latinx immigrant community. First, our previous work [5] suggests this population does not seek out resources for protecting user privacy. Nonetheless, we found community members to be eager to improve their technology literacy and privacy strategies. We thus brought trainings into the community, working closely with immigrant advocacy organizations to coordinate such events at spaces that community members deemed safe.

Secondly, we strived to make the trainings inclusive and safe for the community. Three of our co-authors had prior experience delivering digital security trainings for at-risk communities. Additionally, the trainings were led in Spanish, with presenters interpreting questions and comments to English-speaking attendees as needed. We exercised caution in advertising the training, publicizing it as a Spanish-language training for Latinx people rather than based on immigration status.

Third, we tailored our training to consider the networked nature of social media, as well as acknowledged a spectrum of comfort with disclosure of immigration status on their social networks. We adopted this approach rather than a more traditional “tool-centric” security training in consideration of the significant benefits that undocumented immigrants report to receive from social media and their mobile devices. Thus, we refrained from deterring

community members from using existing apps or advising them to adopt yet a new tool and rather focused on using their current tools safely.

STRUCTURE OF INITIAL TRAINING

We based our training on interview responses regarding what topics members wanted to learn about. We organized our pilot training into three modules: how information flows through cellular networks and the Internet; managing permissions on mobile devices; and controlling the flow of information on social media apps. Each module incorporated either real-life examples that underscore the importance of securing devices or diagrams that elucidate complex systems. To explain how data is transferred through networks, for instance, we used the analogy of a postcard to show how different entities are involved in transporting unencrypted messages (such as mail deliverers). Likewise, we used a sealed envelope to represent encrypted messages.

The modules on managing information mobile devices and social media apps included demonstrations to raise awareness about how these tools to collect information about ourselves and our contacts with third parties, as well as the risks of leaving phones unencrypted and without passcodes. We guided attendees in checking their phones to help them perform a cost-benefit analysis on whether they need to share certain information to reap the benefits of these tools. A guiding factor was to provide clear and actionable advice rather than a multitude of options.

CONCLUSION

Post-training evaluations for a pilot training showed high levels of satisfaction with our training and that our training can fulfill the desire for tailored content for parents and youth. Consulting with advocacy organizations, immigration attorneys, and community members is paramount for designing for a breadth of identities that intersect with being undocumented, such as being a parent, teenager, immigration activist, or an individual benefiting from Deferred Action for Childhood Arrivals (DACA) [1], a recipient of the recently cancelled Temporary Protected Status program (TPS) [2], and different ethnicities and languages. Pre-training surveys can gauge technological literacy and topics of interest of members of the community, which can inform the content of customized trainings in the future. Finally, strategies for assessing the effectiveness of trainings should include ways to gather this valuable feedback while protecting the anonymity of undocumented immigrants.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

3rd SOUPS Workshop on Inclusive Privacy and Security (WIPS). 2018. August 12–14, 2018, Baltimore, MD, USA.

REFERENCES

- [1] Department of Homeland Security. 2018. Deferred Action for Childhood Arrivals. (29 January 2018). <https://www.dhs.gov/topic/deferred-action-childhood-arrivals-daca> [Online; Retrieved May 2018]
- [2] Department of Homeland Security. 2018. Temporary Protected Status. (22 May 2018). <https://www.uscis.gov/humanitarian/temporary-protected-status> [Online; Retrieved May 2018]
- [3] M.H. Cooper. 2008. Information security training: lessons learned along the trail. In Proceedings of the *36th annual ACM SIGUCCS fall conference: moving mountains, blazing trails* (SIGUCCS '08). ACM, New York, NY, USA, 207-212. DOI: <http://dx.doi.org/10.1145/1449956.1450020>
- [4] M.H. Cooper. 2009. Information security training: what will you communicate?. In Proceedings of the *37th annual ACM SIGUCCS fall conference: communication and collaboration* (SIGUCCS '09). ACM, New York, NY, USA, 217-222. DOI: <http://dx.doi.org/10.1145/1629501.1629541>
- [5] T. Guberek, A. McDonald, S. Simioni, A.H. Mhaidli, K. Toyama, and F. Schaub. 2018. Keeping a Low Profile?: Technology, Risk and Privacy among Undocumented Immigrants. In Proceedings of the *2018 CHI Conference on Human Factors in Computing Systems* (CHI '18). ACM, New York, NY, USA, Paper 114, 15 pages. DOI: <https://doi.org/10.1145/3173574.3173688>