Usable Security and Privacy in Muslim Communities

Elham Al Qahtani
University of North Carolina
Charlotte
ealqahta@uncc.edu

Yousra Javed
National University of Sciences
and Technology
yousra.javed@seecs.edu.pk

Heather Lipford
University of North Carolina
Charlotte
richter@uncc.edu

Mohamed Shehab
University of North Carolina
Charlotte
mshehab@uncc.edu

CHI'20,, April 25–30, 2020, Honolulu, HI, USA
ACM 978-1-4503-6819-3/20/04.
https://doi.org/10.1145/3334480.XXXXXXX

Abstract

Usable security and privacy research on Muslim communities have been relatively less explored. It is however important to study the unique needs of this population. This paper provides an overview of the existing literature on this topic. It then discusses the unique challenges faced by researchers when investigating this population both for general HCI research as well as for security and privacy.

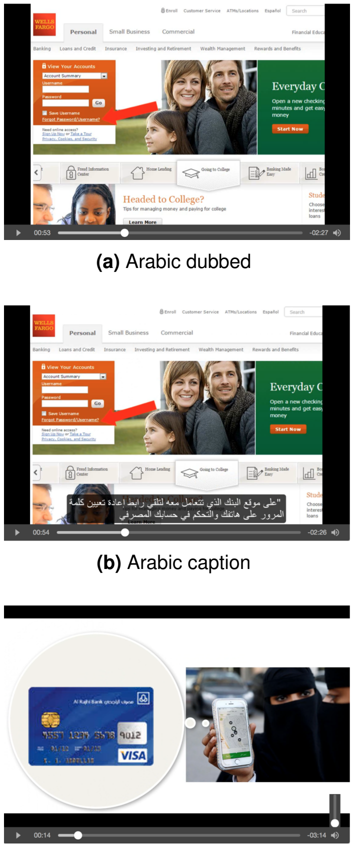
Introduction

There is a perception that humans are often the weakest link in the security chain [11]. Security and privacy researchers have, therefore, focused on devising strategies for communicating security and privacy risks to the end-users and evaluating the usability of existing security and privacy tools. However, one specific population, namely, users in conservative societies such as Muslim communities, has been relatively less explored. The cultural context of these communities emphasizes the need for studying digital security and privacy in this population. In this paper, we first provide an overview of the prior efforts of usable security researchers in studying the needs and perceptions of this population. We then discuss the unique challenges faced when investigating HCI and security and privacy in Muslim communities.

Security and Privacy Studies on Muslim Communities

In this section, we present recent security and privacy studies on Muslim populations.

Risk communication. It is important to study strategies tailored for Muslim communities to communicate security risk to incur behavior change. For instance, using culturally relevant vocabulary seems to help address the risks and fears of this population. We conducted a study [6] to examine the effectiveness of fear appeal (Arabic dubbed video, video with Arabic captions, Saudi-customized video) shown in Figure 1) in changing Saudi Arabians' risk perceptions and behavior for adopting screen lock on their smartphones. We found that the Saudi-customized video was extremely effective in changing participants' locking behavior (72.5% of the participants enabled the screen lock). The dubbed video was the second-most effective (62.5%) in impacting screen lock behavior.



"على موقع البنك الذي تتعامل معه لتلقي رابط إعادة تعيين كلمة
المرور على هاتفك والتحكم في حسابك المصرفي

(a) Arabic dubbed

(b) Arabic caption

(c) Customized video

Figure 1: Screen shots of videos used in the study [6]

Source of security advice. The channels (e.g., ISPs and Government) through which Muslim populations receive security advice can be different from that in the western world. We performed a preliminary investigation on the sources of the receiving the Smartphone security advice (e.g., enabling a screen lock, deleting the suspicious text messages, using a secure WIFI, and updating the software) by Muslim women outside the workforce in Saudi Arabia and Pakistan. We found (see Figure 2)that a majority of the participants 34% use their Family/friends' past negative experiences of security threats to receive such information. 21% of the participants reported Internet Service Providers (ISPs) as the second source. ISPs send text messages to inform their customers about the security risks and how to prevent them. 14% of the participants mentioned that they obtain security advice from their Government through their messages, emails, and websites.

Phishing comprehension. Cultural upbringing and lower awareness in the Muslim world can increase the vulnerability of the Muslim population to phishing attacks compared to users in the Western world. Al-Hamar et al. [4] investigated Qatar citizens' vulnerability to e-mail phishing. They found that Qatari citizens put too much trust in technology and their abilities to detect email phishing, making them an easy target for phishing.

Privacy perceptions and strategies. Unlike the western world, the need for privacy (e.g., data ownership and photo sharing) in the Muslim world is strongly affected by religion and family-oriented cultural restrictions. Abokhodair et al. [1] analyzed Twitter posts to understand the meaning of privacy in Qatar. They found that the need for privacy in this community is often supported by Quranic text, advice on how to protect privacy is frequently discussed, and the use of paternalistic language by men when discussing women's privacy is common. Above all, privacy is framed as a communal attribute, including not only the individual but the behavior of those around them; it even extends beyond one's lifespan. For example, women's photos can only be seen by men who are blood-related and non-marriageable. It is important to understand the privacy norms in public places. Abokhodair et al [2, 3] identified the collective vs autonomous aspect of photo sharing in the Arab context (e.g., Saudi Arabia and Qatar) as well as the privacy perspective of using social media in the Middle East.

Sambasivan et al. [10] conducted a qualitative study in India, Pakistan, and Bangladesh about how women perceive, manage and control their personal privacy on shared phones. The participants employed five performative practices to maintain individuality and privacy, namely, management of phone and app locks, content deletion, technology

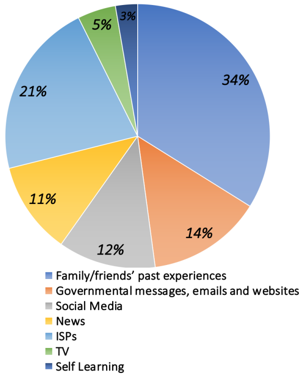


Figure 2: The Source of security advice from Saudi Arabia and Pakistan

avoidance, and use of private modes.

Challenges to HCI and Usable Security and Privacy Research in Muslim Communities

Running an HCI-based study in Muslim communities have unique challenges. Moreover, there are some added challenges specific to studying security and privacy in this population.

Religious and Cultural Norms. There are many cultural norms in the Muslim communities that can impact HCI research in this population and have security and privacy implications. For instance, cultural expectations in Bangladesh and Pakistan dictate that women should share mobile phones with family members and that their digital activities be open to scrutiny by family members [10]). Gender segregation is another factor. Two researchers [5] mentioned one of the challenges in conducting user experiments and usability studies in Saudi Arabia at a segregated female campus without including male participants. Also, individuals in conservative societies present themselves in a good light that will reflect on other groups, such as sharing appropriate photos that will reflect upon collectivist [e.g., users' families] [2]. With the new Saudi Arabia policies of modernization, this should warrant studying these effects.

Participant Recruitment. Participant recruitment from these communities for both short experiments and long-term studies is another challenge [8]. This challenge can be faced while engaging users during any phase of the need-finding and user-centered design process. For instance, the strong enforcement of male/female segregation in the Arab and Southeast Asian countries mandates that data collection from men be done by male researchers and from women by female researchers. The recruitment problem is intensified by the lack of proper ethics approval process, lack of incentive for participation [7], and the unavailability of online crowdsourcing platforms such as Amazon Mechanical Turk.

User Evaluation. The security and privacy perceptions in Muslim communities significantly impact the technology usage and security feature adoption (e.g., using password managers and adopting two-factor authentication). The low awareness plays a vital role in the interaction between users and security features/tools. Moreover, the inference of security and privacy problems with customized technologies that emerge from user studies rely on users' self-report and observations. Formulating design committees for user-centered design and participatory design for testing the usability and user experience of projects in industries, governmental organizations, ministries, and business sectors could improve the user experience and participation approaches [9].

Ecological Validity. Since users consider security as a secondary task, the ecological validity of experiments is a challenge. Replicating user studies conducted in the Western world (both HCI focused and security-focused) can present new challenges since researchers need to ensure that the scenarios simulate what users in the Muslim communities see and hear in the real-life. Few studies [2, 3] have provided solutions to improve the cultural design implications for non-western audiences and enhance user experience towards these technologies.

Conclusion

There is a need for future efforts by HCI and usable security and privacy researchers to address solutions for challenges faced by them when investigating Muslim communities. We provided an overview of the existing literature on usable security and privacy in Muslim communities and the associated challenges.

REFERENCES

[1] Norah Abokhodair, Sofiane Abbar, Sarah Vieweg, and Yelena Mejova. 2016. Privacy and Twitter in Qatar: Traditional Values in the Digital World. In *Proceedings of the 8th ACM Conference on Web Science (WebSci '16)*. Association for Computing Machinery, New York, NY, USA, 66–77. DOI: http://dx.doi.org/10.1145/2908131.2908146

[2] Norah Abokhodair, Adam Hodges, and Sarah Vieweg. 2017. Photo sharing in the Arab Gulf: Expressing the collective and autonomous selves. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 696–711.

[3] Norah Abokhodair and Sarah Vieweg. 2016. Privacy & social media in the context of the Arab Gulf. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. 672–683.

[4] Mariam Al-Hamar, Ray Dawson, and Lin Guan. 2010. A culture of trust threatens security and privacy in Qatar. In *2010 10th IEEE International Conference on Computer and Information Technology*. IEEE, 991–995.

[5] Shiroq Al-Megren and Najwa Alghamdi. 2019. Working Towards Culturally Sensitive Predictive Models. *With an Eye to the Future: HCI Research and Practice in the Arab World* (2019).

[6] Elham Al Qahtani, Mohamed Shehab, and Abrar Aljohani. 2018. The effectiveness of fear appeals in increasing smartphone locking behavior among Saudi Arabians. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 31–46.

[7] Ebtisam Alabdulqader, Norah Abokhodair, and Shaimaa Lazem. 2017. Human-computer interaction across the Arab world. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 1356–1359.

[8] Galal H. Galal-Edeen, Yasmeen Abdrabou, Maha Elgarf, and Hala M. Hassan. 2019. HCI of Arabia: The Challenges of HCI Research in Egypt. *Interactions* 26, 3 (April 2019), 55–59. DOI: http://dx.doi.org/10.1145/3318215

[9] Danilo Giglitto, Shaimaa Lazem, and Anne Preston. 2018. In the eye of the student: an intangible cultural heritage experience, with a human-computer interaction twist. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[10] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 127–142. https://www.usenix.org/conference/soups2018/presentation/sambasivan

[11] Bruce Schneier. 2011. *Secrets and lies: digital security in a networked world*. John Wiley & Sons.