Computer Security and Privacy for Refugees in the United States

Lucy Simko*, Ada Lerner†, Samia Ibtasam*, Franziska Roesner* and Tadayoshi Kohno*
*Paul G. Allen School of Computer Science & Engineering
University of Washington, Seattle, WA 98195
†Wellesley College
Wellesley, MA 02481

***Abstract*—In this work, we consider the computer security and privacy practices and needs of recently resettled refugees in the United States. We ask: How do refugees use and rely on technology as they settle in the US? What computer security and privacy practices do they have, and what barriers do they face that may put them at risk? And how are their computer security mental models and practices shaped by the advice they receive? We study these questions through in-depth qualitative interviews with case managers and teachers who work with refugees at a local NGO, as well as through focus groups with refugees themselves. We find that refugees must rely heavily on technology (e.g., email) as they attempt to establish their lives and find jobs; that they also rely heavily on their case managers and teachers for help with those technologies; and that these pressures can push security practices into the background or make common security "best practices" infeasible. At the same time, we identify fundamental challenges to computer security and privacy for refugees, including barriers due to limited technical expertise, language skills, and cultural knowledge — for example, we find that scams as a threat are a new concept for many of the refugees we studied, and that many common security practices (e.g., password creation techniques and security questions) rely on US cultural knowledge. From these and other findings, we distill recommendations for the computer security community to better serve the computer security and privacy needs and constraints of refugees, a potentially vulnerable population that has not been previously studied in this context.**

I. Introduction

Recent years have seen a number of crises around the world in which individuals flee their home countries in the hopes of ultimately resettling somewhere else. As of 2016, there were 22.5 million refugees worldwide, and 84,995 were resettled to the US in 2016 alone [1], [2]. Prior work suggests that technologies play a critical role in the lives of these refugees in refugee camps, in transit, and once resettled (e.g., [3]–[8]).

Our research is driven by the following questions: To what degree must refugees, once resettled, depend on technology in their efforts to integrate into their new societies and reestablish their lives? On which technologies do refugees depend, and how could they be harmed if they are unable to adequately secure their digital footprint? What computer security and privacy practices do refugees have, and what barriers do they face that prevent them from implementing stronger security and privacy practices? And, perhaps most importantly, what could be done to empower refugees with greater capabilities to protect their computer security and privacy?

We hypothesize that refugees — a vulnerable population according to the United Nations High Commissioner for Refugees (UNHCR) [2] — may be different from other user populations in terms of their interactions with technology and their computer security needs and practices. Refugees, by definition, are fleeing from real threats, and hence might have unique perspectives on threats and adversaries. Further, there might be a range of cultural, linguistic, and technological challenges that refugees must overcome in order to sufficiently protect their computer security and privacy.

Thus, in this work we study the computer security and privacy needs, practices, and challenges among refugees — specifically, refugees from East Africa and the Middle East who resettle to the United States. While we believe that the inquiry into this population and our results are of scientific interest, we also believe that our work can provide a foundation for helping refugees have a secure and private digital presence.

Methodology Overview. Refugees around the world are a large and heterogeneous population. We study specifically Middle Eastern and East African refugees in the United States — allowing us to both focus our efforts and dive deeply into the concerns of these populations, while still considering refugees from a variety of backgrounds. We conducted semi-structured qualitative interviews and focus groups to broadly explore the computer security and privacy challenges, needs, and opportunities for this population. As is common for formative studies of this type [9], [10], we focused in-depth on a small number of participants.

Through initial contact with an NGO committed to assisting refugees and immigrants, we learned that arriving refugees are assigned case managers (who help their assigned refugees find jobs and otherwise matriculate into society) and English teachers. Both case managers and teachers play a central role in the lives of refugees, and they often introduce refugees to or help them with technologies necessary for their lives in the US (e.g., setting up an email account to communicate with potential employers). Similar to other work studying resettled refugees [11], [12], we conducted interviews with case managers and teachers because of the broad perspective they have across the many refugees they work with, and because refugees themselves are a potentially vulnerable population.

DOI 10.1109/SP.2018.00023

We interviewed four teachers and five case managers, four of whom were refugees themselves.

We then used the results of the interviews with case managers and teachers to help guide our direct interactions with refugees, which complemented and corroborated the interviews with case managers and teachers. At the suggestion of a case manager, rather than interview refugees individually, we conducted several small focus groups, where each focus group had participants who fled from the same country (Syria or Somalia), and the discussions largely took place through an interpreter. Our use of focus groups, rather than one-on-one interviews, enabled free-flowing conversations with the refugees, and in less intimidating settings than one-on-one interviews. In total, we conducted three focus groups, one with four Syrian refugees and two with five Somali refugees each.

Foundations for Refugee Computer Security. Our interview and focus group results shed light on the computer security and privacy needs of the refugee population we study, as well as the unique barriers they face to protecting their digital security and privacy. Example themes that emerged include:

- Consistent with our hypotheses, we find that refugees today *are* highly dependent on technology in order to establish themselves in the US. However, we did not anticipate just *how* dependent on technologies they are. Whether to apply for jobs, or to find housing, it is impossible for them to escape the need to use technology. This reliance on technology makes computer security both critical as well as (in some cases) in tension with other, primary goals (such as finding a job).
- When refugees enter the US, they must learn not only how to use technology, but must also overcome language and cultural barriers. Critically, we find that many computer security and privacy related practices include deeply embedded US or Western cultural knowledge and norms, including the use of birth dates as authenticators and common techniques for creating memorable passwords. Indeed, the very notion of a scam seems foreign to some refugees.
- We know, from our preliminary conversations with a local NGO focused on refugee and immigrant support, that case managers play a central role in helping refugees establish themselves in the US. However, we did not anticipate the extent to which refugees must trust their case managers, even when in some cases they do not want to trust them. The computer security practices of refugees are thus intimately tied to the security practices of their case managers, and their relationships with them.

From these and other findings, we make concrete recommendations to bridge gaps we observe in how refugees are able to protect their digital security and privacy — for example, to support more secure use of public computers or account management solutions that explicitly support access by trusted parties like case managers.

Ultimately, by providing a broad basis for understanding how recently resettled Middle Eastern and East African refugees in the US interact with technology, our work provides a foundation for future, deep-dive investigations into specific technical needs, which may also apply more broadly to other groups sharing some of the same characteristics.

II. Background on Refugees

The processes surrounding how people become, and how countries accept, refugees are complicated. We provide essential background about refugees and the refugee process here, focused on — given the scope of our study — refugees who resettle in the US.

Definition of a Refugee. Refugees are people who have left their home country due to a "well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion" [13]. In 2016, there were an estimated 22.5 million refugees worldwide, and an additional 2.8 million asylum-seekers (people who want refugee status but have not received it yet) [1].

Resettlement Process. Before arriving in the US, refugees must pass extensive background checks and interviews. Refugees will, in many cases, have also spent years in intermediate countries or refugee camps before arriving in the US [2]. Before resettling, refugees attend a cultural orientation, which provides a breadth of information about the US.

Aid after Resettlement, Case Managers, and Teachers. The US State Department assigns each refugee to one of nine national resettlement agencies [2]. To assist in their transition, refugees are also paired with local NGOs, like the one we recruited from. The NGO we recruited from, and others, assigns refugees *case managers* and offers English classes. Case managers refer to their assigned refugees as *clients*, a term that we will also use interchangeably. Case managers, who may be refugees themselves, can have diverse responsibilities, but in general those responsibilities include helping their assigned refugees (clients) find jobs and otherwise matriculate into the US [14]. Case managers typically speak their clients' native language. The English classes are taught by English as a Second Language (ESL) *teachers* and are intended to help refugees communicate in their new environment.

III. Motivation and Research Goals

There is a growing body of work considering diverse populations in computer security literature, with recent studies focused on specific potentially vulnerable user groups, including low-income people in the US [15], domestic abuse victims [16], [17], and journalists [18]. Refugees are a population with unique backgrounds (e.g., fleeing threats in other countries) and constraints (e.g., at least initially, lack of familiarity with the English language, and highly dependent on the US government and NGOs for support).

Our ultimate goal is to help refugees protect themselves from computer security and privacy threats. To address this goal, however, we cannot blindly set out to design and build security tools, or develop security education campaigns, intended

[Case managers and teachers]

Participant Description	# Participants	Avg Years in Job (Range)
ESL teachers	4	1.9y (0.5y - 3y)
Case managers	5	2.4y (0.4y - 5y)

[Refugee focus groups]

Participant Description	# Participants	Avg Years in US (Range)
Syrian refugees	4	0.5y (0.4y - 0.6y)
Somali refugees	10	8.1y (2y - 18y)

TABLE I
SUMMARY OF ALL PARTICIPANTS.

for refugees. First, we must deeply understand the world in which resettled refugees operate, and how they interface with technology. We use interviews and focus groups to form this deep foundation (Section IV).

For our interviews and focus groups, we do not want to presuppose that refugees should use technology, or, if they use technologies, that the so-called security best practices for most users are the optimal security best practices for refugees. This perspective — both valuing security, but not wanting to assume that *our* views of security will match the views of refugees — guides us to formulate the following specific research questions for our interviews and focus groups:

1) How do refugees use technology as they settle in the US, if at all, and how might their relationships and life goals influence that use?
2) What barriers inhibit the implementation of strong security and privacy practices among refugees?
3) What computer security and privacy practices do refugees have?
4) What do refugees learn (e.g., from case managers and teachers) about computer security and privacy?

These research questions are intentionally broad and exploratory, enabling us to step back, ask, and answer higher-level questions, such as: Are refugees exposing themselves to unnecessary computer security and privacy risks? If they are, is it due to a lack of awareness, a language barrier, a lack of education, or something else? Is conventional wisdom about computer security best practices sufficient to enable secure practices for refugees, or are unique solutions needed? And, if there are any shortcomings, what could be done by the computer security and privacy community to empower refugees with greater computer security and privacy?

IV. METHODOLOGY

We use semi-structured interviews with case managers and teachers and focus groups with refugees to answer the research questions outlined in Section III. We conducted interviews and focus groups between May and September of 2017. All our activities were approved by our institution's IRB, and we discuss human subjects ethics further below. Table I summarizes our participants.

Semi-structured interviews with case managers and teachers. We conducted semi-structured interviews with four ESL teachers (T1-4) and five case managers (CM1-5) from a local NGO that provides support to refugees and immigrants. Each interview was conducted by two interviewers, and all but one of the interviews were audio recorded and transcribed for later data analysis. One case manager interview was not audio recorded because the interviewee did not wish to be recorded; one interviewer took detailed notes, which served as the basis for that interview's later data analysis. Interviews were conducted in English, in which all participants were fluent, and lasted 1-2 hours. We conducted interviews until reaching thematic saturation, and then turned to focus groups of refugees to corroborate and complement the teachers' and case managers' perspectives.

By asking teachers and case managers for their observations of their clients, we elicited a broad view of refugees' technology usage and threat models: case managers had between 42 and 50 clients, and class size for teachers varied from 12 to 34 clients. After accounting for the overlap between teachers and different case managers, we conservatively estimate that we talked about approximately 150 refugees from 22 countries, with the most common countries being Eritrea, Ethiopia, Iraq, Somalia, and Syria. Since the case managers and teachers drew on many years of experience, they likely drew their answers from experiences with a far greater number of refugees. Additionally, four of the five case managers were themselves refugees, and provide personal insight into refugees' views as well as a high level view of their clients'.

Driven by the research questions in Section III, each interview covered the following broad topics: technology usage, threat models, and technology education. We asked about each of these topics in the context of both refugees' lives currently in the US and — to develop an understanding of why refugees might have whatever practices and beliefs they currently have — we asked about each of these topics in the context of their lives prior to the US, including time spent in refugee camps, home countries, and any intermediary countries. We waited for participants to bring up security and privacy organically; if they did not, we brought it up about halfway into the interview.

We note that case managers' and ESL teachers' view of refugees may be skewed towards those who do not yet have jobs, or who do not have the technological or English skills to independently get a job yet; therefore our results are biased to apply more strongly to the population of refugees with weaker English and technology skills. However, this subpopulation — refugees who do not have jobs or are not fluent with technology — is a critical population to assist.

Focus groups with refugees. To complement the case managers' and teachers' interviews, we conducted three focus groups with refugees. All focus groups had two researchers and a professional interpreter, and the focus groups were audio recorded and transcribed for later data analysis. We chose to use focus groups with the refugees, instead of semi-structured one-on-one interviews, because focus groups — unlike interviews — would allow refugees the opportunity for free-flowing conversations amongst themselves, and because we wanted to create a non-intimidating environment where the

refugees could follow the norms of their peer group regarding what to share.

The first focus group was with four Syrian refugees (R1a-d), and the second and third groups were each with five Somali refugees (R2a-e, R3a-e). To facilitate discussions, we asked participants to arrive in groups with whom they were already comfortable (e.g., families or friends). However, asking participants to arrive in groups resulted in a lack of diversity. For example, the Somali subjects spanned multiple generations, but all ten were female, commensurate with most case managers' and teachers' observations that most of their clients were female (T1, T3, CM1, CM2, CM3, CM4).

Interviewing Syrians and Somalis allowed us to speak to refugees who represented the majority of the clients that the case managers and teachers were discussing.

Data analysis. To categorize and coalesce the data from our interviews, we iteratively developed a codebook with hierarchical descriptive codes through several rounds of coding, first using open codes, and then combining them to create axial codes. Each interview was then coded by two members of the research team, one of whom coded every interview (the primary coder). Intercoder agreement was high: using Cohen's Kappa, a standard measure for two coders, our average intercoder agreement was .98. When we report raw numbers in this paper, we use numbers based on the primary coder's codes in the case of (rare) disagreement between coders.

For the focus groups, when reporting on the number of people who mention a topic, the reported numbers will be lower bounds on the views of the participants since, if one participant says something and another agrees, that second participant may not say anything. Additionally, because each audio recording reflected multiple voices, particularly when refugees had a discussion in their native language which was then summarized by the interpreter, it is in some cases difficult to attribute individual comments to specific participants. Instead of coding for each refugee, the researchers developed a consensus on all themes across the full group and, when reported on in this paper, worked to attribute specific statements to individual participants.

Human subjects and ethics. Our entire study protocol was approved by our institution's IRB. Because we were working with a vulnerable population, we took care to design our study to protect participants' privacy and treat our subjects ethically. We did not unnecessarily collect personally identifying information, we asked participants to anonymize names in their own stories, and we redacted names and other personal details in our transcripts. With explicit consent, we audio recorded all interviews except for one, because the participant was not comfortable with it.

In developing the interview and focus group protocols, we focused on technology use as much as possible and avoided asking about potentially sensitive or emotionally difficult topics. Participants were explicitly not required to answer questions (and some exercised the option not to answer).

In presenting our results, we do not name the NGO from which we drew participants, and we omit some details (such as gender) so that they cannot deanonymize each other.

V. Results

We now turn to the results from our interviews with case managers and teachers, as well as our focus groups with refugees. We organize our results around the four core research questions raised in Section III: (1) How do refugees use technology as they settle in the US, and how might their relationships and life goals influence that use (Section V-A), (2) What barriers inhibit the implementation of strong security and privacy practices among refugees (Section V-B), (3) What computer security and privacy practices do refugees have (Section V-C), and (4) What do refugees learn (e.g., from case managers and teachers) about computer security and privacy (Section V-D).

A. Refugees and Technology

We begin by considering the technologies that refugees use (Section V-A1), their relationships with case managers and teachers (Section V-A2) and others in their community (Section V-A3), and their life goals (Section V-A4). These findings provide context for later subsections, in which we also consider how those relationships and goals might interface with their technology use and computer security behaviors.

Some results, such as those about technology use, may apply to groups beyond refugees, such as non-refugee immigrants from the same regions. Other results, such as those about refugees' relationships with their case managers and teachers, are more specific to refugees. Future work could explore these issues more deeply, to better understand which issues are inherent to refugees, and which issues are faced by other groups.

1) Technology Use

Overall, we find that there is a dichotomy between refugees who are fluent using technology, and refugees who are not. Over both groups, prior email usage is low. Despite the diversity in technical and educational backgrounds, the goals for their lives are similar now that they are in the US.

Experience with technology prior to the US. T4 and CM3 observed a clear division between refugees who use phones and computers fluently, and refugees who are much less tech literate. The first group is typically refugees from modern cities who are comfortable with technology, smartphones, computers, have social media, and are well-versed in messaging and VoIP apps but still may not have experience with email (CM3). These refugees are likely to be from wealthier countries like Syria or Iraq, and some from larger cities in Ethiopia (CM1, CM3).

In contrast, refugees who grew up in rural areas or spent many years in refugee camps have little to no experience with technology. Some have never used a computer or a mouse before: "*Somebody that comes from a refugee camp… you have to explain to them what e-mail is, what does it do for*

Common Smartphone Uses	Participants
Connecting with friends/family	
Messaging	T*, CM*, R2{bde}, R3{ab}
Social media	T*, CM{135}, R1{ab}, R2e, R3{cde}
General everyday use	
Navigation	T{124}, CM{125}
Translation	T{124}, CM{35}
Photos of important documents	T2, CM{123}, R1a
Other	
Email	T*, CM*, R1{cd}, R2{bce}, R3b
Watching videos	T{24}, CM1

TABLE II
CURRENT SMARTPHONE USE BY REFUGEES. NOTATION: T{24} DENOTES PARTICIPANTS T2 AND T4; CM* MEANS ALL CASE MANAGERS (CMS).

you? How do you communicate with people that you don't see, but you're still talking, e-mail. What kind of information should I share with them?" (CM3). This quote also points to circular issues around teaching email and information security and privacy to refugees whose mental models of computers and the internet are not well-developed.

While some refugees have not used a computer before, many do arrive in the US familiar with smartphones (T3, T4, CM2, CM3). In both groups, refugees were unlikely to have email addresses; instead, refugees with more technical experience used apps like WhatsApp and Viber (CM2).

The majority of refugees that the teachers and case managers spoke about were in the latter group — uncomfortable using computers, and with a varying amount of smartphone experience. Refugees in the focus groups were more technologically proficient. We hypothesize that this difference is due to the country of origin for the first group (Syria), and the length of time in the US for the second and third groups (Somalia). (Table I summarizes these demographics.) This supports the case managers' and teachers' view of Syrians having more experience with computers, and shows that refugees who may enter with less tech fluency, such as Somalis, go on to incorporate technology in their daily lives after living in the US for years — suggesting that teaching computer security and privacy practices is critical early on.

Tech use in the US: Computers. Teachers and case managers said their clients typically do not have computers at home (except some Iraqi and Syrian families). Thus, the majority of their computer usage is on public or shared computers, e.g., at a library, a community center, or in a computer room in a local NGO (T1, T2, T3, T4, CM2, CM4). Refugees use these shared computers for job searches and job applications, raising potential security concerns for their personal information due to the shared nature of public computers. These practices have implications for both the administrators of the machines and teachers and case managers who are teaching computer etiquette and security.

Tech use in the US: Smartphones. All teachers and case managers said that most if not all of their clients have smartphones; all the refugees in our focus groups had smartphones. Because many refugees own smartphones, but *not* computers, it is important to understand that their smartphones are the connection to their digital lives.

Table II shows the most common smartphone uses, including connecting with family and friends abroad via WhatsApp, Viber, and Facebook (among other platforms): *"I like to use Facebook to communicate with my parents and my family members back home... If the apps were not there, I would have to buy phone cards and call people overseas, but now because of the technology and the apps, it's easier for me to communicate without purchasing those phone cards" (R3c).* They also use smartphones for everyday tasks like navigation, translation, and storing photos of important documents, a practice that we will return to in Section V-C.

Notably, we have put "email" in the "other" category in Table II, since teachers and case managers told us that a main use of email for refugees is to contact potential and current employers (T4, CM2, CM4, CM5), and, depending on the refugee's English level, they may wait for their case manager to help respond (CM3). Although one case manager observed that refugees may also get personal emails, this case manager was adamant that case managers should ignore those emails when accessing a clients' account to help with job-related activities (CM5); we return to a deeper discussion of email use in Section V-C.

2) ROLE OF CASE MANAGERS AND TEACHERS

Refugees must trust their teachers and case managers in order to leverage their knowledge and services, but this also puts them at risk, since in doing so they must trust the security measures of every person or organization they give their information to. While case managers and teachers gave us every reason to think they were trustworthy, there is always the potential for mistakes or for a malicious insider — making this requirement to give out information a significant and unavoidable potential vulnerability for refugees.

Case managers help refugees settle into their lives in the US; the main responsibility of the case managers we interviewed was helping their clients find a job. Because their employer (the NGO) requires it, case managers must collect sensitive and personal information from clients such as photocopies of their social security card and first paycheck, but are required to adhere to strict confidentiality agreements (CM1, CM2).

Teachers and case managers indicated that they trust their colleagues completely, and that their clients should as well. However, T2 said that refugees sometimes do not trust their case managers with their personal information; T2 attributed this to trauma from their past. "*It's not every day, it's kind of like a wave, where one day they're totally fine with their case manager and the next day it's like, 'I don't know this person, I don't trust them.'*" This causes problems for both refugees and case managers because refugees have to share sensitive information with their case managers in order to get the case manager's help. This trust relationship with teachers and case managers extends to trust in the digital domain, a topic we return to in Section V-C.

Teachers do not have as much interaction with clients that revolves around their own personal information. At the

NGO we recruited from, the ESL curriculum covers practical English skills (T2). Some ESL teachers devote a small amount of time per week or month to teaching computer skills, such as typing, logging onto email, and clicking on links (T1, T3, T4). ESL classes can also include discussions about security, like how to avoid scams or how to understand if a news source is reliable, but security is *not* the main goal of the class. Nevertheless teachers report that refugees do share with them their passwords, so that the teachers can help them log into their email accounts (T2, T3). This act raises questions of refugee autonomy when interacting with computers, as well as the question of who else they must share their passwords with in order to achieve their computing objectives.

Case managers and teachers reported that refugees had complete trust for teachers; T2 suggested that "*because I have a relationship with the students on a day-to-day basis, they trust me maybe more so than they trust their case managers.*"

3) Role of the Community

Newly resettled refugees find communities of others from their country who speak their language. These communities are a major source of cultural and security knowledge. R3a said she heard of scams from her community, but only after it was too late and she had already been scammed. This situation speaks both to the role of communities in sharing security-related knowledge, and the fact that scams may be an unknown concept to refugees.

In addition to explicit security advice, participants told us that that refugees receive advice about American culture and "official" offenses. CM2 said that relatives, friends, and people in the community "*will tell you, 'Okay, never make any mistake with parking or traffic accidents,' or anything like that. Never have any illegal things. Immediately they will try to scare you or train you mentally like that.*"

Both these examples speak to the broader observations that refugees form their security practices in part from the advice of others in their communities, in addition to advice from their case managers, teachers, and official resettlement orientations.

4) Refugee Goals in the US

Finally, we provide additional context about refugees' broader goals once they arrive in the US. Understanding these goals is critical to our efforts to understand and improve computer security and privacy for this population, since, as we discuss further below, commonly recommended security practices can be in tension with these core goals.

- *Establish their lives in the US.* Teachers and case managers expressed that the foremost concern for refugees is reestablishing their lives: obtaining housing and, most of all, getting a job (T1, T2, CM3, CM4, CM5). Achieving these goals requires navigating web pages filled with jargon, filling out online forms, and sending emails to various agencies and companies.
- *Keep in touch with family and friends.* Refugees' families and friends are often scattered around the world. Participants often described refugees' use of messaging apps or social media in the context of exchanging news with distant friends and family (T2, T3, T4, CM2, CM3, CM5, R1ab, R3ce).
- *Learn US culture and English.* Refugees need a working knowledge of English to thrive in a job, so they attend ESL class four times a week to learn English. Sometimes, T3 speculated, their desire to learn English and US culture leads them to be insufficiently skeptical of people speaking English. We also observe throughout our results that both technical *and* US cultural knowledge are needed for many common security features.
- *Increase technology use.* Although teachers and case managers said that they sometimes had to pressure their clients to use technology (T2, T3, CM3, CM4), we also heard about clients who were excited about using email and the internet to connect with faraway friends and family (T2, T3, T4, CM1). "*For students who understand it, it's really exciting because it's a new way to connect with the world. They'll get a new email address and they'll be like, 'I hear my brother has an email,' and we're like, 'Yeah, you can write your brother now.'*" (T4). With increased proficiency on the computer, refugees can apply for jobs by themselves, but may also increase their risk to computer security threats.

B. Refugee Security Barriers

Given the above context, we now turn to our second core research question: what barriers inhibit the implementation of strong security and privacy practices among refugees?

Past Experiences: Trauma. Many refugees feared surveillance and government-perpetrated violence in their home countries. Among our study population, the countries about which we heard concerns expressed included Eritrea, Syria, and Iraq; by contrast, we heard that there were not such concerns in Somalia (CM2, R3c).

Case managers identified a fundamental difference with "*[those who] were born in, for example, a stabilized country, they are different than people who come from a war, who are suppressed*," (CM5) such as those from Eritrea, Syria, and Iraq. CM5 said that in Iraq, "*the walls have ears*," meaning that anyone, even the neighbors, could be reporting back to the government. "*You never know who's listening and you could be killed for it, you could disappear overnight for it*" (CM3).

CM2 drew a distinction between Somali clients, who "*talk [about] anything they want*" and Eritrean clients, who "*you never see…talking about the government or anything like that.*" Compared to a country with censorship, CM1 explained, "*in Eritrea…you can use [any website]. There is not any problem. The problem is on what things you are writing or you are speaking.*" T2 and CM4 additionally identified trauma from the past as an irrational but unavoidable factor in refugees' decisions to trust certain people or entities. As we discuss in Section V-C, refugees must trust people — such as their case managers — for assistance, when establishing themselves in the US.

Language: Dependence on Assistance. Refugees face linguistic barriers (T1, T2, T3, T4, CM2, CM3, CM5), increasing their reliance on others for help with tasks that must be completed in English, like a job or housing application. The impact of this language barrier manifests in multiple ways, ranging from email account management, to website validity verification, to scam avoidance.

Culture: Awareness of Risks. We also found that while certain types of security risks are well-known within US culture, they are new concepts to many refugees. Consider, for example, scams and identity theft. From our interviews, we observed that a concern for identity theft and scams was typically instilled by case managers, teachers, or others over time, or through direct experiences (e.g., R3a was scammed twice before learning to be cautious), rather than a concern refugees brought with them from their home countries. Case managers and teachers suggested that refugees were surprised by the possibility of such threats: "*They always ask me why. 'Why would they do that? Why would they take my social security?' ... They're surprised that [on] this side of the world, somebody will go through all this hassle just to destroy somebody's identity or life*" (CM3). T3 remarked, "*I don't think they have the idea that there might be something that could be potentially risky for them in their inbox*" (T3). CM4 suggested that the novelty of these types of threats may cause refugees to treat their personal information with insufficient caution: "*Imagine someone who has no exposure or little knowledge about computer hacking.*[1] *They can't believe, and they can simply provide all information.*"

Case managers emphasized that there *are* refugees who are already skeptical of putting their information on the internet (though they may be a minority), such as the participants in R3, who together listed identity theft, catfishing, being taken advantage of by a trafficker, and having their locations tracked through the use of various apps on their phones: *"the internet has benefits as well as risks"* (R3a). We further discuss perceived threats like these in Section V-C5.

Culture: Exploiting Barriers. Our interviews surfaced the fact that refugees' lack of awareness of risks, and their dependence on assistance, make them particularly vulnerable to scams. For example, we heard anecdotes about scam websites and phone calls asking for information for a (fake) low-income housing application, ads for (fake) minimum-wage jobs, (scam) phone calls about utility bills being overdue or arrest warrants, or tax scams around tax day (T2, T3, T4, CM4). Refugees — particularly recent arrivals — are only just learning the US bureaucratic processes, as they do not have experience living in the US, paying US taxes, or applying for jobs in the US, and hence can have a particularly difficult job distinguishing a legitimate request from a fake request. Indeed, T5 observed that when someone calls a new refugee on the phone, and speaks to them in English, they assume that the person must be someone of authority who is there to help them.

[1]In this case, CM4 — not a technical expert — used the term "computer hacking" generically to include attackers like scammers.

Culture: Secrecy and Sharing of Information. Case managers and teachers said that refugees from some areas, particularly more rural areas, have a different set of personal information, and may share that information more or less freely than is commonly expected in US culture. For example, in some cultures birthdays are not awarded the same significance they are in mainstream US, so when refugees arrive from these cultures and do not know their actual date of birth, they are assigned a birthday of January 1. Even with refugees whose children do have officially documented birthdays, the parents may have difficulty remembering the precise day: "*You know, when they come here, the last thing they want is to remember ... if you have, especially seven, eight kids, to remember, each one of them, the day the month and the year. 'Cause you worried about getting them housing, and you worried about food stamp doesn't get cut, worried about getting the work, and just standing on your feet. The last thing you want to know is who was born in July, who was born in December.*"

Security mechanisms that rely on a high-entropy distribution of birthdays will not be as secure for refugees from these cultures (i.e., East Africa, but *not* Syria); relatedly, other security mechanisms or common password generation algorithms may use other information, such as the personal information of close family members, which may be shared to a different set of people. R3a, from Somalia, expressed concern that matching birthdays and other information like name with someone else could cause issues: *"You will find someone with the exact same birthdate, name, whatever, the only difference is the address. And maybe this person did something ... and now ... [the government] just hold your identity on hold, and maybe travel, like traveling out of the country, and someone with same information as you has been flagged to travel out of the country ... And if you need to cross the border, to another country, that name is going to pop out because it is flagged. And you matched with them so you're going to have to go through the questions to identify if this is the official person or not."*

Technical: Lack of Experience. As Section V-A1 observed, refugees can have varying degrees of experience — some have had prior technology experience, whereas other do not have experience with computers or keyboards. And, as noted above, email is a new concept to many refugees, even those with prior technical experience. When encountering a new technology, refugees naturally focus on the primary goal of trying to learn how to use that technology to accomplish a task (e.g., read email, or use YouTube to learn English), rather than how to use it securely and privately.

C. Refugee Security Practices

We now turn to our analysis of the security and privacy practices that refugees have. One salient observation we have is that computer security is *not a priority* for refugees, due to a combination of the barriers they face: for example, if initially

they do not know about scamming, they do not prioritize securing themselves and their assets against scammers. But, even when they are well aware of scamming as a threat, they may not be *able* to prioritize security against scammers, for multiple reasons: (1) even if they want to prioritize security goals, they may not have the technical knowledge to do so, and (2) other goals under the umbrella of establishing their lives in the US, such as going to appointments or getting jobs, may take priority over security.

1) Online Authentication

We find that refugees face significant hurdles with online authentication. These challenges cause them to rely on their case managers and teachers for help with account creation and access, particularly in the case of email accounts (which refugees need in order to obtain many jobs). Broadly, these challenges indicate that text-based passwords and security questions do not allow refugees' accounts strong security because of the barriers that refugees face in implementing them.

While case managers and teachers focused their discussions on email account creation and access, since that fell under the scope of their jobs, many of the issues raised below apply to authentication in general.

Password Creation. One initial challenge refugees encounter when trying to create email accounts — and likely other accounts as well — is password creation. There are two key challenges with password creation for refugees: the privacy of passwords and the entropy of passwords.

For email accounts, case managers frequently help create usernames and passwords for their clients. In doing so, some case managers rely on password creation strategies that scale for their purposes but are "*not... unguessable*" (T2), including simple algorithms based on personal information about the client (for some case managers) as well as the same password for all their clients (for other case managers).

While there are natural security concerns with having someone else pick passwords for refugees, T3 also expressed concern about refugees picking their own passwords: "*They need to be a little more careful of passwords... if they don't do that very generic password [set by their case manager], they will pick their child's name, the year they were born, something like that, that they can remember easily.*" Indeed, this practice is confirmed by R1a, when discussing how to pick a password: "*As much as I know, lots of people use their birthdays, but it doesn't mean they put it in a proper way. They put the birthday, but they make some changes in it. Maybe we add a star or a zero or something extra.*"

Password Memory. Case managers and teachers commonly identified forgotten passwords as an issue (T1, T2, T3, T4, CM1, CM2, CM3, CM5, R1a). CM3 attributed this partly to a cultural and language barrier: "*So, the last thing they want to remember is numbers, passwords, usernames, all this new to them. And add to that, is a different language. So it's a really a challenge.*" Typically, the case manager or teacher helps the client recover the password, either by setting a new one, or, in some cases, by logging in with the real password that the case manager or teacher has saved. In extreme cases, clients lose access to their email accounts permanently if they forget the password, recovery phone number, recovery email address, or security question answers (T4).

Password Entry. Even when refugees know and remember their own passwords and security question answers, typing them correctly can present difficulties for refugees with limited prior experience with computers (CM2, CM5, T2, T3, T4). T3 said that capitalizing letters, i.e., with the shift or caps lock key, is sometimes difficult, especially if the password is not visible. Attempting to avoid this challenge may result in refugees creating weaker passwords (e.g., using only one character set).

Security Questions. Though security questions for account recovery provide questionable security [19], they are nevertheless common. However, we find that security questions are designed with implicit US cultural knowledge and norms embedded — sometimes making these questions inapplicable to refugees. For example, questions about a mother's maiden name are not useful for people from cultures in which women do not take their husband's name (T4). Other questions are difficult or impossible for people with limited English skills or who did not grow up in the US: some refugees have never gone to school or owned a car, and small villages in East Africa, for example, may not have street names. Similarly, some questions may ask about information that is typically private in the US but common knowledge in other cultures (e.g., family or childhood details), or may ask about information not considered important or distinct (e.g., birthdates). As a result, refugees' responses to security questions may be insecure or easily forgotten: "*For a newcomer, they might not be used to keeping that kind of information in their heads, so I think that they might make up answers and then forget, or forget what the question was asking*" (T4).

2) Email Account Management

Since a primary goal of case managers is to help their clients find jobs, and since email access is critical to refugees' job search, we now turn more deeply to the relationship between case managers and their clients' email.

Case managers and teachers often become primary users of these accounts, maintaining credentials as well as reading and responding to job-related emails on behalf of their clients. This practice (particularly when a refugee also uses that email account for personal purposes) trades off potential vulnerabilities with the critical utility of an email account as part of the job search process. In short, refugees rely heavily on their case managers and teachers for help with email use and account management, which means that refugees must trust their case managers significantly.

Password Management Across Refugees. In order to efficiently check 40-50 clients' emails every day, and to help

clients in the (frequent) cases where they forget their passwords, case managers have developed certain password management strategies to streamline their process. Three case managers keep spreadsheets with all their clients' email usernames and passwords, and another case manager keeps the credentials "*on a paper in the [client's] file,*" which "*gets locked up every day.*" One of the case managers who keeps a spreadsheet also uses the same password for all clients for whom they create a password. Likewise, teachers keep copies of clients' email credentials to help with email account access and recovering from forgotten passwords.

These password management strategies — including storing and reusing passwords — do not conform to many common password "best practices" and are vulnerable to certain classes of attackers. However, these strategies reflect the tensions inherent in the time constraints and main goals of case managers and teachers: to efficiently and effectively help refugees find jobs. Thus, for case manager and teachers, the benefits of insisting on more secure password strategies may be outweighed by the benefits of efficiently logging in to their clients' email accounts.

Email Content Access. Because case managers and teachers often have access to their clients' email accounts, the contents of these accounts are not private, and are also subject to the security and privacy decisions of the teachers and case managers. CM5 mentioned seeing clients' personal emails, but ignores them out of respect for the client's privacy: "*when I check emails... they're sometimes sent from friends, back home. I don't care about them. I look for ones that are job related. I can tell when they are personal. Sometimes the emails are in [their native language, which CM5 fluently speaks], so I can tell it's from a friend or relative.*" Though CM5 ignores these emails, this speaks to the power that case managers and teachers have to access these accounts.

3) Web Site Legitimacy

Earlier we note that teachers and case managers try to help clients understand the importance of protecting against scams and identity theft. But even if refugees know it is important, teachers and case managers said that many of their clients lack the technical experience to protect themselves online and with their digital assets. Teachers and case managers felt that their clients need to be more careful giving out information online (T1, T2, T3, CM2 CM3) and indicated that their clients often do not look for technical clues of illegitimate websites, like inspecting URLs or domains (T2, T3, CM3, CM4).

Although case managers and teachers generally did not observe refugees directly inspecting URLs to judge the legitimately of websites, refugees do sometimes employ strategies to ensure that they only visit trusted websites. For example, R3c discussed only visiting websites that she already knows, and CM1 advises their clients to only trust websites printed on a job application or a business card. Over the course of our interviews, standard security measures — like HTTPS or browser phishing warnings — did not come up.

We also find that refugees commonly turn to their teachers and case managers for help determining whether a website is legitimate. CM1 recounts: "*Most of [the] clients, they don't want to put their private things on the internet, they don't trust that much. They are new, they say, 'oh, is it okay to put in this, I try to apply this job on this website, is it proper to put my social security here?'*"

However, other case managers and teachers observed that caution with website identity was rare. For example, T3 was happily surprised to see that some of their clients did not fill out their social security number on a job application, but emphasized that they were a minority.

Even those who know to be cautious do not have the technical expertise and experience to independently decide whether a website is legitimate. R3a explained that she puts her information into websites when necessary, even knowing risks: *"Everything has risks – social worker, case managers – whoever you share your information with, you have no idea what they will do with that information. But if you do not provide your information, you cannot get what you are trying to get from them. It's a gambling situation. In order to gain something, you have to give up."*

4) Physical Documents Security

Because refugees frequently interact with various bureaucratic processes (e.g., with government agencies or potential employers) requiring identifying documents, they frequently carry these documents on their person. In some cases — and sometimes on the advice of case managers or teachers who encouraged refugees not to carry the original copies — refugees instead keep social security numbers and other PII stored on their phones, as well as photos of documents like passports and social security cards.

Whether carrying physical documents or photos of documents on (potentially unlocked) phones, the need to carry this information creates a risk for identity theft when this information is compromised. Further, the practice of storing these documents on the phones makes the protection of these phones — and their digital contents — important. Indeed, participants told anecdotes about lost phones (T2, CM2, CM3, R1a) and CM3 expressed concern about the resulting potential risk of identity theft (though none of the scam anecdotes we heard were due to lost phones or documents): *"She's like, 'When I go to these appointments, whether it's electric help, whether it's the housing help, they need the information, and I can't grab all the papers all the time, so I have on my phone.' And I said, 'Oh,* ***you have a bigger problem on your hand than just losing your phone.****' And it was unlocked, no code. I said, 'No.' I told her ... 'hopefully you don't get your identity stolen that way but social security, date of birth, and name, and addresses,* ***you gave it to them on a golden plate****"* [emphasis added].

5) Safety of Communications

Despite fleeing very real threats of state-sponsored violence, many refugees are no longer worried about violence or

surveillance from their home governments once they resettle in the US because they feel sufficiently protected by the US government (T1, T2, T3, T4, CM1, CM2, CM3). In general, refugees also trust the US government since it brought them to the US, and say that they are not concerned about any potential surveillance from the US government (T1, T3, T4, CM1, CM2, CM3). "*They feel safe saying whatever they want to say because they come to this country, they know they have that freedom of speech and stuff. They're okay to say whatever they want to say . . . Once [they]'re here, they feel like, 'Okay, I can voice myself now*' " (CM3).

For example, T3 told a story about a refugee who was in great danger in his country for filming human rights violations on his phone, but felt very safe in the US. In answer to a question about whether they or any of their clients would talk about politics outside Eritrea, since talking about politics inside Eritrea is dangerous, CM1 said: "*Outside, yeah. As you like, yes.*"

However, these concerns remain for some refugees, though case managers and teachers said that these refugees are exceptions to the rule. CM1 did indicate that some refugees censor themselves in the US as they did in their home country, out of fear of informants or other surveillance from their home country. The Syrian refugees we spoke with indicated that they would not talk about politics for fear of something bad happening to their friends and family who are not in the US: "*Here, we don't feel, you know, we aren't afraid of anything, we feel very comfortable here, but we are worried about our relatives in different countries, in Syria, to say something that might affect them*" (R1d).

Although few participants directly said so, some indicated that there was concern about the US government as well. For example, while deciding whether to consent to audio recording, one focus group participant asked whether the interview data would make its way back to the CIA. (We note that this participant did consent, and we received permission from our IRB to include this observation.) And although teachers and case managers said refugees were not worried about surveillance from the US, they told anecdotes in which refugees were uncomfortable with the information that they had to give out. CM4 said that Muslim refugees in particular might censor their speech or actions due to recent US politics, but also indicated that was not the majority.

Finally, some participants said that refugees preferred to conduct business in person. Related to refugees' attention to physical security, we found that they use non-digital and in-person information exchanges as a strategy for protecting information. R3a, for example, conducts business in person if at all possible after being scammed twice because she does not know how to truly verify identity over the phone or online: *"In person, yeah. If it's an office, I try to visit way ahead of time. If it's making a payment, I like to visit the actual location I need to submit my payments to instead of doing it online or over the phone. Because even over the phone you have no idea what they're going to do with that. Scary thing"* (R3a).

CM1 said that in general, when asked for information that could be given over multiple media, clients "*feel comfortable to give the paper rather than to send the picture*" but because they are extremely busy, "*they send the picture because of the time limit*" (CM1). The decision to share information only in person may have perceived or actual security benefits, but it can also create barriers to refugees' other goals, including establishing a life in the US (CM4).

D. Computer Security Advice Given to Refugees

Finally, we consider computer security and privacy advice given to refugees, either directly by case managers or teachers, or by others with whom refugees interact (e.g., friends or family). Similar to prior work on security advice more generally, understanding this advice helps shed partial light on the sources of refugees' concerns and practices [20], [21]. Because most or all of the people from whom refugees receive advice are not themselves technology or security experts, this advice reflects the (potentially incomplete or inaccurate) threat models or mitigation strategies of these people. Thus, interventions to improve security and privacy for refugees must consider this broader ecosystem of technology users.

General Constraints on Security Advice. All teachers give some security advice (physical or computer) to their students in class, but T1, T2, and T3 expressed a desire to include *more* security advice in their classes (though we note that these statements may have been influenced by the fact that they were speaking to us, security researchers). They, along with T4, CM4, and CM5, identified time and resources (i.e., access to computers for teaching) as a limitation. CM4 explained that both time and the clients' own prioritization of computer skills (including secure behavior and mental models) are both limitations: "*They're adults. It's very hard in one shot to convince them that this is very important for your life, in day to day life. Just only delivering that information doesn't make them change, it has to touch their heart, it has to touch their soul, they have to feel it. Just giving them one lecture about the use of computers. . . It has to go beyond that.*"

Some of the same case managers and teachers indicated that they have advice that they do *not* give, either because their clients are not technically ready for it (T1, T2, T3), or because they, the case managers, prefer to let their clients make their own decisions (CM3).

Now, we turn to the concrete advice that case managers and teachers do give their clients about protecting themselves.

Advice about Protecting Personal Information from Scams. Recall from Section V-B that case managers and teachers identified scams and identity theft as potentially new risks for refugees, and said that they try to instill an awareness of these risks. T4 and T1 talk to their classes specifically about phone scams. T1 advises their clients to "*just hang up*" if "*you get a call from a number that you don't know and they're saying something and asking you questions*," and T4 tells them about "*information that you never tell anybody over the phone because nobody will ever ask you for it*," like "*your social security number*."

Like T4, CM3 also emphasizes the importance of not giving out social security numbers, and CM1 and CM2 said that refugees hear about the importance of keeping their social security number private from other sources, such as other, more experienced refugees from the same community.

The cultural orientation that refugees receive before resettling in the US also includes information about potential scammers and the importance of keeping certain personal information private. The orientation "*let[s] you know that there could be scammers, you should keep your personal information safe and in a secure place, you shouldn't share your personal information with others*" (CM1).

Advice about Website Identity. Beyond general advice about protecting personal information, case managers and teachers also attempt to teach their clients how to avoid scam websites in particular. T1 and T3 send emails to their classes with links, and try to get their students to actually read the emails before clicking on links. CM1 tells their clients to "*use the link that they trust*," such as on websites that they already know, or printed on a business card.

CM1 alluded to a whitelist of company websites and job application URLs which they can send to clients, but when a company or job is not on their list, they either verify it themselves, or recommend the following strategy for checking: "*I google it, the nearest address of that company. I told him, this place is 15 minutes drive from here. I give him the directions — I mean, I printed out the map. Then I told him you can drive to the address, you can go in, and you can ask them for their business card. Or you can ask them how to apply on the website. If you get it from them, it's trustful...*"

However, no participant explained *how* they learn a new URL is safe, or what advice they would or do give to their clients about trusting a new URL without verifying it in person or on paper — perhaps because they themselves are not aware of foolproof strategies to recommend. This is a difficult problem even for digital natives, who may be more accustomed to looking for browser-level signs like HTTPS indicators or searching through search engine results.

Advice about Account Security. Though teachers generally support their clients' security and privacy by teaching them how to protect themselves from scams, they typically do not include (email) account security or password hygiene. Their main goals with computer education are for clients to log in to their email addresses in a browser, send emails, read emails, attach documents, and log out, but creating the accounts or picking good usernames and passwords is a one-time process so it is not a priority (T1).

When case managers and teachers do convey advice about keeping email accounts secure and private, they advise their clients to remember their passwords and not to share passwords with anyone else (T1, T2, T3, CM5). We note that this latter piece of advice may be directly counter to the case managers' and teachers' own practices of retaining access to clients' passwords — again highlighting the tension between security "best practices" and the day-to-day requirements of their work, as well as subtle differences between whom a user may reasonably need to trust with a password and from whom passwords should be protected.

Case managers and teachers also impart advice about password creation, often while helping create or reset a password. This implicit (or sometimes explicit) advice comes in the form of the password creation algorithms the case managers or teachers themselves employ: "*I try to help them create something that's easy to remember, so I'm like, 'your birthdate, your child's name, or your child's birthdate'*" (T1). These strategies focus more on creating memorable passwords rather than creating secure passwords, reflecting the teachers' and case managers' assessment of their threat model for their clients' email accounts: they often encounter cases where clients have forgotten their passwords and need help accessing their accounts, but told no anecdotes about accounts that had been compromised.

Two teachers also mentioned teaching their clients to log off of their emails when they are done on the computers, "*so that when someone else gets on the computer, they don't open up your email address*" (T1).

Summary of security advice. Overall, in Section V-D, we observe that case managers and teachers seem aware of common security best practices around account management and avoiding suspicious websites — however, their technical knowledge may be incomplete, they may struggle with fundamentally hard usable security challenges (such as identifying phishing websites), and they may trade off teaching and practicing hypothetically stronger security measures with the need to achieve other goals (e.g., helping their clients find jobs as quickly as possible).

VI. Discussion

We now step back to highlight key lessons and develop recommendations for the computer security community and other technologists designing for refugees; since refugees have significant overlap with other underserved populations, these lessons and recommendations may apply more widely to populations other than refugees.

A. Lessons

Refugees have heterogeneous technical expertise and threat models, and intersect with other vulnerable populations.

In our interviews, we encountered and learned about refugees with highly variable technical skills and experiences. This heterogeneity leads to a diversity of threat models, security-related actions, and effectiveness of existing or proposed security solutions. Some refugee subgroups share concerns and threats with other vulnerable populations in the US — e.g., people with low incomes, low literacy, limited technical expertise, or limited English skills — while others may not. The observation that "one size does not fit all" echoes recent work within the computer security community studying the needs of particular user groups (e.g., [15]–[18], [22]). For example, the importance of studying vulnerable populations

like refugees is highlighted by anecdotes from our study about scams targeted particularly at people looking for low-income housing or minimum wage jobs; similarly, many of the account practices of refugees are unique to their situations and relationships with case managers. Computer security researchers may not be aware of these threats or challenges without specifically studying the vulnerable populations that they affect.

Computer security is not a primary concern. Echoing a common lesson in usable security, we observe that security is generally not a primary concern for refugees. However, unlike other user populations, refugees are often trading off security-related decisions not with convenience or functionality, but with existential needs that include finding a job, making an income, and establishing a life in the US. Thus, any computer security solutions or advice that impact the efficiency with which refugees can achieve those primary goals will be ignored or circumvented.

Common security mechanisms require cultural knowledge. Many refugees share in common the fact that their entry and integration into the United States involves a major cultural shift. In addition to language and other barriers, these cultural differences can create barriers to establishing their new lives. We find that these cultural barriers also directly affect computer security. We observe that many common end user computer security practices rely heavily on US-based cultural knowledge and norms, including: the fact that social security numbers must be kept private except under certain circumstances (e.g., when applying for a job); the existence of scams and identity theft as a common threat (and the language skills needed to identify likely scams); the information requested by account recovery security questions; and the use of one's birth date as an authentication token. It is critical to identify such cultural assumptions embedded in computer security technologies and account for them in technology designs.

Common security advice and assumptions may be inapplicable to refugees. Among the heterogenous experiences and needs of refugees, we observed cases in which common security advice may be inapplicable to them, or even counterproductive. For example, we found that refugees commonly share email account access with their case managers, due to the importance of finding a job quickly in the face of limited cultural, linguistic, and technical skills. However, this practice contradicts common security advice which instructs people, without regard for their situation, never to share access to accounts or account credentials. (For example, Apple, Google, and Microsoft all officially advise not sharing account credentials, even with friends or family members.[2]) However, following this advice can be counterproductive — for example, leading to refugees who are locked out of their email accounts due to forgotten passwords — and directly conflicts with a refugee's primary goal of quickly finding a job and settling in the US.

[2]https://support.apple.com/en-us/HT201303, https://support.google.com/accounts/answer/46526?hl=en, https://www.microsoft.com/en-us/safety/online-privacy/prevent.aspx

Refugees' computer security practices are limited by their sources of advice. We find that refugees' computer security threat models and practices are heavily influenced by their case managers and teachers, who act as key facilitators of their establishment of a life in the US. Other refugees, friends, and family also provide security-related advice. As a result, the security-related beliefs and practices of refugees are composed of a patchwork of advice and anecdotes shared by people who themselves are typically not technology or computer security experts, and are thus limited by the gaps in their threat models or technical knowledge (echoing findings about a digital divide in prior work on security advice more generally [20], [21]). For example, though case managers and teachers often discussed attempting to teach their clients to be cautious about which links to click on and which websites to trust, they often did not describe concrete strategies for how to make these trust judgments. It is not reasonable to expect that everyone working with refugees (or other vulnerable populations) be a computer security expert — instead, this observation further emphasizes the need for usable security more generally.

B. Recommendations

Informed by our findings, we make recommendations for concrete technical directions that can better serve the security and privacy needs of recently resettled refugees in the US.

Security for public computer users. Since many refugees do not have computers at home, we found that they frequently use public computers for personal activities, including email and job applications, raising a number of potential security concerns. Ideally, administrators of public or semi-public computers should anticipate that some of their users may leave behind sensitive artifacts (and may rely on accessing them later), like resumes, or logged-in email accounts, and implement technical protections to protect the users' privacy between sessions. This solution relies on the individual administrators of these machines, however, and to our knowledge, research methods for secure, trustworthy kiosks have not been widely deployed [23]. By contrast, we found that refugees frequently *do* have smartphones. One potential opportunity for future work is to leverage these personal devices to help provide security for personal accounts and artifacts on public computers.

Security education and training. Refugees typically learn computer skills and security from people who are not themselves computer security experts, and thus whose advice is subject to the gaps in their own knowledge and threat models. While it would be unreasonable to expect refugees or their case managers and teachers to become computer security experts, there may be targeted education and training interventions that could be effective. Future work should consider how to most effectively train and educate non-experts, such as case managers and teachers, who educate, in high volume, a less

technically-adept population. For example, we suggest that security advice take into account the unique needs and tensions of technology use in this population, such as the reliance on case managers for handling job-related emails — i.e., rather than advising people never to share account access, directing people to more secure alternatives that may better balance their security and access needs (such as mail delegation in Gmail[3]).

Password and account management. Our results reveal that refugees need to share their email accounts with their case managers, and case managers need to be able to efficiently access many different email accounts — causing them to engage in practices that may violate common security "best practices," such as reusing passwords, using weak passwords, or storing them in plaintext files. We observe that there already exist technologies that case managers and refugees *could* use to balance these efficiency and security goals, such as password managers and email account delegation. However, we also observe that these existing solutions may not serve this particular use case. Password managers, for instance, may be difficult to use on a public computer, and not every password manager allows sharing credentials. Some email providers, such as Gmail, allow email account delegation[3], but this feature seems designed more for use cases where the primary account owner has an assistant — it would not allow the case manager to actually act *as* the refugee when replying to emails, and would not give the case manager direct access to the password, which they sometimes need for account recovery purposes. Furthermore, we observe that other account security measures, such as two-factor authentication, may be entirely impractical for refugees' use cases, as they would prevent intended access by case managers. These observations raise several challenges for future directions: When existing password and account management solutions are appropriate, how can knowledge of these solutions be imparted to refugees and case managers? And when existing solutions are not appropriate, how should other, more appropriate mechanisms be designed?

Design to leverage refugees' trust in case managers and teachers. We learned that many refugees trust and rely on their case managers and teachers, who pass on a lot of technical and cultural knowledge. An area for future research is how to effectively leverage that trust and use technology to help case managers and teachers pass on their knowledge asynchronously and effectively. One example of existing work along this line is Lantern [12], a smartphone application that helps newer refugees leverage the expertise of more experienced members of the community by scanning strategically placed NFC tags in places like resettlement agencies, bus stops, or grocery stores. Based on our findings, we observe other such opportunities — for example, a browser extension or smartphone application — that could allow refugees to consult remotely with their case managers about their impression of the trustworthiness of a particular website, or check a site against a whitelist precompiled by the case manager, a practice that we observed occurring manually in Section V-C.

Security for digital documents. Another area where technology may be helpful for refugees is in providing security for digital documents, such as photos of sensitive documents that we learned refugees may carry on their (potentially unlocked) smartphones. There do exist smartphone applications for storing encrypted or hidden photos (e.g., KeepSafe[4]), as well as digital wallet applications (e.g., DigiLocker[5]). Future work should study these types of applications in detail to determine whether they have the security, functionality, and convenience properties needed for refugees' use cases — and if not, develop new applications or other approaches that do.

C. Limitations

Finally, we present several limitations of our study that should be considered when interpreting our results.

First, although qualitative methods can be insightful probes into vulnerable or hard-to-access populations, such as ours, they do not allow for statistically significant results. However, qualitative work on the security needs and concerns of various populations is valuable, e.g., [15]–[17], and the depth of the results forms recommendations and lessons for future researchers. Additionally, there is inherent bias in any interview study, particularly about security and privacy, from the fact that participants self-select to participate. For example, it is possible that highly privacy-conscious individuals may be less willing to speak with researchers about technology usage and concerns, and this might skew our results.

Further, as discussed in Section IV, our sample skews towards refugees who rely on assistance from case managers and teachers, and may thus have lower English, technology, or other skills than others. Furthermore, our case manager and teacher interviews reveal their third-person perspective on the refugees they work with, rather than those refugees' own views directly. We valued the case managers' and teachers' perspectives spanning experience with many refugees and grounded in a deeper understanding of US culture. We also found that our refugee focus groups corroborated information we learned from the case managers and teachers. Because of our focus on resettled refugees who rely on case managers and teachers for assistance, many questions still remain about how resettled refugees' use of technology evolves, and what similarities they have to other groups, such as groups with low-income.

Finally, while we attempted to establish good rapport with all subjects — teachers, case managers, and refugees — it is possible that participants did not fully trust us. Although our interviews and focus groups surface numerous findings (Section V), these results should be interpreted with the knowledge that our participants might have omitted more sensitive information.

[3]https://support.google.com/mail/answer/138350?hl=en

[4]https://play.google.com/store/apps/details?id=com.kii.safe

[5]https://digilocker.gov.in

VII. Related Work

Finally, we present related work on refugees and technology in particular, and on computer security and privacy for different populations more generally.

Refugees and Technology. Prior work studied refugees' use of technology in various stages of the refugee process; Talhouk et al. [24] broadly consider the role of the Human-Computer Interaction community in responding to the refugee crisis. Prior work does not consider computer security and privacy in particular, but provides broader context and in some cases surfaces security or privacy related findings. For example, Gillespie et al. [6] thoroughly overview refugee technology usage in and en route to Europe, including surveillance and physical risks as well as the use of social media to spread trusted information; Flemming [3] and Peterson and Fisher [25] study technology use among resettled refugees, particularly for communication with family and friends. Other work has studied technology usage within refugee camps, such as works that surveyed smartphone usage of Syrian refugees in a refugee camp [4], [7], works that studied a computer club in a Palestinian refugee camp [5], [26], [27], and work that broadly examined barriers to technology usage [8]. Other groups [28], [29] have examined the role of technology specifically for education in refugee camps.

Yafi and Said [30] consider WhatsApp usage by resettled refugees, and Almohamad and Vyas [11] more broadly examine the challenges faced by refugees and asylum seekers integrating themselves into host communities and present possible technical design interventions.

There also exist efforts to develop technology specifically to help refugees navigate their new communities, including Lantern [12], a smartphone app that connects new refugees with experienced refugees via NFC tags placed physically around the community; Rivrtran [31], a human-in-the-loop translation platform for recently resettled refugees; and RefUnite [32], a social network.

Computer Security and Privacy for Different Populations. Our research echoes other recent work in computer security and privacy that has observed the importance of understanding the nuanced needs and constraints of different user populations, in order to best serve the security and privacy needs of those populations. For example, recent work has considered potentially particularly vulnerable user groups, including low-income people in the US [15], domestic abuse victims [16], [17], older adults [22], journalists [18], and activists [33]–[35]. Sawaya et al. [36] conducted a large-scale cross-cultural survey of security habits of people from seven countries, and find that security habits and knowledge vary across cultures. Similarly, Redmiles et al. [37] and Wash et al. [38] found difference in security beliefs and behaviors among different demographic groups within the US. Like many of these prior works, our work suggests that the population we study — recently resettled refugees in the US — have distinct computer security and privacy needs and constraints that must be understood before technologies can best be designed for this population.

VIII. Conclusion

Refugees are a potentially vulnerable population, relying increasingly on technology while attempting to establish lives in their new homes. We studied East African and Middle Eastern refugees recently resettled to the US to understand their interactions with and reliance on technology, the barriers they face in implementing strong computer security and privacy practices, as well as their existing security and privacy practices and the guidance they receive from their case managers, teachers, and others. We conducted in-depth semi-structured interviews with case managers and teachers who work with these refugees, as well as focus groups with refugees themselves. We find that refugees are highly dependent on technology and on their case managers and teachers to help them navigate that technology, and we identify numerous cultural, language, and knowledge barriers that impede or are otherwise in tension with commonly recommended computer security best practices. We draw lessons and recommendations for the computer security community, laying a foundation for technologies that can help overcome these barriers and better meet the computer security and privacy needs for refugees and other potentially vulnerable populations with similar barriers and needs.

Acknowledgments

We thank Richard Anderson, Zakariya Dehlawi, Nicola Dell, Kurtis Heimerl, Karl Koscher, Kiron Lebeck, Katharina Reinecke, Alex Takakuwa, and Reem Talhouk for early discussions and efforts on this topic; Eric Zeng for his insightful feedback on our paper; and Brian Rogers and Alison Simko for their copyediting. We thank Jialin Li, Danyang Zhuo, and Haichen Shen for helping us practice running a focus group. We thank Michelle Mazurek for shepherding this paper through the revision process. Finally, a massive thank you to our anonymous participants for giving us their time and invaluable insights.

This work was supported by the NSF Graduate Research Fellowship, NSF Award CNS-1463968, the Short-Dooley Professorship, the Marilyn Fries Endowed Regental Fellowship, and the Bill and Melinda Gates Foundation.

References

[1] 2017, [accessed 19-October-2017]. [Online]. Available: http://www.unhcr.org/globaltrends2016/

[2] 2017, [accessed 28-October-2017]. [Online]. Available: http://www.unhcr.org/en-us/resettlement-in-the-united-states.html

[3] J. Flemming, "Making online connections," October 2011. [Online]. Available: http://www.fmreview.org/technology/flemming.html

[4] R. Talhouk, S. Mesmar, A. Thieme, M. Balaam, P. Olivier, C. Akik, and H. Ghattas, "Syrian refugees and digital health in Lebanon: Opportunities for improving antenatal health," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 331–342.

[5] G. Yerousis, K. Aal, T. von Rekowski, D. W. Randall, M. Rohde, and V. Wulf, "Computer-enabled project spaces: Connecting with Palestinian refugees across camp boundaries," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 3749–3758.

[6] M. Gillespie, L. Ampofo, M. Cheesman, B. Faith, E. Iliadou, A. Issa, S. Osseiran, and D. Skleparis, "Mapping refugee media journeys: Smartphones and social media networks," 2016.

[7] Y. Xu and C. Maitland, "Communication behaviors when displaced: A case study of Za'atari Syrian refugee camp," in *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*. ACM, 2016, p. 58.

[8] L. Leung, "Telecommunications across borders: Refugees' technology use during displacement," *Telecommunications Journal of Australia*, 2010.

[9] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? an experiment with data saturation and variability," *Field Methods*, vol. 18, no. 1, 2006.

[10] K. Charmaz, *Constructing Grounded Theory*, 2nd ed. SAGE Publications Ltd, 2014.

[11] A. Almohamed and D. Vyas, "Vulnerability of displacement: challenges for integrating refugees and asylum seekers in host communities," in *Proceedings of the 28th Australian Conference on Computer-Human Interaction*. ACM, 2016, pp. 125–134.

[12] J. Baranoff, R. I. Gonzales, J. Liu, H. Yang, and J. Zheng, "Lantern: Empowering refugees through community-generated guidance using near field communication," in *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 2015, pp. 7–12.

[13] "Convention and protocol relating to the status of refugees," 1951, http://www.unhcr.org/3b66c2aa10.html.

[14] 2017, [accessed 29-October-2017]. [Online]. Available: http://refugees.org/explore-the-issues/our-work-with-refugees/refugeeresettlementprocess/

[15] M. Madden, "Privacy, security, and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity," Data & Society, Sep. 2017, https://datasociety.net/output/privacy-security-and-digital-inequality/.

[16] T. Matthews, K. OLeary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill, and S. Consolvo, "Stories from survivors: Privacy & security practices when coping with intimate partner abuse," in *CHI Conference on Human Factors in Computing Systems*, 2017.

[17] D. Freed, J. Palmer, D. Minchala, K. L. T. Ristenpart, and N. Dell, "Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders," in *PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing (CSCW)*, 2017.

[18] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the computer security practices and needs of journalists." in *USENIX Security Symposium*, 2015, pp. 399–414.

[19] S. Schechter, A. Brush, and S. Egelman, "It's no secret: Measuring the security and reliability of authentication via 'secret' questions," in *IEEE Symposium on Security and Privacy*, 2009.

[20] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How I learned to be secure: a census-representative survey of security advice sources and behavior," in *ACM Conference on Computer and Communications Security*, 2016.

[21] E. M. Redmiles, A. R. Malone, and M. L. Mazurek, "I think they're trying to tell me something: Advice sources and selection for digital security," in *IEEE Symposium on Security and Privacy*, 2016.

[22] D. Oliveira, H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin, and N. Ebner, "Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing," in *CHI Conference on Human Factors in Computing Systems*, 2017.

[23] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X. Zhang, "Trustworthy and personalized computing on public kiosks," in *6th International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2008.

[24] R. Talhouk, S. I. Ahmed, V. Wulf, C. Crivellaro, V. Vlachokyriakos, and P. Olivier, "Refugees and HCI SIG: The role of HCI in responding to the refugee crisis," in *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 2016, pp. 1073–1076.

[25] A. Peterson Bishop and K. E. Fisher, "Using ICT design to learn about immigrant teens from Myanmar," in *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development*. ACM, 2015, p. 56.

[26] K. Aal, M. Mouratidis, A. Weibert, and V. Wulf, "Challenges of CI initiatives in a political unstable situation-case study of a computer club in a refugee camp," in *Proceedings of the 19th International Conference on Supporting Group Work*. ACM, 2016, pp. 409–412.

[27] K. Aal, G. Yerousis, K. Schubert, D. Hornung, O. Stickel, and V. Wulf, "Come_in@ Palestine: adapting a German computer club concept to a Palestinian refugee camp," in *Proceedings of the 5th ACM international conference on Collaboration across boundaries: culture, distance & technology*. ACM, 2014, pp. 111–120.

[28] N. Dahya and S. Dryden-Peterson, "Tracing pathways to higher education for refugees: the role of virtual support networks and mobile phones for women in refugee camps," *Comparative Education*, vol. 53, no. 2, pp. 284–301, 2017.

[29] S. Dryden-Peterson, N. Dahya, and D. Douhaibi, "How teachers use mobile phones as education tools in refugee camps," March 2017. [Online]. Available: https://www.brookings.edu/blog/education-plus-development/2017/03/14/how-teachers-use-mobile-phones-as-education-tools-in-refugee-camps/

[30] E. Yafi and M. Said, "Empowering refugees in Malaysia: WhatsApp as a dominant tool," 2017.

[31] D. Brown and R. E. Grinter, "Designing for transient use: A human-in-the-loop translation platform for refugees," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 321–330.

[32] 2017, [accessed 31-October-2017]. [Online]. Available: http://refunite.org/

[33] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson, "When governments hack opponents: A look at actors and technology," in *23rd USENIX Security Symposium*, 2014.

[34] S. Hardy, M. Crete-Nishihata, K. Kleemola, A. Senft, B. Sonne, G. Wiseman, P. Gill, and R. J. Deibert, "Targeted threat index: Characterizing and quantifying politically-motivated targeted malware," in *23rd USENIX Security Symposium*, 2014.

[35] S. L. Blond, A. Uritesc, C. Gilbert, Z. L. Chua, P. Saxena, and E. Kirda, "A look at targeted attacks through the lense of an NGO," in *23rd USENIX Security Symposium*, 2014.

[36] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada, "Self-confidence trumps knowledge: A cross-cultural study of security behavior," in *ACM CHI Conference on Human Factors in Computing Systems*, 2017.

[37] E. M. Redmiles, S. Kross, and M. L. Mazurek, "Where is the digital divide?: A survey of security, privacy, and socioeconomics," in *CHI Conference on Human Factors in Computing Systems*, 2017.

[38] R. Wash and E. Rader, "Too much knowledge? Security beliefs and protective behaviors among United States internet users," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015.