"In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya

Collins W. Munyendo, Yasemin Acar*, Adam J. Aviv
The George Washington University, * Paderborn University

***Abstract*—Cybercafes remain a popular way to access the Internet in the developing world as many users still lack access to personal computers. Coupled with the recent digitization of government services, e.g. in Kenya, many users have turned to cybercafes to access essential services. Many of these users may have never used a computer, and face significant security and privacy issues at cybercafes. Yet, these challenges as well as the advice offered remain largely unexplored. We investigate these challenges along with the security advice and support provided by the operators at cybercafes in Kenya through $n = 36$ semi-structured interviews ($n = 14$ with cybercafe managers and $n = 22$ with customers). We find that cybercafes serve a crucial role in Kenya by enabling access to printing and government services. However, most customers face challenges with computer usage as well as security and usability challenges with account creation and password management. As a workaround, customers often rely on the support and advice of cybercafe managers who mostly direct them to use passwords that are memorable, e.g. simply using their national ID numbers or names. Some managers directly manage passwords for their customers, with one even using the same password for all their customers. These results suggest the need for more awareness about phone-based password managers, as well as a need for computer training and security awareness among these users. There is also a need to explore security and privacy advice beyond Western peripheries to support broader populations.**

1. Introduction

Cybercafes are privately-operated facilities with computers, printers, and other equipment where customers pay to access the Internet and perform other computer-related tasks [73]. Quite popular in the early days of the Internet when broadband internet access was less common, cybercafes have recently fallen out of favor in developed countries as personal computers with Internet access in the home become ubiquitous. In developing countries, however, cybercafes remain an extremely common way for many users to access the Internet and other digital services as ownership of personal computers remains relatively low [5].

In Kenya, the government recently transitioned to an e-government portal called eCitizen [24] to improve service delivery. This portal provides a one-stop electronic access to common government services including immigration, drivers' license application, and renewal, etc. However, only around 8.8% of the 12 million Kenyan households own a computer or laptop [16]. Most Kenyans have thus turned to cybercafes to access these services. Many of these users may have never used a computer before and likely face significant usability and security challenges, including computer usage, online account creation, and password management.

In this study, we explore the most common services accessed at cybercafes in Kenya as well as the challenges, particularly related to security and privacy, that customers encounter at these facilities. We are also interested in exploring the security and privacy advice and support offered by cybercafe managers to their customers. More specifically, we seek to answer the following five research questions:

RQ1: What are the most common services that are sought or provided at cybercafes in Kenya?

RQ2: What challenges, especially related to security and privacy, do customers encounter at cybercafes?

RQ3: What security and privacy advice and support is provided at cybercafes and how does it impact cybercafe customers' digital security and privacy?

RQ4: What security and privacy advice do users in Kenya consider important for staying safe online?

RQ5: What are general security and privacy concerns, practices, and behaviors at cybercafes in Kenya?

To answer these research questions, we conducted $n = 36$ semi-structured interviews at cybercafes in Kenya: $n = 14$ with cybercafe managers and $n = 22$ with cybercafe customers. To recruit participants, one researcher, who is a native Kenyan, visited 14 cybercafes in Nairobi, Kenya in July 2022. The researcher made all efforts to visit diverse cybercafes located both in Nairobi's Central Business District as well as in residential areas. As most cybercafe managers and customers were busy at the cybercafes, only five non-recorded interviews with managers were conducted on-site. For the other participants, the researcher collected their contacts and conducted the interviews remotely through direct phone or WhatsApp calls at times that were convenient to the participants. These interviews were all conducted between July and September, 2022 and were audio-recorded and transcribed with permission from the participants.

We asked cybercafe managers to detail the equipment at their facilities, including the number of computers and OS update practices, followed by services that customers most commonly use along with any challenges they encounter. We then asked the managers about the advice and support

they offer to their customers and any standard practices they have at the cybercafe to protect customers' security and privacy. Lastly, we asked managers about their top three advice for staying safe online, similar to previous work on security advice [14], [39]. When interviewing cybercafe customers, we asked about the services they typically use at the cybercafe, as well as any challenges they faced. Afterward, we also asked them to share any security and privacy advice they have received at cybercafes, followed by advice they consider important for staying safe online.

Our results indicate that cybercafes continue to play a critical role in the developing world by allowing many people to access printing, government, and other internet services. In Kenya, most customers use cybercafes because they do not have regular access to personal computers or printers, and rely on the available assistance from cybercafe managers to complete computer-related tasks. At the same time, customers experience significant usability and security challenges around general computer usage, online account creation, access, and recovery. Password management is particularly challenging for many customers who experience difficulty selecting and recalling passwords across accounts, leading to many getting locked out of their accounts.

Most customers rely on advice and support from the cybercafe managers when navigating these challenges, similar to refugees' reliance on their case managers in the US [72]. Many customers are novice computer users, at best, and tend to regularly forget their passwords and sometimes even emails used to register their accounts. The managers end up selecting passwords for them that are easy for the customer (and the manager) to remember, such as customers' national ID numbers, names, children's names or some combination of these. Some managers directly manage the account passwords for some of their customers, with one manager using the same password for all their customers. Unlike security and privacy advice in Western contexts [14], [39], we additionally find that the most important security and privacy advice in Kenya centers around the use of public or shared computers, with most managers and customers indicating that logging out of their accounts after using these facilities is their top advice for staying safe online.

As a community, we need to consider the security and privacy needs of broader user classes, rather than framing all security and privacy solutions for Western audiences. For example, while several managers and customers indicated not saving passwords in the browser of public computers to protect themselves, it is still critical to explore alternative ways of password management that better fit these users' needs. Current password managers, either browser-based or third-party, are not good fits for these users, but mobile phone-based password management offers some promise as phone usage is high. At the same time, device-sharing is quite common, complicating such solutions. We explore these challenges, offer recommendations, and suggest promising areas for future work that can further protect broader user bases, including general computer training and security awareness as well as the need for additional research on security and privacy advice beyond Western contexts.

2. Background on Cybercafes in Kenya

A cybercafe, also known as an internet cafe, is a facility typically equipped with computers, printers, and other equipment where customers pay to access the Internet, play online games, edit, scan, photocopy, and print documents among other computer-related tasks [73]. The first cybercafe, known at the time as cyberia, is believed to have been established in London in the United Kingdom in 1994 [37]. It became an instant success as the Internet was still in its early days and most people did not own personal computers or laptops. More cybercafes were subsequently established in other places and countries around the world. However, recent ubiquity of the Internet coupled with the proliferation of personal computers have seen a rapid decline of cybercafes, particularly in developed economies.

While smartphone adoption and usage has been steadily growing in developing economies [3], many people in developing countries still do not own personal computers or laptops, with only an estimated 7.7% of households in Africa owning a computer in 2019 [5]. Coupled with growing social media adoption as well as digitization of government services, many users in this region are increasingly relying on cybercafes to access essential services.

Kenya is one of the countries in Africa that have recently transitioned to an e-government portal in a bid to "hasten service delivery, reduce transaction costs and safeguard revenue" [2]. Known as eCitizen [24], the portal provides a one-stop electronic access to essential government services including, among others, immigration, land transactions, business registration, and motor vehicle purchase, and registration. To use eCitizen, users create an online account on the portal, fill out the relevant application forms, make the required payments and print the filled forms before finally presenting them to the relevant government department. This portal stores a significant proportion of sensitive user information, including their identification and passport details, date of birth, address, next of kin, and their personal details. It is therefore imperative to protect these accounts.

However, with only about 8.8% of 12 million Kenyan households owning a computer, laptop or tablet [16], a large proportion of Kenyans have turned to cybercafes to access these essential government services (examples of cybercafes in Nairobi, Kenya, are found in Figure 1). Even those that own computers often do not have printers at home and usually visit cybercafes whenever they have to print, scan, or photocopy documents outside of work or school. Further, some cybercafe customers are novice users and have never previously used a computer nor created an online account before, and face significant challenges throughout.

It is the goal of this research to both understand the challenges encountered by cybercafe users, particularly those related to security and privacy or account management, and the advice and support that these users receive at the cybercafe from other customers and the cybercafe management. We also seek to understand the impact of this advice on the customers' security and privacy perceptions, practices, and behaviors at the cybercafe and beyond.

(a) Customers using computers in a cybercafe.

(b) A customer receiving assistance in a cybercafe.

Figure 1: Customers at different cybercafes in the Central Business District in Nairobi, Kenya, in July 2022.

3. Related Work

Cybercafes and public libraries. Cybercafes have not received much attention in the research community of late. However, earlier studies investigated the role of cybercafes, as well as characteristics of customers and their usage patterns in different regions and countries. Through street surveys, Gitta and Ikoja-Odongo [32] demonstrated how cybercafes were enabling Ugandans to access information in 2003, and Haseloff [36] found that cybercafes were the most-commonly used means to access the Internet in Bangalore, India in 2005. Haseloff further found that most cybercafe customers tended to be younger and able to communicate in English while another study in the Philippines in 2012 found that most cybercafe customers were male [13]. Public access venues, such as telecenters, libraries, and cybercafes, have also been shown to be fundamental in enabling communities access the Internet in Colombia [33].

Most closely related to our work are four studies that have investigated security and privacy practices at cybercafes in Morocco [38] and public libraries in the US [23], [45], [47]. Through a field study complemented by questionnaires for both cybercafe managers and customers in Morocco, Houmz et al. [38] found that managers were hesitant to update the cybercafe computers' operating systems because of limited resources on the devices, a theme also noted in our study of cybercafes in Kenya. The study further found that an alarming 60% of the cybercafe computers were infected with malware. Recently, Dooley et al. [23], Luo and Warford et al. [45], and McDonald et al. [47] have conducted interviews with IT professionals working in public libraries in the US, exposing challenges and constraints to privacy as well as general security and privacy practices at these facilities. Different from these studies, we use semi-structured interviews with Kenyan cybercafe managers and customers to investigate cybercafe practices and behaviour, as well security and privacy advice offered to customers. We additionally investigate advice that users in Kenya consider important for staying safe online and compare our findings to previous work [14], [39] focusing on Western contexts.

Security and privacy advice. Security and privacy advice has been the subject of much research in the community. Through two online surveys in the US with expert and non-expert users in 2015, Ion et al. [39] noted differences between what experts and non-experts consider important for staying safe online, with experts recommending OS updates, strong passwords and two-factor authentication. In contrast, non-experts indicated that using anti-virus software, strong as well as constantly-updated passwords were more important. Through a replication study with European participants, Busse et al. [14] confirmed most of these findings in 2019. In our study with cybercafe managers and customers in Kenya, we find that most participants consider logging out of their accounts, strong passwords, avoiding clicking on suspicious links and not saving passwords in the browser as the most important advice for staying safe online. The differences with previous work can be attributed to different ways in which people access the Internet in different places, suggesting that security and privacy advice is only effective if it considers the specific needs of the target population.

Researchers have also investigated the sources of security and privacy advice as well as its perceived efficacy, comprehensibility, and actionability. By first identifying search queries for security advice on the web with crowd workers from MTurk followed by user studies with experts and non-expert users in the United States, Redmiles et al. [64] found that users perceive most security imperatives as fairly

actionable but struggle to prioritize, similar to Reeder et al.'s findings [65]. The study suggests the identification of a minimal set of highest impact and most practical advice to help end-users. Through a census-representative survey in the United States, Redmiles et al. [62] also found that socioeconomic status influences advice sources for users, with the socioeconomically advantaged more likely to take advice from their workplaces while those with lower skills rely on family and friends. The cost vs benefit tradeoff of following advice [25] as well as the trustworthiness of the source [63] also seem to play a part in users' decisions to follow recommended advice. Some of these results, including trustworthiness of the source of advice, are confirmed in our study with participants from Kenya.

Social media has also proven to be a useful source of security and privacy advice. During the BLM protests across the US in 2020, Boyd et al. [12] were able to identify various classes of security and privacy advice for protesters through Twitter and Google searches. By analyzing security and privacy advice on Twitter during the Russian invasion of Ukraine in 2022, Schmüser et al. [70] found that prioritization of advice remained a persistent challenge, similar to prior work [64], [65] while Wei et al. [77] have recently demonstrated how "anti-security" and "anti-privacy" advice provided on TikTok unfortunately enables surveillance and control in interpersonal relationships. At the same time, Bhagavatula et al. [10] have recently found that user interactions with security advice on Twitter and Facebook are scarce.

Understudied and at-risk populations. Due to the varied security and privacy needs and practices across different countries and cultures [9], [19], [40], [66], [69], a growing body of research has advocated for more consideration of different populations' needs in the design of security and privacy solutions. Similar to the reliance on cybercafe managers by customers for security advice and guidance from our study, Simko et al. [72] found that refugees in the US rely and trust on their case managers in managing their digital security and privacy. The study further found that security is not always a priority for this user group because of competing needs, similar to mobile loan app users in Kenya [53]. Due to an expectation to share their phones with others in the household, women in South Asia have been found to resort to techniques including content deletion and app locks to protect their privacy [68].

Other studies have focused on at-risk populations because these users' unique needs and threat models often amplify the risks or harm they face in their usage of technology [76]. In their study with Sudanese political activists, Daffalla and Simko et al. [22] found that while activists could be better supported with defensive technology design, it is difficult to generalize these design recommendations. Additional studies have investigated other at-risk populations including incarcerated individuals [57], [58], undocumented immigrants [34], inter-partner violence victims [15], [26]–[28], [74], [75], [78] human trafficking survivors [17], journalists [49], sex workers [7], [35], [46], Muslim-American women [1], LGBTQ+ folks [31], refugees [71], [72], children [42], [43] and older adults [29], [50]–[52], [54], [59]–[61], highlighting the need to consider these populations' unique needs in the design of security and privacy tools. Researchers have further developed frameworks and guidelines that can help explore and support research in these populations [8], [11], [18], [76]. Our study highlights the unique needs of users of cybercafes in the developing world, and offers recommendations, including the need for additional work, to further support them.

4. Methodology

We conducted $n = 36$ semi-structured interviews with Kenyan cybercafe customers and managers to explore security and privacy challenges and practices at cybercafes: $n = 14$ interviews with cybercafe managers (M01-14) and $n = 22$ interviews with cybercafe customers (C01-22). We also investigated the scope and nature of advice that is provided to customers at these facilities and its impact on their security and privacy actions and perceptions. In this section, we describe our recruitment procedure and interview script followed by our approach to data analysis. Finally, we discuss the limitations and ethical considerations of our study and how our views and subjectivity likely influenced the study design and interpretation of the results.

Recruitment and demographics. To recruit participants, one researcher, who is a native Kenyan, visited 14 cybercafes in Nairobi, Kenya in July 2022. Additional participants were recruited through snowballing [30] where participants recommended other potential participants that have previously or currently use, work, or own cybercafes in and around Nairobi. We made all efforts to diversify our sample, with the researcher visiting cybercafes located both in Nairobi's Central Business District as well as in residential areas. We had a total of $n = 36$ participants, $n = 14$ cybercafe managers and $n = 22$ cybercafe customers.

Participants had to be at least 18 years old and previously have or currently use, own, or work at a cybercafe in Kenya. Most of the cybercafe managers own the cybercafes (10 were owners while 4 were employed there) and had between one to five years of experience owning or working at the cafe. While most of the managers were male aged between 26 to 30 years, we had an even split between male and female participants for the customers. Most customers were young and between 18 to 25 years. Tables 1 and 2 summarize the cybercafe managers' and customers' demographics.

Interview procedure. The interview procedure centered around the research questions outlined in Section 1. The protocol was also informed by prior studies that explored security and privacy where users share computing facilities, such as libraries in the US [23], [45], and research on users that rely on others for digital assistance, for example newly resettled refugees in the US [72]. Similar to studies that have investigated security and privacy advice [14], [39], we also explored the security and privacy advice that participants in Kenya consider important for staying safe online and how

TABLE 1: Demographics of Cybercafe Managers.

		No.	%
Gender	Female	3	21.4
	Male	11	78.6
Age	18 - 25	2	14.3
	26 - 30	5	35.7
	31 - 35	4	28.6
	36 - 45	1	7.1
Own Cybercafe	Yes	10	71.4
	No	4	28.6
Cybercafe Experience	Less than a year	3	21.4
	1 - 5 years	9	64.2
	Over 5 years	2	14.3
Education	College	6	42.9
	Bachelors	7	50.0
	Masters	1	7.1

Bachelors and Masters degrees in Kenya are offered by universities, with colleges mainly offering vocational training.

TABLE 2: Demographics of Cybercafe Customers.

		No.	%
Gender	Female	11	50.0
	Male	11	50.0
Age	18 - 25	15	68.2
	26 - 30	6	27.3
	31 - 35	1	4.5
Own a Computer	Yes	16	72.7
	No	6	27.3
Employment	Employed	7	31.8
	Not employed	14	63.6
	Prefer not to say	1	4.5
Education	High school	7	31.8
	College	4	18.2
	Bachelors	9	40.9
	Masters	1	4.5
	Prefer not to say	1	4.5

this compares to Western perspectives. The full interview procedure is available in Appendices A and B.

Cybercafe managers were interviewed first as a way to broadly explore general practices at cybercafes. We began by asking managers general questions about their experience level with cybercafes, the number and type of equipment in their facilities, and how often these devices are updated. We then inquired about common services that users typically seek, along with any challenges they face. Following, we asked them to detail any assistance and advice they offer to their customers, both generally as well as relating to security and privacy, if they did not mention it themselves. We then asked for their top three security and privacy advice for staying safe online and if they had any standard practices at their cybercafes to protect customers' security and privacy.

For the cybercafe customers, we first asked them to state their reasons for using cybercafes and what they like and dislike about using cybercafes. We inquired about how frequently they visit cybercafes, along with factors they consider when selecting a cybercafe. Following, we asked them to describe any challenges they have faced when using cybercafes and any assistance they received, both generally and specifically relating to security and privacy. Similar to the managers, we also asked for their top three advice for staying safe online. Lastly, we asked customers questions about their mobile phone usage, including the websites they access, whether they share their devices with others, and any authentication they use to protect access to their devices.

Data collection. The study was piloted twice. Foremost, two cybercafe managers in Kenya participated in two separate preliminary interviews conducted through WhatsApp calls. After an iteration based on their feedback, two mock interviews were conducted with qualitative researchers, with each acting as a cybercafe manager and customer. Based on that feedback, we added more branching questions and deeper probes to the interview questions [20].

One researcher, who is a Kenyan native, visited 14 cybercafes for recruitment and data collection in Nairobi, Kenya in July 2022. Nearly all the cybercafes were relatively small, containing between 1-to-10 computers (one had 20 computers) that were all running Windows. Two cybercafes also had CyberCafePro [21] to help manage user sessions and payment. A majority of the cybercafes had one or two printers, with only three cybercafes having more than two.

Five non-recorded interviews with managers were conducted on-site. However, since most of the managers and customers were busy using the cybercafe services or assisting customers, the researcher collected their contacts and conducted recorded interviews later at their convenience through WhatsApp or phone calls. These interviews were conducted between July and September 2022. Each participant was compensated with 2 gigabytes of internet data or 125 minutes of call time as an appreciation for participating. On average, the cybercafe manager interviews lasted 41 minutes while the customer interviews lasted 30 minutes.

All interviews were audio-recorded except five on-site interviews with cybercafe managers who were uncomfortable being recorded at the cybercafes. The interviewer took comprehensive notes during these interviews. While all interviews were conducted in English, one of Kenya's official languages [56], participants occasionally provided some responses in Swahili. These were all translated to English during transcription by the Kenyan researcher who is fluent in both languages.

Data analysis. We qualitatively analyzed the interview transcripts and notes using open-coding techniques [67]. One researcher independently coded all the interview transcripts from cybercafe managers and customers to develop a primary codebook. A secondary coder then used this codebook to independently code half of the interviews from the cybercafe managers and half of the cybercafe customer interviews. Throughout the process, the two researchers frequently met to resolve coding differences and update the codebook. The researchers also used these meetings to discuss broader themes emerging from the study [48]. The results in Section 5 are based on the primary codebook (available in Appendix B). Due to the qualitative nature

of this work, we do not report counts to avoid implying generalizability. Instead, we use quantifiers such as most, few, some etc. to show the prevalence of common themes.

Limitations. Our study has several limitations. Foremost, our sample size is relatively small, urban, and limited to participants that agreed to participate. A few potential participants, particularly managers, declined to take part for various reasons, including being busy or concerns about leaking competitive information. While we do not claim our results to be fully representative – there are likely themes that we could not capture due to the size or recruitment of the sample – we argue that the themes we did identify are likely common and relevant at cybercafes in Kenya, and potentially other regions with similar demographics.

This study may also suffer from social desirability bias where participants try to look more favorable to an outside observer, particularly if that behavior may cast them in a poor light, like using bad security or privacy practices. We tried to mitigate this by encouraging participants to be honest throughout, citing that we were not testing their knowledge but simply interested in their honest thoughts and real practices. Our results suggest participants were forthcoming, with some participants going as far to share what may be considered unflattering behavior. A few managers, for instance, admitted they do not "interrupt" customers when they are facing challenges so that they can spend more time and ultimately more money at the cybercafe.

Lastly, the top security and privacy advice reported by cybercafe managers and customers could be attributed to these users mostly relying on public computers at the cafes. Despite cybercafes' popularity, more work is needed to broadly explore security and privacy advice in Kenya beyond cybercafes.

Ethical considerations. This study was approved by both our Institutional Review Board (IRB) and the National Commission for Science, Technology, and Innovation (NACOSTI) [55], the body that oversees and approves research activities in Kenya. We fully informed participants about the purpose of the study, its duration, and any anticipated risks. Participants were also free and encouraged to withdraw from the study or not respond to any uncomfortable questions without any consequences. Additionally, we did not collect any personally identifying information from participants to minimize any risks of potential disclosure. Any personally identifiable information captured was scrubbed off the transcripts before we performed qualitative analysis.

Positionality statement. We believe that it is important to highlight how our views, subjectivity, backgrounds, and experiences influenced the study design and interpretation of results [44]. Our team consists of three researchers from Africa, Europe, and North America. We used our diverse technical expertise and experiences to design the study, with the Kenyan researcher conducting the interviews. The Kenyan researcher is well-versed with cybercafes, and has extensively used them in the past. His fluency in English and Swahili – the national languages in Kenya – helped him recruit and communicate with participants. We do not make assumptions about how cybercafe customers and managers should manage their security and privacy. Instead, we purposefully made our questions open-ended to allow participants to share their thoughts. Our analysis and interpretation of the results are also subject to our own views and subjectivity, and may be interpreted differently by others.

5. Results

This section is structured around our five research questions outlined in Section 1. We first discuss the important role that cybercafes play in enabling people to access government and printing services in Kenya, followed by challenges that customers encounter at these facilities. Afterward, we detail the advice and support provided, followed by security and privacy concerns, practices, and behaviors at the cybercafes and beyond. Since our results are qualitative in nature, we do not report counts to avoid implying generalizability. The counts provided in Table 3 are only meant to highlight common themes and unique perspectives.

5.1. RQ1: Role of Cybercafes in Kenya

Reasons for establishing cybercafes. When asked their reasons for establishing the cybercafe, most managers indicated doing so to address the demand for Internet and printing services, particularly relating to government services, as well as to provide for their livelihoods. M03 stated that they established their cybercafe because people need *"the cyber services, things like printing and other Internet services."* M14 *"saw it as one way of helping the society and then on the other hand, at least generating some small income."* Those employed at the cybercafes as managers, who were not owners, indicated that they are interested in and passionate about computers, or that they have the relevant skills to operate them from school or past experiences.

Common services provided at cybercafes. Printing and government services accessed via eCitizen [24] are by far the most widely-used services at cybercafes. M10 indicated that *"there are these online services, you know them, application for police clearance, you have application for NTSA*[1] *services ... application for smart DL, you can have PSV*[2] *badge, you can also have passport application, that is the department of immigration. So most of my customers ... maybe deal with government services."* Other common tasks performed at the cybercafe include job applications, email access, photocopy, assignments or school projects, document typing or editing, scholarship or school applications, social media access, remote work, movie streaming or downloading, gambling, filing of taxes through iTax [6],

1. The National Transport and Safety Authority (NTSA) is the governmental body in Kenya that manages the road transport sub-sector.

2. A public Service Vehicle (PSV) license is a document issued by NTSA to drivers who serve the public sector by offering transport services.

and computer training. Beyond cybercafe services, some cybercafe managers further indicated that they sell phones, computers, stationery, and other equipment that customers often require. Other services mentioned by more than one cybercafe manager included gaming, banking and mobile money services as well as repairs. For repairs, M14 stated that *"you will find that I also have a category of customers who bring machines to be repaired, who bring machines to be installed for the operating system."*

Services requested but not provided. When managers were asked about the services their customers sought, some wanted services that were not provided or are illegal. This included certificate or document forgery, website design or development, music downloading, phone formatting, photography, bulk and passport photo printing. Most managers are hesitant to forge documents or download music for their customers due to personal integrity or legal liability. As an example, M06 stated that *"forgery is not healthy, it's like you're lying to somebody that this person is so able to have this thing, like somebody never did form four*[3] *but you're giving this person a form four certificate."* M03 wondered *"what happens if you're caught doing it"* while M09 said they do not download music for their customers as they do not have a license[4] to do so: *"I don't put Kenyan music or East African music for customers because that is illegal in Kenya, because unless you have the copyrights from the government, you cannot put those kinds of songs. When they find you, you are arrested."* M08 even mentioned that *"some people want to disable their partners' Facebook accounts."* For the advanced tasks including website design and bulk printing, the managers often indicated that they lack either the required expertise, equipment or time to offer them.

Factors when choosing a cybercafe to visit. When choosing a cybercafe, a majority of the cybercafe customers consider the environment where the cybercafe is located, the cybercafe manager friendliness or their ability to offer assistance, the Internet speed at the cafe, and cost. For instance, C08 stated that one of the things they consider *"is the person behind the counter. How are they receptive? How are they addressing my issues?"* Other factors that customers often consider include proximity of the cybercafes to where they are or live, the state or speed of the cybercafe computers, availability of working space, electricity stability, physical safety, and privacy. Regarding privacy, C02 stated: *"I don't like those [cybercafes] that are open . . . you have a computer here and then there's no partition. It's just like somewhere where you can find some privacy and do your work without somebody peeping at what you're doing."*

Additional cybercafe positives. Beyond the relatively fast Internet available at cybercafes, most customers appreciate the availability of equipment, such as computers and printers, that they may not have access to regularly. C01 indicated that *"in the cybercafes, I easily get the printers and maybe more advanced equipment that I may want to use in my projects."* Several customers also mentioned affordability of services, availability of assistance and perhaps surprisingly, privacy as other things they appreciate about cybercafes. C19 mentioned that the cybercafe they use is *"partitioned in such a way that the neighbor, the person sitting next to you can't see or access what you're doing."* C03 even mentioned that they feel they have more privacy at the cybercafe compared to working from home: *"There's a lot of privacy there, more than using my own laptop, and my son also sometimes would like to use it [at home]. So in the cybercafe, I think there is some privacy there."*

RQ1 summary. Cybercafes play an important role in Kenya by providing customers access to printing, government, and other Internet services that they may otherwise not have access to due to a lack of required equipment such as printers or personal computers. Customers additionally seem to prefer cybercafes where the managers are friendly and can therefore assist them whenever they encounter challenges.

5.2. RQ2: Challenges at Cybercafes

Cybercafe challenges. When asked for general challenges or drawbacks when using or operating cybercafes, an overwhelming majority of cybercafe managers and customers mentioned slow internet that sometimes makes it difficult to access websites or perform other Internet-related tasks. C13 said that the *"challenge I have faced is the network. Sometimes it's slow, because we have so many people in that cafe, using the Internet."* M13 underscored the importance of having an alternative internet plan in case of connectivity issues: *"Even if I'm using a good internet connection from fiber, sometimes there is a downtime and you don't understand why. So . . . you must always have a backup plan."*

Other common challenges include electricity outages, old or faulty equipment, and slow computers. Several customers also complained about the printing quality in some cafes, with C02 saying that *"there are some cybercafes where the printers are, I think outdated, because once you print, the documents don't come out clearly."* Some customers additionally indicated unhelpful or unfriendly managers, and crowded as well as noisy cybercafes as aspects they disliked about some cybercafes. Some managers cited harassment from the government or law enforcement as well as expensive equipment as additional challenges they encounter. M10 complained that *"with [the] county police, they require a license for single business permit, they require license for fire*[5]*; they require license for advertisement. But you see, you cannot have all of them. So for my case, I have a license for single business permit. I have an advertisement board, but I don't have the license. I also use electricity but I don't have the license for fire. So the main challenge is that when you hear that county police are around, you have to close your business whether you like it or not, because*

3. The final year of secondary school in Kenya is known as form four.

4. If you play music in your business, or want to use music in the promotion of a product, you need clearance from the owners of that music.

5. A fire license in Kenya certifies compliance with fire safety standards.

you will be arrested." M03 added that *"even though we have paid their licenses, they usually come and rough up the operators inside the cyber."*

Customer challenges. The most common challenge that customers face at cybercafes is generally not knowing how to use or operate the computers. M10 said that some customers are sent to the cybercafe, for example by their family members, but forget or do not know what to do: *"Most of the time, you get a person, they don't know how to use a computer, and they tell you I want to do this thing. He has no clue. So you have to start from scratch, and ask him what he has been sent to do."* C08 added that *"when doing things to deal with government tax, filing my returns, sometimes, I don't know how to go about it."* Customers also struggle with either printing, binding or scanning, using certain programs as well as typing. M05 said that *"maybe a customer doesn't know how to type, and the documents he wants to send; he or she is unable to compose the email."*

Another challenge that customers often encounter is difficulty accessing or recovering access to their online accounts because they have forgotten their account passwords. M07 said that *"the main challenges are that sometimes the accounts are not functional, that they have been locked out because of lost passwords."* Several managers also mentioned that some customers usually forget the emails or phone numbers used to create their accounts. M10 said that *"someone comes and tells you: I have a KRA*[6] *PIN, I don't know the email that I used or the phone number that I used [to create the account]. So I find it as a challenge because if someone does not know the email that they used, or the phone number used, so it means that they have a challenge creating an email, setting up their account."* C20 indicated that *"I had forgotten my email, my password . . . and they [cafe managers] helped me."* Some customers, however, give up on the account recovery process as mentioned by M07: *"Maybe you lost your password and this is something that is so common here and now you have a process that you have to follow so that the provider can reset the password. But some of them, they don't want to wait or they don't want to contact the customer care. So they will just leave it and say they don't want to use that site for now."*

Some managers and customers mentioned website downtime and bad user interfaces, especially on government websites, as other challenges in accessing user accounts. C04 complained about *"the government systems. When you're browsing, they may be a bit frustrating, maybe system failures in terms of those websites . . . like, our taxing system."* M08 was similarly frustrated about the *"bad user interface from some government sites for example NTSA."*

Customers also encounter challenges when setting up their accounts, with some customers struggling to comply with certain password requirements, not knowing the appropriate password to use, or not caring about passwords all together. This leads to poor memorability of these passwords the next time they need to access these accounts. M10 said that *"most of the people, they are not aware which password they can use,"* while M08 added that *"some sites have specific password requirements, some require a mixture of characters which can be challenging for customers."*

Other challenges that customers encounter include struggling to understand websites in foreign languages and a fear of computers. M08 stated that *"some websites are in foreign languages and customers are not aware about [Google] Translate"* while M01 added that *"some customers fear using the computer."* To navigate these challenges, managers usually provide guidance and assistance to their customers. This is discussed in Section 5.3.

Reasons for not facing challenges. Customers who have not faced any challenges at the cybercafe indicated that they mostly visit cybercafes that they are familiar with to do familiar tasks, or that they are experienced with computers. C19 stated that *"personally, when I go to the cyber* [7]*, I know what I'm going to do and I have these specific sites or websites that I'm going to access, . . . and I've been dealing with these, these websites for some time. So I don't get those challenges, unless it's a new site."* C06 cited their computer knowledge: *"You will find that, maybe, more so I have more of the computer knowledge because the work that I always do, it's computer-dependent. So I think it's also my computer knowledge that always makes me not to ask a lot of questions because it is what I use in my day to day basis."* Some customers further indicated that the tasks they do at the cybercafe are easy while others pointed to the availability of assistance as reasons for not experiencing challenges.

RQ2 summary. There are several challenges at cybercafes, especially relating to internet and electricity outages that often times make their services unavailable. Customers experience challenges with the general usage of computers and other cybercafe equipment including printers, as well as difficulty accessing or recovering access to their online accounts. To resolve these challenges, customers often turn to the cybercafe managers for assistance.

5.3. RQ3: Advice and Support at Cybercafes

Account and password management. As general computer usage and account recovery are the most common challenges at cybercafes, the most common advice and support offered to cybercafe customers relates to account and password management. Most managers encourage customers to select easy to remember passwords including their national ID card numbers[8], birthdays, phone numbers or some combination. M03 said that *"if we find, like a novice user, in most cases we just use a password that has a feature in them or what they have. So for example, a user has come to just apply for or create an account for government services. In most cases,*

6. Kenya Revenue Authority (KRA) is the governmental body in Kenya responsible for the assessment, collection, and accounting of all revenue.

7. Cybercafes are commonly referred to as cybers in Kenya.

8. An Identity Card (ID) is an identification document with a sequential 8-digit national ID number issued to Kenyans that are at least 18 years.

we use their identity card numbers as their password, or their mobile [phone] numbers . . . A combination of mobile, and year of birth, those common characteristics that define a person. So we usually give them or create for them just a password they can easily remember."

M05 said that if the customer name is *"John, I use the first letter of your name, your ID [number] and then add a full stop, just to make them remember."* M06 indicated using a mix of the name of the customers' children and their birthday: *"For the majority of them, I like asking them: What is the name of your first child? When was he born, or she born? Then, let's say it's William. I take, I just use William@2004#."* M04 encourages their customers to only use their ID numbers as using words or names can make these passwords hard to remember, especially with multiple cases: *"I usually recommend them to use the ID number as the password because with the names of their first-borns, they can forget if the name was in capital or lowercase."*

To help customers recall their passwords, some managers encourage customers to save their passwords in the cybercafe browsers, write the passwords down for the customers, or even select the passwords for the customer. M10 stated that *"in most of the cases, I can say in eighty percent of the cases, I select the password for them; twenty percent, they select the password for themselves."* M06 said that they store the passwords for the customers by writing them down and then providing them when they request: *"They come to you and tell you: What was my password? Then you get where you wrote the password and give the person the password."* M01 uses a standard password for all novice customers so that they can easily provide it to them on request: *"I use a flat password for anyone new to computers; it's the same password for all of them."* C14 said that their cybercafe manager encourages them to save their passwords in the cybercafe browser for seamless access whenever they visit the cybercafe: *"The advice I got was that they are able to save my password so that the next time I visit, I just go through without even asking."*

At the same time, some managers encourage their customers to use passwords that are uncommon or difficult to guess and to not save them in the browsers on the cybercafe computers. M08 tells their customers not to *"use passwords that are common for example phone numbers, ID numbers"* as well as *"common passwords like Godspeed, Godsent."* M02 asks customers *"not to save passwords in the browser"* while C04 said that *"when you access those cybers, you're told not to save your password for the purpose of privacy."*

Support and guidance with tasks. Due to challenges using computers, several managers said that they often have to do the actual tasks for their customers. M11 said that *"most customers ask me to do the actual tasks for them as they do not know how to do them or are unable to do."* M02 added that *"some tasks are also more technical for example explaining how to do something in Microsoft Word or Excel can be very hard, so I just have to do it myself."* C10 said that *"most of the time, they do it for you. Printing, photocopy, like they do for you everything."*

Account recovery. Since customers tend to forget their passwords, cybercafe managers use various ways to try and recover access to these accounts, including resetting passwords or contacting relevant customer care. M04 said that most customers that forget their passwords *"are old-aged people. They usually come and they have forgotten their passwords. Or you can get the other person has forgotten their Gmail account . . . So I usually use their phone number to retrieve the Gmail account or the password. So when they come, I usually use the verification code through the phone number to retrieve their Gmail [account]."* M08 reaches out to customer support, particularly for local government-related accounts: *"For account recovery, if local, such as the government, I try to make calls to [the] relevant people. If I cannot get assistance, I ask them to go to the help desk of the relevant government service."*

Account recovery, however, is not always successful as some customers usually forget the emails associated with the accounts, or no longer have the phone number used to register the account. M01 said that *"the challenge that's usually hard to resolve is resetting passwords for users who have lost their phone numbers, some people even forget their email addresses. Others have many emails but cannot even remember these emails."* M10 indicated that some customers forget the usernames that are set for their accounts: *"You've created an account for someone, you've created a password, someone comes back and asks you: What username had we used? What password had we used? So it gives you a challenge remembering your customers' passwords, the username you had used."* To navigate these challenges, some managers write down account details for their customers, encourage customers to save their passwords in the cybercafe computers' browsers, or even select a standard password for all novice customers as described earlier.

Teaching or training customers. When customers encounter challenges using computers, cybercafe managers usually guide them or teach them how to do the tasks. M09 said that they first *"inquire where they need help. After they have told me this is where I need help, I personally teach him or her. This is where you go, this is what you do so that [the] next time when he or she comes, she doesn't have the problem anymore."* M05 added that they *"advise them to familiarize themselves with computers and some of them come back as our students for computer packages."*

Other guidance and advice. To protect their customers' accounts, some managers additionally encourage their customers to always log out and never to save their passwords in the cybercafe computers' browsers. M09 said that *"a lot of customers don't know how to log out of their Gmail accounts . . . So anytime a customer comes to my cybercafe, I must tell them, after you have logged in to your account, please log out and delete the account because I don't want to get in trouble because of identity theft . . . So by the time I'm closing up, I have to check in every computer, which account is not my mine or associated with the cybercafe, and I delete it."* M01 encourages customers using their own

computers to constantly update their operating system, while C01 said they were advised not to save any documents on the desktop of the cybercafe computers by a manager.

Sources of advice. When asked for their sources of security and privacy advice, a majority of customers and managers often mentioned the Internet, with C03 saying *"I just Google."* Most managers leverage their personal experiences with computers when assisting or guiding their customers. M03 said that *"after doing something for long, you are very much conversant, you get experience on it."* M14 added that *"the advice that I usually rely on by the way is based on my personal experience. Because I have dealt with computers, I've been in the IT industry for a very long time. So at the end of the day, there are some things that don't actually force me to go and seek suggestions from people."* Managers also reach out to other cybercafe managers when customers experience challenges they are not familiar with. Other sources of security and privacy advice for both customers and managers include school or training, as well as family and friends.

Reasons for (or against) following advice. A majority of cybercafe customers follow the advice provided to them by managers because it helps resolve their challenges, they believe the advice helps protect their personal information, or because they trust the cybercafe manager. C08 indicated that *"if I asked them something that I don't know, then I have to take the advice and try it out, but almost all the time it has worked out."* M14 further added that *"most of them have come back to me actually confessing that they did get help, and they're doing well."* C15 follows the advice *"because they are very important in . . . securing the data that I interact with."* M01 pointed to the trust they have developed with their customers: *"Yes they follow the advice, others take time to write it down. They follow the advice because of the trust we have developed. Some will even call me at night to ask for their password, and some even travel from afar just to come and find me."* Some customers also follow the advice from managers because they view or find the manager to be an expert or friendly, or have limited time to perform the tasks which are sometimes very urgent.

At the same time, a few customers sometimes fail to follow advice provided by the managers. Often, the managers said the customers have contradictory beliefs, they are too elderly or have been advised differently. Other times, the customers are skeptical of the advice, do not have time or the tasks they are performing are non-urgent. M08 said that *"some refuse to follow the advice because they may have been advised differently. For example, some believe [that] having many emails is criminal. Some have religious beliefs and believe social media accounts are evil. For example, one came and applied for a job, and I helped them create a LinkedIn account. The next day, they came back to ask me to delete it since they were informed it is evil."* M08 said that *"some listen with suspicion. Some suspect that I am advising them so that they spend more money here."*

Satisfaction (or lack thereof) with advice. For customers that had received advice or assistance at cybercafes, about half of them were satisfied while the other half were unsatisfied with the assistance they had received. Those satisfied indicated that their challenges had been resolved while those unsatisfied often pointed to the manager taking longer than expected to assist them which often forced them to spend more money at the cybercafe. Some customers were further unsatisfied because their challenges were not fully resolved.

RQ3 summary. Cybercafe managers offer usability and security advice and guidance to their customers, particularly relating to account and password management as well as account recovery. As customers tend to forget their passwords, most managers encourage them to use passwords that are easy to remember, for example their ID numbers. Some managers even select and manage passwords for their customers. Most customers follow the advice provided as they trust the cybercafe managers and view them as experts.

5.4. RQ4: Top Three Security and Privacy Advice

Important advice for staying safe. When asked for their top three recommendations for staying safe online, both cybercafe managers and customers mostly provided similar responses, with logging out of accounts after using public computers mentioned the most (see Table 3). C20 said that *"when you're using, maybe you want to log into your account and maybe you're not using your phone or your own computer. The best thing is to log out, make sure you have cleared everything that you were doing; maybe on someone else's phone or computer."* The next most common recommendation for staying safe online is avoiding clicking on suspicious links or visiting websites you are unsure of. M13 said they *"avoid clicking websites that are suspicious. Because nowadays, we have so many popups on the websites, people tend to click because those pop ups are offering, like, some ridiculous offers about how you can earn this money. . . "* Participants further mentioned the use of strong or secure passwords as important. M11 pointed to the use of *"passwords that are not phone numbers or ID numbers, use mixed characters including numbers and words"* while C02 mentioned avoiding *"commonly-used passwords."*

Other important recommendations for staying safe online mentioned by several participants include not saving passwords in the browser when using public computers, using a password for accounts, and not sharing passwords. Participants further mentioned not using public Wi-Fi and using firewalls. While some of the advice mentioned by participants including using strong passwords, multi-factor authentication and use of anti-virus software match inquiries from Western contexts [14], [39], we find that most of the recommendations center around shared computers at cybercafes, which are relevant to this demographic. This includes logging out of accounts, not saving passwords on public computers, clearing history, and deleting downloads after using the public computers at cybercafes.

TABLE 3: Cybercafe Managers' and Customers' Top Three Advice for Staying Safe Online.

Code	Freq.	Sample Participant Quote
logout	12	"When you log in to a computer using your account, always log out after you've finished what you're doing in your websites, log out and delete your account." – M09
avoid-links/malicious-sites	11	"I just avoid clicking on links I don't know about; if those links have asked for information about yourself, you just avoid giving." – C02
strong/secure-passwords	10	"Ensure that passwords are symbols, letters and alphabets . . . and numbers. Have a mix of these so that it's not plain and avoid using things like date of birth and pet names." – C08
don't-save-passwords	9	"When you login, for example on Facebook, when the browser asks you that they need to remember your password, always click on, never, never remember the password." – C15
use-a-password	6	"Protecting accounts using passwords majorly." – M06
don't-share-passwords	5	"I don't give out my passwords, I don't share my passwords with people." – C02
avoid-public-wifi	4	"Try as much to avoid public WI-FI, somebody can easily access my work if I use a public WI-FI. So I normally try and use private internet access." – C01
unique-passwords	4	"Using different passwords on different sites." – C21
firewall	3	"Have a firewall." – M01
multifactor-authentication	3	"You should use multiple ways or multiple methods like two-factor authentication." – M03
clear-history	3	"Delete the history of your browsing because at times you might download documents and if you don't delete history, then you will be endangering your information." - C19
being-aware	3	"Being aware of recent CVEs; what happened and what you are supposed to do." – M10
delete-downloads	2	"Make sure that you clear your information when you're using a cyber because . . . someone else will be coming and if you leave information there, they may use it to do something bad." – C11
use-safe-browser	2	"Using a safe browser, I like using Brave because it blocks many pop-ups." – M13
anti-virus	2	"If you're using a laptop, the anti . . . Those software that protect any kind of virus." – C04
avoid/skip-ads	2	"I couldn't advise anyone to ever open the popping advertisements on top of the screen." – C09

Note that each quote can be assigned multiple codes. Only codes mentioned by two or more participants are shown in this table.

Following top three advice. When asked if they follow their top three advice, most customers and managers indicated in the affirmative. M07 said that they *"follow them because I work online and I would really hate to be a victim of something that I was aware was harmful. So I do follow them myself and I'm encouraging others to follow them."* Those that do not follow their advice cited the negative usability impact of following the advice or unavailability of options to do so. C14 said that they *"normally use a difficult password and forget"* while M08 said that they *"try to have many levels of authentication but some sites do not have that."*

Not following top three advice. When asked what would happen if they did not follow their top three advice, most participants indicated that they would be susceptible to attacks including viruses, hacking, malware, ransomware, and impersonation. M13 detailed how they once *"clicked on the wrong link and my computer got infected with a very bad virus. So I guess I have also made mistakes before, but it has taught me more to avoid such things."* Several managers and customers also mentioned unauthorized access, data leaks, loss or manipulation, and financial loss or fraud as possible consequences of not following their top three advice.

RQ4 summary. Cybercafe managers and customers believe that logging out of their accounts when using public computers, avoiding unknown links, strong passwords, and not saving or sharing passwords is the most important advice for staying safe online. This advice is slightly different from what other studies in Western contexts [14], [39] have noted. This is possibly a result of users mostly accessing the Internet through shared computers in this region, unlike in Western contexts, where most people have access to personal computers. This underscores the need to consider specific populations' needs and practices when curating security and privacy advice, as well as technology design in general.

5.5. RQ5: Concerns, Practices, and Behaviors

Security and privacy concerns. When asked for any security or privacy concerns, most cybercafe managers and customers indicated being worried about hacking or online account takeover which can lead to impersonation and loss of money. M13 said: *"Let's say my name is John, John something. I don't want to find another John something online. . . . If someone takes your identity, he can do so much online, tarnish your reputation, name. Yeah, so my greatest worry online I would say is identity and then my financial information, nowadays there is online banking."*

Several participants also indicated being worried about unauthorized account access. C15 stated that *"in the cyber, if you get to maybe login to, to maybe social, social websites, maybe you are going to the cyber just for a hobby or for fun, you login to a social website like Facebook, then you forget to log out of your account and then someone comes in,*

notices that there is an account that has not been logged out. They get to your account and post funny, funny posts, just for fun." Other concerns mentioned included a worry about leaving data in the cybercafe that can subsequently lead to data theft or manipulation. Some customers were worried about accidentally saving their passwords in the cybercafe computers as well as being shoulder-surfed in the cafe.

Concerns about customers. About half of the cybercafe managers indicated being worried about their customers accessing pornography or illegal sites at their cybercafe. M11 said that *"sometimes people may use sites they are not supposed to for example downloading music when we have no license for this, or access pornography."* Some managers were also worried about theft of their equipment as well as scams, frauds, or identity theft targeting their customers. M05 said that sometimes a *"client comes, familiarizes with the stuff. Maybe someone downloaded a CV and left it there. So this client comes, the CV has contacts for the other client and the person says: can we meet somewhere? So this client uses that opportunity to steal from the other person saying: I am an employer, I found a CV, when he's not."*

Cybercafe standard practices. To protect their customers as well as to avoid legal liability, several managers indicated that they log the customer out of logged-on accounts and delete any documents or information left on the computer at the end of a customer's session. Some managers clear downloads because of space constraints while others check browser history to see if the customer accessed anything illegal. Several managers also indicated that they have physical partitions at the cybercafe for customers' privacy, while others block certain websites as well as USB drives to protect their computers from any viruses. Other precautions include having warning signs in the cybercafe to deter people from accessing illegal sites as well as disabling downloads.

Operating system updates. About half of the cybercafe managers regularly or automatically update the cybercafe computers' operating systems to either improve the speed of the computers or access the latest features, but not for security. M04 said that they *"usually update because, before updating the machine, it goes slow. After updating the machine, you see it processes faster."* Those who do not update pointed to their customers being familiar with old operating systems, for example Windows 7, or not being concerned about security. Some managers also indicated that updates often slow down computers, consume a lot of storage or data, and require reboots that are sometimes inconvenient. M14 indicated that they *"chose to stick to Windows 7 to help my customers save time because when I compare Windows 7 with these other Windows, for operating systems, I find that there's a difference. There are some customers who really struggle using Windows 10 and the others, but when it comes to Windows 7, then they're a bit more conversant with it."*

Customer standard practices. An overwhelming majority of the cybercafe customers in our study indicated that they log out of their accounts once they have finished using the computers in the cafe to prevent unauthorized access of their accounts. Two customers, however, indicated that they log out only because the cybercafes they usually visit have explicit instructions or signs requiring them to do so. C12 said that in *"some cybers, when you go in, they have some instructions, they have some instructions when you enter in the cyber. So, after using a computer, you have to sign out."*

Suggestions and additional thoughts. When asked for additional thoughts at the conclusion of the interviews, a few cybercafe managers and customers suggested the need for computer training to further support cybercafe customers. M10 said that *"we need to do a computer literacy program because most of the people, like 70% of the people, they are computer illiterate. So I can recommend that we have a computer literacy program that is voluntary and free so that people can know how things are done on the computer."*

RQ5 summary. Most concerns in the cybercafes center around unauthorized access of accounts that can happen when customers do not or forget to log out of their accounts. Most managers are interested in protecting their customers, and undertake several measures, including logging them out, to further protect them. However, as noted in Section 5.3, some of these measures are often in tension with usability, leading to some managers to encourage their customers to select memorable passwords and sometimes even save them in the cybercafe computers to recall them.

6. Discussion and Conclusion

In this study, we investigate the role of cybercafes in Kenya as well as security and privacy challenges, advice, and behaviors at cybercafes through $n = 36$ semi-structured interviews. We find that cybercafes play an important role in Kenya by enabling many people to access printing, government, and other internet services. At the same time, customers face several challenges at cybercafes, mostly relating to general computer usage, account creation, and password management. Often, customers rely on the cybercafe managers for assistance when navigating these challenges.

In this section, we discuss other themes that emerged from our study alongside their implications.

Role of cybercafes in Kenya. Cybercafes play a crucial role in the developing world as a public location to access printing, government, and other internet tasks. In Kenya, particularly, where the government recently transitioned to an eCitizen [24] portal for most government services, customers rely on cybercafes to access these essential services, as a majority of them do not own personal computers or printers [16]. At the same time, their lack of experience with computers often causes unanticipated challenges. For example, challenges with typing and general usage of computers usually translate to difficulty selecting and remembering passwords for accounts, subsequently leading to users getting locked out of their accounts. This suggests the need for computer

training to improve these users' computer knowledge and skills, as well as a need for security awareness to protect their information. As the Kenyan government is trying to digitize all its services, we believe that it should also lead these training efforts. Such initiatives should focus on the cybercafe managers who can then transfer the knowledge to their customers. Updates to the education curriculum to promote computer skills and security awareness at school could also provide long-term benefits.

Reliance on cybercafe managers. Similar to refugees' reliance on their case managers in the United States [72], cybercafe customers in Kenya significantly rely on managers for assistance setting up and managing their digital accounts. As some of these customers are novices and may have never used computers, they let the managers select and sometimes manage their passwords. Since managers have to assist several customers, they resort to techniques that help them and their customers remember these passwords, including the use of customers' ID numbers or names as passwords, writing down their customers' passwords, or using the same password for all customers. As none of the managers or customers in our study explicitly mentioned using password managers, there is an opportunity for more awareness about how password managers could assist. Phone-based password managers are promising and could be used in generating and recalling strong and unique passwords for these users as a majority of them own mobile phones. However, their device-sharing practices must be appropriately considered, and can be explored further in future research.

Security-usability tradeoff. When asked for their top advice for staying safe online, both cybercafe managers and customers often mentioned strong passwords for accounts. At the same time, most managers select or advise their customers to use passwords they can more easily remember, for example their names, children' names, ID numbers, or some combination of these, instead of choosing a strong, random password. While some managers believe such combinations make these passwords difficult to guess, the fact that the same advice is often provided to multiple customers means that customers could know other customers' passwords if they gained some personal information. Further, mobile money services such as M-Pesa [41], which are widespread in Kenya, require ID numbers of customers for transactions. It is also common for ID numbers to be recorded when visiting offices in Kenya. This means that users' passwords may be inadvertently exposed. One way to minimize such risks is for systems including eCitizen to use passwordless authentication with phone numbers whereby users receive a One Time Password for every login. This way, users would only need their phone numbers to authenticate. SMS-based two-factor authentication could also be used to improve the security of these systems. Another potential workaround is for the managers to create random and unique passwords for their customers and write them down for them to keep. However, any such efforts must encourage the customers to protect their written-down passwords to be effective.

Security and privacy advice in non-Western contexts. One of the goals of our study was to compare security and privacy advice in Kenya to the advice that has been extensively explored in Western contexts [14], [39]. While some of the advice including strong and unique passwords across accounts is considered important in both contexts, we find that the most common advice in Kenya centers around the use of shared or public devices for Internet access. This includes logging out of accounts and not saving passwords in the browser when using public or shared computers or phones. Our work supports the growing body of research [9], [19], [40], [66], [69] that has shown security and privacy to vary in different countries and contexts. Exploring the relevance, efficacy, and perceived actionability of existing security and privacy advice in non-Western contexts (especially for users that rely on public computers) is a promising direction to further support and protect broader populations.

Operating system updates. About half of the cybercafe managers in our study regularly update the cybercafe computers' operating systems, while the other half do not. Those that regularly update do so to improve the performance or speed of the computers as well as to get new features, not because of security. Those that do not update indicated that customers are familiar with old operating systems or they are not concerned about security. Some managers pointed to updates slowing down the computers or consuming a lot of storage, data or time as reasons for not updating, similar to some of the findings of Houmz et al. [38] and Luo and Warford et al. [45]. This suggests an opportunity to communicate to the managers the role of security updates in protecting cybercafe computers' and customers' information. In their study of users' decisions to use or not use a secure lockscreen, Albayram et al. [4] found that that a lack of risk awareness often results in insecure behaviour. Future work can therefore explore strategies to effectively communicate security risks to cybercafe managers and other users in general to encourage more secure behaviour, including regularly updating their devices' operating systems.

Cybercafe risks and concerns. Despite their obvious benefits, cybercafes can also unfortunately enable crime, illegal activities, and Intimate Partner Violence (IPV). While the managers we interviewed all indicated they do not offer services they deem illegal, for example certificate forgery, music downloading, or activities that can enable IPV, like accessing or disabling partners' accounts, it may be the case that some more unscrupulous managers may indeed provide such services if financially motivated. One customer even expressed concern about children getting exposed to pornography at these facilities. While it is difficult to deter all cybercafes from indulging in such activities, it is still worthwile to educate managers about the dangers of these activities. The use of warnings and other notes in the cafe discouraging or prohibiting illegal activities is promising, with some customers in our interviews revealing they follow them. Nevertheless, future work can explore interventions to prevent or limit such activities from happening at cybercafes.

Acknowledgment

We thank Karen Sowon and Animesh Srivastava for their help designing the interviews, and Lucy Simko for sharing with us an interview protocol of a related study. We thank Miles Grant for his assistance with qualitative coding as well as Noel Warford and Harshini Sri Ramulu for participating in our mock interviews. We also thank all the anonymous reviewers for their constructive feedback. Lastly, we are very grateful to all our participants for their time and invaluable insights. This material is based upon work supported by the National Science Foundation under Grant No. 1845300.

References

[1] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. Aunties, Strangers, and the FBI: Online Privacy Concerns and Experiences of Muslim-American Women. In *Proc. SOUPS*, 2022.

[2] CIO Africa. Kenya's E-citizen portal hits 1.23 million. https://cioafrica.co/kenyas-e-citizen-portal-hits-1-23-million/, Feb 2016.

[3] Jenny C. Aker and Isaac M. Mbiti. Mobile Phones and Economic Development in Africa. *Journal of Economic Perspectives*, 24(3):207–32, 2010.

[4] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. "...better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In *Proc. SOUPS*, 2017.

[5] Thomas Alsop. Share of households with a computer in Africa 2005-2019. https://www.statista.com/statistics/748549/africa-households-with-computer/#statisticContainer, Nov 2021.

[6] Kenya Revenue Authority. https://itax.kra.go.ke/KRA-Portal/, 2022.

[7] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M. Redmiles. "Disadvantaged in the American-Dominated Internet": Sex, Work, and Technology. In *Proc. CHI*, 2021.

[8] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. "So-Called Privacy Breeds Evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW3), 2021.

[9] Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20(5):313–324, 2004.

[10] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. "Adulthood is trying each of the same six passwords that you use for everything": The Scarcity and Ambiguity of Security Advice on Social Media. In *Proc. CSCW*, 2022.

[11] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M Redmiles, and Angelika Strohmayer. Ethical Practices for Security Research with At-Risk Populations. In *Proc. IEEE EuroS&PW*, 2022.

[12] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *Proc. CHI*, 2021.

[13] Rex Bringula, Jenmart Bonifacio, Ana Natanauan, Mikael Manuel, and Katrina Panganiban. Pattern of internet usage in cyber cafés in Manila: An exploratory study. *International Journal of Cyber Society and Education*, 5(2):152–164, 2012.

[14] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Proc. SOUPS*, 2019.

[15] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The Spyware Used in Intimate Partner Violence. In *Proc. IEEE S&P*, 2018.

[16] Africa Check. What share of households in Kenya own a computer? https://africacheck.org/infofinder/explore-facts/what-share-households-kenya-own-computer, May 2020.

[17] Christine Chen, Nicola Dell, and Franziska Roesner. Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors. In *Proc. USENIX Security*, 2019.

[18] Janet X Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *Proc. CHI*, 2022.

[19] Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. A multinational study on online privacy: global concerns and local responses. *New Media & Society*, 11(3):395–416, 2009.

[20] Deborah Cohen and Benjamin Crabtree. Qualitative research guidelines project, Jul 2006. http://www.qualres.org/.

[21] CyberCafePro. CyberCafePro is Cyber Cafe Management Software. https://cybercafepro.com/, 2022.

[22] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas. Defensive Technology Use by Political Activists During the Sudanese Revolution. In *Proc. IEEE S&P*, 2021.

[23] Samuel Dooley, Michael Rosenberg, Elliott Sloate, Sungbok Shin, and Michelle Mazurek. Libraries' Approaches to the Security of Public Computers. In *Proc. WIPS*, 2020.

[24] eCitizen. A portal that offers access to information and services provided by the Kenyan government. https://www.ecitizen.go.ke/ecitizen-services.html, 2015.

[25] Michael Fagan and Mohammad Maifi Hasan Khan. Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. In *Proc. SOUPS*, 2016.

[26] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[27] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proc. CHI*, 2018.

[28] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW), 2017.

[29] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Proc. SOUPS*, 2019.

[30] Benjamin Gardner. Incentivised snowballing. *The Psychologist*, 22(9):768–769, 2009.

[31] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *Proc. USENIX Security*, 2022.

[32] Samuel Gitta and J Robert Ikoja-Odongo. The impact of cybercafés on information services in Uganda. *First Monday*, 2003.

[33] Ricardo Gomez and Luis Fernando Baron-Porras. Does public access computing really contribute to community development? Lessons from libraries, telecentres and cybercafés in Colombia. *The Electronic Journal of Information Systems in Developing Countries*, 49(1):1–11, 2011.

[34] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *Proc. CHI*, 2018.

[35] Vaughn Hamilton, Hanna Barakat, and Elissa M Redmiles. Risk, Resilience and Reward: Impacts of Shifting to Digital Sex Work. *arXiv*, 2022.

[36] Anikar Michael Haseloff. Cybercafés and their potential as community development tools in India. *The Journal of Community Informatics*, 1(3), 2005.

[37] Jay Hoffmann. The window at the cafe. https://thehistoryoftheweb.com/the-window-at-the-cafe/, Jul 2017.

[38] Abdellah Houmz, Mohamed Salim Mezzene, Asmaa Tellabt, Ghita Mezzour, and Mohammed El Koutbi. Field study of cybercafé usage & security in Morocco. In *Proc. IEEE ACOSIS*, 2016.

[39] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Proc. SOUPS*, 2015.

[40] Margaret C. Jack, Pang Sovannaroth, and Nicola Dell. "Privacy is Not a Concept, but a Way of Dealing with Life": Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[41] William Jack and Tavneet Suri. Mobile money: The economics of M-PESA. Technical report, National Bureau of Economic Research, 2011.

[42] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. In *Proc. CHI*, 2017.

[43] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. Co-Designing Online Privacy-Related Games and Stories with Children. In *Proc. CHI*, 2018.

[44] Calvin Liang. Reflexivity, positionality, and disclosure in HCI, Sep 2021.

[45] Alan F. Luo, Noel Warford, Samuel Dooley, Rachel Greenstadt, Michelle L. Mazurek, and Nora McDonald. How Library IT Staff Navigate Privacy and Security Challenges and Responsibilities. In *Proc. USENIX Security*, 2023.

[46] Allison McDonald, Catherine Barwulor, Michelle L. Mazurek, Florian Schaub, and Elissa M. Redmiles. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *Proc. USENIX Security*, 2021.

[47] Nora McDonald, Rachel Greenstadt, and Andrea Forte. Intersectional Thinking about PETs: A Study of Library Privacy. In *Proc. PETS*, 2023.

[48] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[49] Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the Computer Security Practices and Needs of Journalists. In *Proc. USENIX Security*, 2015.

[50] Tamir Mendel. Social Help: Developing Methods to Support Older Adults in Mobile Privacy and Security. In *Proc. UbiComp/ISWC*, 2019.

[51] Helena M. Mentis, Galina Madjaroff, and Aaron K. Massey. Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment. In *Proc. CHI*, 2019.

[52] Imani Munyaka, Eszter Hargittai, and Elissa Redmiles. The Misinformation Paradox: Older Adults are Cynical about News Media, but Engage with It Anyway. *Journal of Online Trust and Safety*, 1(4), 2022.

[53] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. In *Proc. IEEE S&P*, 2022.

[54] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Neha Kumar. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. In *Proc. CHI*, 2021.

[55] NACOSTI. National Commission for Science, Technology and Innovation. https://www.nacosti.go.ke/, Oct 2022.

[56] Nathan Oyori Ogechi. On language rights in Kenya. *Nordic Journal of African Studies*, 12(3):19–19, 2003.

[57] Kentrell Owens, Anita Alem, Franziska Roesner, and Tadayoshi Kohno. Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives. In *Proc. USENIX Security*, 2022.

[58] Kentrell Owens, Camille Cobb, and Lorrie Cranor. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *Proc. CHI*, 2021.

[59] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. "Woe is me:" Examining Older Adults' Perceptions of Privacy. In *Proc. CHI EA*, 2019.

[60] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. "Warn Them" or "Just Block Them"?: Comparing Privacy Concerns of Older and Working Age Adults. In *Proc. PETS*, 2021.

[61] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why Older Adults (Don't) Use Password Managers. In *Proc. USENIX Security*, 2021.

[62] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proc. CCS*, 2016.

[63] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *Proc. IEEE S&P*, 2016.

[64] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *Proc. USENIX Security*, 2020.

[65] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security & Privacy*, 15(5):55–64, 2017.

[66] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp. In *Proc. USENIX Security*, 2020.

[67] Kathryn Roulston. *Analysing interviews*. The SAGE handbook of qualitative data analysis, 2014.

[68] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proc. SOUPS*, 2018.

[69] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proc. CHI*, 2017.

[70] Juliane Schmüser, Noah Wöhler, Harshini Sri Ramulu, Christian Stransky, Dominik Wermke, Sascha Fahl, and Yasemin Acar. "Please help share!": Security and Privacy Advice on Twitter during the 2022 Russian Invasion of Ukraine. *arXiv*, 2022.

[71] Emrys Shoemaker, Gudrun Svava Kristinsdottir, Tanuj Ahuja, Dina Baslan, Bryan Pon, Paul Currion, Pius Gumisizira, and Nicola Dell. Identity at the Margins: Examining Refugee Experiences with Digital Identity Systems in Lebanon, Jordan, and Uganda. In *Proc. COMPASS*, 2019.

[72] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer Security and Privacy for Refugees in the United States. In *Proc. IEEE S&P*, 2018.

[73] Techopedia. What is a Cybercafe? - definition from Techopedia. https://www.techopedia.com/definition/6701/cybercafe, Apr 2016.

[74] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. In *Proc. USENIX Security*, 2020.

[75] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. Care Infrastructures for Digital Security in Intimate Partner Violence. In *Proc. CHI*, 2022.

[76] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. SoK: A Framework for Unifying At-Risk User Research. In *Proc. IEEE S&P*, 2022.

[77] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships. In *Proc. SOUPS*, 2022.

[78] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *Proc. USENIX Security*, 2021.

Appendix

1. Interview Script - Cybercafe Managers

General Questions

1) Can you please explain to me whether you own this cybercafe?
   a) Yes: Why did you establish it?
   b) No: Why did you choose to work here?
2) How long have you operated, worked at, or owned this cybercafe?
3) Please describe the equipment or computers in the cybercafe.
   a) How many computers? How many printers? What software?
   b) How frequently is the software updated? Why or why not?
4) Do you provide any other services other than cybercafe services?
5) How many customers do you have in a typical week?
6) What are the characteristics of your customers?
   a) Dominant age group? Gender? Socio-economic background?
7) Can you please share some of the challenges you have faced operating this cybercafe, if there are any?

Cybercafe Services

8) Based on your observations, what websites or services do your customers most typically use or visit at your cybercafe?
9) Are there services that customers ask for that you cannot provide? Please explain why you do or do not provide that service.
10) How often do you have first-time customers at your cybercafe?
    a) What services are these customers usually seeking?

User Challenges

11) When a customer has a technical challenge, what are some of these challenges? Can you provide any examples?
    a) Examples might include setting up an account or even actual tasks. Please elaborate.
12) To follow up, do these customers ask you for advice or help?
    a) What kind of advice or help do you provide?
    b) Are the issues resolved after you help? If not, why not?

General Advice

13) When you are asked for advice, what information or expertise do you rely on to help?
    a) Examples include your personal experience. Please elaborate.
14) Do you vary your advice or guidance for the customers?
    a) How might advice differ from an inexperienced customer compared to a more experienced customer?
    b) Do you have examples of this occurring? Please elaborate.
15) When you provide advice or guidance, do the customers follow it? Why or why not?
16) Has there ever been a situation where you were asked for help or advice where you did not know the right answer?
    a) If so, what was the question? And what answer did you provide?
    b) If not, what was the most challenging question received and what help did you provide?

Security and Privacy Advice

I am now going to ask you general questions about security and privacy. There are no wrong answers, I am simply interested in your thoughts.

17) In your opinion, what are the top three things you can do or someone else can do to stay safe online?
    a) For each, ask them to elaborate.
    b) For each, ask them if they follow this advice.
    c) For each, ask them if they have offered this advice to any customers, and elaborate on that situation.
    d) For each, what would happen if you don't follow this advice.
18) What is your greatest concern online with respect to your personal security or privacy? Follow up with elaboration.

Users' Security and Privacy

19) Are there any standard practices at the cybercafe regarding the security and privacy of your customers?
    a) If not, explain more about what you do.
    b) If so, [for each] provide some detail on that policy and practice and why you do it.
20) Do you have any concerns regarding how customers might use the computers? Please elaborate.
    a) Yes: Do you take any precautions to prevent those actions?
    b) No: Why are you not concerned?
21) Do you have any general security practices for updating and maintaining the computers? Please elaborate.
22) Is there anything you do after a user has finished using a computer?
    a) Do you reset the session? Why or why not.
    b) Do you log them out, or ask them to log out? Why or why not.

Miscellaneous

23) Is there anything else you would like to share about your experience owning or operating this cybercafe?
24) I am also planning to speak to cybercafe customers about their experiences. Is there anything I should know or advice you can provide for those conversations?

Demographics

Finally I am going to ask you some demographic questions. If you prefer not to answer any of them, please let me know.

25) Do you own a smartphone?
    a) Is it a work or personal phone? What is the phone type and model?
26) Do you own a computer or laptop?
    a) Yes: Is it a personal or work computer?
27) What is your age?
28) What is your gender?
29) What is the highest level of education you have attained?
30) Do you have a background in IT or computers as part of your work experience or school beyond working or owning the cybercafe?
31) Do you have any feedback or questions about this interview?

2. Interview Script - Cybercafe Customers

General Questions

1) Please tell me a little bit about yourself and what you do.
2) Why do use cybercafes?
   a) What is a typical thing you do at the cybercafe? Why do you do this at the cybercafe rather elsewhere?
3) What do you like the most about cybercafes and why?
4) What do you dislike the most about cybercafes and why?

Cybercafe Usage

5) How often do you use or go to cybercafes?
   a) In a month? In a week? In a day?
   b) First time users: Do you see yourself coming to the cybercafe again? How often?
6) How much time (in hours) do you typically spend at the cybercafe when you go there?
   a) Can you provide an example of a task that takes more time than others when you come to the cybercafe?
7) What do you normally consider when choosing a cybercafe to go to?
   a) Examples include the location of the cyber etc.

User Challenges

8) Are there any technical challenges you have faced when using cybercafes? Examples include using the computer or printing a document.
   If user has faced a challenge...
   a) How did you (or do you) resolve these challenges?
   b) Did you ask for help? From whom and why?
   c) What help or advice was provided?
   d) Did you follow this advice/help? Why or why not?
   e) Are you satisfied with the help you received? Why or why not?
      i) If not, is there anything else you did to reach satisfaction?

   If user has not faced any challenge...
   a) Why do you think you have not faced any challenges?
   b) Are the tasks you do there easy or difficult? Please elaborate.
9) Have you received any assistance or guidance relating to security and privacy? Examples include selecting your password. Please elaborate.
   If the user has received assistance...
   a) What advice or guidance was provided?
   b) Who provided this advice?
   c) Did you or do you follow the advice? Why or why not?
   d) Has this advice influenced your behavior online? e.g how you create other passwords?

   If the user has not received any assistance...
   a) Do you have any sources of advice or guidance relating to security and privacy for example how you select your passwords?
      i) Examples include friends etc. Please elaborate.
   b) How did you learn about these sources?
   c) Why do you follow the advice?
   d) Has this advice influenced your behavior online e.g how you create other passwords?
10) Take me through what you do on websites or your accounts when you're done using the cybercafe.
   a) Do you sign out of your accounts? Why or why not?

Security and Privacy Advice

I am now going to ask you general questions about security and privacy. There are no wrong answers, I am simply interested in your thoughts.

11) In your opinion, what are the top three things you can do or someone else can do to stay safe online?
   a) For each, ask them to elaborate.
   b) For each, ask them if they follow this advice.
   c) For each, what would happen if you don't follow this advice.
12) What is your greatest concern online with respect to your personal security or privacy? Follow up with elaboration.

Device Questions

13) What type of phone do you use? (Is it a feature or a smartphone?)
   a) If smartphone: Do you access the internet on your device? What are some of the websites or services you use?
14) Do you share your phone with others?
   a) Yes: With whom and why?
   b) No: Why not?
15) Do you have any concerns with access to your phone?
   a) Concerned: What concerns? What do you do to prevent this?
   a) Not concerned: Why are you not concerned?
16) Do you use any authentication mechanism on your device? Examples include a password, pattern or PIN. Why or why not?
   a) What is protected by the authentication? (Simcard? Phone?)
   b) What strategies did you use to create this authentication scheme?
   c) How did you learn about this? Did you get any advice?

Miscellaneous

17) Is there anything else you would like to share about cybercafes?

Demographics

Finally I am going to ask you some demographic questions. If you prefer not to answer any of them, please let me know.

18) Do you own a computer or laptop?
19) What is your age?
20) What is your gender?
21) Are you employed?
22) What is the highest level of education you have attained?
23) Do you have a background in IT or computers as part of your work experience or school? If so, please explain.
24) Do you have any feedback or questions about this interview?

3. Qualitative Codes

- **cybercafe-establishment/work-reason (17)**
  business-opportunity (10), computer-interest (4), relevant-skills (3)
- **manager-cybercafe-experience (14)**
  1-5-years (9), less-than-a-year (3), 6-10-years (1), over-10-years (1)
- **cybercafe-number-of-computers (14)**
  1-5-computers (8), 6-10-computers (5), over-10-computers (1)
- **cybercafe-number-of-printers (14)**
  2-printers (8), 1-printer (3), 3-printers (2), 4-printers (1)
- **OS-type/software (16)**
  windows (14), cybercafe-pro (2)
- **update-OS (19)**
  yes (11): *automatic (5), improve-speed/performance (3), get-new-features (1), follow-latest-trends (1)*
  no (8): *users-familiar-with-old-OS (2), not-concerned-about-security (2), updates-slow-machines (1), updates-consume-space (1), inconveniencing-reboots (1), updates-consume-data (1)*
- **cybercafe-customer-positives (44)**
  equipment-availability (12), faster-internet (11), affordability (5), availability-of-assistance (5), privacy (4), stable-electricity (2), meet-friends/social-place (2), conveniently-located (2), ample-space (1)
- **cybercafe-customer-negatives (11)**
  unhelpful/unfriendly-managers (3), crowded/have-queues (3), noisy-cybers (3), many-advertisements (1), expensive (1)
- **factors-when-choosing-cybercafe (51)**
  conducive-environment (9), internet-speed (7), manager-friendliness/assistance (7), cost/affordability (7), location/proximity (5), state/number/speed-of-equipment (4), space-availability (4), electricity-stability (3), safety (3), privacy (2)
- **cybercafe-challenges (55)**
  slow-internet (20), electricity-outage (9), old/faulty-equipment (6), payment-issues-with-customers (5), slow-hanging-machines (4), government/law-enforcement-harassment (4), expensive-equipment (3), few-customers (2), drunk/rowdy-customers (2)
- **cybercafe-common-services (132)**
  printing (18), eCitizen (18), job-applications (13), email (10), photocopy (9), assignments/school-projects (9), document-typing/editing (8), school/HELB/scholarship-applications (7), social-media (7), work/online-work (5), KRA/taxes (5), movie-streaming/download (4), gambling (4), lamination (4), computer-training (3), scanning (3), search/Google (3), visa-applications (2), graphic-design (2)
- **other-services-offered-at-cybercafes (16)**
  sell-computers/phones (5), gaming (3), banking-services (2), mobile-money (2), repairs (2), computer-networking (1), passport-photos (1)
- **services-not-offered (15)**
  forgery (5): *have-intergrity (2), fear-consequences (2)*
  web-design (3): *lack-time/skills (3)*
  music-download (2): *illegal/not-licensed (2)*
  rooting/phone-formatting (1): *lack-time/skills (1)*
  photography (1): *different-business (1)*
  bulk-printing (1): *lack-equipment (1)*
  passport-photo-printing (1): *lack-equipment (1)*
  lamination/binding (1): *lack-equipment (1)*

- **customer-common-challenges (77)**
  computer-usage (30): *challenges-printing/binding/scanning (6), using-programs/apps (6), navigating-websites/computers (5), struggle-typing (2), difficulty-opening-flashdisks (1)*
  difficulty-accessing/recovering-account (26): *forgot-password (12), forgot-email/lost-phone (9), bad-UI/UX (2), website-downtime (1)*
  account-setup (7): *difficulty-complying-with-password-requirements (2), users-don't-care-about-password (1), don't-know-password-to-use (1), don't-know-what-to-do (1)*
  information-retrieval (2): *website-in-foreign-language (1) customers-fear-computers (1), customers-sent-but-forgot-details (1)*
  not-faced-challenges (10) *specific-tasks/cybercafes (4), experienced-with-computers (3), tasks-easy (2), availability-of-assistance (1)*
- **customers-ask-for-help (23)**
- **customers-satisfied-with-help (14)**
  yes (8): *issue-resolved (5), answers-satisfactory (1), not-compromised (1)*
  no (6): *took-long (2), challenge-unresolved (2), guidance-not-provided (1), spent-more-money (1)*
- **advice/support-offered-to-customers (69)**
  password-and-account-management (38): use-memorable-password (13): *combination-of-ID/name/birthday (5), use-ID-number (4), use-birthday (1), use-phone-number (1)*
  account-management-for-customers (10): *save/manage-user-password (3), select-password-for-customer (3), standard-email-account-for-customers (1), avoid-selecting-password-for-customer (1), use-phone-number-of-manager (1)*
  use-strong-password (4): *mixed-characters (2) don't-save-password-in-browser (3) avoid-common-passwords (2) password-protect-files (1) use-secret-password (1) frequently-change-password (1) save-password-in-browser (1)*
  do-task-for-customer (7): *tasks-technical (1) teach/guide-customers (7), account-recovery (5), logout (3), use-phone-number-for-accounts (2), update-OS (1), don't-save-files-on-desktop (1), avoid-clicking-on-links (1), use-another-computer (1)*
  no-security-advice-offered (1): *manager-interested-in-money (1)*
  don't-interrupt/help-customers (1): *make-more-money (1)*
- **unresolved/difficult-challenges (11)**
  account-recovery (8): *forgot-email/lost-phone (8) edit-pdfs (1), edit-photos (1), disabling-forgotten-password (1)*
- **question-manager-has-no-answer (11)**
  research (4), say-don't-know (3), refer-customer-to-other-cybers (3)
- **sources-of-advice (62)**
  internet (27), personal-experience (12), managers/other-managers (8), friends/family (6), customer-service (1), tv-shows (1)
- **customers-follow-advice (45)**
  yes (33): *works/good-advice (10), protect-themselves/info (7), trust-manager (4), view-manager-as-expert/knowledgeable (3), limited-time/task-urgent (3), manager-friendly/engaging (2), heard-similar-advice (1), interested-in-computers (1), solve-issues-in-future (1)*
  no (12): *contradictory-beliefs (2), elderly (2), think-manager-lying/skeptical (2), too-technical (1), don't-have-time (1), will-make-them-spend-more-money (1), been-advised-differently (1), many-emails-criminal (1), task-not-urgent (1)*
- **top-three-advice-to-stay-safe (108)**
  logout (12), avoid-links/malicious-sites (11), strong/secure-passwords (10), don't-save-passwords (9), use-a-password (6), don't-share-passwords (5), avoid-public-wifi (4), unique-passwords (4), firewall (3), multi-factor-authentication (3), clear-history (3), being-aware (3), delete-downloads (2), use-safe-browser (2), anti-virus (2), avoid/skip-links (2), close-websites (1), clear-cache (1), use-phone-number-for-recovery (1), block/avoid-unsafe-sites (1), faster-internet (1), use-cctv (1), avoid-unknown-downloads (1), incognito-mode (1), don't-sync-with-browser (1), block-cookies (1), update-system (1), prevent-idleness (1), browser-in-safe-environment (1), follower-cybercafe-guidelines (1), avoid-unsafe-cybercafes (1), avoid-common-passwords (1), use-data-saver (1), keep-username-secret (1), don't-save-to-desktop (1), stick-to-first-google-result (1), disable-notifications (1), frequently-change-password (1), limit-info-shared-online (1), limit-online-interactions (1), computer-knowledge (1), stick-to-one-cybercafe (1)
- **follow-top-three-advice (38)**
  yes (29): *stay-safe (4)*
  sometimes/some (9): *usability-vs-security (3), not-offered/required (2), time-consuming (1), enough-data (1), forget (1)*
- **top-three-advice-offered-to-customers (25)**
  logout (5), don't-save-passwords (3), avoid-links/malicious-sites (2), strong-passwords (2), being-aware (2), 2FA (1), use-a-password (1), incognito-mode (1), delete-files/downloads (1), don't-sync-with-browser (1), avoid-public-wifi (1), block-cookies (1), update-system (1), firewall (1), use-safe-browser (1)
- **not-following-top-three-advice (83)**
  susceptible-to-attacks/compromises (25): *virus (7), hacking (4), impersonation (2), malware (1), ransomware (1) unauthorized-access (16), data-leaks/loss/manipulation (11), financial-loss/fraud (8), monitoring/surveillance (5), loss-of-account-access (2), theft-of-equipment (2), identity-theft (2), slow-internet (2), miss-features (2), unnecessary-pop-ups/ads (1), access-insecure-sites (1), don't-know (1), bans-from-cyber (1), device-failure (1), more-data (1), waste-time (1), get-distracted (1)*
- **security/privacy-concerns (86)**
  concerns-about/for-customers (30): *access-porn/illegal-sites (7), scams/fraud (5), theft-of-equipment (4), download-prohibited-equipment (4), identity-theft(3), easy-passwords (2), physical-damage (2), malicious-activities (2), install/tamper-with-OS (1)*
  hacking/account-take-over (15): *money-loss (6), impersonation (4)*
  unauthorized-access-of-account/info (14): *cyber-bullying (2), disable-partner's-accounts (1), blackmail (1) leaving-data-in-cybercafe (9), data-theft/manipulation (5), lack-of-privacy (3), shoulder-surfing (2), spyware/tracking (2), saving-passwords-in-cybers (2), over-sharing-info (2), forgery (1)*
  no-concerns (1): *used-to-the-internet (1)*
- **security/privacy-standard-practices (78)**
  at-end-of-user-session (30)
  logout-customer (13): *prevent-malicious-use (5), prevent-unauthorized-access (2), increase-trust (1)*
  clear-downloads (9): *prevent-malicious-use (2), space-constraints (2), protect-private-info (2), legal-liability (1) reset/end-user-session (4), sanitize-equipment (1), check-history/downloads (1), sleep-computer (1), close-sites (1)*
  other-standard-practices (39): *partitions-for-privacy (5), block-sites (5), anti-virus (4), block-flash/USB (3), warning/notes (2), dusting (2), disabled-illegal-downloads (2), inspect-files/block-software-installation (2), prevent-idleness (2), monitor-kids (2), safely-store-customer-docs (1), lock-doors (1), chain-equipment (1), firewall (1), format-computers (1), strong-passwords-for-cyber-computers (1), outsource-servicing (1), delete-saved-passwords (1), use-vpn (1), delete-saved-passwords/history (1)*
- **customer-end-of-session-activities (35)**
  logout (20): *prevent-unauthorized-access (14), cyber-directives (2) clear-history (5), clear-downloads (4), don't-save-password (2), close-websites (2), shutdown (1)*
- **customer-and-manager-suggestions (4)**
  need-for-computer-education (4)