Exploring Internet Security Perceptions and Practices in Urban Ghana

Jay Chen
NYU Abu Dhabi
PO Box 129188
Abu Dhabi, UAE
jchen@cs.nyu.edu

Michael Paik
NYU Abu Dhabi
PO Box 129188
Abu Dhabi, UAE
mpaik@cs.nyu.edu

Kelly McCabe
NYU Abu Dhabi
PO Box 129188
Abu Dhabi, UAE
kellymccabe@nyu.edu

ABSTRACT

Security is predicated, in part, upon the clear understanding of threats and the use of strategies to mitigate these threats. Internet landscapes and the use of the Internet in developing countries are vastly different compared to those in rich countries where technology is more pervasive. In this work, we explore the use of Internet technology throughout urban and peri-urban Ghana and examine attitudes toward security to gauge the extent to which this new population of technology users may be vulnerable to attacks. We find that, like in North America and Europe, the prevalent mental threat model indicates a lack of understanding of how Internet technologies operate. As a result, people rely heavily upon passwords for security online and those who augment their security do so with a variety of ad hoc practices learned by word of mouth. We relate and contrast our findings to previous works and make several recommendations for improving security in these contexts.

Keywords

ICTD; Security; Passwords; Facebook; Google; WhatsApp; Social Networks; Ghana

Categories and Subject Descriptors

H.5.m. [**Information Interfaces and Presentation (e.g. HCI)**]: Miscellaneous

1. INTRODUCTION

Users in the developing world face a significantly different Internet landscape than users in rich countries. Connectivity can be poor or absent, understanding of how technologies work can be *ad hoc* without any systematization due to lack of exposure, and threat models can be both different and poorly understood. Relative to rich countries, developing countries have may have substantially less training and experience with Internet technologies [18]. Internet penetration and therefore use are on the rise in the developing world, and in Ghana in particular [13] and it is possible that the uptake of Internet technologies will soon outgrow commonly held security attitudes and commonly practiced security measures.

Networked security has historically been an "arms race" between intruders becoming more sophisticated and security experts rushing to defend against the latest exploits. The battleground has thusfar mostly been isolated to rich countries and large corporations, but as the GDP of countries like Ghana increases [5], these countries become more attractive targets. Furthermore, because the threats can be very advanced compared to the local experience in developing countries, these populations may be especially vulnerable to attacks. This scenario is especially worrying because for many developing countries networked infrastructures are being increasingly relied upon for critical services such as mobile banking, e-health, and e-government [45, 54].

In order to prevent such worst-case scenarios, we need to develop better technologies and improve awareness. Before this, we should understand people's existing perceptions of technology, people's mental models of networked security, and how they defend against threats. To understand the current security environment, we conducted a study to understand the specific use cases and the rationale that people in Ghana rely on to make decisions about their security practices. We conducted surveys and interviews of 193 respondents across 8 regions in Ghana focused on capturing users' perceptions, practices, and experiences. Our contribution is to provide information about the use of the Internet by urban Ghanaians and their perceptions of and measures for maintaining Internet security.

Wash [53] recently studied mental models of home computer security in an attempt to understand how home users make security decisions. Here, our emphasis is not to build distinct categorizations, but instead to gather salient features from asking two basic research questions: 1) Perception of threats: How do Ghanaian Internet users perceive security threats online and how confident are they in their ability to protect themselves? 2) Security measures: What measures do Ghanaian Internet users employ to protect themselves from online threats?

We find that confidence with Internet technologies is relatively high, particularly for mobile phones. Unfortunately, we also find that certain security behaviors are quite lax, and are often based on misconceptions or mischaracterizations of how technologies work. In particular we discovered that terminology regarding threats were often conflated and that the use of passwords is generally seen as an all-encompassing panacea. As a result, all manner of private information is held behind a security model based solely upon passwords. We further find that users are typically only concerned with immediate, local, physical threats in the form of people who may come to the terminal that they had been using and try to extract information from it; threats from the network side, whether from malicious sites posing as innocuous ones or between users and the

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9.11, 2014, Menlo Park, CA.

sites they are using, were not part of users' mental threat model. While these results are troubling, the low incidence of local experience with hacking suggests that this mental model and corresponding security measures taken may be entirely rational.

In the remainder of the paper, we first discuss related work in technology use in developing countries, conventional security perceptions and models as observed in the U.S., and the relevant security countermeasures. We then detail the methodology of our study and our findings. From these findings, we propose several ideas for potential mitigations, suggest ways to educate users, and enumerate avenues for future research.

2. BACKGROUND AND RELATED WORK

To lay the groundwork for our research we discuss some related work and motivating reasons for studying networked security in a developing country like Ghana.

2.1 Understanding Internet Security

Managing computer security is a challenging task and has been studied extensively in the past in conventional contexts such as the home, workplace, and public areas [23, 30, 36, 53]. Dourish's work exploring user attitudes toward computer security in developed countries have revealed that people generally perceive security as frustrating barriers to productivity and ultimately futile [23]. Dourish and Grinter found that users typically delegate security to the technology itself, other individuals, entities, or organizations [23, 30]. Herley argues that users' rejection of the security advice they receive is entirely rational from an economic perspective [31].

Research from e.g. Lindgaard *et al.* [39] and Cyr *et al.* [22] clearly demonstrates that the trustworthiness of a website is dependent, at least in some ways and to some degree, on the way it is presented to the user and the user's perception of its quality. People have been designing webpages with this in mind for at least 15 years, (e.g. Kim and Moon [35]). Research by Everard *et al.* [26] also shows that site presentation flaws can also affect trustworthiness. This phenomenon has also been studied and modeled across cultures by e.g. Cyr *et al.* [21, 22], though cultural impact is less well understood in the developing world. Jakobsson *et al.* find that trustworthiness often relies on cues *not* designed as security features [33].

The perception of threats is a complex problem, as shown by a survey of this research space. Psychological research (e.g. [28]) illuminates this question somewhat, showing that people learn about threats if the perception of the threat is perceptually correlated to confirmatory information, but it is less clear how physical disconnectedness and mental world models correlate with this perception. Recent work by Wash and Rader show the mental models non-expert computer users rely on to make security decisions [46, 53]. They find that much of the knowledge of non-expert computer users is gleaned from stories that act as informal lessons about security. In developing countries because anti-virus software is relatively expensive and formal computer training is less available these perceptions and behaviors may be more dependent upon these informally learned strategies.

2.2 Internet Landscape in Ghana

Prior work in Ghana by Burrell focuses for the most part on computer use in Internet cafes [19, 20]. Burrell found widespread use of Internet (in Accra) and prevalence of social networking and chat services (as well as voice calls) to reach out to foreign and domestic contacts [27]. Online social network use and chatting are widespread across Africa and developing countries elsewhere. Research by Wyche *et al.* [54] has extensively explored the use of social networks in Nairobi, Kenya. Wyche finds that the users she studies in a Nairobi slum use Facebook in myriad relatively sophisticated ways including the creation of fan pages to promote businesses, sharing film, photos, and audio, actively soliciting friends for work, and the like [54, 55]. In our user group, casual chat with friends was the primary and many times only use people had for Facebook, and the uptake of WhatsApp (which essentially provides only social chat functionality) is consistent with this.

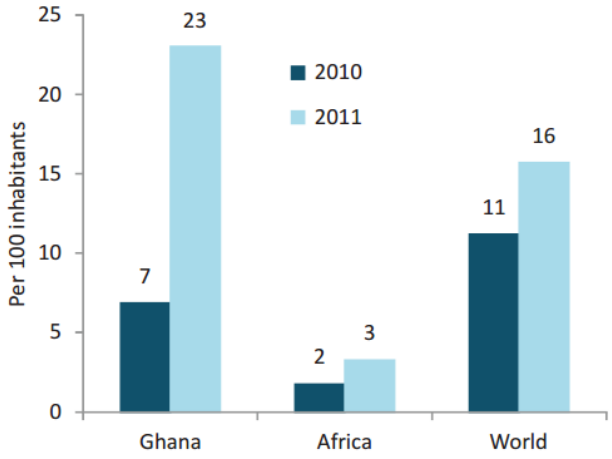

Figure 1: Active mobile-broadband subscriptions per 100 inhabitants, 2010-2011, Ghana in comparison with regional and world average. From [13].

We found that the mobile Internet penetration rate was significantly higher than numbers reported in 2012, in line with strong year-over-year growth. Figure 1 shows data from the International Telecommunications Union indicating that Ghana saw approximately 23% mobile broadband penetration in 2011; in our sample from Ghana the penetration rate was well over 50%, with iPhones, Android and Windows Mobile phones, and data-enabled feature phones all represented. All of the respondents were encountered in urban or peri-urban environments, so this number likely trends high since mobile data coverage and, therefore, penetration drops off precipitously in rural areas. This does, however, illustrate the dramatic progress in mobile data uptake in Ghanaian urban areas and the impending need for usable security tools.

2.3 Internet Security in Developing Countries

Specific to security in developing countries, Ben-David *et al.* have found that technology users face a complex set of security concerns that are deeply tied to a range of contextual factors that make importing security solutions from industrialized countries inadequate [16]. The specific factors that make the problem especially challenging in developing regions include: poor security hygiene due to scarce bandwidth and frequent network failures [44, 54], unique usage patterns (e.g. reliance on non-standardized protocols for mobile banking [45], and shared use of PCs [18]), software piracy [15, 34], and novice users [47]. In terms of security solutions, however, only a few security mechanisms have been designed for developing region contexts [43, 45].

2.4 Passwords and Other Security Mechanisms

Passwords and studies of passwords have been around nearly as long as computer accounts have, as shown by Morris and Thomp-

son's 1979 paper [41]. Passwords can be weak due to human factors, but there is no clear evidence about how stronger passwords actually help [29]. It has been well demonstrated that people do not like to change their passwords very often [32], despite the potential risk passwords weakening over time in the face of increased attacker sophistication and of accidental password exposure. Password strength meters are generally ineffective as people ignore them and changing this behavior is difficult [25, 31, 52]; some sites (e.g. Microsoft accounts) have found it very effective to simply ban popular passwords [7]. In a study by Kuo *et al.* in which users were instructed to use mnemonics, the great majority of passwords in the study generated using mnemonics could actually not be guessed [38]. It is unclear whether users who have had less exposure to hacking choose passwords that are less resistant to attack and whether they should be inculcated with password 'best practices'.

Of additional concern for our userbase, users have been shown by Sun *et al.* to be unable to distinguish real and fake Google login forms even when prompted [50], making the use of passwords potentially less secure. Forcing users to follow best practices is an option, and generally people find it irksome, but feel safer [48]. However, forcing onerous security upon users has been demonstrated to cause them to find ways to circumvent that security [42]. Furthermore, in contexts where hacking is rare, it is especially unclear whether following additional security precautions is actually a rational decision when even in developed countries following best practices may not be a rational decision [31]. Two-factor authentication as recently implemented by Facebook, Google, and Yahoo [3, 6, 12] may be less useful for Ghanaians because a large proportion of users in Ghana are using these services only from their mobile phone. Many other mechanisms such as notifications and browser popups have been proposed by mainstream security and privacy researchers, but user habituation can erode the effectiveness of such methods [24, 37].

3. SETTINGS AND METHODOLOGY

We conducted a qualitative study of how technology users use the Internet and think about security. We used surveys and semi-structured interviews to conduct our research. We conducted 193 surveys and interviews during Summer 2013 and we conducted our analysis in October 2013. Nearly all respondents were surveyed on Fridays, Saturdays, and Sundays. All surveys and interviews were conducted in English (the official language of Ghana) and the interviews were digitally recorded. Interviews averaged 10 minutes each and they were audio recorded and transcribed for analysis. Standard procedures for informed, voluntary consent were practiced. Users were offered a 10 Ghanaian Cedi payment (approximately 5 USD) to participate in the study, and were instructed that they could discontinue taking the survey or refuse to be interviewed at any point (13 respondents opted not to be interviewed and 7 did not wish to complete the demographic information), and still receive this payment. Interviews were conducted by one Ghanaian male and one white American female. Our analysis does not indicate any bias in content of responses correlating to the race or gender of the interviewer.

Respondents were chosen from a sample of technology users we encountered in public gathering places such as streets, Internet cafés, markets, and universities on weekends to select for maximum variation. The respondents were gathered from across 11 urban and peri-urban locations in 8 geographical regions in Ghana. Table 1 lists the locations and settings where we gathered respondents. We began by screening these potential respondents to exclude people who had no experience with mobile phones or computers and those below the age of 18. Ages ranged from students (18 years old) up through executives (55 years old), but the vast majority were between 18 and 31 (the median age was 25).[1] There were 131 male (68%) and 55 female (28%) respondents.

Region/City	Location	# Resp.
Accra-Osu	street and copy center	11
Accra-Nima	street and restaurant	10
Accra-Airport	office	4
Accra-Kokomlemle	Internet café	29
Eastern Region-Korforidua	street and a college	20
Northern Region-Tamale	community event	23
Volta Region-Ada	street	15
Central Region-Takoradi	street outside a market	20
Ashanti Region-Kumasi	college and a street	21
Brang Ahafo-Sunyani	streets	19
Western Region-Cape Coast	university	20

Table 1: Number of respondents by region/city and location.

Education Level	# Resp.
Junior secondary school or less	13 (7%)
Senior secondary school	53 (28%)
Polytechnic or post-secondary teacher training	37 (20%)
University	63 (34%)
Graduate school	20 (11%)

Table 2: Number of respondents by highest education level.

From those not excluded, we selected respondents for maximum diversity by choosing respondents from a wide variety of backgrounds, ages, and socio-economic classes. Socio-economic status was not explicitly measured in terms of income, but occupations ranged from service industry workers (cook, hairstylist, etc.) up to professionals (IT professionals, engineers, etc.). Table 2 lists the education level and Table 3 lists the occupations of our respondents. We believe that our sample is fairly representative of the urban and peri-urban population of Ghana and allowed us to document diverse variations in attitudes toward technology and perceptions of security to identify important patterns. Figure 2 illustrates one street-side interview taking place in Kumasi.

We developed a survey and a face-to-face semi-structured interview protocol that explores several aspects of the use and attitudes toward Internet security. Our interview participants were the subset of surveyed respondents who agreed to an interview. In our interviews we specifically probed for instances where respondents encountered hacking or security indications in their interactions. The majority of the interview was spent on asking questions from a pool of questions regarding potentially risky use of technology, awareness of security precautions, and perceptions of security indicators on the Internet. We probed deeper into the responses of the subject when particularly novel responses were given. This method allowed us get a broad picture of the self-reported reasoning behind certain behaviors and attitudes.

The focus of our interviews was exploratory. We asked about incidents or stories regarding hacking and about precautions on the Internet both in terms of security and privacy. We also asked about mobile phone, website, and pen-drive use. We probed deeper into each of these areas to find out the indicators that respondents used to mitigate risk (e.g. appearance of websites, padlock icon on

[1]The median age in Ghana in 2013 was 20.7 years old [1].

Occupation	# Resp.
Student	46 (24%)
Service Industry	15 (8%)
IT / Engineer	12 (6%)
Teacher	10 (5%)
Administrative / Clerical	9 (5%)
Film / Design	5 (3%)
Business / Entrepreneur	5 (3%)
Mobile Banker	3 (2%)
Farming	2 (1%)
No Response	62 (32%)
Other	24 (12%)

Table 3: Number of respondents by occupation.

Figure 2: Respondents filling out surveys in Kumasi.

browsers, etc.).

After collection and transcription of the data, two of the co-authors coded the data independently to look for predetermined and emergent themes. We then discussed these major themes among all of the three co-authors to validate the themes and then expanded themes and organized them into a unified data matrix to identify patterns across subjects and check for representativeness. We used this data matrix to highlight specific examples of trends that appear as descriptions throughout the paper.

4. FINDINGS

We received a total of 193 completed surveys from our respondents and completed 178 interviews. We elaborate on these results below, and believe that together, these results illustrate how people use and perceive technology, what people's attitudes attitudes and perceptions are like with regards to security and privacy, and the measures that people take toward securing themselves.

4.1 Technology Use and Perceptions

All respondents used mobile phones and owned an average of 1.93 sim cards. 184 respondents used the Internet. The survey data from Table 2 and Table 3 show a wide variety of education levels and a levels occupations. Table 4 shows the locations where our respondents accessed the Internet. Our respondents generally accessed the Internet from their personal mobile phones (72%) followed by computers at home (50%), Internet cafés (40%), and

Location	# Resp.
On personal mobile	139 (72%)
Computer at home	97 (50%)
Internet café	78 (40%)
Computer at school	70 (36%)
On other mobile	20 (10%)

Table 4: How the Internet is accessed by location.

Use case	Internet	On Mobile
Facebook/Social Networking	67%	58%↓
Searching	63%	60%↓
Email	59%	65%↑
News	58%	64%↑
Education	58%	53%↓
Entertainment	48%	60%↑
Job Search	22%	21%↓
Games	33%	62%↑
Health	25%	25%
Video/Audio Chat	24%	34%↑
Banking	11%	20%↑
Instant Messaging	9%	14%↑
Agricultural	4%	7%↑

Table 5: How the Internet is used in general and on mobile phones. Arrows indicate increase or decrease on mobile phones compared to general use.

schools (36%). Table 5 summarizes the reported purpose of using the Internet by our respondents. Our findings indicate that the Internet is generally used for social networking, searching, email, news, education, and entertainment. These numbers are quite high, but generally consistent with recent notable findings on the popularity of online social media, job search, and branchless banking in Ghana and elsewhere in sub-Saharan Africa [19, 20, 27, 40, 49, 54]. We were surprised by some of these results, particularly how many people used the Internet for health services (25%).[2]

We asked a number of questions about self-reported skill with computers and mobile phones along with general attitudes and perceptions of security and privacy. Respondents rated their responses on a 5-point Likert scale. On average our respondents reported higher mobile phone skill (4.0) than computer skill (3.1). Of our respondents, 48.7% reported that they more than 5 years of experience using the Internet, 14.5% had 3-5 years of experience, 13.5% 1-3 had years of experience, 10.3% less than 1 year of experience, and 6.3% never used the Internet (6.7% did not respond to this question). Most of the respondents who had never used the Internet had junior secondary school or less levels of education.[3]

4.1.1 Social Networking and Chat

Social networks were extremely popular among our survey group and were clearly a primary reason to go online. From our survey we found that social networking was used by 67% of our respondents and 58% of our respondent on mobile phones. In our interviews, Facebook was mentioned by nearly 30% of respondents

[2]We discuss in detail why some of these numbers are subject to interpretation in Section 4.1.2.

[3]Nine respondents who responded that they never used the Internet responded that they used Internet services. We included those respondents in our results and discuss this issue in Section 4.1.2.

when asked what they do most frequently online (though some were asked specifically whether they had Facebook accounts), with WhatsApp Messenger second most frequently mentioned and Google+, Twitter, Yookos, Yahoo Messenger, and unspecified social networks and messaging applications trailing far behind. Among users of Facebook, person-to-person and group chat were far and away the most mentioned features used; in the words of one respondent:

Interviewer: *What do you do on Facebook?*
Respondent: *I chat.*

and another:

Interviewer: *What do you do on Facebook?*
Respondent: *Facebook? I chat with my friends. And my family.*

Four users of Facebook reported that Facebook was the *only* reason they went online, that they didn't visit any other sites, e.g.:

Respondent: *It's just Facebook, that's all.*

Chatting appeared, for most users of Facebook, to be the only reason to use the site, with users chatting with friends, colleagues, and customers. Of those who chatted with friends, the attraction of chat seemed not to be the ability to convey particular information or to reach particular friends on demand, but to have casual ad hoc chats; that is, it was more important to chat with *someone* than with anyone in particular. Of the dozens of people who had Facebook accounts, during the interviews only two mentioned posting or commenting, one mentioned music and movies, and one mentioned photos; this again despite several users going online only to use Facebook, leading us to believe that many were therefore ultimately going online only to chat. In addition, we found during the interviews that chatting was the most commonly reported use of mobile phones after calling, SMS, and web browsing. This is in contrast to the survey results, which indicate much lower numbers likely because chat was often folded into the responses for social networking and Facebook.

This predilection for chat helps to account for the relative popularity of WhatsApp Messenger [11]. WhatsApp is a cross-platform free messaging app supported by nearly every phone platform and offering free unlimited messaging for the first year. Mentioned, unprompted, by 9 respondents and used by many others, the uptake of WhatsApp, boasting 300 million monthly active users worldwide as of August 2013 [10] (compared to Facebook's 1.15 billion monthly active users [4] as of July 2013), was a surprise. Users of WhatsApp in our survey group reported using it for person-to-person chat as well as for group chat, with at least one user reporting using this group chat feature for work:

Respondent: *I do spend a lot of time, maybe on WhatsApp. Because I'm a media man, and normally we use to discuss, we have a crew page over there we use to discuss concepts we are about to shoot [unintelligible], so normally I'm on WhatsApp.*

Moreover, several users indicated an increasing preference for WhatsApp over Facebook, though the reason for this is not made clear:

Respondent: *Nowadays WhatsApp. So, Facebook has become a little bit, yeah, down, so I do WhatsApp in most.*

If chat is the "killer app" for this user group, it stands to reason that as the cost of data on mobile platforms decreases and its availability increases, the always-on nature of WhatsApp messaging vis-à-vis having to log into Facebook or another social network site on the web will make it increasingly attractive. This is particularly the case as text-based chat, which was the only use of WhatsApp mentioned, consumes paltry amounts of data and is therefore less sensitive to the speed of the underlying data connection, something that is untrue for media-rich sites such as Facebook (though the mobile-friendly version of Facebook improves upon this).

We surmise that the reason that the homogeneity of social networks (nearly all Facebook of those who specified) and chat applications (nearly all WhatsApp) reflects the positive externalities of network effects in tandem with the relative expense and slowness of Internet access: as the number of participants in a network increases, the value of that network increases, and on an expensive connections, users will tend to optimize by only visiting those few sites that provide them the most value per access. For instance, visiting Google+ in addition to Facebook might allow a user to connect with a few more friends, but would incur double the cost in data. Users, therefore, have tended to gravitate towards one or two select sites or applications in each domain of Internet use.

4.1.2 Conflation of Network Services

The interviews revealed several general trends around Internet use and perceptions that we found interesting. One such trend is that among those who mentioned during interviews, unprompted, using the search engine Google, more than 58% specifically referred to it as an educational or research website rather than a general web portal or search engine:

Respondent 1: *Educational websites, go there to research, like Google, yeah?*
Respondent 2: *I go to Google to search for information - I use it to learn.*
Respondent 3: *If it comes to education, I try with Google.*

No respondents indicated that they used Google for any non-educational purpose, such as searching for entertainment, media, or even for news.

Many of the respondents calling Google a research or education site were students at various levels of education, and one specifically mentioned Google Scholar, but the group also included various professionals and at least one person who was unemployed. However, only just over 25% of respondents asked to name the things they do online most frequently mentioned Google.

One result of the spread of mobile connectivity is that for an increasing number, phones are the primary way in which people use network services over alternatives such as Internet cafés. Users expressed reasons such as immediacy and convenience as motivating factors; travel time was also a factor.[4] One user in particular highlights this trend:

Interviewer: *So, do you not usually go to the Internet café?*
Respondent: *No, I don't usually go there.*
Interviewer: *Why is that?*
Respondent: *[chuckles] I don't have the time!*

A direct result of this shift from fixed-line, computer-based Internet use to immediate, mobile, phone-based use is that rather than having a clear delineation between use of the Web and use of other Internet-enabled applications such as instant messaging or phone-

[4]As we will see in Section 4.2.4, perception of insecurity is also a factor.

based apps, users tend to conflate all Internet activities into a class of activities that require data plans on their mobile phones. Thus on the one hand, whereas a user in the United States might say that they are browsing the web *on their phone*, the same idea is expressed without this modifier among our respondents. On the other hand, whereas a user in the US might say that they are using the Facebook *app*, our respondents simply say that they are using Facebook. To our respondents these modifiers appear to be differences without distinctions; the content dictates the label and people appear agnostic to the mode of access, whether from a café or a phone, via an app, or a browser.

4.2 Security

The primary focus of our survey and interviews was to evaluate commonly held security practices and attitudes among respondents, and the interviews revealed several significant insights.

4.2.1 General Perceptions

We first measured general perceptions of individual skill levels, threat level of attacks, and ideas on software piracy and self-efficacy levels of protecting against attacks. Figure 3 summarizes our findings. Our scores here are all on a 5-point Likert scale. From our results, we that computer skill (mean=3.2) is generally lower than mobile phone skill (mean=4.1), but they converge at the higher levels of education. Since this is survey data, we cannot say if there is a causal relationship, but these self-reported skill levels for computers and mobiles are both positively correlated with education level ($p<0.0001$), ($p=0.0020$) respectively.

We also find that feelings of 'dread', e.g. worrying about security (mean=4.0) and thinking that you could be a target for hackers (mean=3.6) are relatively high. Both measures of dread are positively correlated with self-reported skill with computers ($p<0.0001$), mobiles ($p<0.0001$), and education ($p=0.0039$), ($p=0.0125$). Meaning, despite increasing confidence in skill with technology and overall education level, worries about security and being attacked also increase. Also, respondent's overall concern of viruses being on computers was very high across the board (mean=4.4).

Interestingly, we found that respondents believing pirated software to be dangerous is somewhat high (mean=3.6) and positively correlated with education ($p=0.0003$), computer skill ($p=0.0305$), and mobile skill ($p=0.0216$). While the absolute numbers could be higher, this is positive finding because pirated software is a common vector for malware infection.

Finally, we found that confidence in protecting private information on computers is fairly high (mean=3.9). This confidence is not significantly correlated with education, but it is positively correlated with self-reported skill with computers and mobiles ($p<0.0001$). We explore the potential source of this confidence later in Section 4.2.5. Another interesting result was that we found that the general perception of mobile money transfer safety was high (mean=4.1) and was positively correlated to computer skill ($p=0.0001$) and mobile skill ($p=0.0006$), but not correlated to education. Mobile money transfers appear to be somehow outside of the categorically vulnerable set of Internet technologies. This may be yet another symptom of the conflation of network services discussed previously in Section 4.1.2.

4.2.2 Quality and Security

One finding from our interviews was that there was a strong correlation between perceived quality of websites and their perceived security or safety. This finding corroborates previous findings by Lindgaard [39] in the U.S. on judgments of trust being linked to appearance of webpages. When asked how users determined whether a website was safe, one respondent, for example, said:

Respondent: *Anytime I go on it, and it does not hesitate giving me information, that's why I think it's safe.*
Interviewer: *So because the information comes fast, you think it's safe?*
Respondent: *Yes.*

In the same vein, another expressed that those sites that return reliable information rather than false information are safe. Other reponses mentioned things like popups and advertisements indicating low quality and therefore lack of safety and sites with pornographic content being inherently unsafe. This is in contrast to other cues, such as the lack of SSL encryption typically indicated by a padlock icon in the browser or a website asking for more information than should be required to gain access to a site or service, neither of which were mentioned by even relatively expert users such as IT technicians. This result corroborates with previous works that find user assessment of trustworthiness often relies on cues not designed as security features [33] and that a majority of users ignore SSL warnings in a wide variety of conditions [51].

Various other measures of quality were expressed. Sites that send spam emails were unsafe; users said in response to this question that they stopped accessing websites if they became slow, etc. It is unclear whether these perceptions are due, as we suspect, to some sense that websites that seem well-made would naturally pay more attention to security in the same way that any well-manufactured object inspires confidence, or to some difference in the lexical range of the words "safe" and "trustworthy" in these contexts of which we are not aware. Evaluations were very subjective. One respondent identified unsafe websites as ones that "look mischievous". These findings are also consistent with findings by Wash that describe some users whose mental models dictate that they should only browse webpages from trustworthy sources [53]. We did not find any mention of the more sophisticated measures found by Wash during our interviews (e.g. disabling scripting, not clicking on attachments, or being careful downloading from websites).

4.2.3 Imputed Trustworthiness

In the same vein, many users commented that rather than trying to determine what sites were safe or not, they simply restricted their Web use to a handful of well-known sites such as Facebook, Google, Yahoo!, Wikipedia, and other sites that were recommended by friends, the referral by the crowd or by their friends thereby imputing some measure of trust. As a result, very few respondents said that they surfed the web by browsing - clicking through as they found links of interest in undirected exploration - rather, over 83% of interview respondents said that they went to specific sites or executed specific searches on trusted sites. One respondent mentioned that he never fills out online forms and when they are encountered he leaves the page.

The use of Google and Yahoo! raised a question for which we were unable to find a clear answer from our respondents: if search engines such as Google and Yahoo! are considered safe, are the links that they return in response to queries also considered safe as a result? Do the perceived brand quality or reliability of these search engines have a halo effect, or a social capital-like referrer effect on the returned pages, passing on imputed trust? Moreover, does this mean that users are abdicating the responsibility to understand whether pages are safe, relying upon these web properties to take care of that for them as described by Dourish [23]?

4.2.4 Security Measures

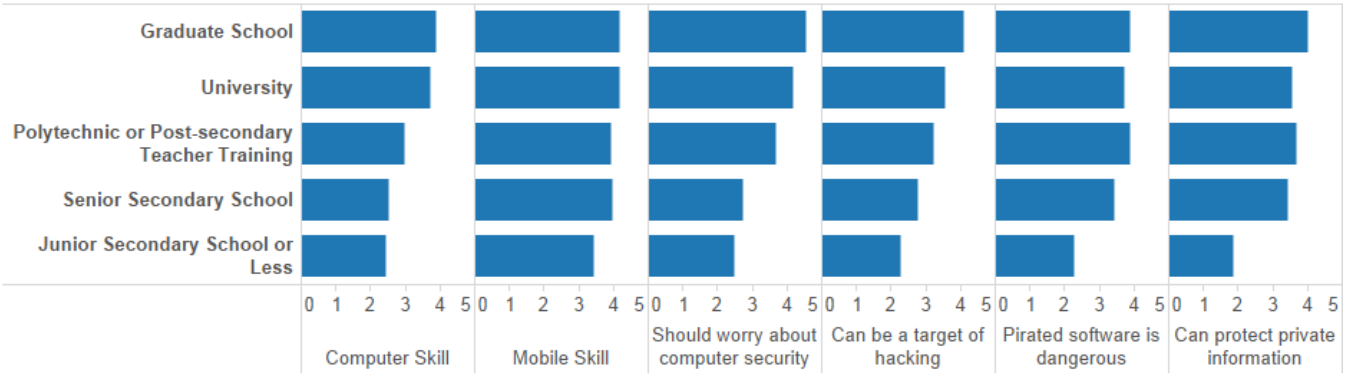

Figure 3: Self-reported skill levels and and perceptions of security and privacy on a 5-point Likert scale.

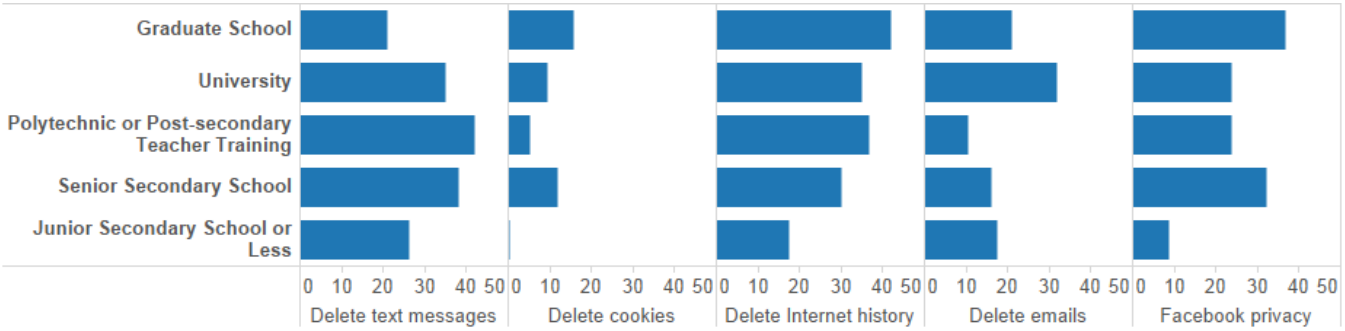

Figure 4: Security measures taken by percentage of respondents.

Measure	% Resp.	Education	Computer Skill	Mobile Skill
Delete texts	35.2%	0.13	0.67 **	0.59 **
Delete cookies	9.3%	0.30 **	0.02 .	0.02
Delete history	32.6%	0.05 *	0.07 * * *	0.06 **
Delete emails	21.2%	0.02	0.03 .	0.04 *
Facebook privacy	25.9%	0.02	0.06 **	0.05 **

Significance codes: 0 '* * *', 0.001 '**', 0.01 '*', 0.05 '.', 0.1 '' Coefficients for correlation from a linear regression where values are on a 100-point scale vs a 5-point Likert scale for education levels.

Table 6: Correlations between defensive measures taken and education, computer skill, and mobile skill.

One of the primary research goals motivating our study was to determine what behaviors characterize the measures that people in these contexts took in order to protect their security and privacy online, and whether such measures were correct, commonly held, and adequate. We asked our respondents several survey questions on specific measures taken to defend against attacks. Figure 4 and Table 6 summarize our results. These results show that only up to 35.2% of respondents use even the most basic measures (deleting texts) to secure their private information. Other simple measures such as deleting history and emails follow close behind, but the instances of deleting cookies is far lower at 9.3% of respondents.

Surprisingly, 25.9% of respondents used Facebook privacy settings, which is high considering its complexity relative to simple deletions, but this may be due to the overall high level of Facebook use. From our results we find that users deleting Internet history is correlated to education and skill level. Deleting cookies, however, is only correlated to education level and computer skill level, but, unsurprisingly, not correlated to mobile skill level. We find that computer skill is correlated to performing all security and privacy measures. However, education is not correlated to deleting texts, deleting emails, or Facebook privacy settings. Figure 4 visually illustrates these trends.

During our interviews we directly asked interviewees how they stayed safe online. The most popular method by far was the use of a password, which we examine in greater depth in the following subsection. Other responses varied from nothing:

Interviewer: *What do you do to stay safe on the Internet?*
Respondent: *I don't do anything.*
Interviewer: *You don't do anything?*
Respondent: *Yeah.*

to relatively sophisticated measures including deleting cookies, deleting Internet browser history, private Googling (which we take to mean something akin to Incognito mode in Chrome), deleting chat history, logging out, rebooting the computer when done, not saving anything to desktop, restricting privacy settings on Facebook, avoiding unknown sites, and avoiding unknown people on social networking. We did not capture quantitatively in our surveys the prevalence of these more sophisticated measures other than deleting cookies and Internet history.

Through our interview data, we found that these measures were rarely used in any coherent regime, but were assembled ad hoc from information gathered from hearsay from various sources. This finding closely reflects previous work by Rader on stories acting as informal lessons about security [46]. Several respondents noted that they learned their safety measures from assistants at Internet cafés or had learned from friends, but only after they proactively requested help; this type of information does not appear to be proactively disseminated, according to our respondents.

Interviewer: *And how did you learn how to clear your history? Who taught you, or how did you know how to do it?*
...
Respondent: *That is the café assistant. I asked him 'What can I do so that people cannot gain access to my account?' And he tell me this is the way you can do it.*

It does appear that, among our respondents, there is a common distrust of shared computers (with strangers), which may be helping drive the adoption of connectivity via mobile phones and away from places like Internet cafés:

Interviewer: *Do you ever feel like it's unsafe to go on the Internet?*
Respondent: *Yeah, sometimes, sometimes I feel unsafe- especially when I go to the Internet café. There are people there who are also waiting for you to go so they also come. And they will be pressuring you to leave there so that they come.*
Interviewer: *So how is it unsafe?*
Respondent: *Maybe they can go to your history, the web history and then get access to your password, and then go into your accounts.*

and schools:

Interviewer: *So, what do you do to stay safe on the Internet?*
Respondent: *I browse at home most of the time, or at work, but I don't browse at school. Yeah, so at work I'm sure we're just using the work's, the office Internet, and then at home I have my own modem. So that's what I do.*

Aside from perceived quality, as mentioned earlier, users could not typically ascertain which sites were safe and which were not. Some relied upon software like antivirus programs, others explicitly claimed ignorance on the matter, a few were skeptical about security and felt that even commonly-used sites and services like Facebook and Skype were unsafe. One user expressed a sentiment that appeared to be widely held:

Respondent: *If it has a password, a place where you can put your password, only you can get access to it, and I know it's safe.*

4.2.5 Passwords

Passwords were the *de facto* gold standard for security among those interviewed. Of those asked about safety measures they took on the Internet, over 76% expressed that use of a password in one form or another was their only or primary means of staying safe; no doubt was expressed about the security of password mechanisms. Passwords were commonly recycled across all websites used, when asked "how often do you use the same password or PIN on different accounts", respondents responded with a mean score of 3.6 (moderately often). The distribution of rate of password reuse appears inverse normal (i.e. people either reuse their passwords often or never at all). 53% of respondents always or often use the same password for different accounts. 58% of respondents never changed their passwords, 22% changed their passwords once a year and 15% changed passwords once a month or less (5% did not respond to this question). Only a single person discussed password strength during the interviews, several respondents explicitly mentioned that they never changed passwords.

Passwords were considered effective so long as two measures were taken. The more commonly mentioned was memorization of the password (80% of respondents) as opposed to writing it down (24% of respondents):

Respondent 1: *[. . .] and then there's password. And, my password, I always memorize it so it's hard for you to get my password and access my stuff on the Internet as well.*
Respondent 2: *Normally I memorize my password, I always memorize on it.*
Respondent 3: *Yeah, I have a password [. . .] I keep it for memory.*
Respondent 4: *I've never changed a password [. . .] It's off head.*

Other respondents mentioned not sharing passwords except with a few trusted people such as family or close friends (10% of respondents).

An interesting and unforeseen effect of this implicit trust in passwords is that many users held sensitive personal information, including other passwords, in password-protected devices or services. Two examples of this were in email:

Interviewer: *How do you stay safe on the Internet?*
Respondent: *By keeping my informations in my email and then locking it up with my password.*

and on phones:

Respondent 1: *To avoid everything, I normally put passwords or PIN on my mobile phones. But apart from that, let's say if someone gets access to my, I wouldn't like them to see my financial information, maybe my personal photos or maybe my bank account details [. . .]*
Respondent 2: *I have account numbers on my phone, like my bank account number, I have it on my phone [. . .] I use a lot of password to block so that people might not see it.*

with the latter being far more common. Types of information held on phones included bank balances, bank account details, passwords for websites, medical and health information, and PIN codes. Of our respondents, 7% sent passwords to themselves via email and 7% did so through text messages. While this appears to be unsafe by security experts, considering the threats both perceived and real that face Ghanaian users this may in fact be a fairly rational practice.

4.2.6 Perceived Threat Model

It was clear from the responses and the types of approaches that respondents were using to stay safe during online activities that the mental model that users had of potential threats was significantly different than users in developed countries, perhaps more closely reflecting the actual threat model on the ground in their context.

Nearly all respondents expressed fears and to our respondents countermeasures such as passwords surrounded the human-computer interface. The most clear and present danger was from the person to the right or left. In other words, the context where respondents

accessed the Internet and threats from humans were either physically present or would be at some later time. As a result of this mental model, passwords were considered a strong safety measure so long as they were kept secret, as a human (or so they perceived) would find it impracticable to guess a password at random. Our findings here largely echo those by Klasnja *et al.* where relatively low user understanding of the underlying technology results in the dominance of a physical threat model [36].

This physical threat model is even further narrowed to people who make use of accounts that have not been logged out of, which is potentially the most common attack vector for this user base. Interestingly, despite the focus on threats from people physically nearby, no mention was made of shoulder surfing, keyloggers, or other slightly more sophisticated methods of local attack at the man/machine boundary layer.

Users displayed high confidence in the security of systems that they had logged into, as evidenced by the use of email for storage of sensitive information. When pressed on the possibility, for instance, that someone could intercept chat information, users were not concerned:

Interviewer: *Do you think anybody could take your conversation and do something with it?*
Respondent 1: *No, because we chat alone. So no one can hear any information about us.*

Interviewer: *Do you ever worry that your chats are being saved somewhere, and someone's using the information for something else?*
Respondent 2: *No, I don't think somebody can use my information.*

Especially noteworthy to us is the first response above; the respondent goes on to explicitly state that no one can get that information unless they get into his email, and that's not possible because he always logs out, clears history, and reboots the computer. Again, the attack surface, in the respondent's mind, was limited to the particular physical terminal that he used - the network beyond that terminal represented a safe zone. This appears to be a very commonly held belief, that while the network may go down between the terminal and the site, no other danger exists in the network; that it is effectively a direct link between the terminal and the various sites, and that danger must come either from the site accessed or at the terminal; that no danger can be interjected between the two. Again, our results here corroborate very closely with findings by Klasnja *et al.* [36] that show how users often have no awareness of data visibility when interacting with a remote web server through a network.

Other aspects of the threat model were unusual to our minds as well - users had implicit trust that their phones would not be compromised if they had passwords - this despite many users specifically mentioning that the reasons that they chose the phones that they did was because there were many phone shops that could repair them. These same repair shops could, of course, also reset the passwords and access whatever is inside, something that did not appear to occur to any of our respondents. Furthermore, from our interviews respondents appeared to understand the difference between phone passwords and a "SIM passwords" (SIM PIN). We did not have quantitative results for proportion of users using each kind of password, but in our interviews we found a predominance of phone passwords being used. It is possible that SIM PINs are only used when necessary in cases such as repair shops or users simply do not worry as much about their contacts being stolen.

Further, aside from scant mentions of antivirus software, the topic of viruses and malware never arose, despite having among the highest infection rates in Africa [14]. It is particularly unclear whether any participants were aware of the various forms of malware that capture passwords and other information that is entered into computers and how that may have affected their opinions of the use of passwords.

4.2.7 Fear of and Experience of Hacking

In our quantitative findings we discovered a high level of dread related to hacking and being targeted. However, during interviews respondents did not consider hacking an immediate threat. While many had heard of hacking, few had a clear idea of what it entailed or what possible repercussions could occur. As with the threat model described above, people's idea of the danger of hacking was mostly limited to those threats in the immediate vicinity.

A select few respondents had direct knowledge of hacking as victims, but only one displayed understanding that transcended guesswork:

Respondent: *Yes, one of my accounts has been hacked. [. . .] It's like PayPal. So they hacked it, immediately I transferred money to like, under a few seconds they took the money. I transferred 200 Cedis [(20 USD at the time)] into it, and someone else from nowhere took the money. They started tracking the IPS [sic] address and they were like, it's in India or something, but I just forgot about it. And since then I've never done anything online transaction.*

Other firsthand victims of hacking had much more benign stories, mostly of having their Facebook accounts broken into, or their email accounts broken into and passwords changed to lock them out. Secondhand stories, included friends whose email accounts had been hacked and the accounts used to send email to friends asking for money, a friend who had posted his bank account details online without a password and whose account was promptly emptied, someone who had all his money stolen by someone in France, someone whose Mastercard was hacked, and various other perfidy.

The concept and scope of hacking is vaguely defined. The term 'hacking' may include activities such as phishing, scams, spam, etc. Most of our respondents use hacking as an umbrella term rather than more specific terminological distinctions. To our respondents hacking included scams (including 419 scams) and phishing. One user who was 'hacked' had responded to a phishing text and had his MTN (a major GSM cell operator in Ghana [9]) phone credit balance stolen because he provided his PIN.

The potential consequences of being hacked tended to gravitate around three potential outcomes. First, several respondents indicated that a hacker who gained access to their online accounts would ask their friends for money:

Respondent: *Most hackers will send mails asking for money. So, maybe ask for money from my friends. That's what most hackers do.*

A second possible outcome is theft of personal information, again, for the purpose of stealing money:

Respondent: *[. . .] and get sensitive information like my bank details, my personal information, and use it against me.*

A third major possibility expressed was the nuisance of being locked out of their own accounts, as some other respondents had experienced firsthand. Others mentioned that hackers might blackmail them, or implicate them in a hacking attack on another per-

son, use their account to send out spam messages, do damage to their work, etc., but the most common fear is the direct loss of money. In relation to the mental models about hackers as described by Wash [53], most of our respondents' mental models could be captured by the "Burglar" folk model: the identity of the hacker is "some criminal whose reason for break-ins is to look for financial and personal information and possibly harm the computer or expose personal information opportunistically".

The way people are hacked was not made clear to us. As is consistent with our prior observations about attitudes towards passwords and threat models, in general people blamed hacking attacks on lack of passwords or people having given out their passwords.

5. DISCUSSION

We have found that there are substantial security gaps (according to common 'best practice' security advice) in the way online services are used by urban Ghanaians. Online threats are global, but perception of threats, in general, are very localized. Informal lessons result in a patchwork of ad hoc mechanisms being used to secure personal information. Password use, deleting messages, emails, and browser history are currently the key mechanisms for protecting against hackers. Network technology is mentally construed as being a black box; what goes on behind the screen is not part of the mental threat model. The conflation of services and agnosticism to the device or software application being used are also suggestive of this mental model.

We also found that, like in rich countries, people's perceptions of trustworthiness are also predominantly ad hoc and from the perspective of the immediately visually apparent. E.g. appearance, lack of popups, loading speed, specific safe websites, etc. People's confidence in their ability to defend themselves against security threats is similarly based on the apparent. We found that the most common defense is to depend on passwords and memorization of passwords. Unfortunately, passwords are rarely changed by most and stored in an unsafe manner and often reused. We found there is a strong worry about security and of being hacked, possibly due to the unknown nature of hacking, but despite this concern, respondents reported feeling that they were able to defend themselves despite passwords often being the only line of defense. This confidence is likely due to the low incidence of hacking. Finally, we found that the concept of hacking being typically confined to stories and conceptions of private information being stolen and monetary loss.

Despite this possibly bleak picture of Internet security in Ghana, given the low incidence of local cybercrime, the mental threat model and existing practices actually appear largely adequate for the time being. Unlike in rich countries where users are largely ignoring onerous security advice [31], we found that some users actually go to great lengths to protect their security and privacy even if the way they do so is imperfect (clearing history, deleting messages, etc). Social engineering by 419 scams and phishing in spam are relatively well known to our respondents and are mostly captured by the existing mental model and countermeasures. Other types of hacking such as large-scale data theft and botnet infections that fall outside of the existing mental model have not yet occurred likely due to the present lack of profit to be made when compared to targets in rich countries.

While the existing defensive measures may be sufficient and even appropriate for the actual threats on the ground at present, given the continued trends it is unlikely that this will continue to be the case. As network bandwidth increases along with penetration, the restriction of Internet use primarily to a few popular sites, is unlikely to hold, and Ghanaian Internet users will become exposed to the wider array of Internet-based threats including, but not limited to, malware, phishing, and various illegitimate sites. Of special concern is the fact that as bandwidth increases and costs come down, use of the Internet (as opposed to burned CDs as are currently the more popular option) for the acquisition of pirated software, a popular vector for malware, will likely increase. This is not currently a problem for devices that are often disconnected or have low bandwidth, but as connectivity improves these devices may be more attractive to attackers. Already some interview respondents mention using the Internet to visit "warez" sites to download software.

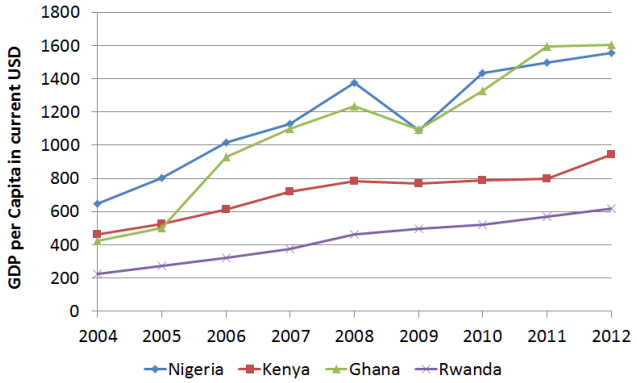

Figure 5: GDP per capita in current USD, from [2]

Further compounding the near-term threat is the general trend towards affluence in many sub-Saharan nations such as Ghana, Nigeria, Kenya, and Rwanda, a trend clearly seen in Figure 5. As users, on average, become wealthier, they will naturally become riper targets for online exploitation of various kinds aimed at appropriating that wealth. Finally, the promulgation of mobile financial, health, and governmental services in these developing contexts without commensurate security precautions is of concern.

5.1 User Education and Threat Mitigation

To mitigate the confluence of these trends, all of which will tend to reduce the security of the average user of the Internet in Ghana, steps could be taken proactively. One possibility is to educate users on the the reality of the types of threats they may face on the wider web. Rather than the ad hoc self-education our respondents reported, more education and resources could be delivered to users of the Internet. Unfortunately, conventional security awareness programs are unlikely to completely solve the problem when security advice continues to grow in complexity and following this advice has been shown to have unclear benefits [31]. Instead, targeted security advice specific to particular applications and services may be more easily followed if easier to follow. Much as health information is delivered in increasingly clever ways, information about avoiding hazards online might be delivered packaged with the service being used. For example, on SMS applications security advice could be sent as informational SMSs as part of the service or for mobile data plans the mobile-operator could give advice.

Another possible focus of education is for the common user to be made aware of the nature of the Internet. Basic concepts such as there being an ungoverned expanse between the user's terminal and the site they are trying to access, the importance of the use of technologies like SSL to prevent man-in-the-middle attacks, traffic sniffing, etc. could prove to be eye- opening and might cause a change in security-related behaviors. We have not quantitatively studied the prevalence of the notion that passwords are

impregnable, but if this is indeed the case then educating users or demonstrating the fallibility of passwords e.g. using John the Ripper [8] might prove enlightening. Similarly, warnings that passwords on smartphones and feature phones alike can be bypassed and, as such, that phone handsets do not serve as secure repositories, would likely be of help.

Given the current preference for mobile phones and passwords, two-factor authentication as recently employed by Facebook, Google, and Yahoo [3, 6, 12] may be more appropriate if the second authentication factor were not tied to the mobile phone. In addition to this it may, at least in the near term, be advisable to set up ISP-based blocking on sites known to carry malware or questionable content. However, this type of regulation creates censorship challenges and is also unlikely to help people who will specifically be looking for pirated software or illegal music or media downloads.

The ad hoc nature of communication of security information may, alternatively be leveraged through the use of social networks, making use of social capital within social graphs to improve uptake of informal security stories and security advice [17].

5.2 Avenues for Further Research

Our findings thus far suggest avenues for further research. Evaluating how users in this context develop their mental threat models could prove to be fruitful despite their fundamental complexity - to what extent these models are based on hearsay through their social graph, personal experience, news, and other sources is certainly worthy of deeper investigation. Also interesting would be an analysis of how imputed trustworthiness works - whether sites are perceived to lend legitimacy to sites they link to by default - and whether this can be modeled in the same way as social capital flows through social graphs. Google's PageRank already incorporates imputed trustworthiness to a degree - pages linked from reliable pages are considered more reliable - so these types of assumptions, depending on search terms, may not be far off.

Also worthwhile would be an effort to front-run the inevitable increase in hacking and establish certain baseline attitudes and practices, and evaluate how these evolve over time as this increase takes place. It is also unclear whether greater use of mobile phones rather than computers to access the Internet result in less worry about viruses and malware.

Finally, new mechanisms for usable security and privacy designed to be appropriate for these developing region contexts could have a big impact as existing mechanisms transplanted along with the default technologies do not appear to be widely adopted. There may be interesting opportunities for novel solutions based due to mobile phones being the primary means of access to services.

6. CONCLUSION

This paper makes two main contributions. First, this is the first study to our knowledge to focus on exploring security perceptions and practice in a developing country context. We have examined technology users throughout Ghana to comprehensively understand the technology landscape and people's perceptions regarding security. Second, we examined the security measures that people take to protect themselves online. We found in our survey corresponding to 193 participants that the characteristic attitudes include: 1) reliance and trust in password systems, 2) vague understanding of how networked systems work and therefore what factors constitute realistic threat models resulting in an asymmetric focus on local threats, 3) a conflation of perceptions of quality and perceptions of security, consistent with existing research, and 4) various observations on security-related behaviors, Internet and social network usage patterns, and other miscellany.

Interestingly, the physical threat models and lack of understanding of how networked systems work are very similar to previous findings in rich countries. The ad hoc acquisition of security knowledge is also similar to previous findings. The difference in Ghana is that the low incidence of local cybercrime makes these existing threat models and practices relatively adequate for the time being. Some would argue that this is the case even in rich countries, but given the continued trends in Internet penetration, income, and dependence on the network for basic services we do feel that this is a risky proposition.

It is yet unclear to what extent the users we are interacting with can serve as representative of users elsewhere in sub-Saharan Africa or the developing world as a whole, but we hope our contributions are able to help characterize the overall shape of security in the developing world and provide a starting point for discussion and research.

7. ACKNOWLEDGMENTS

We thank the respondents who participated in the study and our reviewers for their helpful feedback. We would also like to thank our shepherd Joseph Bonneau for his help improving this paper.

8. REFERENCES

[1] CIA World Factbook. **https://www.cia.gov/library/publications/the-world-factbook/fields/2177.html**.

[2] Data | The World Bank. **http://data.worldbank.org/**.

[3] Facebook Login Approvals. **http://www.facebook.com/note.php?note_id=10150172618258920**.

[4] Facebook Reports Second Quarter 2013 Results. **http://investor.fb.com/releasedetail.cfm?ReleaseID=780093**.

[5] Ghana Economic Outlook. **http://www.afdb.org/en/countries/west-africa/ghana/ghana-economic-outlook/**.

[6] Google 2-Step Verification. **https://www.google.com/landing/2step/**.

[7] Hey! My friend's account was hacked! **http://blogs.windows.com/windows_live/b/windowslive/archive/2011/07/14/hey-my-friend-s-account-was-hacked.aspx**.

[8] John the Ripper password cracker - Openwall. **http://www.openwall.com/john/**.

[9] MTN. **https://www.mtn.co.za/Pages/Home.aspx**.

[10] The Quiet Mobile Giant: With 300M Active Users, WhatsApp Adds Voice Messaging. **http://allthingsd.com/20130806/the-quiet-mobile-giant-with-300m-active-users-whatsapp-adds-voice/**.

[11] WhatsApp :: Home. **http://www.whatsapp.com**.

[12] Yahoo 2-Step Verification. **https://edit.yahoo.com/commchannel/sec_chal_manage**.

[13] Measuring the Information Society. **http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf**, 2012.

[14] Global Virus Map. **http://home.mcafee.com/virusinfo/global-virus-map**, 2013.

[15] Bagchi, K., Kirs, P., and Cerveny, R. Global software piracy: can economic factors alone explain the trend?

Communications of the ACM 49, 6 (2006), 70–76.

[16] Ben-David, Y., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P., Chen, J., and Brewer, E. A. Computing security in the developing world: A case for multidisciplinary research. In *Proceedings of the 5th ACM workshop on Networked systems for developing regions*, ACM (2011), 39–44.

[17] Besmer, A., Watson, J., and Lipford, H. R. The impact of social navigation on privacy policy configuration. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM (2010), 7.

[18] Brewer, E., Demmer, M., Du, B., Ho, M., Kam, M., Nedevschi, S., Pal, J., Patra, R., Surana, S., and Fall, K. The case for technology in developing regions. *Computer 38*, 6 (2005), 25–38.

[19] Burrell, J. *Invisible users: Youth in the Internet cafés of urban Ghana*. Mit Press, 2012.

[20] Burrell, J. Technology hype versus enduring uses: A longitudinal study of internet use among early adopters in an african city. *First Monday 17*, 6 (2012).

[21] Cyr, D. Modeling web site design across cultures: relationships to trust, satisfaction, and e-loyalty. *Journal of Management Information Systems 24*, 4 (2008), 47–72.

[22] Cyr, D., Head, M., and Larios, H. Colour appeal in website design within and across cultures: A multi-method evaluation. *International Journal of Human-Computer Studies 68*, 1 (2010), 1–21.

[23] Dourish, P., Grinter, R. E., De La Flor, J. D., and Joseph, M. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing 8*, 6 (2004), 391–401.

[24] Egelman, S., Cranor, L. F., and Hong, J. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2008), 1065–1074.

[25] Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., and Herley, C. Does my password go up to eleven?: the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2013), 2379–2388.

[26] Everard, A., and Galletta, D. F. How presentation flaws affect perceived site quality, trust, and intention to purchase from an online store. *Journal of Management Information Systems 22*, 3 (2006), 56–95.

[27] Fair, J. E., Tully, M., Ekdale, B., and Asante, R. K. Crafting lifestyles in urban africa: Young ghanaians in the world of online friendship. *Africa Today 55*, 4 (2009), 29–49.

[28] Fischer, P., Kastenmüller, A., Greitemeyer, T., Fischer, J., Frey, D., and Crelley, D. Threat and selective exposure: The moderating role of threat and decision context on confirmatory information search after decisions. *Journal of Experimental Psychology: General 140*, 1 (2011), 51.

[29] Florêncio, D., Herley, C., and Coskun, B. Do strong web passwords accomplish anything. *Proc. Usenix Hot Topics in Security* (2007).

[30] Grinter, R. E., Edwards, W. K., Newman, M. W., and Ducheneaut, N. The work to make a home network work. In *ECSCW 2005*, Springer (2005), 469–488.

[31] Herley, C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, ACM (2009), 133–144.

[32] Herley, C., and Van Oorschot, P. A research agenda acknowledging the persistence of passwords. *Security & Privacy, IEEE 10*, 1 (2012), 28–36.

[33] Jakobsson, M., Tsow, A., Shah, A., Blevis, E., and Lim, Y.-K. What instills trust? a qualitative study of phishing. In *Financial Cryptography and Data Security*. Springer, 2007, 356–361.

[34] Karaganis, J. *Media piracy in emerging economies*. Lulu. com, 2011.

[35] Kim, J., and Moon, J. Y. Designing towards emotional usability in customer interfaces.trustworthiness of cyber-banking system interfaces. *Interacting with computers 10*, 1 (1998), 1–29.

[36] Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., and Wetherall, D. When i am on wi-fi, i am fearless: privacy concerns & practices in eeryday wi-fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2009), 1993–2002.

[37] Kowitz, B., and Cranor, L. Peripheral privacy notifications for wireless networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, ACM (2005), 90–96.

[38] Kuo, C., Romanosky, S., and Cranor, L. F. Human selection of mnemonic phrase-based passwords. In *Proceedings of the second symposium on Usable privacy and security*, ACM (2006), 67–78.

[39] Lindgaard, G., Dudek, C., Sen, D., Sumegi, L., and Noonan, P. An exploration of relations between visual appeal, trustworthiness and perceived usability of homepages. *ACM Transactions on Computer-Human Interaction (TOCHI) 18*, 1 (2011), 1.

[40] Mas, I., and Morawczynski, O. Designing mobile money services lessons from m-pesa. *Innovations 4*, 2 (2009), 77–91.

[41] Morris, R., and Thompson, K. Password security: A case history. *Communications of the ACM 22*, 11 (1979), 594–597.

[42] Norman, D. A. The way i see it when security gets in the way. *interactions 16*, 6 (2009), 60–63.

[43] Paik, M. Gotta catch'em all!: innoculous: enabling epidemiology of computer viruses in the developing world. In *Proceedings of the 5th ACM workshop on Networked systems for developing regions*, ACM (2011), 51–56.

[44] Pal, J., Nedevschi, S., Patra, R. K., and Brewer, E. A. A multidisciplinary approach to open access village telecenter initiatives: The case of akshaya. *E-Learning 3*, 3 (2006), 291–316.

[45] Panjwani, S. Towards end-to-end security in branchless banking. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, ACM (2011), 28–33.

[46] Rader, E., Wash, R., and Brooks, B. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM (2012), 6.

[47] Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q., and Li, S. A cross-cultural comparison of us and chinese computer security awareness. *Journal of Global Information Management (JGIM) 16*, 2 (2008), 91–103.

[48] Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., and Cranor, L. F. Encountering

stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM (2010), 2.

[49] Smyth, T. N., and Best, M. L. Tweet to trust: social media and elections in west africa. In *Proceedings of the Sixth International Conference on Information and Communication Technologies and Development: Full Papers-Volume 1*, ACM (2013), 133–141.

[50] Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., and Beznosov, K. What makes users refuse web single sign-on?: an empirical investigation of openid. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, ACM (2011), 4.

[51] Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. Crying wolf: An empirical study of ssl warning effectiveness. In *USENIX Security Symposium* (2009), 399–416.

[52] Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., Passaro, T., Shay, R., Vidas, T., Bauer, L., et al. How does your password measure up? the effect of strength meters on password creation. In *Proc. USENIX Security* (2012).

[53] Wash, R. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM (2010), 11.

[54] Wyche, S. P., Forte, A., and Yardi Schoenebeck, S. Hustling online: understanding consolidated facebook use in an informal settlement in nairobi. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2013), 2823–2832.

[55] Wyche, S. P., Schoenebeck, S. Y., and Forte, A. Facebook is a luxury: An exploratory study of social media use in rural kenya. In *Proceedings of the 2013 conference on Computer supported cooperative work*, ACM (2013), 33–44.

Appendix A: Interview Questions

Talking points for interviews, number of ∗ indicates priority.

Security Practices, Attitudes, and Anecdotes

∗∗∗**1.** Have any of your accounts ever been hacked or do you know anyone who has had an account hacked?

∗ ∗ ∗**2.** What do you do to stay safe on the Internet?

∗ ∗ ∗**3.** How often do you use a pen-drive?

∗∗**4.** Is there any personal information, or anything you wouldn.t want other people to see on your phone?

∗∗**5.** If someone hacked your email, what other things could he do with your email account? (do you use the same email/password for other services, etc.)

Internet

∗ ∗ ∗**6.** How do you tell which web pages are safe or trustworthy and which are not?

∗ ∗ ∗**7.** [Ask what their email address is, check what information is public on their G+ or FB profile - if they have Twitter or equivalent, check visibility of their stream]

∗∗**8.** Do you ever search for your own name online?

9 What websites do you regularly visit?

∗∗**10.** Do you spend a lot of time on social network sites like Facebook, Google+, or Twitter?

∗**11.** When you use the Internet, do you usually go online for something specific (score of a football match, today.s news, information about jobs) or do you .browse. by clicking through from page to page?

12 How would your life be different if you couldn.t use the Internet?

13 Do you use email or SMS more?

Mobile Phones

∗∗**14.** Can you show me the kinds of things you do using your mobile phone?

∗∗**15.** Does your mobile phone have a password? If so, is the password for the phone or for the SIM?

∗**16.** Why did you choose the mobile phone you chose?

Appendix B: Intermediate Data

Resp. ID	What do you do on the Internet	Staying safe on the Internet	Social networking	...
53	search for engineering, design, business research	privacy settings e.g. facebook	yes	...
54	mail, jobs, fb, news, games, entertainment	passwords on documents	yes	...
55	research	don't open certain sites	no	...
56	company, contacts, work	don't keep personal info, email is encrypted	seldom	...
57	interact with friends and colleagues			...
...	...	...	...	...

Table 7: A fragment of the data matrix for analyzing interview data. This matrix includes the characteristic behaviors and comments from interviews.