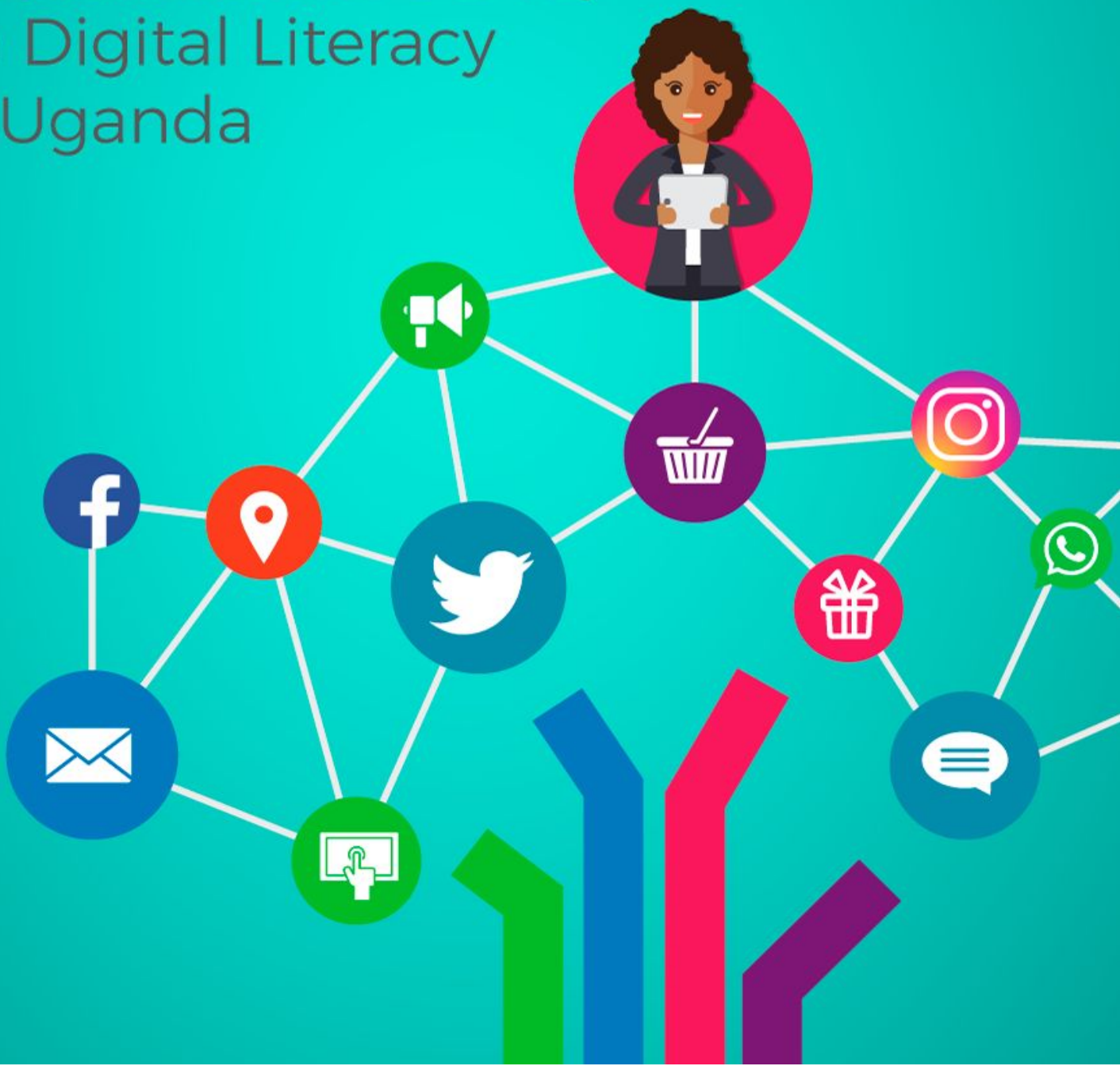
Ugandan Women Online

A Quantitative Survey on Digital Literacy in Uganda



About

Pollicy is a *civic technology organization* working to improve public service delivery for citizens in Uganda, and across Africa. We believe in the power of data, design and technology to revolutionize civic engagement and participation. Through new technologies, we plan to bridge data gaps from grassroot level all the way up to national level. Our passion is focused on influencing how this data is eventually used by governments, civil society and citizens.

Acknowledgements

This survey was conducted by Pollicy led by Neema Iyer. The data collection was conducted by Jovia Najjemba, Ndatsi Kaabeho and Zipporah Kekihembo. The visualization of the report was done by Neema Iyer. We would like to thank Helen Nyinakiiza and Neil Blazevic for their input and advice throughout the process.

This report was made possible through funding and support from Internews. A special thanks to Haley Slafer for her continued support and positivity!

Table of Contents

Summary

With a rise in technology use globally, Ugandans too have been rapidly growing their digital footprints. The country continues to experience growth in internet subscription. As part of the creation of a guide on digital security amongst women in East Africa, Pollicy conducted a short survey with women in the Kampala area to better understand their knowledge, attitudes and perceptions towards their digital security. The report compiles together 300 in-person interviews conducted in Kampala as part of the first deep dive looking into how women perceive their digital identities and respond to threats online.

Introduction

Uganda has seen tremendous growth in mobile penetration, and access to the internet. Teledensity estimates in 2015 were 64%[1]. The country also continues to experience growth in internet subscription, with a 37.4% internet penetration rate in the same time period. This has been largely attributed to proliferation of cheap smart phones and steady reduction in data costs. In 2016, the average cost for a daily 10MB mobile internet bundle was 300 Uganda Shillings (UGX) while in 2017 it reduced further to UGX 250. Similarly, a monthly 1GB bundle currently costs between UGX 30,000- 35,000 depending on the provider, compared to UGX 40,000 in 2016.

Legislation

With these advancements in access, there is also a marked rise in incidence of cybercrime such as fraud, hacking and identity theft. Cyber threats are causing economic losses for Uganda valued at UGX22[2] billion annually, as reported in the Africa Cyber Security Report 2016. The reasons given for the increase in the cost of cybercrime is due to increased sophistication of local cyber criminals and a lack of practical regulatory guidance from the government and industry stakeholders. Currently, the East African Community (EAC) has no specific legislation on data protection and privacy. There is only a framework[3] for Cyber laws which was developed in 2008[4].

While legislation on access and disclosure of information does exist in Uganda by way of the Computer Misuse Act, 2011, Access to Information Act, 2005, and Regulation of Interceptions of Communications Act, 2010, these laws do not adequately protect citizens from cyber threats and their perpetrators. In February

---

[1] UCC, Post, Broadcasting and Telecommunications Market and Industry Report, July-September 2015. 2015. http://www.ucc.co.ug/files/downloads/Q3-Market%20Report%20%20for%20Third%20Quarter%20-%20July-September%202015.pdf

[2] Serianu, African Cyber Security Report 2016: Achieving Cyber Security Resilience. 2016. http://observer.ug/news/headlines/54458-uganda-loses-shs-122bn-annually-to-cyber-attacks-says-report.html

[3] UNCTAD, Harmonizing Cyberlaws and Regulations: The experience of the East African Community. 2013. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Harmonizing%20cyberlaws%20-%20East%20Africa%20Community%20.pdf

[4] CIPESA Comments to Data Protection Bill. 2018. Available from https://cipesa.org/?wpfb_dl=263

2018, the Parliament of Uganda called for submissions on the Draft Data Protection and Privacy Bill, 2015 to provide stakeholders with an opportunity to provide input to ensure that the law complies with generally accepted international standards.

Violence against Women

An increasingly worrying trend amongst cybercrimes is online violence against women. More women in Uganda are online now than ever before. Private information, such as photos and videos, are leaked[5] onto social media without women's consent. Women are often victims of harassment, stalking and cyberbullying but the extent of this violence is unknown as most cases go unreported. In a recent U.N. report[6], cyber violence was found to be just as damaging to women as physical violence. The report goes on to indicate that women are becoming increasingly vulnerable to cyber violence with growing access to internet across the world, which could in turn detrimentally impede the uptake of broadband services by girls and women worldwide.

"Online violence has subverted the original positive promise of the internet's freedoms and in too many circumstances has made it a chilling space that permits anonymous cruelty and facilitates harmful acts towards women and girls"
- Phumzile Mlambo-Ngcuka, UN Women

Types of Cybercrime

There are numerous kinds of cybercrime, with women oftentimes bearing the brunt of certain acts such as cyber harassment, stalking and release of private information without consent.

---

[5] Franco, B.b. NAKED AMBITION: Ugandan celebrities whose nude pictures/sex videos have leaked. 28-01.2014; Available from: https://www.howwe.biz/news/lifestyle/622/naked-ambition-ugandan-celebrities-whose-nude-pictures-sex-videos-have-leaked

[6] Urgent action needed to combat online violence against women and girls, says new UN report. 24-09-2015; Available from: http://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release

1. ## Cyber Bullying and Harassment

   Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.This can include blackmail, threats of violence, sexual messages with the aim of discreting, defaming or subduing the victim.

2. ## Cyberstalking

   Cyberstalking is when an individual uses the Internet to systematically or repeatedly harass, stalk or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging clients and any other online medium. Cyberstalking can also occur in conjunction with the more traditional form of cyberbullying and offline harassment.

3. ## Sharing Private Data on Public Platforms without Consent

   This is essentially obtaining and disseminating private information such as photographs or videos, without consent, usually for purposes of defamation. A growing example of this is revenge porn, whereby naked pictures of women are leaked onto social media and oftentimes, the victims are attacked, shamed and made to apologize.

4. ## Identity Theft

   Identity theft is a crime in which an imposter obtains key pieces of personally identifiable information, such as a National ID number or driver's license numbers, in order to impersonate someone else for financial gain, or similar personal benefit on behalf of their victim.

5. ## Hate Speech

   Hate Speech is any communication with the intent to attack a person based on any identifying characteristics such as their race, religion, gender, opinions

etc.

6. ## Doxxing

   Doxxing is search for and publishing of private or identifying information about a particular individual on the Internet, typically with malicious intent. This information is typically meant for public consumption to target and contact a victim through social media, chat rooms, and perhaps even in person.

7. ## Trolling

   Trolling is the act of sowing discord on the Internet by starting arguments or upsetting people, by posting inflammatory or off-topic messages in an online community, usually on social media or a similar forum, with the intent of provoking readers into an emotional response or of otherwise disrupting normal, on-topic discussion.

8. ## Hacking

   Hacking is the unauthorized intrusion into a computer or a network, and is the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Hacking can be done to access or steal information such as passwords, data, documents etc.

Internews has been supporting digital security experts in East Africa to conduct trainings and to create content aimed at promoting increased uptake of online safety measures. As part of this work, this research was conducted to better understand the current landscape including measuring perceptions of digital security, knowledge and application of protection measures, and experiences of online harassment. Data was collected from 300 women in different areas of Kampala during a one week period in February 2018. The research is an effort to begin collecting data on women's experiences and knowledge so as to tailor content, trainings and advocacy for safer participation in the online world.

The main motivation for this research was insufficiency of data, particularly from women in different fields of work and life. There is little to no data on the online experiences of women regarding their safety and practices in East Africa. This report aims to begin this conversation on improving documentation within the region, and in Africa more broadly.

Objectives

This research report seeks to document the online experiences and digital security practices of women in Uganda, as part of an effort to tailor instructional content for women across the East Africa region on best practices when using the internet. The report utilizes both quantitative and qualitative data to assess both cyber harassment and digital literacy related to safety and security online. Lastly, the report aims to begin a broader conversation around collecting robust data on women's online experiences to advocate for more stringent regulations against cybercrimes and harsher penalties for perpetrators of actions such as cyberbullying and harassment.

Methodology

The survey was created in collaboration with digital security experts from Uganda. The study took on a quantitative cross-sectional research design that was conducted in Kampala, the capital city of Uganda. Kampala is divided into 5 administrative divisions – Central, Kawempe, Nakawa, Makindye and Rubaga, from which two communities were conveniently selected based on proximity and available resources. Respondents were randomly approached on the streets, markets, shopping malls and offices, which locations were purposefully selected for their densely populated nature. Respondent enrollment continued until the target sample size of ~300 respondents was reached. The target group for the study were women who owned smart phones, aged 15-65 years with access to internet services on their electronic devices.. A semi-structured interviewer-guided questionnaire derived from literature review and research experience was administered to the respondents. The questionnaire included demographic information as well as attitudes and perceptions towards digital security.

Participation in the interviews was voluntary, and informants were informed of the study purpose and data collection procedure in advance. The informants were informed of their rights as well as their freedom to withdraw from the interview at any point and were also reassured about the confidentiality of the information they shared.

Data were electronically collected using Kobotoolbox, and cleaned and analyzed in STATA version 13.1.

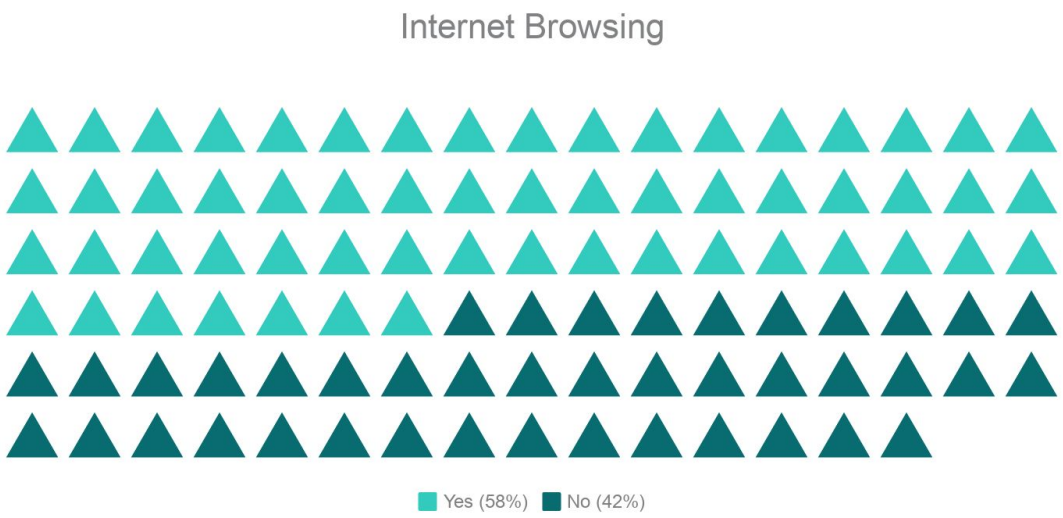
Analysis

Demographics

For this survey, only women who owned smartphones were included as participants. The mean age of participants was 30 years. A majority of women (42%) were college-educated with at least a Bachelor's degree. At the time of the survey, sixty percent of women were currently employed, while 40% were unemployed. The women who were actively employed worked within diverse sectors such as commerce, hospitality, education, health, civil society etc.

Internet Use

Forty-two percent of women surveyed claimed that they did not browse the internet. Fifty-six percent of respondents did not own a computer and solely used the internet on their mobile devices.



Perceptions of Security

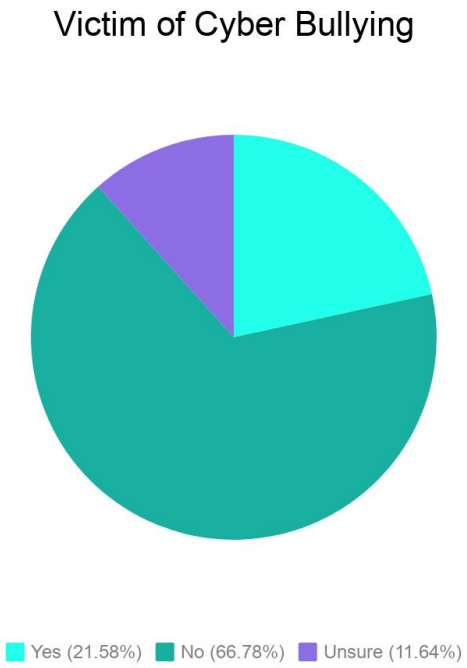
Overall, 92% of women were either concerned or very concerned regarding their physical security. Only 2% of the women were not concerned or not very concerned about their physical security. Conversely, only 55% of women were concerned or

very concerned about their digital security, with up to 10% not concerned about it at all. There were similar attitudes regarding identity theft, with 50% concerned and 12% not concerned.

In terms of self-reported knowledge, 65% of respondents claimed to know the crucial steps to take in response to their digital security. Only 8% of respondents did not feel confident that they knew how to adequately protect themselves online.

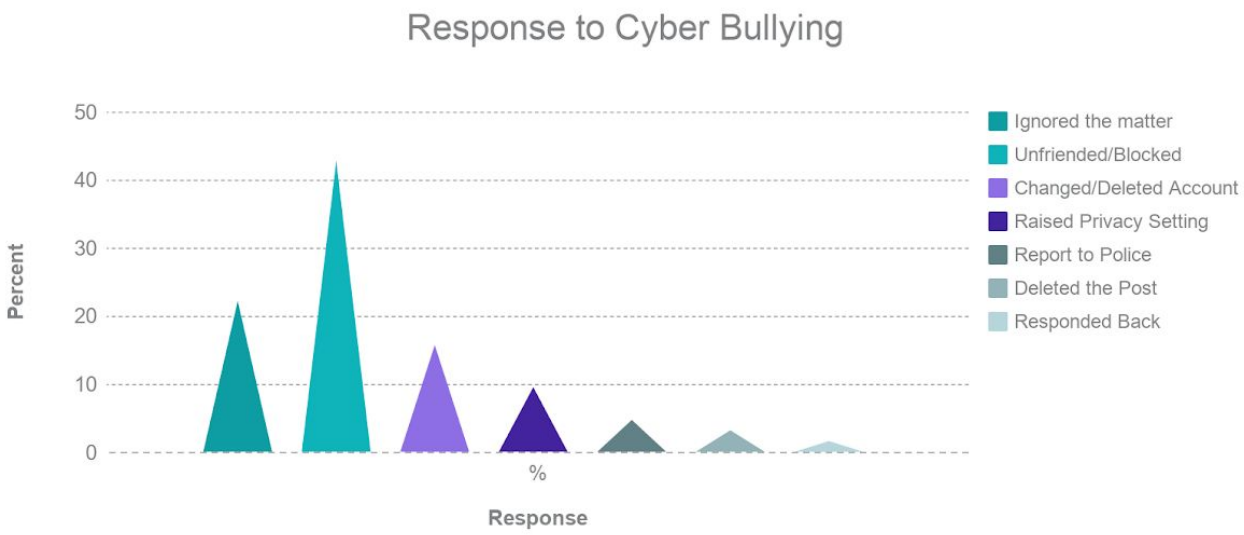
Cyberbullying

The respondents were asked if they had ever been a victim of online harassment of cyberbullying. Twenty-two percent of women surveyed claimed to have been a victim of cyberbullying, whereas 12% of women were unsure.



The survey went on to ask women who had been victims of cyberbullying about how they responded to the situation. 22% responded that they ignored their perpetrator while 37% said that they blocked them. 13% reacted by changing their

phone number or accounts altogether. Only 5% of victims reported the matter to the police.

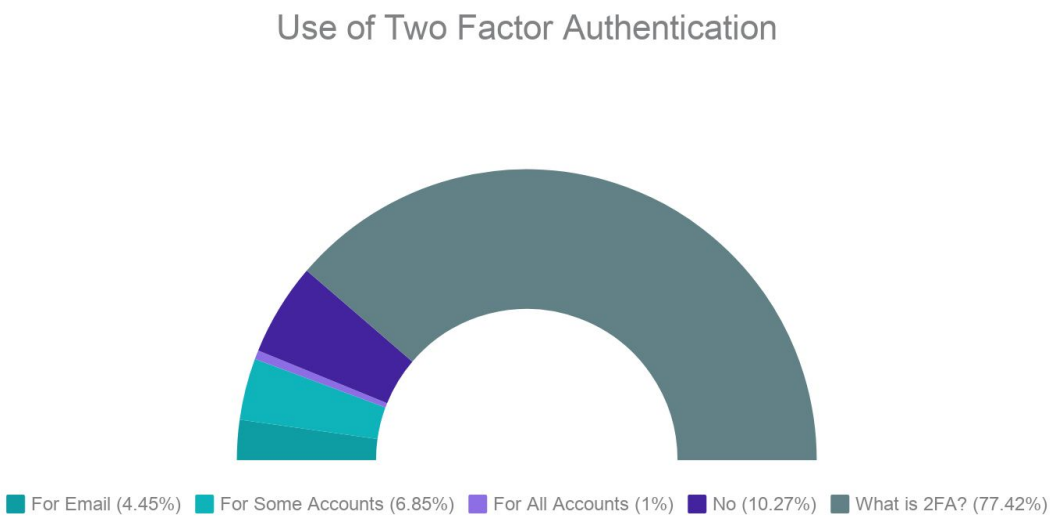


Knowledge and Use of Digital Security Tools

Women were queried on a number of techniques to protect themselves online. Overall, knowledge and use of digital tools was low.

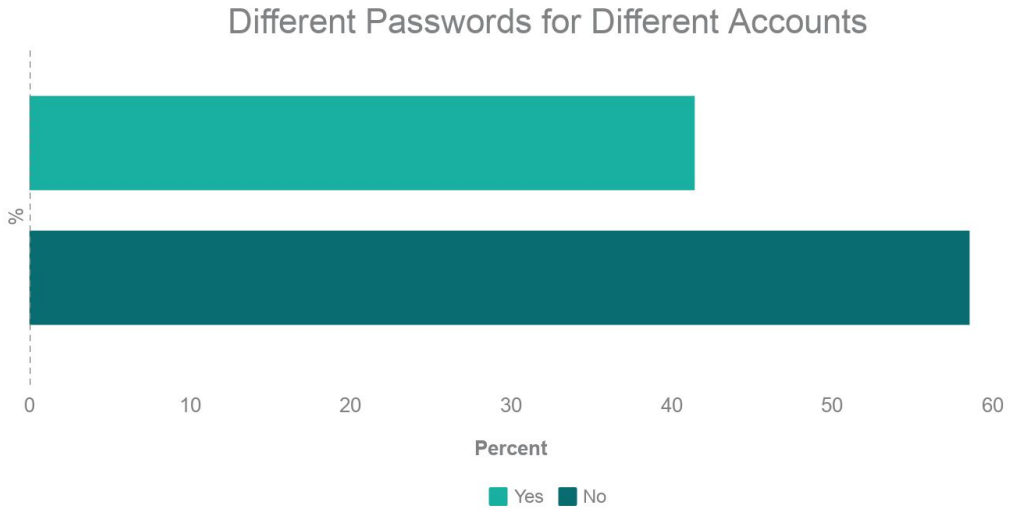
Two-Factor Authentication (2FA)

Seventy-seven percent of women surveyed did not know about 2FA. Ten percent said that they do not use it, which the remaining 11% said that they used it on their email or on some accounts. Only 1% of respondents claimed to use it on all their accounts



Passwords

Fifty-nine percent of participants do not use different passwords for different accounts. That means that 59% of women surveyed use the same password across all their accounts.

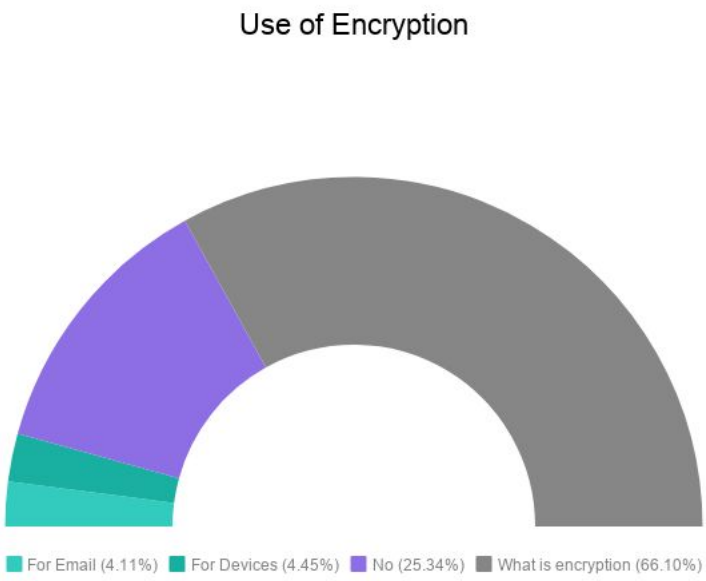


Only 17% of women said that they shared their passwords with their friends, loved ones or colleagues. Eighty-four percent of women used a password to unlock their phones.

In terms of changing passwords, 70% of women said that they never changed their password for their email accounts, whereas 57% of women said they never changed passwords for their social media accounts. A majority of respondents only changed their passwords when prompted to do so or when they forgot the password associated with the account.

Encryption

Sixty-six percent of women did not know what encryption means, whereas 25% of the women stated that they did not use encryption at all. Of the remainder who did use encryption, 4% said that their devices were encrypted and 4% said that their emails were encrypted.

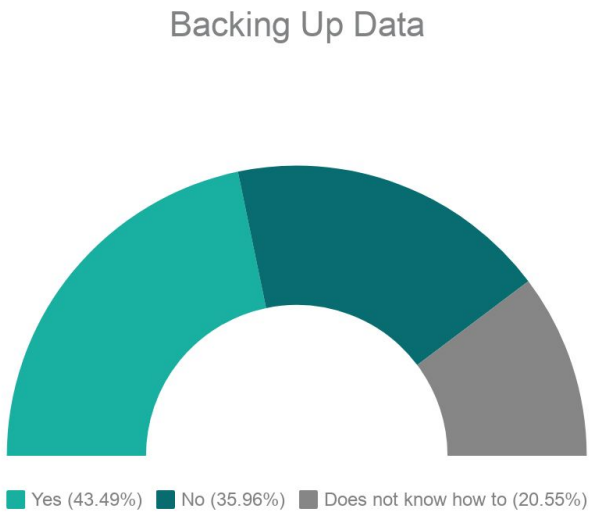


Anti-virus

A majority of respondents (56%) did not own a computer. Of those who did, 40% said that they were currently using an anti-virus, whereas 5% said that they did not have an anti-virus installed.

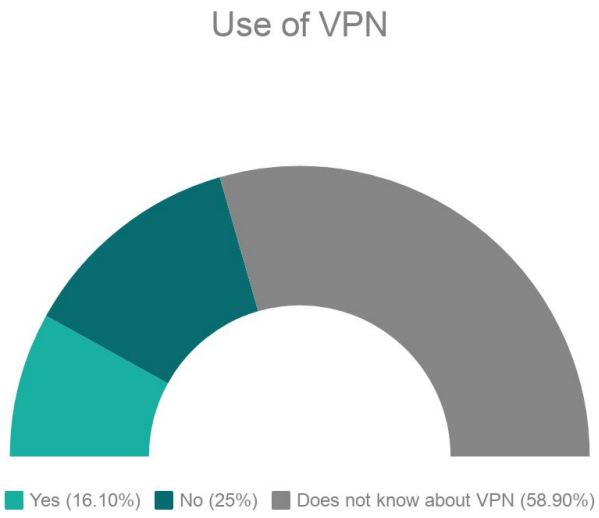
Backup Data

Twenty-one percent of respondents did not know what it means to back up data. While 44% of the women stated that they knew how to back up their data, 36% responded that they do not know how to back up their data.



VPN

When queried on VPN knowledge, 59% of women did not know about the concept of VPNs. Twenty-five percent of women had never used a VPN previously, whereas 16% of the women had used a VPN in the past.

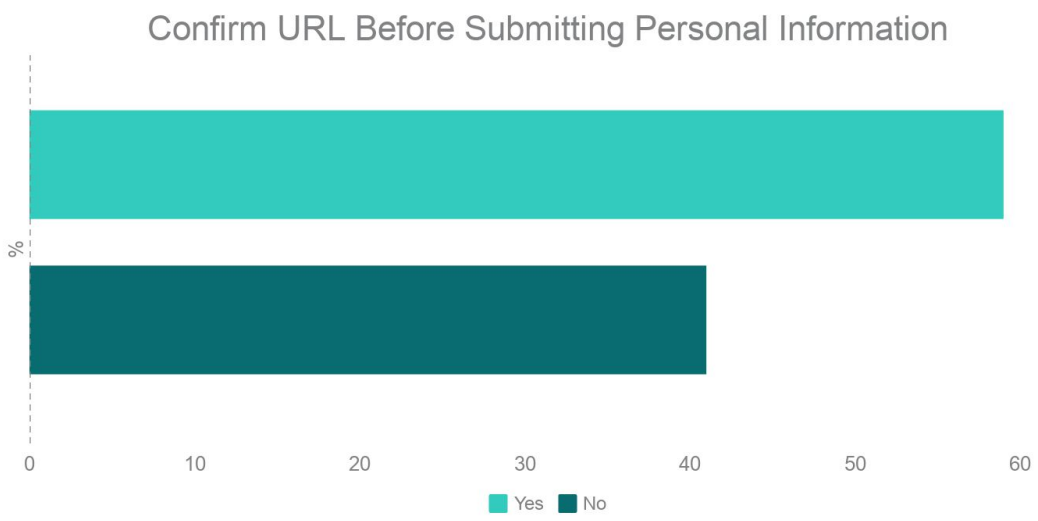


Geotagging

The women surveyed seemed to have the most knowledge in relations to geotagging on social media platforms. Of the respondents, 40% stated that they do not give permissions to their devices to access their location. Thirty-two percent said that they do, 15% stated that they sometimes do whereas 13% were not sure.

URL Confirmation

Surprisingly, of the women surveyed, 42% claimed that they do not actually browse the internet. Out of those who do browse the internet, 59% do check of the website before entering in private information whereas 41% do not.



Further Explorations

The last question of the survey was open-ended and asked participants what they might like to learn about digital security.

The main topics mentioned include:

1. How to report a harasser?
2. How do hackers operate?
3. How to prevent hacking?
4. What happens to data that has been illegally acquired?
5. How to retrieve a device after theft?
6. How to secure personal information, social media accounts and passwords?
7. What is digital security?

Research Limitations

1. The research was conducted by enumerators in several locations around Kampala using a largely quantitative survey. Given that the surveys were conducted in person, there is likely to be response bias to appear more favorable by providing socially desirable answers to the questions.

2. The topic of digital security is still quite nascent in Uganda and it is likely that the participants did not understand the questions being asked, and as such may not have provided appropriate or accurate responses. We provided a basic training to the enumerators on the topic to enable them to clarify any difficult topics to the survey participants.

3. The surveys were only conducted with women who possessed at least a smartphone. It was assumed that in order to ask questions regarding digital security, the basic criteria to judge access to the internet would be a smartphone. Due to this measure, several women were not included in the survey and these numbers are not known. There is definitely a digital divide in access to information communication technology amongst men and women, as well as in access to basic feature phones versus smartphones amongst women of different socio-economic groups. However, women without a smartphone might have access to computers at a school or place of work. In future surveys, it would be beneficial to include these women to better understand their access and attitudes as well.

Recommendations and Conclusion

Based on the results of this report, we found that knowledge around digital security amongst women in Kampala is quite low. A high proportion of women have been victims of cyberbullying without any obvious routes to seeking justice against perpetrators. There is an urgency for law enforcement and government to hand down stricter penalties for offenders and to provide measures that protect women from online gender-based violence. Furthermore, there is a large role for service providers and civil society to play in building the capacity of women to take precautionary steps to protect their online identities as well as to advocate for regulations and policies that can readily address the growing and changing threats to digital safety and security. As more women continue to access the internet, we must focus on keeping the internet a safe space where these women can benefit rather than become victims of violence and fraud.

Our Recommendations:

Law Enforcement
Maintain personnel who have been through gender-sensitized digital security training to address complaints of cyberbullying, cyber harassment, leaked private information etc. and to provide assistance, counselling and legal support to these women.

Civil Society
Create awareness campaigns in local languages to highlight key issues around digital security to foster dialogue around safety when accessing the internet. Conduct capacity building for women to improve their digital literacy skills through the use of free tools, to better understand online threats and to learn how to take action against these threats.

Private Sector
Work with developers to create digital tools and products that are suited to local contexts and that can be accessed in local languages. Features should be easy to access, utilize and troubleshoot.