The State of Access to Digital Tools, Usage of ICT and Digital Threats to CSOs in Uganda:

A Baseline Study

SEPTEMBER 2024

About this Baseline Study

This Baseline Study is a product of the USAID/Uganda's Civil Society Strengthening Activity (CSSA). USAID/Uganda's CSSA is made possible by the support of the American people through the United States Agency for International Development (USAID). The CSSA is a seven-year USAID-funded Activity implemented by East-West Management Institute (EWMI) in partnership with the International Center for Not-for-Profit Law (ICNL) and a number of local CSOs. This Policy Brief falls under Component 3 of CSSA, whose objective is to promote a more enabling environment that sustains a vibrant civil society in Uganda.

The State of Access to Digital Tools, Usage of ICT and Digital Threats to CSOs in Uganda:

A Baseline Study

Published in September 2024

Table of Contents

Abbreviations and Acronyms

2FA	Two-factor authentication
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
COVID-19	CoronaVirus Disease 2019
CSO	Civil Society Organisation
EWMI	East West Management Institute
GBV	Gender Based Violence
HTTPS	HyperText Transfer Protocol Secure
ICNL	International Center for Not-for-Profit Law
ICT/s	Information and Communication Technologies
LAN	Local Area Network
NDP III	National Development Plan III
NITA-U	National Information Technology Authority
OTT	Over-the Top
PDM	Parish Development Model
SDG/s	Sustainable Development Goals
SSL Certificates	Secure Sockets Layer Certificates
VAT	Value-Added Tax
VPN/s	Virtual Private Networks

1. Introduction

This report documents the findings of a baseline study on access to and use of digital tools by civil society organisations (CSOs) and activists in Uganda. It explores the capacity of CSOs to use digital tools in response to emerging digital threats while engaging in human rights advocacy, collaboration and accountability initiatives. The report identifies the various forms of digital threats that CSOs face and the effectiveness of the approaches that CSOs adopt to mitigate these threats, about the status of access to digital security tools.

1.1 BACKGROUND TO THE STUDY

In recent years, as journalists, human rights defenders (HRDs) and CSOs beyond and in Uganda have harnessed technology to build movements, promote transparency and accountability in governance and respect for human rights. There has been an unprecedented increase in threats to their work. These threats are exacerbated by hostile environments online and offline maintained by autocratic governments. These environments have become more precarious in the wake of the Coronavirus 2019 (COVID-19) pandemic, which has seen the introduction of additional restrictive measures that stifle civic engagement and critical reporting.

Common digital threats include censorship, surveillance, disinformation, and misinformation campaigns, among others.[1] Digital threats have manifested and have narrowed the space for fundamental rights and freedoms including the exercise of expression and access to information, privacy, assembly, association and movement of persons.

Whereas uptake of various online platforms and tools is on the rise, there is a cross-section of activists who do not understand the nature and scope of the prevailing digital threats. On the other hand, access to and use of digital technology has been limited by high tax levies on data and devices and government controls such as network disruptions which have included the partial or complete blockage of access to the internet or social media platforms.

To promote safety and resilience online, it is important to understand the current state of play including the extent of access to, and usage of technology among CSOs, journalists, HRDs and activists, and the prevailing threats, in order to identify needs, capacity gaps and effective response measures.

1 CIPESA, State of Internet Freedom in Africa Report, 2021 "Effects of State Surveillance on Democratic Participation in Africa," http://cipesa.org/download/State-of-Internet-Freedom-in-Africa-2021-Report.pdf.

Uganda's Information and Communication Technologies (ICT) sector has experienced commendable growth over the past three decades.[2] With the help of innovation for self-reliance, the ICT private sector has expanded significantly to become a key contributor to national revenue, contributing up to 19.8 percent annually.[3]

As of January 2022, there were 13.92 million internet users in Uganda, representing an internet penetration rate of 29.1 percent of the total population.[4] There are an estimated 69 active telephone subscriptions per 100 inhabitants.[5] For the majority of Ugandans, the internet remains out of reach, particularly in rural areas, where 75.5% of Ugandans live. Universal and affordable access have remained unattainable due to high taxation despite the expansion of infrastructure.[6]

Currently, the net price of internet data is subject to a 12% tax in addition to the 18% Value-Added Tax (VAT).[7] The 12% levy replaced the Over-the Top (OTT) tax[8] introduced in 2018, which failed[9] to generate the anticipated revenues.[10] Multiple taxes end up being a burden transferred to consumers; this exacerbates accessibility and affordability issues.

As of January 2022, there were 13.92 million internet users in Uganda, representing an internet penetration rate of 29.1 percent of the total population.

2 Freelyformd, "The History of Uganda's ICT Sector," January 31, 2020, available at https://freelyformd.com/the-history-of-ugandas-ict-sector/ (accessed September 13, 2022)

3 Ministry of Information and Communications Technology "ICT Sector Strategic and Investment Plan (2015/16 – 2019/20)," available at http://ict.go.ug/wp-content/uploads/2020/02/ICT-Sector-SIP.pdf.

4 Uganda Communications Commission, "Market Performance Report 2Q22," available at https://www.ucc.co.ug/wp-content/uploads/2023/10/UCC-June-2022-Market-Intelligence-Report.pdf.

5 Uganda Communications Commission, "Market Performance Report 1Q22," available at https://www.ucc.co.ug/wp-content/uploads/2023/10/UCC-March-2022-Market-Intelligence-Report.pdf.

6 Research ICT Solutions, "ICT Sector Taxes in Uganda: Unleash, not Squeeze, the ICT Sector," https://s3-eu-west-1.amazonaws.com/s3.sourceafrica.net/documents/119695/Unleash-Not-Squeeze-the-ICT-Sector-in-Uganda.pdf (accessed September 13, 2022)

7 Reuters, "Uganda introduces 12% internet data levy, critics say move will stifle online access," April 30, 2022, available at https://www.reuters.com/world/africa/uganda-introduces-12-internet-data-levy-critics-say-move-will-stifle-online-2021-04-30/ (accessed September 13, 2022)

8 Benson Tumusiime, "OTT tax stops today," The Monitor, June 30, 2021, available at https://www.monitor.co.ug/uganda/news/national/ott-tax-stops-today-3455434 (accessed September 13, 2022)

9 Daniel Mwesigwa, "Uganda Abandons Social Media Tax But Slaps New Levy on Internet Data," CIPESA, July 1, 2021, available at https://cipesa.org/2021/07/uganda-abandons-social-media-tax-but-slaps-new-levy-on-internet-data/ (accessed September 13, 2022)

10 CIPESA, "Digital Taxation in Uganda: A Hindrance to Inclusive Access and Use of Digital Technologies, 2022" available at https://cipesa.org/wp-content/uploads/2022/04/Digital-Taxation-in-Uganda-A-Hinderance-to-Access-and-Use-of-ICTS.pdf (accessed September 13, 2022)

Meanwhile, a 2020 research by the World Wide Web Foundation found that the gender gap in basic internet access in Uganda is 42.9% (19.2% women and 27.9% men), which is still lower than the regional average for Africa of 49.6%.[11]

According to the 2022 nation-wide survey by the National Information Technology Authority - Uganda (NITA-U),[12] 94.3% of the households did not have internet access at home with 13.4% reporting connectivity in Urban areas and only 3.2% reporting connectivity in the rural areas.[13]

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) supported by the USAID/Uganda Civil Society Strengthening Activity (CSSA), a USAID-funded Activity implemented by East-West Management Institute (EWMI) in partnership with the International Center for Not-for-Profit Law (ICNL), sought to establish the state, access and use of digital tools so as to troubleshoot the CSOs' vulnerability to digital threats.

The specific objectives that guided the study were:

1. To assess the utilization of digital tools by CSOs, journalists, HRDs and activists in Uganda.
2. To assess the status of access to digital security tools by CSOs, journalists, HRDs and activists engaging in human rights advocacy, voice, and accountability activities in Uganda.
3. To assess the capacity and digital literacy levels of CSOs engaged in human rights advocacy, voice, and accountability activities.
4. To identify common and trending digital threats faced by CSOs and journalists engaging in human rights advocacy, voice, and accountability activities in Uganda.

This report forms the basis for CSOs, journalists and HRDs reflections on their digital security preparedness, including identifying and applying digital security measures and strategies to protect their work.

1.2 STUDY METHODOLOGY

The study employed a mixed methods approach which investigated Knowledge, Attitudes, and Practices (KAP). In particular, an online survey coupled with desktop research and key informant interviews helped collect sufficient data to capture the capacity, perceptions, experiences and aptitudes of civil society actors and organisations engaged in human rights advocacy, voice, and accountability activities.

11 World Wide Web Foundation, "WOMEN'S RIGHTS ONLINE: Closing the digital gender gap for a more equal world, 2020," http://webfoundation.org/docs/2020/10/Womens-Rights-Online-Report-1.pdf

12 NITA-U, "National Information Technology Survey 2022," available at https://www.nita.go.ug/sites/default/files/2022-12/National%20IT%20Survey%20Report%202022%20-%20Final.pdf (accessed April 03, 2024)

13 Ibid.

The survey was administered to 80 respondents from 80 organisations through Microsoft Forms between July and September 2022. The CSOs reached work in the Central (36.25%), Eastern (3.75%), Nationwide (18.75%), Northern (20%), South Western (5%), West Nile (6.25%) and Western (10%) regions. The survey included the use of structured and unstructured questions on CSOs' experiences in access to digital tools, usage of ICT, capacity of CSOs, the rate and extent of exposure to digital threats and the response mechanisms. The questionnaires targeted key decision makers in CSOs defending human rights across the themes of Women Rights, Children Rights, LGBTQI+ Rights, Health Rights, Environmental, Land and Extractives. The key decision makers consulted include Executive Directors, Program Managers, Department Heads and Advocacy Officers.

The quantitative survey responses were coded and analysed using the STATA 17 data analysis programme while the qualitative responses were transcribed to identify themes. In the presentation of study results, some direct quotations are chosen and used to ensure originality of text.

Various research reports, government policy documents and other publications and unpublished works were reviewed with a focus on literature that documents record of ICT, its application and usage in the country. The study was able to compare data from different sources including the government and its agencies and the private sector such as telecommunication companies (telcos) and internet service providers (ISPs) as well as CSOs. This approach enabled the researchers to analyse the existing data on access, affordability, and usage and reach concrete findings and conclusions.

2. Baseline Study Findings

2.1 SUMMARY OF KEY FINDINGS

The survey establishes that 34.1% of all Internet users had been victims of a virus or other computer infection in the last 12 months. Of all persons who had fallen victim to online attacks, only 3.0% had ever reported the attacks.[14]

2.2. CHARACTERISTICS OF THE POPULATION CONSULTED

The study involved consultation with youth and adults including women and men. In terms of age, the respondents were constituted by 18-29 years (30%), 30-39 years (47%), 40-49 years (20%), 50-59 years (1.25%) and 60 years and above (1.25%). In terms of gender, 67.5% were male, 26.25% were female and 6.25% were non-binary.

Individuals consulted were drawn from organisations working on different issues including digital rights advocacy (18.75%), environmental rights advocacy (6.25%), health rights advocacy (3.75%), Land and Extractives (5%), LGBTQI+ rights advocacy (7.5%), media and journalism (25%), voice and accountability (16.2%) and women's rights advocacy (17.5%).

In terms of the period spent in the CSO sector by the respondents, those who had worked for less than five years constituted 56.96%, five to ten years were 35.44% while those who had worked for ten or more years were 7.9%.

2.3 ACCESS, USAGE OF DIGITAL TOOLS

The majority of respondents (98.8%) had access to a laptop or a computer, with personal and organisational work being the primary purpose of use for 76.6% of those surveyed.

Graph 1: Utilisation of Computer or Laptop by Respondents

14 Ibid

Windows was the most popular operating system - used by 90% of respondents, followed by Mac OS (8%) and Linux (1.25%).

Graph 2: Do you Use Mobile Phones to Access Work Related Resources?

96.3%

Yes

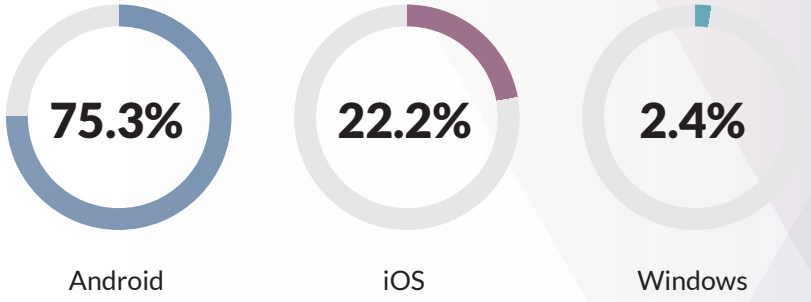
3.7%

No

Mobile phone access and usage were most popular, with nearly all respondents (96.3%) using their mobile devices to access work-related applications and resources compared to 3.7% who did not.

Majority of respondents (75.3%) indicated that they used Android phones, while 22.2% said they used IOS phones, with only 2.4% reporting use of Windows-based smartphones.

Graph 3: Type of Smartphones Used to Access Work Related Resources



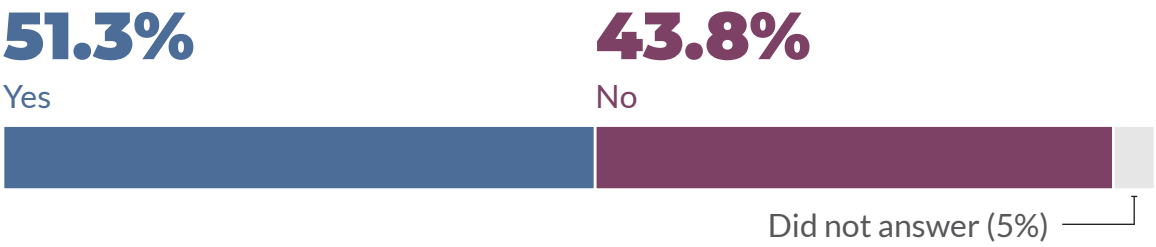
The primary means of internet access was office Wifi (50.41%). Other respondents indicated accessing the internet via Smartphone Hotspots (40.50%) and Local Area Network (LAN) cable (9.09%).

> Mobile phone access and usage were most popular, with nearly all respondents (96.3%) using their mobile devices to access work-related applications and resources.

2.4 UTILISATION OF CLOUD COMPUTING RESOURCES

Cloud computing services such as Google Workspace, Microsoft 365 and Dropbox provide on demand computing resources such as data storage and software.[15] These services have become popular in the wake of the Covid 19 pandemic, which saw many organisations adapt remote working models.

Graph 4: Usage of Cloud Resources



The study found that 51.3% of the organisations used cloud computing services while 48.8% said they did not use any cloud services.

2.5 ACCESS TO GENUINE SOFTWARE AND MAINTENANCE

Genuine computer software protects computers from external attacks including malware and spyware, viruses and bugs.[16] Genuine software also strengthens privacy of individuals, data and information. The study explored the use of genuine software by the respondents. Of the 79 respondents, 41% were not sure whether they were using outdated, bootleg or counterfeit software on their computers. 35% indicated that they were using genuine software while 24% indicated that they were using outdated, bootleg or counterfeit software on their computers. The responsibility for installing and updating software on respondents' computers varied across organisations with some having dedicated staff (IT Officers or Administrators) while others indicated that it was individuals' responsibilities. Similarly, there were differences in frequency of installation of updates.

Only 17.72% of respondents indicated running updates monthly. Those who run weekly updates were 12.66%, while 8.86% were running annual updates. Incidentally, only 3.8% were updating their software daily while 7.6% had never run any software updates on their computers.

15 AWS, "What is Cloud Storage?" https://aws.amazon.com/what-is/cloud-storage/#:~:text=Cloud%20storage%20is%20a%20cloud,your%20own%20data%20storage%20infrastructure.

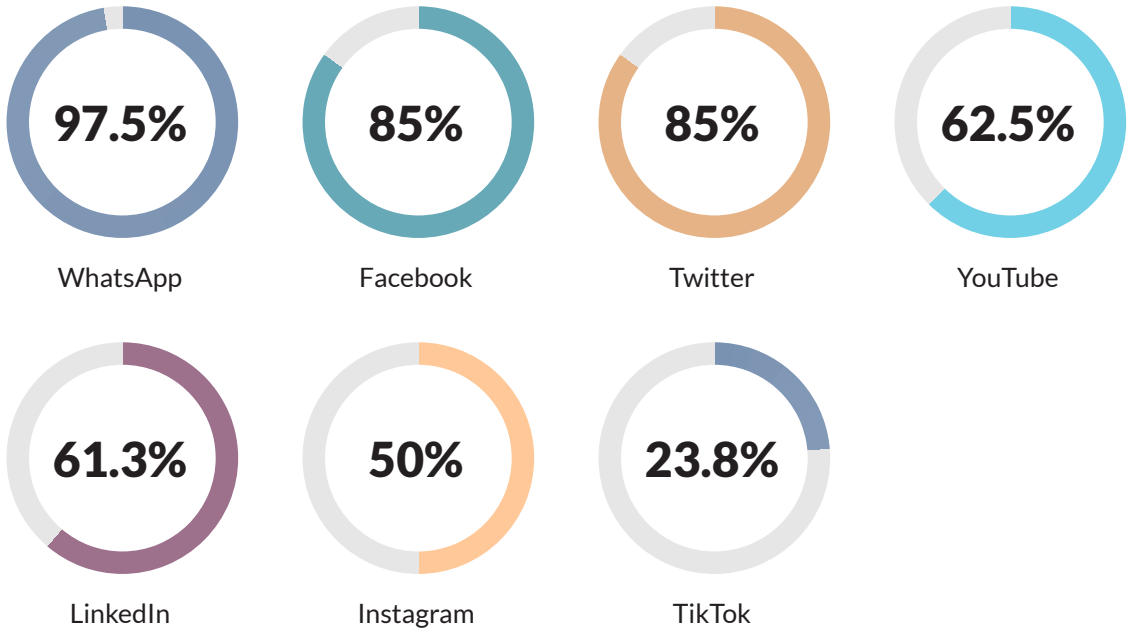
16 Malware encompasses malicious software like viruses, spyware, and worms designed to harm computers. Viruses are programs that replicate and damage files, spreading through downloads or attachments. Bugs are software errors, not malware, causing system issues and security vulnerabilities. See "What is Malware? Malware Definition, Types and Protection – Malwarebytes," https://www.malwarebytes.com/malware; and Clicked Online, "Benefits of Genuine Software," https://press.farm/6-benefits-using-genuine-software/.

2.6 WEBSITE AND SOCIAL MEDIA USAGE

While 80.8% of the respondent organisations maintained websites, 16.7% did not. However, there was widespread organizational use of social media platforms: 85% of respondents said their organizations used Meta (Facebook), 82.5% used Twitter, 41.3% used YouTube, 36.3% used Linkedln, 28.8% used Instagram while 11.3% indicated that they use other social media networks.

Personal social media usage was also high, led by WhatsApp at 97.5%, Facebook at 85% and Twitter at 85% (see graph 5 below for full data). As with software installations and updates, the role of social media management was assigned to different staff including Communication Officers, IT Officers, Social Media Managers, Online Content service providers, team leaders and in some cases all staff.

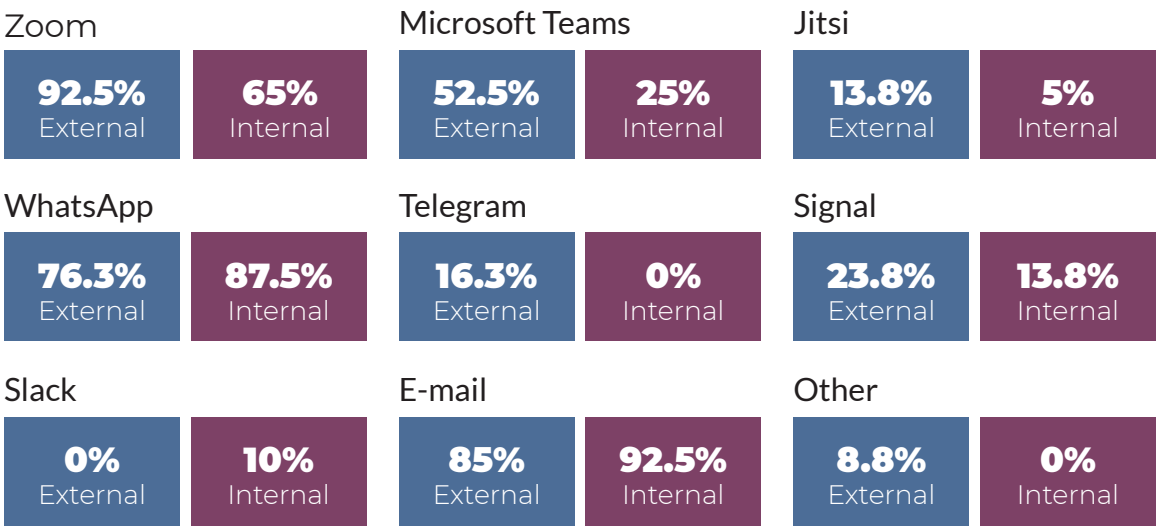
Graph 5: Personal Social Media Usage in Percentages (%)



3. Digital Communication Platforms

The research also sought to identify the types of digital channels used by organisations for internal and external communication. Organisations used a combination of channels including virtual conferencing platforms, instant messaging platforms and email.

Graph 6: Preferred Communication Tools



3.1 EFFECT OF ACCESS TO DIGITAL RESOURCES ON PRODUCTIVITY

Overall, it was agreed that access to and use of digital tools promoted efficiency, helped streamline operations and improved service delivery.

According to respondents:

> "Without digital tools I would be unable to do my work. I am a field worker, so when I am connected to the internet, I can effectively transfer documents and communicate with people at the Kampala headquarters, making my work easy. So, access to digital tools have increased efficiency at work without an added cost of travel." (Respondent 1)

> "It has played a very significant role in executing my work. I can very easily communicate with my team and other stakeholders. I can also communicate to different stakeholders in different regions at the same time. Access to digital tools has also made research and access to information very easy. Access to digital tools enables me to spend less time executing my work. I work with excel sheets and these can compute data and draw conclusions at a much faster rate than when we were doing this manually." (Respondent 2)

However, difficulties arise when working in areas with poor or non-existent network connectivity or where connectivity is intermittent at best. Similarly, internet censorship especially through levy of high taxes and through internet shutdowns or internet throttling during elections has gradually impacted productivity and efficiency. Furthermore, respondents claimed that the lack of an effective internet infrastructure in rural areas prevented internet-based businesses from offering their services nationally. However, they remained concerned that the high prices of ICTs made widespread internet and computer use impractical.

One of the respondents noted,

> "Our efforts to combat gender-based and sexual violence have been hampered by the lack of digital tools like cameras, phones, and computers. We can record witness accounts for evidence or take pictures of the victim thanks to cameras, or at the very least, smartphones.
>
> The network in our area is very poor. It is on sometimes and off a lot of the time. This affects communication in real time and has subsequently affected our response to gender-based violence cases."

Another respondent observed that:

> "Digital tools such as computers are very expensive. They also go hand in hand with the internet. A computer without the internet affects our ability to work remotely and deliver on the assignment. Because of the high cost of these tools, we end up buying substandard or second-hand gadgets (like phones and computers). This also affects our work; a cheaper phone will affect the quality of the audio of a phone interview recording, and a substandard computer will limit the type of software you can install."

4. Digital Safety and Protection

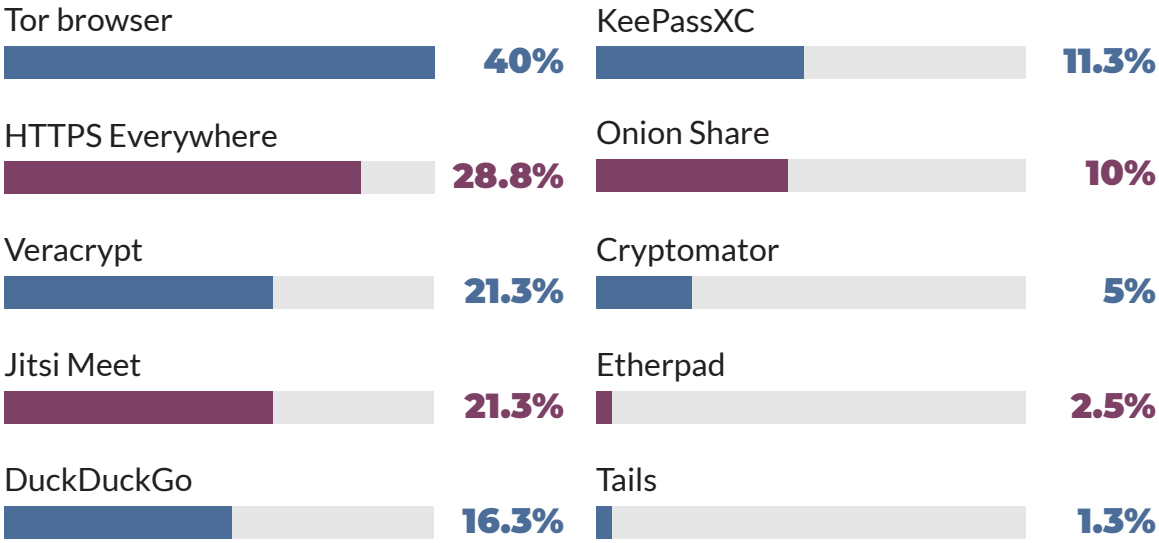
4.1 ACCESS TO DIGITAL SECURITY TOOLS AND MECHANISMS

The use of digital security tools is important for data protection measures including data backups, creation, management and implementation of strong passwords and navigation of digital restrictions.[17]

Digital hygiene awareness and putting in place necessary measures was found to be limited among the respondents. For instance, frequency of change of Wi-Fi passwords was low with only 19.74% indicating change of passwords monthly. Other practices included frequent use of free Wi-Fi, following links received from unknown sources, use of unlicensed software and lack of SSL certificates for organisation websites. Cost was highlighted as a key barrier for adoption of safe practices. As stated by one respondent, "genuine software and programmes are expensive, so most people have to use pirated copies."

The survey investigated the organisations' familiarity with various digital security tools including for secure communications, circumvention and encryption. Respondents were most acquainted with the Tor Browser (25.4 percent). Awareness about other tools was limited: Veracrypt (13.4 percent), HTTPS Everywhere (18.25 percent), Jitsi Meet (13.4 percent), DuckDuckGo (10.32 percent), KeePassXC (7.1 percent), Onion Share (6.3 percent), Cryptomator (3.1 percent), Etherpad (0.7 percent), and Tails (0.7 percent).

Graph 7: Familiarity of Respondents with Digital Security Tools

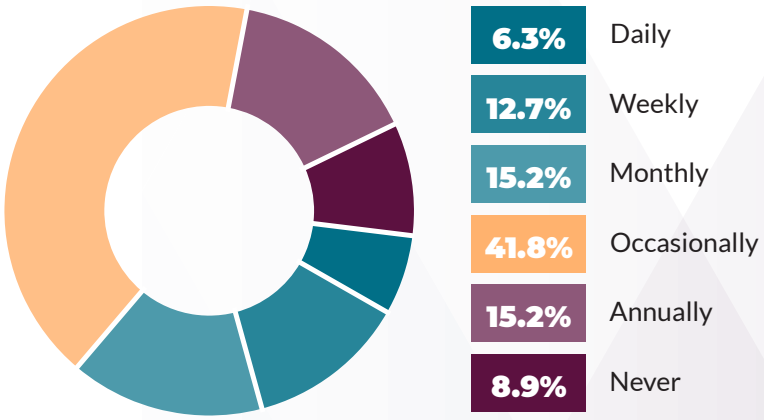


17 Digital Security Tools Clinics in the Context for Human Rights Defenders, https://outbox.co.ug/outbox-stories/digital-security-tools-clinics-context-human-rights-defenders#:~:text=Protecting%20data%2C%20looking%20at%20basic,accessing%20blocked%20or%20censored%20content ; gb-advisors, "5 types of digital security tools every company should have," https://www.gb-advisors.com/5-types-of-digital-security-tools-every-company-should-have/

Whereas there was some level of awareness of some tools, the frequency of their use was mostly occasional.

Notably, use of antivirus software was widespread. Over three quarters of respondents (77.5%) used antivirus to protect against malware and against spyware attacks. However, the frequency of updates was again not regular.

Graph 8: Updating Anti-Virus Tools

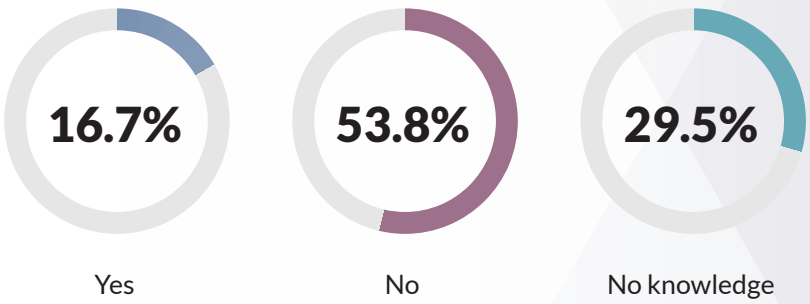


Most respondents run antivirus updates occasionally (41.77%), followed by monthly (15.19%), annually (15.19%), weekly (12.66%), and daily (6.33%). 8.86%, on the other hand, indicated that they never update their anti-malware software.

4.2 USE OF VIRTUAL PRIVATE NETWORKS AND ENCRYPTION

Virtual Private Networks (VPNs) and encryption play an important role in safety of data and communications. Knowledge of tools such as Pretty Good Privacy (PGP) encryption for email was low.

Graph 9: Do You Use PGP for Encryption?

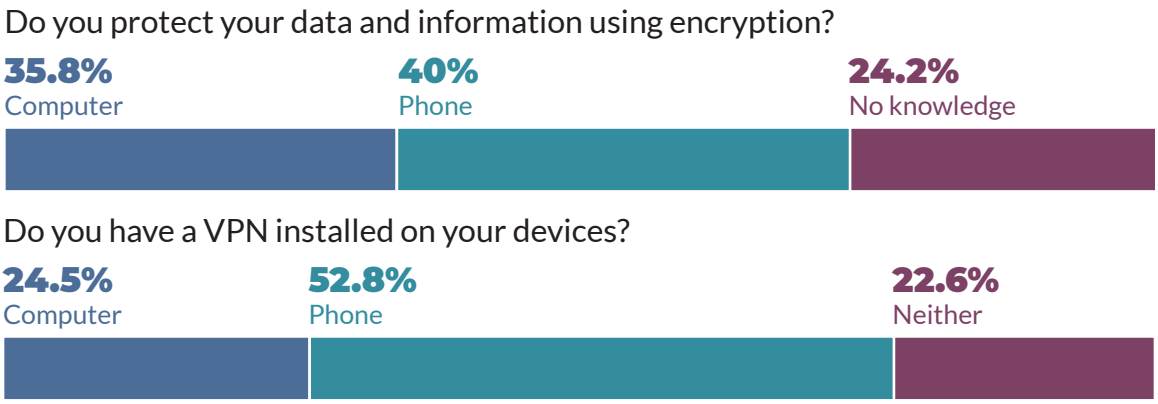


> Virtual Private Networks (VPNs) and encryption play an important role in safety of data and communications. Knowledge of tools such as Pretty Good Privacy (PGP) encryption for email was low.

The majority of respondents (53.85%) did not use PGP while 29.5% had no knowledge of it. Only 16.7% had used it before.

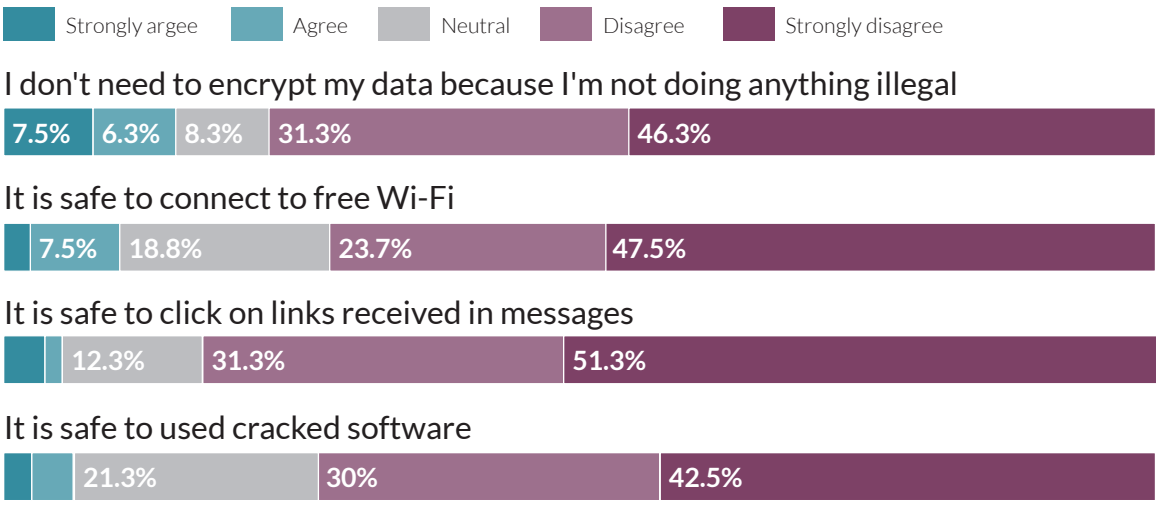
Similarly, use of encryption for data storage was low. About a third of respondents (35.79 percent) encrypted data stored on their laptops or desktop computers, while 40 percent encrypted their data stored on smartphones. On the other hand, 4.21% of respondents indicated that they were not familiar with the meaning of encryption.

Graph 10: Comparing Encryption and VPN Use on Computer vs. Phone



The survey further examined the number of organisations that had installed VPNs on their smart devices and computers. The results revealed that only 24.53% had installed VPNs on laptops or computers, 52.83% had installed VPNs on handheld (smart) devices while 22.64% did not have VPNs on either their laptops or computers or handheld (smart) devices.

Graph 11: Perception of Digital Security Tool Use

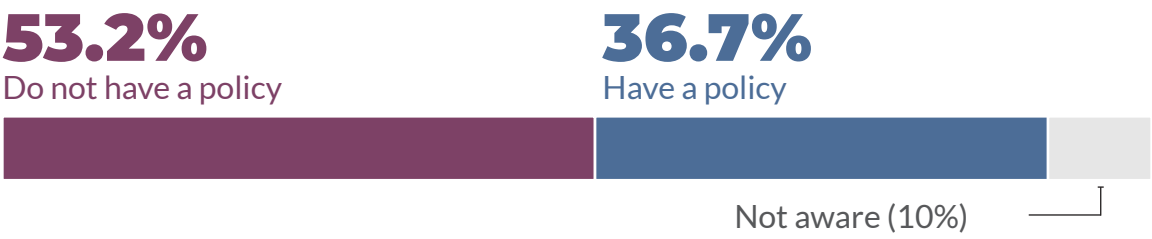


Incidentally, some of the responding organisations indicated that they did not engage in the use of VPN because they were not engaged in any illegal activities. To them, use of a VPN literally translates into admission that the user is engaged in some sort of criminal activity. Thus 6.25% indicated that they did not install VPNs while 31.25% disagreed. 46.25% strongly disagreed while 7.50% strongly agreed to the precept that installation of VPNs was determined by engagement in illegal activities. On the other hand, 8.25% neither agreed nor disagreed that use of VPNs is justified by engagement in illegal activities.

4.3 EXISTENCE OF A DATA PROTECTION POLICY

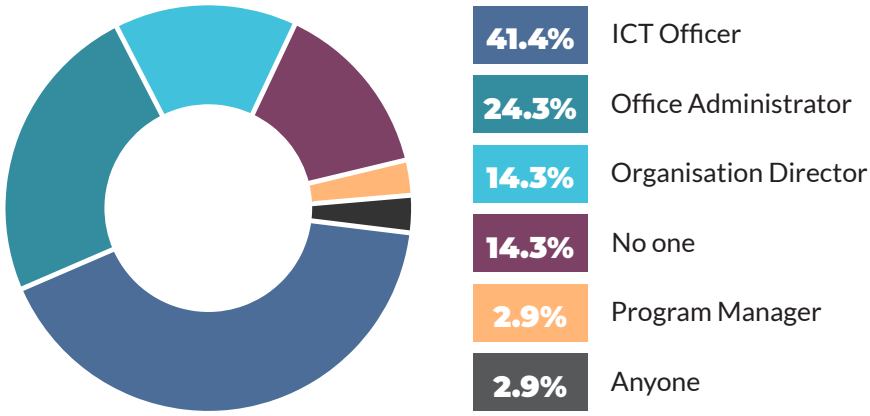
Data protection policies are important for assuring organization clients of the safety of their data and privacy. They reflect compliance with the Data Protection and Privacy Act, 2019 requirements. They also set out the principles, rules, and guidelines for data protection. Thus, the presence of a data protection policy is an assurance of adherence to data protection principles and respect for the rights of data subjects.

Graph 12: Availability of Data Protection Policies



Just over half of the organisations surveyed (53.16%) did not have internal data protection policies compared to 36.71% who had in place data protection policies. Worryingly, 10% of respondents were not sure whether or not they had data protection policies.

Graph 13: Who Manages the Cloud Application Services of Your Organisation?



83.33% of respondents who responded that they had an ICT policy answered "yes" when asked whether or not their organisation had a policy that enforces strong and complex passwords. Although only 41.43% of the total respondents answered that their organisations have a dedicated IT officer who oversees administering the organisations online resources including cloud services. The majority, 58.6% of respondents claimed that their organisations utilise a non-ICT professional to manage their resources.

The research further looked into the use of two-factor authentication (2FA). The use of multi-factor authentication (2FA) allows users of online accounts to use more information in addition to the password to gain access. Organisations utilise online applications and accounts to carry out daily activities which exposes them to digital risks and threats. Unlike some of the other safety tools covered above, use of 2FA was found to be more common with 65% of respondents utilising it. Despite this tremendous result, it was not an output of internal organisations' data guidelines and practices but a result of some platforms' requirements.

4.4 DATA BACKUP AND DISASTER RECOVERY

Safeguarding against loss of organisation data and resources is critical to organisation continuity and sustainability.[18] Out of the 80 respondents, less than half (45.57%) had a data backup or disaster recovery plan and a near similar number (44.30%) indicated that they did not have a data backup or disaster recovery plan while 10.13% were not sure whether they had such a plan in place.

18 Paul Crocetti, "Create your data backup strategy: A comprehensive guide," TechTarget, November 3, 2021, https://www.techtarget.com/searchdatabackup/Create-your-data-backup-strategy-A-comprehensive-guide#:~:text=Data%20backup%20planning%20is%20an,company%20reputation%20and%20employee%20morale.

5. Digital Security Threats

Digital security threats are acts and actions aimed at stealing data, disrupting functioning of computer systems, or causing damage to computer systems.[19] Some of the most common examples of digital security threats include data breaches,[20] malware and virus attacks, hacking, phishing, pharming and spamming.[21] CSOs in Uganda have widely faced digital security attacks which often compromise their security systems.

Most of the digital security threats are perpetrated by individuals, criminal organisations, governments, terrorists, Industrial spies, hackers, business competitors and organized crime groups.[22]

Many of the respondents indicated that they had experienced a digital security threat (78.75%) at organisational and individual level. Only 12.5% indicated that they had never experienced digital security threats, while 8.75% were not sure as to whether they had ever or never experienced digital security threats.

In the study, respondents revealed that digital threats happen frequently and may occur throughout the year. The results of incidences of receipt of digital threats were revealed as on; a daily (6.35%), weekly (14.29%), monthly (9.52%), yearly (15.38%) and seasonal (52.38%) while 1.59% stated that they had never experienced any digital threat.

5.1 FREQUENCY OF THREATS VS VIRUS UPDATES VS USE OF DIGITAL SECURITY TOOLS

The study further revealed the frequency of computer software updated. A majority of the respondents (39%) indicated that they run updates on a seasonal basis while 17.72% indicated running updates on a monthly basis. Those who run updates on

> Many of the respondents indicated that they had experienced a digital security threat (78.75%) at organisational and individual level. ... respondents revealed that digital threats happen frequently and may occur throughout the year.

19 Imperva, "Cyber Security Threats," https://www.imperva.com/learn/application-security/cyber-security-threats/#:~:text=What%20are%20Cyber%20Security%20Threats,to%20or%20disrupt%20computing%20systems.

20 A data breach is the unauthorised exposure of confidential, sensitive, or protected information.

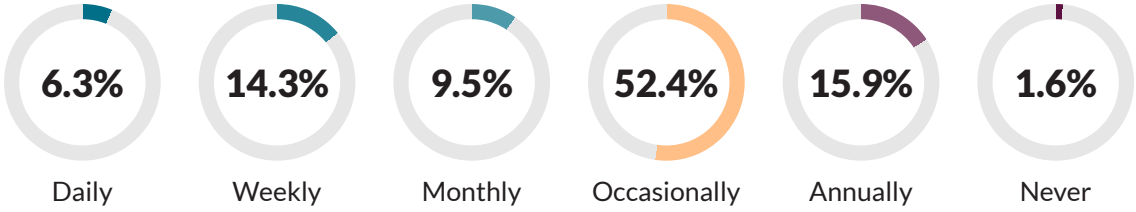
21 Spamming refers to messages which are indiscriminately sent to individuals especially in their email with an ill intent.

22 See for example, Hugh Taylor, "What Are Cyber Threats and What to Do About Them," https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them

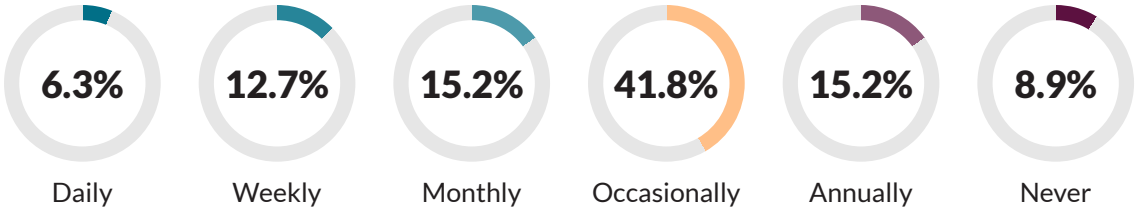
a weekly basis were 12.66% and on yearly basis 8.86% were running updates. Incidentally, only 3.8% were updating their software on a daily basis while 7.6% had never run any software updates on their computers.

Graph 14: Frequency of Digital Threats vs. Anti-Virus Updates vs. Use of Digital Security Tools

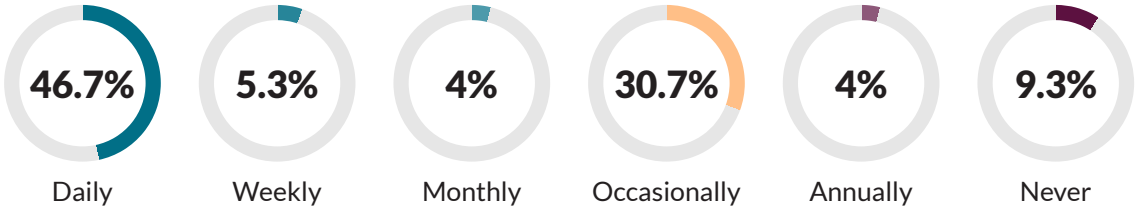
How often do you receive digital threats? (63 respondents)



How often do you perform anti-virus updates? (79 respondents)



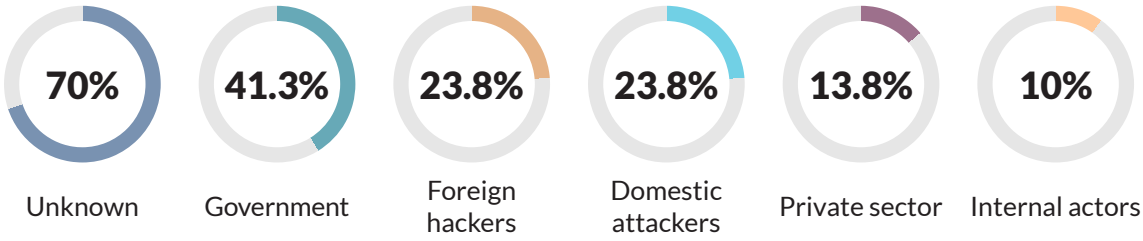
How often do you use digital security tools? (75 respondents)



5.2 PERCEIVED ORIGIN OF DIGITAL THREATS ENCOUNTERED

Respondents identified several perceived sources of digital threats with unknown actors (hackers) accounting for 70%, followed by the government (state agencies) (41.3%), foreign hackers 23.8%, domestic attackers (organisations, individuals) 23.8%, private sector (corporations and firms) 13.8%, and internal actors (colleagues) 10%.

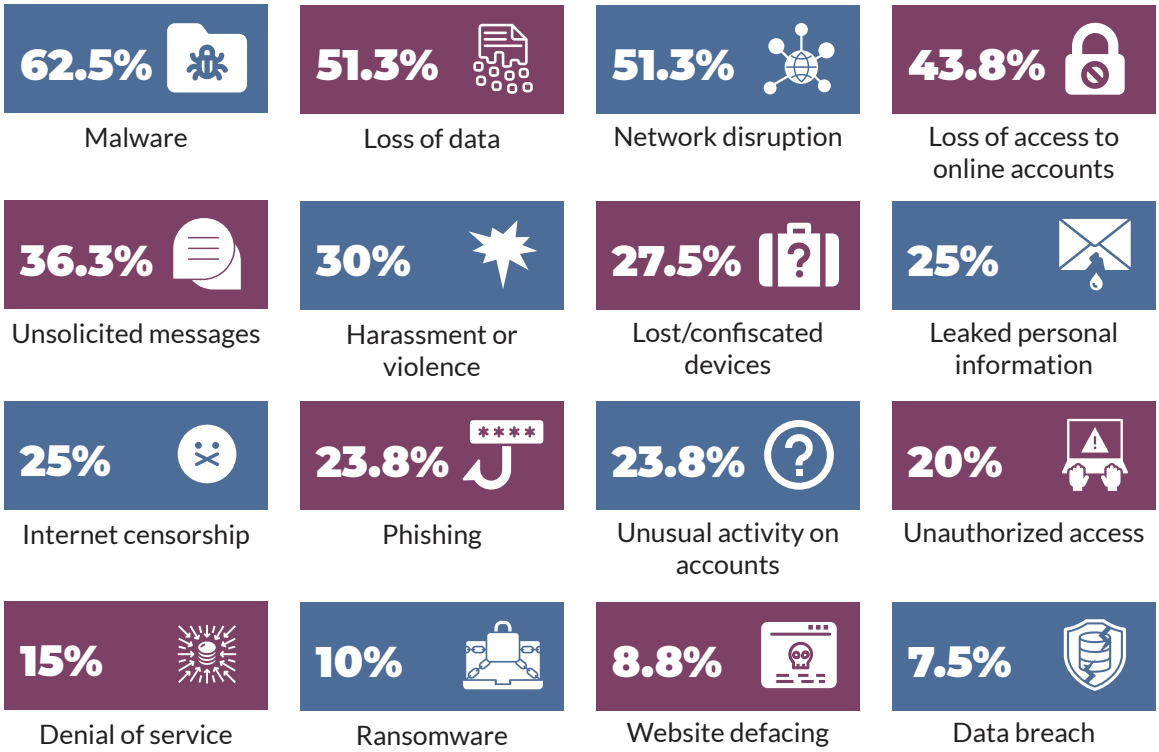
Graph 15: Perceived Origin of Digital Threat



5.3 NATURE AND EXTENT OF DIGITAL THREATS

Malware, data loss, network disruption, and lost access to online accounts were cited as the most prevalent types of digital security risks that respondents had experienced.

Graph 16: Types of Digital Security Threats Experienced



For the most part, the threats experienced by respondents were of a private or personal nature and less connected to their work. At 49.47%, handheld devices were the most prone to attacks, closely followed by laptops and computers (47.37%).

5.4 SPILL OF DIGITAL THREATS INTO PHYSICAL THREATS

Digital threats often spill into exposure to physical threats such as attacks on individuals, office raids, arrests and detention. In some instances, the physical threats involve the seizure of information and devices, which are ultimately destroyed.

One of the respondents revealed that:

> "Our offices were also broken into, and the computer and we lost all our case logs.
>
> The police are some of the biggest perpetrators of arbitrary arrest of HRDs and torture and they make us delete videos and photographs that are evidence of this. If we knew how to backup, we would be able to save this information."

The respondents also noted that there has been wide misapplication by security agencies of the Computer Misuse Act of 2011, as amended in 2022, to forcefully access and take data saved on computers. The Computer Misuse Act provides for safety and security of electronic transactions and information systems and prevents unlawful access, abuse or misuse of information systems. Section 28 authorises security officers to search, seize or confiscate suspected computer systems. Some of the respondents lamented having fallen victim to this section.

> "We have been raided by police before and lost some data saved on computers and hard drives that have been confiscated."

Worryingly, only 36% of the organisations surveyed indicated having procedures or mechanisms in place to counter or respond to existing threats. Furthermore, only 27.85% of the organisations had ever filed a report of the digital threats/incidents faced while 72.15% had never filed any report.

Out the 80 respondents, 31% indicated that they reported the digital security incidents to the ICT officer while 32% indicated reporting to a colleague, and 19% made a report to third parties with a support mechanism including Access Now, Digital Security Alliance and Frontline Defenders. 18% indicated reporting or speaking about digital threats during digital security meetings and briefings. Additionally, 41.33% of the total respondents indicated that they received support to mitigate the impact of the digital security threat while 48% indicated that they never received any support and 8.67% were not sure whether they had received support or not.

6. Impact of Digital Threats on Organisation Operations

Digital threats widely impact the work of organisations. They may paralyse operations and work in cases of major attacks on computers and network systems. Hacks may also deprive organisations of resources such as in cases where hackers deceive donors into wrongly sending them monies after stealing the identity of CSOs, thereby affecting their work. At the same time, digital threats may lead to loss of data and loss of existing communication platforms such as Facebook (Meta) and Twitter (X) among others. These measures often disorganise organisational operations and established contacts.

For most respondents (44%), digital threats were deemed to pose a very high impact on their work while 29% and 27% deemed digital threats as moderate and low impact, respectively. From the responses collected, some of the respondents indicated that the impacts were both positive and negative.

The positive impacts gathered from the study are:

- Organisations which had fallen victim organized cybersecurity trainings for their employees. Those that had done them before embarked on more trainings to counter emerging digital threats. The trainings also explored online safety.
- As a result of the various digital threats, organisations are now better informed on how to best store and secure organisations' data for future use without getting compromised.
- Increased organisational vigilance to take more concerned preventive action on digital security, such as regulating access to internet services within the organization.

As observed by one respondent:

> "I have come across suspicious emails. So, I have become more vigilant, learnt how to protect myself against threats like spam and scammers. I have also experienced online threats from state and non-state actors due to the nature of my work but I have managed to soldier on despite the threats."

Hacks may also deprive organisations of resources such as in cases where hackers deceive donors into wrongly sending them monies after stealing the identity of CSOs, thereby affecting their work.

The negative impacts of digital security threats on organisations include:

- Significant setback after loss of data, necessitating measures towards recovery, yet in some instances, the lost data was never recovered. This also comes with loss of information which CSOs, HRDs and journalists use for communication, mobilisation and running of daily activities.
- Bringing activities of the organisation including social activities and interactions to halt as a result of network disruptions, hacks on individuals and organisations accounts and theft of laptops, computers, cameras, recorders, internet modems, and flask disks.

> "Feeling threatened and insecure has affected my ability to do my work. Once my computer was hacked. Someone was able to turn on my camera remotely. I also received a threat from someone in prominent circles. They told me they were aware of the article I was writing and warned me about the possible consequences of having it published. The article was about an internal attack on an armoured brigade in Mukono by some of the internal staff (soldiers). Sometimes articles have disappeared when we were trying to upload them online."

Another respondent noted that:

> "I have faced many digital threats. I have been blocked out of my accounts multiple times. I used to post a lot of content about controversial political issues. I faced a lot of online violence which would force me to withdraw/ stay offline. This I believed affected my online advocacy work because of inconsistency."

- Forced change of organization accounts such as on social media platforms including Meta accounts and Twitter handles.
- Lost access to email and the resulting loss of important organization documents. There have also been continued receipt of Spam and scam mail from cyber criminals.

> "We have a common email address where all members share information. We receive a lot of spam through that email address. We have had emails spreading negative information about the cooperative industry." (respondent)

- Leak of confidential organization and personal information to the wrong people including unfriendly sources and foes.
- Loss of time and resources in efforts identify viable solutions for countering threats such as through the hiring and paying of consultants to help address the problem.
- Instilling fear and intimidating staff and employees from performing their duties using digital devices.

> "I received threats via email when I was pursuing a case against someone charged with defilement. I was fearful because I did not know who it was from. This was compounded by the fact that there are many guns in our area. So, my ability to move was restricted. This affected my community outreach work." (respondent)

- Online harassment has frequently led to mental distress to individuals and thereby affecting their performance at work

> "We have mostly been affected by online threats targeted towards our beneficiaries especially those in the rural areas. Once women have been bullied online, they tend to shy away from the digital's tools and initiatives that our organization offers." (Respondent)

- Destabilization of relations between individuals, organisations and donors or partners. In some instances, hackers used affected organisations email and wrote to stakeholders, funders, and partners, informing them of changes in the organization's management and asking them to send them money so that they use it to for proper transition.

In most of the cited negative impacts, the privacy of CSOs, HRDs and journalists is compromised. They become easy targets for surveillance and trolling since their data is often in the wrong hands. As a result, mobilisation, assembly, freedom of expression and freedom of information are limited due to fear of intimidation, threats, arrests and prosecution.

7. Capacity Building and Remediation

7.1 DIGITAL SECURITY AWARENESS AND CAPACITY BUILDING

Some of the respondents had previous exposure to digital security capacity building - 20% within the 12 months prior to the survey and 35% within the previous six months. 16.25% had some training in more than 6 months but in less than 12 months, and 16.25% had had some training over twelve months ago while 12.5% had never had any form of digital security trainings.

Respondents recognised the need for more training and awareness to promote proficiency in digital safety and security. They further noted that efforts should be continuous and not one-offs to ensure effective mitigation of the adverse impacts that come with digital threats, risks and attacks.

Some of the respondents noted that:

> Training on how to use these tools would help us a lot. Right now, we have basic/elementary knowledge on how to use them. If I had known how to backup information on my phone or computer, we would not have lost all that information. (Respondent 1)

> I believe the best solution would be continued sensitization. I only learned about digital security and cyber threats that I may have been exposed to, this year during the training organized by CIPESA. (Respondent 2)

> More people need to be trained on how to use digital tools. I have received training through conferences but not many people have access to these opportunities. (Respondent 2)

> I believe there is a need for more education on ICT. I believe the biggest tech threat is lack of information. Most people in Uganda are just embracing digital technologies and they are not aware of the risks/dangers and how to protect themselves, data privacy among others. So, the masses need to be educated about digital security. (Respondent 2)

7.2 BARRIERS TO TIMELY RESPONSE TO DIGITAL THREATS

As earlier noted, digital threats and attacks often require timely counter measures. However, the study revealed that a number of organisations did not respond to digital threats and attacks in a timely manner due to various reasons. These were identified as including insufficient level of familiarity with digital technology, Poor response mechanisms or lack of knowledge to effectively respond to data breaches, limited experience in use of passwords and use of digital security tools, and the absence of well-defined channels through which to report breaches in digital security in order to receive assistance or support.

Some of the respondents observed that:

> I believe I don't have enough knowledge and information about the digital and technology space and this would go a long way in having the ability to anticipate and respond, even recover from technological threats. (Respondent 1)

> Ignorance about technological threats and how to counter them is the biggest gap in our ability to anticipate them and respond to them. (Respondent 2)

> Lack of knowledge. There are so many digital threats that we do not get to learn about until we are dealing with them. I think if I had enough exposure to technology I would be better equipped to anticipate and respond to these threats. (Respondent 3)

> We still have a lot of knowledge gaps in technology. We need a lot of training on digital security not only to protect the university data but also personal data. (Respondent 4)

Consequently, there is need for consistent knowledge building, awareness raising and capacity building in digital rights, digital security preparedness, compliance and resilience if digital threats are to be effectively addressed.

8. Conclusion and Recommendations

The use of ICTs is now an indispensable aspect of CSOs' operations. CSOs increasingly depend on ICTs to manage a wide array of organizational tasks, such as engaging with stakeholders, facilitating information flow and exchange, and conducting financial transactions. However, CSOs face a myriad of digital threats, both established and emerging, which pose risks to their work and personnel. These threats predominantly target the access and use of digital security tools.

Key digital security threats encountered by CSOs encompass malware (virus) attacks, data loss, network disruptions, loss of access to online accounts, reception of unsolicited messages with malicious links, harassment and violence, device confiscation and loss, exposure of private and personal information, internet censorship, phishing attacks, unusual activities on individual online platforms, unauthorized access to restricted resources, online account takeovers, denial of services, ransomware incidents, website defacement, and data breaches. Several factors contribute to these threats and subsequent responses. These include the inadequacy or absence of relevant skills, capacities, and competencies to address these threats, the lack of internal data protection policies tailored to CSOs, and resource constraints that hinder the employment of competent digital security professionals and the acquisition of necessary digital security tools.

The result is often the imposition of limitations and curtailment of assembly, association, expression often arising from data leaks and breaches. Data leaks and breaches lead to exposure of individuals and enhance easy identification of CSOs, individuals, HRDs and journalists. They become easy targets to cyber criminals who use their data for the wrong reasons and security agencies which often engage in intimidation, arrest and persecution of actors.

To effectively address these emerging challenges, it is imperative to take immediate actions that promote the adoption and effective use of digital security tools to facilitate and safeguard CSO activities.

8.1 GOVERNMENT

- Lower taxes on digital tools and ICTs so as to facilitate access and use of ICT tools.
- Offer tax incentives to digital tools investors and innovators to make this equipment more available and affordable locally by directly leading to lowering of costs which often translate into high costs.
- Undertake deliberate infrastructure development efforts which aim to extend internet infrastructure in rural and remote areas to ensure enhancement of access to the internet by all persons.

- Desist from practices that distabilise and limit access to the internet and social media platforms such as shutdowns and blockages so as to ensure sustainable use of the internet by organisations and individuals.

8.2 CIVIL SOCIETY ORGANISATIONS

- In partnership with government and other stakeholders, raise awareness of digital tools amongst the populations.
- Regularly build capacity of citizens and organization workers in digital tools utility and response in case of security threats and attacks including through digital security trainings.
- Organisations including their employees should never connect to suspicious networks and, should never click on suspicious links as these expose them to digital threats, risks and attacks.
- Push the government to respect digital rights and the use of digital tools like encryptions and VPNs.
- Develop internal privacy policies to ensure that appropriate safeguards to data protection and privacy are in place.

8.3 INTERNET SERVICE PROVIDERS

- Work collaboratively with civil society and government to provide organisations and individuals with reliable and affordable access to the internet.
- Establish and install relevant infrastructure in rural and remote communities to enhance access to reliable internet.
- Observe human rights while doing business. This should be done through the observance of the UN Guidelines on Business and Human Rights and integrating these principles in their internal policies that aim to promote human rights in business.

8.4 DEVELOPMENT PARTNERS

- Take deliberate efforts that aim to promote and enhance digital security awareness and capacity by among others increasing resources to invest in digital rights and security programs.
- Engage in support legislative reforms by supporting advocacy campaigns that seek to enhance digital security capacities and awareness among CSOs, HRDs, and Journalists.

Annex: Survey Questionnaire

STATUS OF ACCESS, USAGE OF DIGITAL TOOLS, AND DIGITAL THREATS FACED BY CSOS IN UGANDA

A. Personal Information

1. Name
2. Email Address
3. Organisation or Affiliation
4. How old are you?
    e. a. 18–29
    f. b. 30–39
    g. c. 40–49
    h. d. 50–59
    i. 60 and above
5. What is your gender?
    a. Woman
    b. Man
    c. Non-binary
    d. Prefer not to say

B. Organisational Information

6. What is your organisation's operational area of focus?
    a. Women's rights advocacy
    b. Health rights advocacy
    c. LGBTQI rights advocacy
    d. Environmental rights advocacy
    e. Digital rights advocacy
    f. Voice and accountability
    g. Media and journalism
    h. Land and extractives
7. What is your position within the organisation?
8. How long have you worked with this organization?
    a. Less than 5 years
    b. 5 – 10 years
    a. 10+ years

9. What is the location of your organization's operations?
    a. Northern Uganda
    b. Eastern Uganda
    c. Central Uganda
    d. Western Uganda
    e. South Western Uganda
    f. West Nile
    g. Nationwide

3. Access to Digital Tools

10. Do you have access to a laptop or a computer for your work?
    a. Yes
    b. No
11. What is the operating system on your computer?
    a. Windows
    b. Mac OS
    c. Linux (Ubuntu)
12. Do you use your laptop or computer for personal or private purposes aside from organizational tasks?
    a. Yes
    a. No
    a. Maybe
13. Do you use a mobile device (smartphone) to access work-related applications and resources?
    a. Yes
    b. No
14. What type of handheld (smart) device do you use?
    a. Android
    b. iPhone
    c. Windows

15. Which social media platforms do you use?
    a. Facebook
    b. Twitter
    c. TikTok
    d. Instagram
    e. LinkedIn
    f. WhatsApp
    g. YouTube

4. Digital Security and Threats

16. When was your last digital security training or retraining workshop?
    a. Within the last 6 months
    b. More than 6 months ago
    c. Almost a year ago
    d. Over 12 months
    e. Never
17. Have you ever experienced a digital security threat?
    a. Yes
    b. No
    c. Maybe
18. What digital security threat have you experienced?
    a. Malware (virus)
    b. Loss of data
    c. Leaked private/personal information
    d. Lost access to online accounts
    e. Confiscated/Lost devices
    f. Website defacing
    g. Online account takeover
    h. Phishing
    i. Ransomware
    j. Data breach
    k. Unauthorised access to restricted resources
    l. Denial of Service
    m. Harassment or Violence
    n. Internet censorship
    o. Network disruption

p. Unsolicited messages with clickable links
q. Unusual activity on your online accounts

19. Where did you experience the digital threat?
    a. Laptop or Computer
    b. Handheld (smart) Device
    c. Online Platform
20. What was the digital threat in relation to?
    a. Organisational work
    a. Personal or Private matters
    a. Not sure
21. What is your perception of the origin of digital threats?
    a. Government (state agencies)
    b. Foreign hackers
    c. Unknown threat actors (hackers)
    d. Private sector
    e. Internal actors (colleagues)
    f. Domestic attackers
22. What was the impact of the threat to your organisation's operations? (1 for low impact and 10 for higher impact)
23. How has the perceived digital threat impacted your organization?
24. How often do you receive or experience a digital threat?
    a. Daily
    b. Weekly
    c. Monthly
    d. Seasonal
    e. Yearly
    f. Never

5. Digital Security Practices

25. Do you have procedures or a mechanism to report any digital threats?
    a. Yes
    b. No
26. Have you filed a report of any digital threats/incident recently?
    a. Yes
    a. No
27. Who did you report the digital security threat or incident to?

a. ICT Officer
b. Colleague
c. During a security meeting/briefing
d. Third party support mechanism

28. Did you receive any support/outcome to mitigate the impact of the digital security threat?
    a. Yes
    b. No
    c. Maybe
29. Does your organisation have an ICT or data protection policy?
    a. Yes
    b. No
    c. Not necessarily
30. Does your organisation have a data backup or disaster recovery plan?
    a. Yes
    b. No
    c. Maybe
31. Do you use outdated, bootleg or counterfeit software on your PC?
    a. Yes
    b. No
    c. Maybe
32. Who is responsible for installing and maintaining software on your computer?
    a. Myself
    b. Administrator
    c. IT Officer
    d. Other

6. Network and Internet Usage

33. How do you connect to the internet at work?
    a. WI-FI
    b. Smartphone Hot-Spot
    c. Local area network (LAN) cable

34. How often is the WI-FI password changed at your organisation?
    a. Monthly
    b. Yearly
    c. Rarely
    d. Never
35. How often do you update your computer's software?
    a. Daily
    b. Weekly
    c. Monthly
    d. Seasonal
    e. Yearly
    f. Never

7. Organisational Digital Infrastructure

36. Does your organisation have a website?
    a. Yes
    b. No
37. Does your website have an SSL certificate (HTTPS)?
    a. a. Yes
    a. b. No
38. What social media pages does your organisation manage?
    a. Facebook
    b. Twitter
    c. LinkedIn
    d. Instagram
    e. YouTube
    f. Other
39. Who is in charge of updating the organisation social media pages?
    a. Any staff member
    b. IT Officer
    c. Communication officer
    d. Other
40. Does your organisation use cloud application services such as Google Workspace, Microsoft 365 or Next cloud?
    a. Yes
    b. No

41. Who manages the cloud application services of the organisation?
    a. IT Officer
    b. Administrator
    c. Director
    d. Other
42. Is multi-factor authentication (2FA) required to gain access to the organisation's online application services?
    a. Yes
    b. No

8. Digital Tools and Communication

43. What digital tools do you use for external communications?
    a. Zoom meetings
    b. Microsoft Teams
    c. Jitsi
    d. Signal Messenger
    e. WhatsApp Messenger
    f. Telegram Messenger
    g. Email
    h. Other
44. What digital tools do you use for internal communication within the organisation?
    a. Signal Messenger
    b. WhatsApp Messenger
    c. Email
    d. Jitsi
    e. Slack
    f. Zoom Meetings
    g. Microsoft Teams
    h. Other
45. Which of the following digital security tools are you familiar with?
    a. Tor Browser
    b. Veracrypt
    c. Cryptomator
    d. Onion Share
    e. KeePassXC
    f. DuckDuckGo

g. Tails
h. Etherpad
i. uBlock Origin
j. HTTPS Everywhere
k. Jitsi Meet
l. Other

46. How often do you use these digital tools for work?
    a. Daily
    b. Weekly
    c. Monthly
    d. Seasonal
    e. Yearly
    f. Never
47. How does your access to or lack of access to digital tools affect your day-to-day operations?

9. Digital Security Measures

48. Do you use PGP encryption for your email conversations?
    a. Yes
    b. No
    c. I do not know what PGP encryption means
49. Does your computer have anti-malware (antivirus) software installed?
    a. Yes
    a. No
50. How often do you update your antivirus software?
    a. Daily
    b. Weekly
    c. Monthly
    d. Seasonal
    e. Yearly
    f. Never
51. Do you have a VPN installed on your devices?
    a. Laptop or Computer
    b. Handheld (smart) Device
    c. None

52. Do you protect your data and information using encryption?
    a. Laptop or Computer
    b. Smartphone
    c. What is encryption?

10. Attitudes Towards Digital Security

53. How much do you agree with the following statements? (Strongly agree, agree, agree, neutral, disagree or strongly disagree)
    a. I do not need to encrypt my data because I am not doing anything illegal.
    b. It is safe to connect to free WI-FI.
    c. It's safe to click on links received in messages.
    d. It is safe to use cracked software.