A WEB-BASED SYSTEM FOR REPORTING AND CREATING AWARENESS ABOUT SOCIAL MEDIA THREATS AND CRIME IN UGANDA

BY

JIMMY HAGUMA

2016/HD05/416U

SUPERVISOR:

DR. REHEMA BAGUMA

A PROJECT REPORT SUBMITTED TO SCHOOL OF COMPUTING AND INFORMATION SCIENCES IN PARTIAL FULLFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN INFORMATION SYSTEMS OF MAKERERE UNIVERSITY

January 2023

Declaration

I Haguma Jimmy, do hereby declare that this project report is original and has not been published and/or submitted for any other degree award to any other University before.

Signed: Date: **6th January 2023**

Jimmy Haguma

Approval

This project report has been submitted for examination with the approval of the following supervisor.

Signed.. Date.08/01/2023

Dr. Rehema Baguma
Department of Information Systems
School of Computing and Informatics Technology
Makerere University.

Dedication

This work is dedicated to my wife, who inspired me to undertake Graduate studies, and my beloved children Josiah, Jollin, Johnette and Jovanice who always inspired me. Thank you so much for your prayers, support, guidance and encouragement from time to time. Special thanks to my supervisor Dr. Rehema Baguma who was deliberated and persistent to see this as a success.

Acknowledgement

I would like to thank the Almighty God, who has enabled me to achieve this. My special thanks go to my Supervisor Dr. Rehema Baguma once again who guided and reviewed my work tirelessly throughout the entire project period.

Finally, I am grateful to all authors whose work appears in this report as references.

Thank you all.

TABLE OF CONTENTS

Table of tables

Table of Figures

LIST OF ACRONYMS

CERT	Computer Emergency Response Team
CIPESA	Collaboration on International ICT Policy in East and Southern Africa UPF – Uganda Police Force
COVID	Coronavirus Disease
DNA	Deoxyribonucleic Acid
ECMU	Electronic Counter Measures Unit
EPOOLICE	Early Pursuit Against Organized Crime Using Environmental Scanning, the Law and Intelligence Systems
FGD	Focus Group Discussion
GSMA	Global System for Mobile Communications
HTML	Hyper Text Markup Language
ICT	Information Communication Technology
JLOS	Justice Law and Order Sector
MoICT &NG	Ministry of Information and Communication Technology and National Guidance
NITAU	National Information Technology Authority of Uganda
PHP	Hypertext Preprocessor
SEO	Search Engine Optimization
SMS	Short Message Service
SQL	Structured Query Language
UCC	Uganda Communications Commission

UPF	Uganda Police Force
USSD	Unstructured Supplementary Service Data

ABSTRACT

The Internet is increasingly becoming a significant tool for social, economic, and human rights development in Uganda and Africa at large. Average citizens, human rights activists, civil society organizations, media houses, and more recently, politicians and government institutions, have resorted to the use of various forms of social media platforms in particular Facebook, WhatsApp and Twitter - for expression, association and information sharing. In countries such as Uganda, which is characterized by high rates of unemployment, wage inequality and poverty, social media crime is attractive, easy and cheap with the fact that anybody with access to the internet could become a social media perpetrator. Social media crimes cannot be sufficiently investigated using traditional methods of recording lengthy statements, visiting the scene of crime, submitting the file to the Resident State Attorney for perusal, compelling witnesses to court, obtaining expert opinions from computer experts and tracing for suspects. Furthermore, there is a deficiency in the numbers and capabilities of law enforcement officers to investigate computer related crimes since such occur randomly in any part of the country with access to the internet. The main objective of this project was to develop a web-based system for reporting and creating awareness about social media threats and crime in Uganda. The study followed an agile methodology which included: Systems Study, Systems Analysis and Design, systems implementation and finally systems testing and validation. Qualitative and quantitative data was collected from respondents through the use of questionnaires and Focus Group Discussions. The Information System was developed using open-source technologies namely: PHP and JavaScript running on MySQL database and the graphical user interface of the system running on HTML5 platform. As part of the case study, a total of 20 respondents were interviewed from law enforcement officers to investigate the needs of stakeholders of the proposed social media crime reporting and awareness system. The results show that implementation of the proposed system will solve the problem of social media crime awareness since it is able to integrate and merge data from different sources. Therefore, the web-based system for reporting and creating awareness about social media threats and crime will be one of the solutions to reduce the social media crimes and increase awareness about social media crime in Uganda.

CHAPTER ONE: INTRODUCTION

1.0 Introduction

The Internet is increasingly becoming a significant tool for social, economic, and human rights development in Uganda and Africa at large. Average citizens, human rights activists, civil society organizations, media houses, and more recently, politicians and government institutions, have resorted to the use of various forms of social media platforms especially Facebook, WhatsApp and Twitter - for expression, association, and information sharing (Magelah, 2016).

The growth of social networks during the last decade has been astonishing. Aside from the well-established brands such as Facebook, WhatsApp, LinkedIn, Twitter, Instagram and YouTube, there are over 200 social networking sites that are active and full of all kinds of people from introverts who only desire a small digital presence to social predators and people with oversharing tendencies (InfoSec, 2020). Facebook alone has over 3 billion users that among other information, post over 350 million photos each day (Noyes, 2020). This is followed by YouTube with 2 billion, WhatsApp at 1.6 billion, WeChat with 1.2 billion and sixth-ranked photo-sharing app Instagram with 1 billion monthly active accounts (Clement, 2020). Social networks have a great impact on society including providing entertainment, generating information, facilitating communication, digital marketing and influence (Smith, 2019). Social media's role in promoting businesses is significant. It facilitates communication with customers and enables the melding of social interactions on e-commerce sites. Furthermore, its ability to collect information of various metrics, aids in marketing efforts and market research (Drury, 2020).

In Uganda, by January 2019, Facebook was estimated to have over 2.4 million users which contributes 5.5% of the overall population in the country (NapoleonCat, 2020). Out of the 2.4 million user accounts, 8% of those accounts are estimated to be fake user accounts that are used to commit social media related crimes (Noyes, 2020). Organized criminal groups are increasingly using digital technologies to facilitate their illegal activities such as theft, fraud or rendering of new crimes such as attacks on computer hardware, software, hacking into emails & social media accounts, cyber bullying and cyber stalking among others (World Bank, 2016).

In countries such as Uganda, which is characterized by high rates of unemployment, wage inequality and poverty, social media crime is attractive, easy and cheap due to the fact that anybody with access to the internet could become a social media perpetrator (Clement, 2020).

In Uganda, the information technology space has grown rapidly, be it the digital economy and its facilitating tools, such as mobile payment platforms or the information and communication space where people freely interact and share experiences through the use of social media platforms (Bos, 2019). The use of social media is universal and cuts across all age groups, social classes and cultures. However, the increased use of social media is accompanied by privacy issues and ethical concerns which may be breached resulting into social media related crimes (Peters , 2019). For a fast-growing cyberspace, the supporting legal framework needs to be dynamic enough to foster the growth while robust enough to protect all parties involved in it (Bos, 2019).

Privacy issues can have far-reaching professional, personal and security implications. Ultimate privacy in the social media domain is very difficult because these platforms are designed for sharing information (Lynch & Nadine, 2020). The blurred layer between privacy and safeguards in this space coupled with the inadequate information security awareness levels has resulted into unethical and undesirable behaviour online. Consequently, the breach of privacy, where the victim's private information is released online in the public domain especially for the most vulnerable and less informed groups of online users (Snyder, Kanich, Doerfler, & McCoy, 2017).

Furthermore, today's social networks have become the platform of choice for hackers and other perpetrators of anti-social behaviour (Nouh, 2019). These networks offer large volumes of information ranging from an individual's date of birth, place of residence, place of work or business, to information about family and other personal activities. In many cases, users unintentionally disclose information that can be both dangerous and inappropriate. There should be clear distinctions between what should be seen by the general public and what should be limited to a selected few (Barrett, 2020). One school of thought is that the only way to avoid social media related threats today is not to share information or to opt out if you don't agree with the legal disclaimers in these networked communities (Caplinskas, 2015). However, achieving privacy and control over information flows and disclosure in networked communities is a gradual process especially in an environment where technology is dynamic, and, the boundaries between private and public are blurred (Peters , 2019). This therefore, requires intentional development of information systems that are designed to create awareness and report social media related threats and crimes.

1.1 Background

Digital forensics science is a well-known initiative to unearth computer-assisted crimes (InfoSec, 2020). In order to withstand the difficulties caused by the complexity of crime, forensics investigation frameworks are being tuned to adapt with the nature and earnestness of the crimes being committed (Abulaish & Haldar, 2018). Social Media forensics offers the capability to search multiple social networking information system databases in real time, uncover identities, correlations, networks of associates and available geographical information of persons or users accounts online (SocialNet, 2020).

Performing social network forensics needs be done by qualified and experienced professionals. However, there is a deficiency in the number and capabilities of law enforcement officers to investigate computer related crimes in Uganda since these crimes occur randomly in any part of the country that has access to the internet (NITAU, 2016). The current cyber legal and regulatory framework of Uganda is limited in terms of jurisdiction and thus may not compel giant social media platform owners in certain jurisdictions to disclose or pull-down content from their platforms (Bos, 2019)

In addition, most of the big tech social media giants currently enjoy broad immunity from civil lawsuits stemming from what users post because they are treated as “platforms” rather than “publishers” and thus not being held liable for content that may be posted by its users (David, 2020). The digital age today offers widespread use of social media platforms (Barrett, 2020)

According to the Association of Certified Fraud Examiners’ 2020 Report to the Nations, risk and threat awareness contributed up to 56% of cultivated tips and reporting mechanisms (Dorris, 2020). In Uganda, the National Information Technology Authority of Uganda (NITA-U) started the Cyber Laws awareness drive campaign during COVID-19 (NITAU, 2020). However, to the contrary, not many citizens and law enforcement officers know the provisions of such laws, and how to even apply them, once they encounter social media threats or crime in their areas of jurisdiction (LASPNET, 2017). In addition, NITA-U developed the social media user guidelines to facilitate Government Ministries, Departments and Agencies in the process of adopting social media as one of the platforms for engaging with the citizens of Uganda (NITAU, 2013). These guidelines are meant to ensure uniformity in communicating and appropriate consultation before posting government communication online. However, the guidelines are still in draft form and have not yet been domesticated in most of the Ministries, Departments and Agencies of Government (NITAU, 2013). This preceded the inauguration of the Communication Computer Emergency Response Team (CERT) at the Uganda Communications Commission with the aim of; monitoring and handling cyber security incidents occurring within the communication sector, guiding service providers on critical information infrastructure to adopt best practices in information security and raising awareness levels of information security among consumers or subscribers of the services in the Communication sector (UCC, 2019).

The Commission CERT set up an incident handling email address, a formidable team of experts and equipment to handle social media related incidents (Mwesigwa, 2015) . However, the email is not interactive enough to create awareness and report social media threats in Uganda, leading to low adoption rates.

Notably, the Uganda Communications Commission issued a public notice warning against irresponsible use of social and electronic communication platforms (UCC, 2017) and further created complaint handling procedures for consumers which are embedded with a live chat forum for escalation of all computer emergency risks to the CERT (UCC, 2020). However, this has not been extensively popularized, and thus low usability rates.

The measures are an invaluable tool for social, economic and human rights empowerment since they offer a cheaper platform for mass communication, mobilization and dissemination of information in form of awareness drives. On the contrary, there is limited guidance and support from the Uganda Communication Commission (UCC) and NITA-U in the deployment of social media in communicating (CIPESA, 2018). In addition, the draft guidelines do not provide for a supportive automated system for the collection of views and opinions from the social media users anonymously. (Agena , Ojok , & Achol, 2019). Therefore, timely response and investigation of specific complaints or tips may take long to be realized.

In addition, in 2014, Uganda Police Force launched the cyber barometer as part of the centenary celebrations. This paper is now rated at only 1690 user downloads and the ability of receiving feedback or even reviewing the social media threats that were quoted is still lacking (UPF, 2019). Furthermore, the Uganda Police has established an Electronic Counter Measure Unit (ECMU) with the aim of detecting and investigating crimes committed using online platforms such as Facebook, WhatsApp, Instagram and Twitter (Sekyewa, 2019). However, the unit is normally overwhelmed by the increased number of cases and yet it has limited capacities in terms of numbers of skilled personnel and equipment to deal with the avalanche of reported and detected social media threats and crimes in Uganda (Nankinga, 2017).

Therefore, the focus of this research is to design a web-based system for reporting and creating awareness about social media threats and crime that can create a platform for timely reporting social media threats and crimes and alert social media users, the general public as well as the law enforcement agencies involved in investigating such crimes about the different forms and categories of social media crimes, attack surfaces and the techniques used by perpetrators to commit such crimes.

1.2 Problem statement

. The dramatic rise in use of social media sites such as Facebook, Twitter and YouTube in the last decade has also led to an increase in criminal activities and offences on such interactive spaces (InfoSec, 2020). These crimes include; spamming, social engineering, ransomware, phishing attacks and electronic fraud (Soomro, 2019).

Such crimes cannot be sufficiently investigated using traditional methods of recording lengthy statements, visiting the scene of crime, submitting the case file to the Resident State Attorney for perusal, compelling witnesses to court, obtaining expert opinions from computer experts and then tracing for suspects. This coupled with the increase in costs of justice while handling social media related offences (Patton, 2017) makes the entire process expensive, time consuming and complex.

In addition, there are also low-capacity levels among the law enforcement and security agencies to obtain credible admissible evidence in courts of law due to deficiencies in modern digital forensic analytical tools and the available skillset (Ajayi, 2016).

Therefore, the time constraint in reporting and investigating social media threats and crime coupled with the inadequate efforts to create awareness among the public is a justification for the web-based system for reporting and creating awareness about social media threats and crime in Uganda that will facilitate timely reporting and feedback to the victims of crime but also provide content to create awareness/sensitization about the threats and crime on that can be committed social media platforms

1.3 Objective

1.3.1 General objective

The main objective was to develop a web-based system for reporting and creating awareness about social media threats and crime in Uganda.

1.3.2 Specific objectives

(i) To collect requirements for a web-based system for reporting and creating awareness about social media threats and crime.

(ii) To design a web-based system for reporting and creating awareness about social media threats and crime in Uganda.

(iii) To implement a web-based system for reporting and creating awareness about social media threats and crime in Uganda

(iv) To test and validate the developed system.

1.4 Research questions

(i) What are the requirements for a web-based system for reporting and creating awareness about social media threats and crime?

(ii) What web-based system design and implementation can support reporting and creating awareness about social media threats and crime?

(iii) To what extent does the developed system support reporting and creating awareness about social media threats and crime?

1.5 Significance of the Study

The findings of this study bridged the knowledge gaps regarding the impact associated with social media related crimes and threats and its challenges in reporting and investigations within Uganda.

The findings of this study were useful for policy formulation among the different players in Uganda. The included the Uganda Police Force, Office of the Director of Public Prosecution, ICT Regulators (Uganda Communications Commission), Civil Society Organisations and Financial Technology Service Providers. These findings informed the leadership of the stakeholders on how best to address the challenges associated with social media crimes and threats that require unique and tailored interventions. This further supported the efforts to counter the risks that come with the use of social media by empowering the consumers/users.

The findings of the study may further be used by the Uganda Police Force to understand and solve various social media related glitches including uncovering cyber bullying, hate speech and fraudulent activities (Pinem, Hidayanto, Sandhyaduhita, Donie, & Phusavat, 2019) and may influence further scholarly research.

1.6 Scope of the study

The study sought to find out the status of social media threats and crime awareness and reporting in Uganda, existing challenges and possible solutions.

CHAPTER TWO: LITERATURE REVIEW

2.0 Overview

The chapter reviewed relevant literature on social media related threats and crimes in Uganda. It highlighted the different categories of social medial threats, crimes and challenges posed by social media spaces, tools that could be used to investigate such crimes, legislative frameworks that guide identification of such crimes and the requirements for a social media crime and threat awareness system. The rest of this chapter is organized as follows: 2.1 discusses the benefits of social media, 2.2 presents the negative effects of social media, 2.3 discusses categories of social media threats and crimes, 2.4 Social media threats and crimes in Uganda, 2.5 Is about theoretical underpinnings to social media crime, 2.6 presents an analysis of social media threats and crime awareness frameworks and methods, 2.7 Presents web-based system for reporting and creating awareness about social media threats and crimes, and its comparison with other systems, 2.8 Presents the Cyber Legislative Framework in Uganda , 2.9 Presents challenges of investigating social media crimes and threats , 2.10 Discusses remedies to social media threats and crimes and section 2.11 concludes with a web-based system for reporting and creating awareness about social media threats and crime as a solution in Uganda.

2.1 What is Social Media?

Social media constitutes websites that are designed to enable users share information, exchange ideas and participate in online content development. These include platforms such as Facebook, YouTube, Twitter, Instagram, LinkedIn, Google+ and other similar interactive websites. Social media is widely used by different sections of society including students at different levels of education since it has the potential to facilitate collaborative learning. (Feyisa & Dawit , 2018)

Social media is becoming an important intermediary for interaction between governments, governments and citizens, and governmental agencies and businesses. This is due to its unique characteristics namely; openness, participation and sharing. However, despite rapid adoption, a growing concern and skepticism regarding the use of social media exists in the public sector.

2.2 Benefits of Social Media

The Internet and social media provide people with a range of benefits, and opportunities. The use of social media is increasingly becoming popular among the youths worldwide due to its interactive features. Global digital statistical reports indicate that the number of social media users is increasing from time to time and exceeding billions due to the fact that social media platforms are cheaper, user-friendly and more interactive than other modes of communication channels (Feyisa & Dawit , 2018).

For business, social media has enhanced brand messaging to the right people at the right time and clientele (Sam , 2019). The lines between professional and personal are blurring online, and many times, we refer to our online presence as our "Personal Brand". Your personal brand can be both the personal and professional "YOU" (Lauren , 2014)

Social media is not just about brands connecting with their customers. Social media is about connecting people to people (Friedman, 2014). One of the most noticeable benefits of using social networks is the ability to instantly reach people from anywhere. You can use Facebook to stay in touch with your old high school friends who may have relocated all over the world, Google Hangouts with relatives who live halfway around the world, or connect with new people on Twitter from different cities and other regions of the world (Elise , 2019).

In addition to the simplified lines of faster and easier communication, there is the aspect of general availability. It's now faster than ever before to contact the right people and often times without having to even pick up a phone and it is only becoming easier as more people and brands use social media platforms to keep in contact with the people that matter most to their business. Clients can now communicate real feedback in real time (Sam , 2019).

Social media platforms have played a very big role in the recent times of the Corona Virus Pandemic (Covid-19) throughout the world. There is no better impact of online activity than during this change of the new normal. School assignments were being handed out on Google classroom, meetings are happening on Zoom, Google Hangouts and Microsoft Teams. Social media has facilitated mass sensitizations about the virus through the use of Facebook live and the Facebook COVID-19 Information center. These have played a significant role in both information sharing and live broadcasts to the masses all over the world about the current pandemic (D'Urso, 2020). The rush to these services however, has brought new scrutiny on privacy practices (Koeze & Popper, 2020).

Social media boosts organic visibility. There’s so much potential value to be unlocked through the networking and partnership-produced by backlinks using Search Engine Optimization (SEO). Social media also sends relevancy signals to search engines like Google to ensure popular content is easily visible and shareable (Sam , 2019).

The law enforcement community is increasingly turning to social media monitoring to prevent and investigate crimes. Social media monitoring has helped Law Enforcement Agencies find evidence, identify and locate suspects, solicit tips, and alert the public about crimes. The West Midlands Police agency of United Kingdom used a tip from Tumblr to prevent a teen suicide (William , 2015).

Social media platforms such as LinkedIn give you an opportunity to talk about what you know and what you want to be known for. By doing this, the sharing of expertise is harnessed which in turn revolves into a multiplier effect that will attract potential professional and personal connections. Social media is a land of new opportunity that enables one to present their professional experience, achievements and results and hence getting an avalanche of opportunities to connect with like-minded people which is termed as social capital (Koch, 2018).

Social networking is just plain fun sometimes. It relieves stress by providing platforms for general fun and enjoyment. A lot of people turn to it when they catch a break at work or just want to relax at home. Since people are naturally social creatures, it's often quite satisfying to see comments and likes show up on our own posts, and it's convenient to be able to see exactly what friends are up to without having to ask them directly (Elise , 2019).

2.3 Negative Effects of Social Media

The social media evolution in the arena of government engagements with its citizens, market branding and the security sector has come with both inherent and residual risks. These are cultural, technical and reputational in nature and must be factored into planning (Tran & Bar-Tur, 2020). However, these risks should not dissuade one from using social media.

Social media is often tagged with misinterpretation of material facts. Information and views can be spread very quickly and widely through online social platforms and can easily be subject to misinterpretation and misrepresentation. This is termed as content going viral. A post by government employees may be inaccurate or inappropriate thus creating legal or reputational risk. Once online material is made public, there is little control or influence over how it might be used, modified or integrated (Davis S. E., 2018).

Social media is synonymous with high volume traffic sites and user accounts that are associated with code links like “likes” and “followers” and this may create an opportunity for cyber perpetrators to inject malware or spyware into some of the fancy content like latest fashion brands, sports, political activism and not forgetting pornography. Some sites may be open to manipulation by interest groups or those with malicious intent. In addition, there is no guarantee that privacy can be protected once online (Roger , 2016).

Whilst social media has enriched peoples’ lives and made the world a “smaller” place, it is also an enabler for a range of criminal activities. It is used by cyber criminals for information gathering, escalation of attacks and recruitment (Sandie , 2018). The reach of social media is so wide spread that many people misuse the same for their own selfish gratifications; these may include creating revenge porn materials, cyber bullying, stalking, trolling, creation of ‘fake avatars’ for harassing others especially women. Children are considered as most vulnerable persons in the social media because of their level of maturity and understanding in regard to privacy and safety settings (Halder, 2015).

2.4 Categories of Social Media Threats and Crimes

A threat refers to a new or newly discovered incident that has the potential to harm a person, system or an entire organization. These include; Natural threats, such as floods, hurricanes, or tornadoes, Unintentional threats, like an employee mistakenly accessing the wrong information and Intentional threats, such as spyware, malware, adware companies, or the actions of a disgruntled employee (Stephen , 2020). Crime refers to the use electronic and digitally based technology to attack computers or a computer network. Such crimes include the hacking of computers or any unauthorized use or distribution of data, denial of service attacks and distribution of computer viruses (Europol, 2022).

The social web and particularly social media data have considerably grown in the past few years. Advancement in technologies over the last 20 years has affected virtually every aspect of the way we live and conduct our daily lives. Whilst these technologies are a source for enabling social and economic progress around the world, hardly a day goes by without news of yet another cyberattack, or the use of technology in the commission of crime (Anderson & Rainie, 2018). These are categorized as crimes against people, property and governments.

2.4.1 Crimes against People

Online threats, stalking and bullying are the most commonly reported crimes that occur on social media. Additionally, creating fake accounts or impersonation accounts to trick people can also be punished as fraud depending on the actions taken by the fake or impersonation account holder (Khoury, 2017). Whilst most of this type of crime goes unpunished or isn't taken serious, victims of these types of crimes frequently don't know when, how or even where to report since at times it may divulge their privacy (Coolidge, 2022).This category includes other crimes as;

(i) Harassment.

This is very common type of harassment through sending letters, attachments of files & content through Social Networking Sites i.e., Facebook, Twitter & Instagram (Cross, 2014).

(ii) Cyber-Stalking:

It is expressed or implies a threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos (Awati, 2021).

(iii)Defamation.

It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some audio-visual content with using derogatory or libelous language to persons (Zakari & Harun, 2020).

(iv)Hacking.

It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network (Berg, 2020).

(v) Pharming.

The fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords and account numbers (Dalla & Geeta, 2016).

2.4.2 Crimes against Property

Unauthorised access (hacking) and fraud is another form of social media crime. Although logging into a friend's social media account to post an embarrassing status message may be forgivable between friends, it can be a serious crime. Connecting over social media for business or buying legal goods or services is perfectly legitimate. However, connecting over social media to buy narcotics, or other regulated, controlled or banned products is illegal. These include but are not limited to;

(i) Intellectual Property Crimes.

Any unlawful act by which the owner is deprived completely or partially of his rights is a crime. The most common type of Intellectual Property Rights (IPR) violation may be said to be software piracy, infringement of copyright, trademark, patents, designs, service mark violation and theft of computer source code (Jürgen , 2022).

(ii) Cyber Vandalism:

Vandalism means deliberately damaging property of another it includes destroying or damaging the data or information stored in computer when a network service is stopped or disrupted. These acts may take the form of the theft of a computer, some part of a computer (Dalla & Geeta, 2016)

2.4.3 Crimes against government

(i) Cyber Terrorism

Cyber terrorism is one of the domestic and global concern. Terrorist attacks on the Internet are normally committed through the distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer network etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation (Daniel, 2014).

(ii) Cyber Warfare

It refers to politically motivated hacking to conduct sabotage and espionage. Distribution of printed software: - It means distributed printed software from one computer to another intending to destroy the data and official records of the Government.

Therefore, as social media technology advances, criminals have taken on such platforms to post videos of their criminal activities. While this sounds somewhat horrifying, it really is just being myopic since law enforcement agencies and prosecutors are probably going to rely on these videos to conduct arrest and convict these criminals (Mohney, 2017).

On the other hand, one common practice among burglars is to use social media to discover when a potential victim is on vacation. If your vacation status updates are publicly viewable, rather than restricted to a friend group, then a potential perpetrator can easily see when you are going to be away for an extended period of time. The fraudster can easily pose as an employee of a company by creating a Facebook page and may invite other employees to join. This may lead to leaking of company’s confidential information and sabotaging its image (Khoury, 2017).

A report conducted by RSA (Rivest, Shamir, and Adleman) Security, an American computer and network security company states that social media fraud initially started in 2011, when e-commerce sites began publishing accounts and credit card details. These sites became a breeding ground for the commission of fraud since they were usually easy, free and had a global reach (Shareen & Tariq, 2018).

2.5 Social Media Threats and Crimes in Uganda

By end of 2018, over 21 million Ugandans were using the internet which makes 48% of the total population (Mukiza, 2019). The increasing use of Internet has given rise to use of social media for sharing advertisements, live streaming of events, news and opinions. Social media has broken down barriers in communicating and is being used by people of different genders, ethnic groups and political affiliations (Stasi, 2019) . However, it has also given birth to online threats and crimes such as hate speech or cyber bullying, because anyone with a smartphone is a potential media house without an editor to scrutinize their content (Shikati, 2017). Social media platforms such as Facebook, Instagram, Pinterest, YouTube, LinkedIn, Google+, Flickr, Snapchat, Twitter and Tumblr whose main purpose is to share information on borderless online communities have become more intrinsic to our daily lives. These are crucial attack vectors that enterprises can no longer ignore (McGuire, 2019).

Social media crimes and threats in Uganda are mainly through email, social networking site scams and SMS where people are defrauded of huge amounts of money to buy non-existent products on promise of some future returns. According to the Uganda Police Force Annual Crime Report of 2019, a total of 248 social media related cases were reported compared to 198 cases of 2018. This resulted into a loss of over Ugx. 11,446,603,500 in 2019 of which only Ugx. 51,890,000 was able to be recovered (UPF, 2019). Such crimes are normally carried out by impersonating persons through the use fake Facebook accounts of "high-profile" personalities to fraudulently obtain money from the victims. Facebook removed more than 3.2 billion fake accounts between the months April and September 2019, compared with more than 1.5 billion during the same period last year (Palmer, 2019). It is also reported to have removed 11.4 million pieces of hate speech, compared with 5.4 million in the same six-month period in 2018 (Palmer, 2019).

Uganda has not been an exception to social media defamation cases. This was witnessed in Thomas Voltaire Okwalinga (TVO), a blogger and harsh critic of President Museveni's case where in a court ruling, the Irish court's ruling granted him immunity for e fear of him being harmed by the Government of Uganda (Derrick, 2016). Furthermore, Dr. Stella Nyanzi, a Ugandan human rights advocate, poet, medical anthropologist, feminist, queer rights advocate, and scholar of sexuality, family planning, and public health was charged with offensive communication and cyber harassment in accordance to the Computer Misuse Act 2011 (NITAU, 2011). Geoffrey Kalele, a resident of Namutumba district was charged over allegedly impersonating as the Inspector General of Police (UPF, 2018).

The release of pornographic material as a blackmailing technique is also considered another social media threat known as revenge porn in Uganda. This was witnessed in the case of comedian, radio personality and photographer, Martha Kagimba, popularly known as Martha Kay's nude photos that were circulated on social media, days after her mobile phone was stolen (Muliisa, 2019). The Buganda Road Chief Magistrate court charged and remanded to Kitalya Prison five people on charges of hacking into Airtel money services and stealing millions of shillings from unsuspecting customers. The group, who are all residents of Namasuba Kikajjjo zone in Wakiso district are said to have defrauded businessman Salim Ssserujja of shs. 10m (Ten million) by gaining access to his phone after sending him One Time Password message (OTP) and convincing him to read the message after calling him. Then they transferred the money from his phone mobile accounts (Namutebi, 2021).

2.6 Theoretical Underpinnings to Social Media Crime

According to William Anderson (Anderson, 2019), social media crime is inspired by four basic theories of crime namely: classic, biological, sociological and interactionist theory.

2.6.1 Classic Theory

In the classic theory, Anderson asserts that social media crime is caused by the individual's free will. Human beings are rational and make decisions freely and with understanding of consequences, but such behaviour weakens society.

2.6.2 Biological Theory

In biological theory, the basic determinants of human behaviour are to a considerable degree, determined by genetics. These basic determinants of human behaviour may be passed from one generation to the next. Human DNA, environmental contaminants, nutrition, hormones, trauma to the brain, exposure to drugs and alcohol during pregnancy and body chemistry can all contribute to criminal behaviour.

2.6.3 Sociological Theory

In sociological theory, social environment is known to be the cause of criminal behaviour. The human behaviour is a product of the social relations within the family and society. The belief systems of society therefore, act as a catalyst to human behaviour. People engage in criminal behaviour because they do not see the benefits of adhering to conventional social values and believe that crime is a way to improve their social and financial conditions.

2.6.4 Interactionist Theory

In interactionist theory, association with other criminals is the factor that mainly contributes to criminal behaviour among individuals. Failure of self-direction and inadequate social roles are the root causes of behaviour. Individuals are always looking for acceptance, social standing and power within that group, and offenders have the responsibility and ability to change their own behaviour.

As a solution, opportunities for positive interaction with society will enable the criminal to choose productive and lawful behaviour to meet needs. But also, punishment is a necessary evil sometimes intended to deter criminals and serve as an example to those who would violate the law and crime prevention is possible through swift and certain punishment that counters possible gains from criminal behaviour

On the other hand, the theoretical connection between social media and crime can be explained from three main perspectives. The Wound Culture Theory (WCT), social control and conflict management theories in a scenario and irrespective of the direction of effect whether positive or negative both strands of theoretical underpinnings rely on technology acceptance models. The three theoretical frameworks are expanded in chronological order. The WCT can be used to elicit some negative socio-economic signals such as crimes, political instability, and violence (Asongu, 2019). According to the WCT, the desire to inflict harm on humans in society is both literal (via mutilation) and figuration (via criticism). The relevance of crime is considered within the theoretical framework as a common focus which enables citizens to engage in wound appreciation: *"One discovers again and again the excitations in the opening of private, bodily and psychic interiors; the exhibition and witnessing, the endlessly reproducible display, of wounded bodies and wounded minds in public*" (Asongu, 2019). In wound culture, the very notion of sociality is bound to the excitations of the torn and open body, the torn and exposed individual, as public spectacle". Social media can be used to fuel the wound culture because it is a mechanism by which information is exchanged to either increase contention or hatred among users or improve harmony and moderation among them.

In the latter scenario, conflict management and social control models are more relevant. Social control and conflict management models have been used to substantiate theoretical underpinnings in recent conflict management literature (Asongu, 2019).

In the third theory, these rational traits could motivate new ideas, notably: either to the resolution of conflicts or in the perception of crime as a solution to conflicts

The three strands of theories clearly explain how social media can either be used to fuel or deter crime. However, the use of social media to fuel crime is consistent with the Wound Culture Theory while the use of the social media to mitigate crime is in line with the social control theory and the Conflict Management Model. Hence, the selection of a social media platform by a user is contingent on the relevance of the social media network in attenuating or fueling crime.

The purpose of reviewing these theories was to understand why people commit crimes and in particular social media crimes. It was observed that some are genetic or in-born with high affinity to commit crime, others it's as a result of the social relations such family background or parenting environment and others its by their individual will. But, needless to say, is the fact that also criminality is groomed through interaction with individuals of bad character. Therefore, the prevention approaches should be able to address all categories which may involve apprehensions and awareness building.

2.7 Social Media Threats and Crime Awareness Frameworks and Methods

2.7.1 Situational Crime Prevention Framework

Situational Crime Prevention (SCP) is a process of multiple stages and seeks to understand where, when, and how crime incidents occur. It has sought to alter environments which host crime behavior in order to make them less suitable for offending. This Framework aims to increase risk and/or minimize reward, thus making either the commission of a criminal act too difficult, or the reward for committing the act too low to risk being caught (Shariati, 2017). When applied to social media crime, SCP measures focus on reducing and/or denying offenders' opportunities for offending and impeding their ability to offend. Technical cybercrime prevention measures are a form of situational crime prevention. A few examples of these technical measures include malware detection software, firewalls which prevent unauthorized access by examining traffic and blocking traffic, and intrusion detection and prevention systems that enable the detection of cyber-attacks and unauthorized access and use of systems, networks, data, services, and related resources (UNODC, 2020).This kind of framework assumes that all the measures are in place to access the vulnerabilities in the environment and create mechanism to prevent crime. It's expensive to implement and requires that the end users are technically prepared.

Several approaches are identified which in different respects imply modifications to the situational crime prevention framework in order to accommodate assumed specificities of 'organized crime', including 'organized' criminal activities transcending space and time, and 'organized' criminals being capable of selecting and shaping crime settings. It is argued that while a situational approach to the study of 'organized crime' is useful in some respects, in other respects the conceptual framework of Situational Crime Prevention (SCP) needs to be modified to a point where its universal applicability is called into question (Lampe, 2011).

2.7.2 Theoretical perceptive and possible remedies to crime causation

The table depicts the offender-based research situational crime prevention approach. It can be used to understand crime causation and prevention approaches, namely by directly determining what works to reduce crime, generating findings that are suggestive of what prevention measures to invent and employ, refining understanding of why a given prevention method reduces crime, figuring out how offenders get around particular prevention measures; and gathering information on not only the positive but also the unintended, negative outcomes of prevention procedures (Scott & Bonomo, 2017).

Table 1: Comparison of crime causation and prevention theories

Theory of Crime	**Characteristics or Beliefs of Theory**	**Solutions to mitigate the crime**
Classical	• Crime is caused by the individuals free will • Human beings are rational and make decisions freely and with understanding of the consequences. • Crime is an immoral form of human behaviour	• Punishment for those who violate the law • More prisons and stiffer criminal laws
Biological	• Genetics to a considerable degree	• Historically, individuals with

Theory of Crime	**Characteristics or Beliefs of Theory**	**Solutions to mitigate the crime**
	determine human behaviour. • These may be passed from one generation to the next • Human DNA, environmental contaminants, nutrition, hormones, trauma to the brain, exposure to drugs and alcohol during pregnancy and body chemistry can all contribute to criminal behaviour (Balhara, 2021).	genetic defects have been sterilized (meaning there will be no offspring) • Need for more Research into finding genes that encourage criminal behaviour. • Research into medicines such as tranquilizers, anti-psychotic drugs and other mood-altering drugs to control behaviour.
Sociological	• Social Environment as the cause of criminal behaviour • Weak, broken bonds with family, school, religion as catalyst to human behaviour • People engage in criminal behaviour because they do not see the benefits of adhering to conventional social values and believe that crime is a way to improve their social, financial conditions	• Social programs that change the cultural and social conditions that lead people to commit crime. • Government programs with funding to alleviate poverty
Interactionist	• Association with other criminals is contributing factor to criminal behaviour among individuals. • Failure of self-direction and inadequate social roles that	• Offenders have the responsibility and ability to change their own behaviour. • Opportunities for positive interaction with society will

Theory of Crime	Characteristics or Beliefs of Theory	Solutions to mitigate the crime
	determine behaviour patterns. Individuals are looking for acceptance, social standing and power within a group (Anderson, 2019)	enable the criminal to choose productive and lawful behaviour to meet needs especially through awareness drives.

2.7.3 Social Media Awareness and Education Framework

This framework presents social media adoption process as a formal educational tool for the development of social media implementation processes, and assists in understanding the influence of social media on education environments (Mostafa & Jamal, 2020). Awareness and education play a fundamental role in preparing all groupings of society for promoting a culture of digital safety as a preventive approach. Particular attention needs to be drawn to the social network's contextual aspects in coping with the fear of victimization on Social Networking Sites (SNS). In that sense, a public awareness campaign can play a vital role in teaching users how to use social media more wisely (Kortjan, 2013). The aim of the awareness campaign is to help users find safer ways to use social media. Despite the fact that there are many benefits of using social media, such as staying connected with friends, interacting with others who share similar interests, and communicating with others by sharing ideas and information, the campaign sheds light on the shortcomings of social media and instructs users on how to take advantage of social media while cautioning them about risks users should avoid (Lee et al., 2019)

Uganda has also stepped-up efforts in creating social media awareness especially during workshops and online forums. For example, Bloggers and Internet Activists have urged people to exercise a sense of sisterhood and brotherhood and practice digital phone etiquette to protect their images when using the Internet. This, they argue, should help steer them clear of potentially being victimized or being caught up on the wrong side of the law (Nabisubi, 2019)

Furthermore, the Uganda Communications Commission issued a public notice on their platforms, warning against irresponsible use of social and electronic communication platforms (UCC, 2017) and further created a complaint handling procedure for the consumers. This is also embedded with a live chat forum that can be used to escalate all Computer Emergency Risks to the Computer Emergency Response Team (UCC, 2020). The Commission has got a formidable team of experts and equipment aimed at identifying, defending, responding and managing social media threats and crimes within the Communication sector. The competent team is able to monitor, coordinate and respond to any alerts of cyber-attacks (Mwesigwa, 2015). However, on the contrary not many Ugandans are aware of its existence or even know how to escalate social media threat incidences. Among the millions of online users in Uganda, only 20.1% are aware that they can report such incidences to law enforcement and other agencies under the Computer Misuse Act 2011 while only 3% have ever reported online crimes. Also, only 90.8% have at least signed up to an online social networking site (CIPESA, 2018). This is a clear indicator that the CERT has not yet been popularized. This approach empowers the end users to detect and prevent crime beforehand. However, it must be conducted regularly or on routine basis since technology keeps evolving.

2.8 Web-based System for reporting and creating awareness about social media threats and crimes.

Social media is the present-day platform for sharing information and getting connected and reconnected with friends and acquaintances. We look at Twitter to know the daily ‘trends’ to know what is happening around us, we get connected to people and organizations through Facebook to grow our information circle. Uploading and sharing private videos with strong messages onto YouTube Channels and TikTok enables the world-wide audience to learn about trending issues such as COVID-19 pandemic, catastrophes like earthquakes, floods, accidents, relief distribution or plight of laborers in the world (Schwind & Bayliss, 2020).

2.8.1 ePOOLICE:

The European Commission under the Seventh Framework Programme for Research and Technological Development (FP7), funded the ePOOLICE (Early Pursuit Against Organized Crime Using Environmental Scanning, the Law and Intelligence Systems) Project, which provides a systematic overview of the surrounding environment to better appreciate, assess and anticipate an emerging crime, by monitoring the environment and capturing in real-time relevant information present in heterogeneous sources. These include: law enforcement analysis reports, governmental information, web, social media, news, academia, non-governmental and international organizations (Pastor & Larsen, 2017). The ePOOLICE solution explores the use of open-source information in order to rapidly detect new emerging organized crime threats. It leverages publicly available data sources such as social media to predict, detect and prevent crime. ePOOLICE has the capability to foresee threats that are likely to emerge (Pastor & Larsen, 2017). Whereas the solution has responsive capabilities, it has got a high dependence syndrome since it relies on various data sources (Larsen, Blanco, Pastor, & Yager, 2017). The emergency of the General Data Protection Regulations for data protection and privacy in the European Union, and the domesticated privacy laws of various states, makes ePOOLICE intrusive in nature and thus violating the said guidelines (Groot , 2020).

2.8.2 The Tip411 Program:

In the United Kingdom, the Leicestershire Constabulary is one of the police departments focusing on being hyper-local and involved with the community through social media that provides for the digital “wanted poster”. The tip411 program developed by the Citizen Observer Corporation is marketed to law enforcement as a web-based notification toolset. Citizen participation in Ashland City of Tennessee has become a big part of fighting crime, and the people at tip411 stress that social media “acts as a ‘force multiplier’ by empowering the community to get involved in the awareness drive. Police in Cincinnati city, Ohio used Facebook and Myspace to follow more than 20 members of a local gang known as the "Northside Taliband." The evidence they gathered helped law enforcement connect members to a multitude of crimes, including a possible homicide (Cohen, 2010). The tip411 project was further adopted in United States of America in particular to the Leander community of Texas. The system operates 100% anonymous by removing all identification information before the police department sees the tip and there is no way to identify the sender. The system permits the community to register via the link so that they can receive and also send alerts from the Leander Police Department. This option is either via email or text message to their cell phone (Leander Police Dept, 2020). This solution has an anonymous tip via Web which enables the public to be proactive thus reduce on the investigative costs. It has a two-way communication with over forty language translation which makes it inclusive. The Tip411 App is embedded with google maps which enables the citizens to view crime trends and threats (Tip411, 2020). The tool is available and user friendly. Therefore, it has extended audience and access up to the prosecution (Gallo, 2015). However, the system does not support the use of basic phones (low end GSMA devices) that use USSD (Unstructured Supplementary Service Data) codes and these are still the most widely used phones in Uganda. As of March 2021, the number of smart phones - multi-purpose mobile computing devices was registered at 8.1 million users well as feature phones - limited application and browsing functionality at 17.9 million users and basic phones – limited to voice calls and text messages were 5.1 million users (UCC, 2021).

2.8.3 Cyber Barometer Information Portal:

The Uganda Police Force created a cyber barometer information portal [1]for creating awareness about the current social media threats and possible remedies (UPF, 2019). In addition, the Uganda Police Force established an Electronic Counter Measure Unit (ECMU) with the mandate to detect and investigate crimes that are committed using online platforms like Facebook, WhatsApp, Instagram and Twitter (Sekyewa, 2019). These developments saw the establishment of a modern forensic laboratory to handle social media cases. Uganda was selected as the Regional Forensic Referral Centre of Excellence for forensics science by The East African Community Chiefs of Police (Nankinga, 2017). However, the facility is now overwhelmed due to increased number cases and has a limited number of qualified personnel to deal with the increased social media crimes (Nankinga, 2017).

2.8.4 Comparison of Web-based system for reporting and creating awareness about social media threats and crimes

In respect to social media threat reporting and crime awareness information systems mentioned in the previous section, it is evident that all systems have unique aspects that can be integrated together to achieve the best web-based system for reporting and creating awareness about social media threats and crime.

[1] https://www.upf.go.ug/download/cybercrime-barometer/Cybercrime-Barometer-A-Uganda-Police-Centenary-Plus-Awareness-Campaign-Paper-.pdf?x89335

However, it should be noted that all these systems have weaknesses and strength as clearly highlighted in Table 2 that provides an overview of some of the web-based system for reporting and creating awareness about social media threats and crimes.

Table 2: Comparison of the functionality of different Web-based system for reporting and creating awareness about social media threats and crimes.

The table highlights the comparison of functionality capabilities of the various systems and approaches in the reporting and creation of awareness about social media threats and crime. These are system that have been used in different parts of the world.

S/N	System Functionalities	ePOOLICE	Tip411	Cyber Barometer Info. Portal
1.	Can be integrated with other social media threat reporting systems.	✓	✓	✓
2.	Supports mobile and web reporting function.	✓	✓	✓
3.	Trend analysis and reporting trends	✓	x	x
4.	Automated and anonymous threat reporting function	x	✓	x
5.	External users and non-registered users can report crimes and threats and crime tips	x	x	x
6.	Location tracking and visualization of locations with high crime concentration rates.	✓	✓	x
7.	Analytics and reports about crime and social media threats.	✓	✓	✓
8.	Language Translation	✓	✓	x

Key

Symbol	Description
✓	System can perform the function
x	System cannot support that functionality.

Table 2 shows eight (8) of the basic functionalities commonly offered by the different web-based system for reporting and creating awareness about social media threats and crimes used in various countries. The two systems can integrate with other systems and produce reports of incidents and crimes. The developed solution was able to address all the functionalities as highlighted.

2.9 Cyber Laws, Prosecution and Specialized Courts in Uganda

With the increased use of computers and more especially the Internet, new types of crimes have evolved that target computers or involve the use of computers to commit crimes. Social media crimes and threats can have a direct impact on peoples' lives where data is lost, money is stolen or a person's privacy is infringed upon (NITAU, 2011). According to the National IT Survey Report of 2022, Uganda has 98% of her labor force in mainstream government Ministries, Departments & Agencies using the Internet for email services and, 78% are using it for social media and instant messaging application (Mugasa, 2022). This underscores the need for a robust cyber legislative framework regime.

2.9.1 The Computer Misuse Act of 2011

The Law provides for the safety of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters (MoICT&NG, 2019). The Cyber laws are meant to tackle social media threats and crime by addressing Intellectual Property Rights, Copyrights Protection, enable e-commerce to facilitate trade and to regulate the use of electronic signatures to ensure security (confidentiality, integrity and availability) of communication and non-repudiation (InfoSec, 2019).

2.9.2 The Electronic Transactions Act, 2010

The Act was passed to provide for the use, security, facilitation and regulation of electronic communications and transactions; to encourage the use of e-Government services and to provide for related matters. Social media has got applications that complement existing e-government services such as Twitter & Facebook. It is therefore, imperative that e-government services are regulated and secure through such legislations (ICT Policy Africa, 2019).

2.9.3 The Electronic Signatures Act, 2010

The law was enacted to make provisions for and to regulate the use of electronic signatures and to provide for related matters. Electronic signature makes everyday life easier and offers a modern way of confirming the signatory's identity. This law supports the enforcement of verifying identities of persons using the social networking sites (Ministry of ICT&NG, 2019).

2.9.4 The Uganda Communications Act, 2013

The Act was enacted to regulate the Communications sector, which includes Telecommunications, Broadcasting, radio communication, postal communications, data communication and infrastructure. Cognizant of the fact that social media is a form of mass communication, this law therefore, provides for remedies for social media threats and crimes. It equally regulates such platforms so as to ensure responsible behaviour. This is stipulated under section 5 (b) which states; to monitor, inspect, license, supervise, control and regulate communications services. Therefore, social media which is now the new media has also now been incorporated in the Uganda Communication Act and Regulations. There is now a call for bloggers and ardent social media users to get registered for regulatory purposes by the Commission (Agencies, 2020).

In 2019, the Uganda Communications Commission gazetted various regulations to operationalized the Uganda Communications Act of 2013. These regulations have created a new licensing framework to new services and industries such as social media. This is aimed at improving the regulatory environment in relation to consumer protection issues (UCC, 2019). These regulations include but are not limited to; Central Equipment Identify Register Regulations, CERT Regulations 2019, Competition and Accounting Regulations. 2019, Consumer Protection, Content Regulations, Emergency Response 2019, Fees and Fines regulations No. 2 of 2020, Intelligence Network Monitoring System, Quality of Service Regulation & Universal Services and Access Fund. These are to establish necessary controls and provide rules for those pushing out content which could easily violate the known parameters of morality, incitement and ethnic prejudice. However, the civil society has tagged them as restrictive, forcing many who publish online content, to pay a yearly fee and register for monitoring purposes. This is an infringement of Ugandans constitutionally protected rights to freedom of speech and expression (Rukwengye, 2019).

2.9.5 The Data Protection and Privacy Act, 2019

The Law was passed in order to protect the privacy of persons and of personal data by regulating the collection and processing of personal information, to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers and to regulate the use or disclosure of personal information. The Law seeks to ensure that social media threats of unauthorized access and identity thefts are addressed by enforcing the right to privacy on public platforms. Furthermore, the draft social media regulations that were issued by the National Information Technology Authority (NITAU, 2013) are all geared towards the protection of online users.

2.9.6 The National Payments Systems Act, 2020

The Act seeks to bridge this gap by providing for the safety and efficiency of payment systems; the regulation of payment systems, payment service providers and the issuance of electronic money, among others. It includes institutions (banks, financial institutions and non-financial institutions), the procedures and technology that is used to facilitate the circulation of money within the country and internationally. This law provisions for regulation of mobile payments and related service providers by creating a safe environment to combat social media threats and crime related to electronic frauds (PwC, 2020).

In conclusion, albeit all the Cyber Legal frameworks in place, for compliance to be enforced, there is need for the acceptable social media operating norms and regulations, consumer protection campaigns, and increase financial inclusion to electronic payment services in Uganda.

2.9.7 National Social Media Guidelines

The National Information Technology Authority of Uganda (NITA-U) developed Social Media User guidelines to facilitate Government Ministries, Departments and Agencies in the process of adopting social media as one of the platforms for engaging with the citizens of Uganda (NITAU, 2013). These guidelines are meant to ensure uniformity in communicating and appropriate consultation before posting government communication online. They are available online for customization. However, the guidelines are still in draft form and have not yet been finalized and are not yet in use in most Ministries, Departments and Agencies of Government Consequently, the National IT survey report of 2018, indicates that 92% of Ugandan Ministries, Departments and Agencies had a social media presence (CIPESA, 2018).

2.9.8 Cybercrime Unit in the Office of the Director of Public Prosecution (ODPP):

The Office of the Director of Public Prosecution created a cybercrime unit to prosecute offences of online related crimes and threats (Kairu, 2020). Whereas all these initiatives are geared towards reducing the increased social media crimes and threats, the current number of judicial officers and prosecutors is still limited compared to the sporadic online threats. Furthermore, the present laws cannot compel other jurisdictions where the crimes or evidence may be resident to cooperate except under Mutual Legal Assistance (MLA). The challenge in the enforcement of social media laws is jurisdiction. Taking into cognizance the time-tested principles of state independence, sovereignty and territorial integrity, each nation of the world has the authority to enact laws that are binding within its geographical entity (Ajayi, 2016).

2.9.9 Standards, Wildlife and Utilities Division

In 2016, Uganda established a specialized court to handle ICT/Utilities related crimes in the Communication sector such as social media threats and crime. This is the Buganda Road Standards, Wildlife and Utilities Court which adjudicates over matters in the sector (Ntezza, 2017). Under the Magistrates Courts, a special division was created to provide specialization in the adjudication of criminal cases involving standards, utilities and wildlife. The Division was empowered to try any offence related to standards, consumption of utilities and any other related Act; this in effect, included the Computer Misuse Act, 2011. Therefore, the Standards, Utilities and Wildlife Division is subject to the provisions of the Computer Misuse Act, 2011 (Timothy, 2021).

2.10 Challenges of Investigating Social Media Threats and Crime

Some of the major challenges when dealing with prevention and prosecution of social media related criminal activity in developing countries in general, revolves around three issues namely: the reach of social media, identification of social media users and the applicability of the legal frameworks and laws (Thaddeus, 2014).

2.10.1 The wide pool of potential victims

Social media has an expansive reach of billions of online users (Akram, 2018) and a pool of potential victims for criminal perpetrators that has grown exponentially. This creates an opportunity for cyber perpetrators to easily reach the intended victims. In addition, it creates a platform to repeat the crimes and can harm victims rapidly and repeatedly (Simon , 2019).

2.10.2 Speed and live spread online crimes

Often, real-time crimes are streamed live on social media which then makes then viral. In such situations, law enforcement needs to be able to quickly inform the platform owners to take down such content or even respond which many times may not be feasible since they do not have compelling powers over another jurisdiction or over a private entity (big data owners) such as Facebook, Twitter & Google.

2.10.3 The Language used on social media

Social media communications are at times difficult to comprehend because of the language style which is dynamic and constantly changing with the use of jargons and emojis to depict content. The most sophisticated disinformation operations use troll farms, artificial intelligence and internet bots to flood the zone with social media posts or messages to make a fake or doctored story appear authentic and consequential (Shelly , 2019).

2.10.4 Capacity Inadequacies

Crimes are often reported by sharing text, photos, or video on social media or directly with law enforcement. In such situations, geo-location or entity resolution of who is in the picture, when the picture was taken, where the incident took place, why it happened and how it all started, is still laborious since the law enforcement officers may not be analytical and vastly exposed to such scenarios (Hollywood et al., 2018).In today's society, cyber criminals are *going dark* and are using technology that is incapable of providing subscriber content to law enforcement officers even when provided with a Legal Court Order. Such tools include the use of: Onion Routers, Proxy Servers, Virtual Private Networks, Anonymized platforms to channel emails. The kind of disinformation now known as fake news has tainted public discourse for centuries. It's been amplified in our digital age as a weapon of fear mongers, mob-baiters, election-meddlers who undermine democracies and bolster authoritarian regimes (Shelly , 2019) .

2.10.5 Jurisdictional Bottlenecks

Whereas, what may be termed as unlawful behaviour in one jurisdiction, it is legal in another. This kind of legal paradox allows offenders to choose jurisdictions for their websites that have the least harsh legal consequences. In addition, maintaining anonymity or bogus identities during the commission of crimes, is easier in virtual spaces than in real physical spaces. Apps, avatars, disposable devices, and the *deep web* where search engines cannot detect websites due to an added layer of security, facilitate the concealment of criminal transactions, socialization into subcultures, and networking of those involved in illicit or nonconventional behaviour like social media crimes (Stalans & Finn, 2016).

2.11 Remedies to Social Media Threats and Crime

There is a predominant need for research and development of law enforcement applications, including research and evaluation on social media monitoring and social network analysis tools and techniques as applied to law enforcement applications; and tools and techniques supporting search and interoperable data extraction from a full range of social media postings such as text, images, videos among others (Serianu, 2018). The use of evidence mining tools that can identify geographic features in images and correlate them with known locations and individuals such as

TrafficCam.com, Google Earth, Maltego, Creepy and Griffeye Analyze have some of these functionalities (Khode et al., 2015).

Identification of knowledge gaps in order to conduct the studies, analyses, and educational material development needed to prepare law enforcement focused materials for social media and social network analysis training (IFIS, 2018). Creating help desks and hotline for interacting with social media companies. On many occasions, law enforcement officers are unable to access non-public social media data needed for specific investigations effectively due to the runtime costs involved, the existence of procedural hurdles, technical barriers such as cloud storage where the data is broken up or shredded and stored in different locations potentially in different countries with different jurisdictional rules and regulations (Hollywood et al., 2018)

Due to the different means of data storage and processing of cloud social networks, social media digital forensics processes need to adapt to innovative approaches of carrying out collection, preservation and presentation of digital evidence as obtained from such platforms. This will improve efficiency and performance of investigations (Filipo , 2013).

2.12 A Web-based System for reporting and creating awareness about social media threats and crime as A Solution

Social media threats and crimes are on the raise (BarefootLaw, 2019). In order to minimize these crimes, new and more stringent regulations and reinforcement of the current cyber laws may not yet yield much without increased awareness about privacy issues, vulnerabilities and digital hygiene (InfoSec, 2019). Creating awareness about such issues should be the primary focus of governments, law enforcement agencies and other stakeholders to prevent people from falling victims of social media threats and crime. Therefore, the web-based system for reporting and creating awareness about social media threats and crime in Uganda will play a key role in solving the problem at hand.

CHAPTER THREE: METHODOLOGY

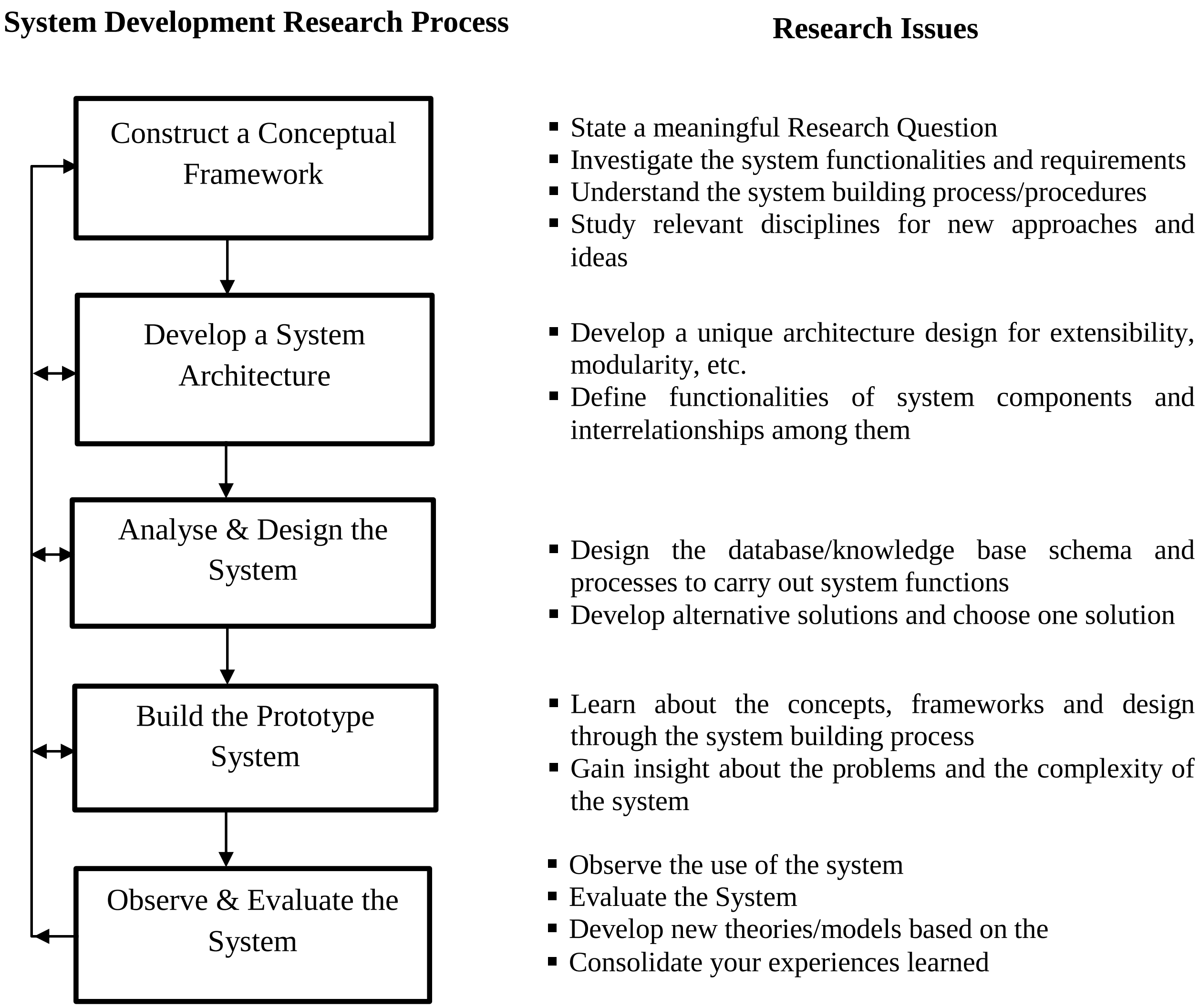
3.0 Research Methodology

This chapter describes the methods and tools that were used to achieve the objectives of this study. The system development methodology, could be thought of as a “proof by demonstration” according to (Burstein, 2002) and was adopted for this project. According to this research methodology, problems exist in a research domain and are encountered by observation. One forms a hypothesis and attempts to confirm and to generalize on the hypothesis through analysis. The analysis may take different forms including development of system prototypes. The result of the analysis becomes the argument (and evidence) in defense of the original hypothesis (Gregg, 2001).

The research methodology is the philosophy of the research process that includes the assumption and values that serve as a rationale for research and the standards or criteria the researcher uses for interpreting data and reaching a conclusion (Nunamaker, Chen, & Purdin, 2001).

3.1 Research Process

A research process involves understanding of the research domain, asking meaningful research questions and applying valid research methods to address these questions (Nunamaker, Chen, & Purdin, 2001). The system development research process is illustrated on the next page.


System Development Research Process
Construct a Conceptual Framework
Develop a System Architecture
Analyse & Design the System
Build the Prototype System
Observe & Evaluate the System

Research Issues

- State a meaningful Research Question
- Investigate the system functionalities and requirements
- Understand the system building process/procedures
- Study relevant disciplines for new approaches and ideas

- Develop a unique architecture design for extensibility, modularity, etc.
- Define functionalities of system components and interrelationships among them

- Design the database/knowledge base schema and processes to carry out system functions
- Develop alternative solutions and choose one solution

- Learn about the concepts, frameworks and design through the system building process
- Gain insight about the problems and the complexity of the system

- Observe the use of the system
- Evaluate the System
- Develop new theories/models based on the
- Consolidate your experiences learned

Figure 1: A Process for Systems Development Research

3.1.1 Problem Analysis

Problem analysis was undertaken using the IDEAL Problem-Solving Model Approach of; identifying the problem and opportunities therein, defining the goals, exploring possible strategies, anticipating outcomes with action and then generating feedback from looking back and learning (Nickols, 2020). This was clustered into five stages of: planning, data collection, recording of the information; interpreting the collected information and specifying the requirements for the web-based system for reporting and creating awareness about social media threats and crime in Uganda.

At the planning stage, the kinds of research questions required to examine the nature and extent of the problem and to investigate the solution to address the need were generated. Targeted respondents were identified and necessary appointments sought by telephone call and email. Furthermore, the data collection guides were prepared in form of online questionnaire using google forms. The data collection stage involved all the fact-finding activities carried out as part of the analysis. The key techniques included Interviews through Focus Group Discussions (FGD), Online questionnaires, observation and document review.

The data collection stage yielded many facts and details about the current and required systems which was recorded and reviewed by some of the respondents to verify the gathered information.

The information collected was interpreted and processed into system requirements for the proposed a web-based system for reporting and creating awareness about social media threats and crime, which were categorized as functional and non-functional (performance and reliability) requirements.

3.2 Requirements gathering

In order to achieve the objective of collecting requirements for development of a web-based system for reporting and creating awareness about social media threats and crime, an online questionnaire was developed using google forms. The questionnaire which was accessed vide: https://forms.gle/Lai6u9DSwsT256PM6 by 63 respondents. In addition, a Focus Group Discussion was also conducted of 10 respondents as study participants.

Furthermore, I conducted document and system review of some of the already existing systems that perform related functionalities as the proposed system.

All these methods were performed in accordance with the Software Development Life Cycle (SDLC) which is a systematic process for building software that ensures the quality and correctness of the software built. SDLC process aims to produce high-quality software that meets end-user expectations. It consisted of a detailed plan which explains how to plan, build, and maintain specific software. Every phase of the SDLC life Cycle had its own processes and deliverables that feed into the next phase (Martin, 2022).

These include; Requirement collection and analysis, System Design, System Development, Testing and Validation, System deployment and Maintenance.

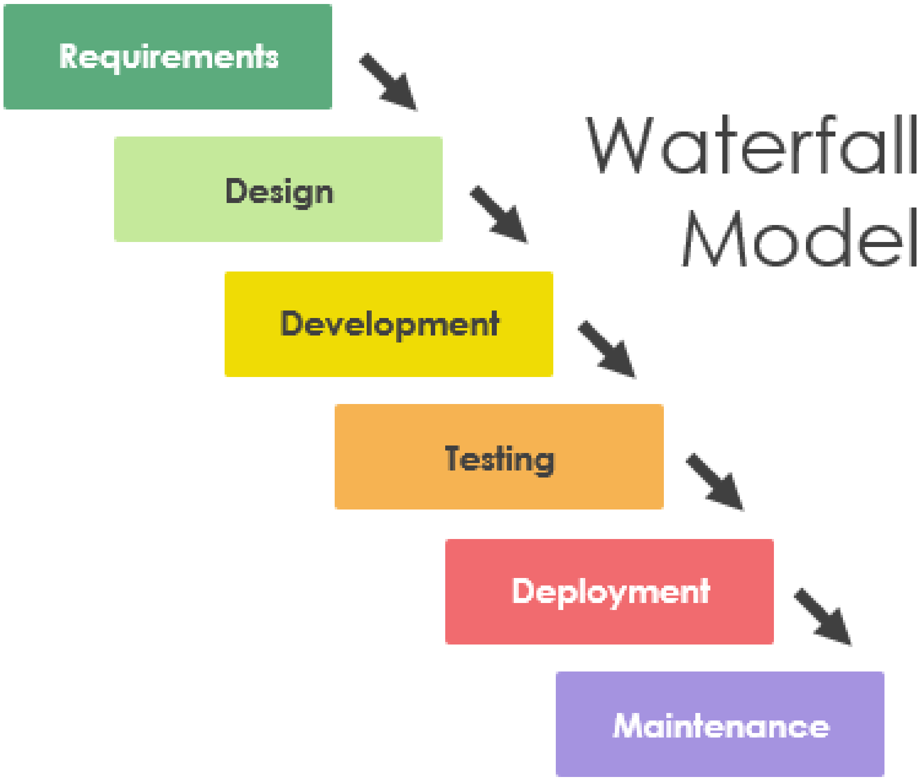


Figure 2: Waterfall Software Development Life Cycle Model

3.2.1 Online questionnaire

The respondents were drawn from the following sectors: Civil Society Organizations (CSO), Non-Governmental Organizations, Financial Technology Firms (FINTECH), Inspectorate of Government, Judiciary, Office of the Director of Public Prosecution, Uganda Police Force, University Students, Telecommunication Companies and the Uganda Communications Commission, the Communication Regulator.

The stakeholders were involved at the inception since they are key players in the social media spaces. For example:

(i) The Civil Society Organization and NGOs

These are advocates of technology inclusion and rights of privacy. Therefore, I opted to get their position of the two aspects. Moreso, they also experience social media threats by virtue of their work so it was important to create a platform to receive their complaints and also provide a system that creates awareness.

(ii) The FINTECH, Telecoms and Communication Regulator (UCC)

These were included at requirement gathering since they are financial end users, providers and regulators of technology and particularly social media platforms in Uganda. Notably, the FINTECH are now using social media for digital marketing and are thus many times victims of social media breach/threats and crime. At the same time, the Telecoms and Regulators provided insight into the approaches that are already at work in the fight against telecom frauds. These inputs created synergy towards the requirements for the system in terms of the type of threats and possible feedback mechanism.

(iii)Government Ministries, Departments & Agencies

This category of stakeholders included; the Uganda Police Force, Office of the Director of Public Prosecutions, Judiciary, Inspectorate of Government. The respondents from this category were able to enrich the requirements for the development of the system by recommended the inclusion of the different social media offences/crimes and Laws the penalize such breaches. In addition, they also stressed the inclusion of data protection and privacy requirements. In addition, as part of the e-governance, they also proposed to the inclusion of the different complaint receipt centers of government and the Toll-free numbers for citizens to find help in case of any suspected social media threats and crime.

(iv)Business community & Students

This category of stakeholders included: Private sector business community such as innovators and exporters as well University students. This is an ardent user group of social media for its routine operations such as digital marketing and research or quest for information respectively. They were able to highlight some of the challenges they face on a daily basis due to social media threats and crimes and thus contributed to the creation of various reporting centers of such crimes and also to the awareness news bulletin since majority of the users are neither naïve or not even informed about the threats on such spaces.

3.2.2 Focus Group Discussion

The FGD drew participants from Law Enforcement, Telecom sector, Civil Society Organization and ICT regulators in Uganda. The discussion was fruitful because it was able to address some of the requirements concerns such as; the common social media threats and crime in Uganda, key strategies being used to disseminate information about social media threats and crimes, how awareness about social media threats and crimes in Uganda can be increased or enhanced and the roles/activities of different players in the prevention and fight against social media threats and crime in Uganda. The stakeholders were selected for the FGD because of the following attributes;

(i) Law enforcement

This category of stakeholder is mandated to enforce all the laws of Uganda. The laws were identified as the Computer Misuse Act, 2011, the Uganda Communications Act, 2013, the Electronic Transactions Act, 2011, the Electronic Signatures Act, 2011, the Data Protection & Privacy Act, 2019 and the National Payment Systems Act of 2020.

In addition, the Uganda Police Personnel were able to inform the discussion about the various social media threats and crime that they are often tasked to investigated. These include: Cyber bullying, Cyber Harassment, Electronic Fraud, Ponzi Schemes, Revenge Pornography and Offensive Communication. All the laws and threats/crimes were incorporated into the development of the system.

(ii) Telecom sector and ICT Regulators

This category was involved in the FGD because of their pivotal role in enabling and regulating communication services either through voice or data. Cognizant of the fact that social media applications are supported by Internet Service Providers of which the telecom sector is not an exception. The telecom sector included participants from MTN and Airtel Uganda and the ICT regulators drew participants from the Uganda Communications Commission. They were able to highlight some of the anti-fraud approaches being used for reporting and creating awareness about telecom related threats and crime and the challenges that the proposed system should be able to address.

(iii)Civil Society Organization (CSO)

The FDG drew participants from two CSOs namely: Women of Uganda Network (WoUGNET) and Collaboration for International ICT Policy for Eastern and Southern Africa (CIPESA). The reason for selecting this category of stakeholder was premised on the fact that they are involving in the advocacy and innovation of inclusive digital technologies as well as digital rights and driving the ICT policy formulation agenda. The participants contributed to the requirement gathering process by recommend for the inclusion of social media threats that address the gender related issues in the use of social media. In addition, they also proposed the inclusion of anonymous users since the laws of Uganda permit for anonymous reporting of complaints.

3.2.3 Document and System review

In order to achieve the second objective of designing a web-based system for reporting and creating awareness about social media threats and crime in Uganda, I embarked on conducting document review and review of some of the already existing system that perform related functionalities as the proposed system. The review of documents is well articulated in the literature review and the systems were mainly public facing systems in Europe namely: Tip411 and ePOOLICE (Early Pursuit Against Organized Crime Using EnvirOnmental Scanning, the Law and IntelligenCE Systems).

(i) Tip411

The system was of reference to the requirements gathering due to its functional capabilities such as: ability to engage the community, alert the public so as to enhance of public safety, connect to social media applications and also customization for citizen driven survey. Lastly, the system is also used by Law enforcement, Schools and Community groups. Such target stakeholders and functionalities were appropriate for the development of the web-based system for reporting and creating awareness about social media threats and crime.

(ii) ePOOLICE

The selection of system for requirements gathering was premised on the key functionalities of the system. Namely; dissemination and exchange of information with the end users, early warning mechanism in particular to online threats, user feedback mechanisms and the bi-lingual support capabilities. The enumerated functionalities were found to be in sync with the proposal system on social media threat reporting and crime awareness.

3.3 System Study

The data was gathered to establish the existing social media information management, crime reporting, and perpetration techniques in relation to social media threats and crimes in Uganda. Qualitative research was carried out using focus group discussions in order to collect information from different respondents from different groups of respondents who comprised of Law enforcement agencies, business managers, Information technology regulatory bodies, telecom operators and civil society organizations. This was done to gather views of different practitioners either regulating, enforcing or advocating for security of social media platforms. Quantitative research was equally conducted using an online questionnaire on google forms which was sent out to the targeted eighty (80) respondents.

3.3.1 Findings from the Questionnaire

A questionnaire was administered to 80 respondents to gather their views about a social media crime and threat reporting system. The respondents included; Civil Society Organisations (CIPESA & WOUGNET), Uganda Police Force (UPF), Office of the Director of Public Prosecution (ODPP), Judiciary, Uganda Communication Commission (UCC), Non-Governmental Organization (ARC - Allied), National Information and Technology Authority – Uganda (NITAU), Education consultant – JDO Foundation (USA), Banking Sector (Housing Finance), Telecom Sector (MTN – Uganda), Business Community (Elohim Exporters Uganda Limited) and University students (Uganda Christian University & Kampala International University). These were contacted through email and telephone calls and they were thus able to test the system in accordance to the online questionnaire.

The respondents shared their views about the status of social media crime and threat awareness among the public. A number of factors were put into considerations, which included anonymity versus registered reporting of threats and crime, social media usability, preferred social media platforms, social media threat reporting and crime awareness, social media regulation and organizational policies in place, and preferred functionalities of the proposed web-based system for reporting and creating awareness about social media threats and crime.

(i) Anonymous Versus registered.

The respondents were free to anonymously respond to the questionnaires or register with their full names before filling of the questionnaire. From the category of respondents as mentioned given, a total of 57 participants responded to the questionnaire, and it was observed that out of 57 respondents, 32 which represents 56% preferred responding as anonymous users, whereas 25 which represents 44% registered their full names before filling the questionnaire. This evidently cascaded to the desired functionality in the system where users required to have an optional functionality of either being anonymous or registration in confidence. This finding is illustrated in figure 3.

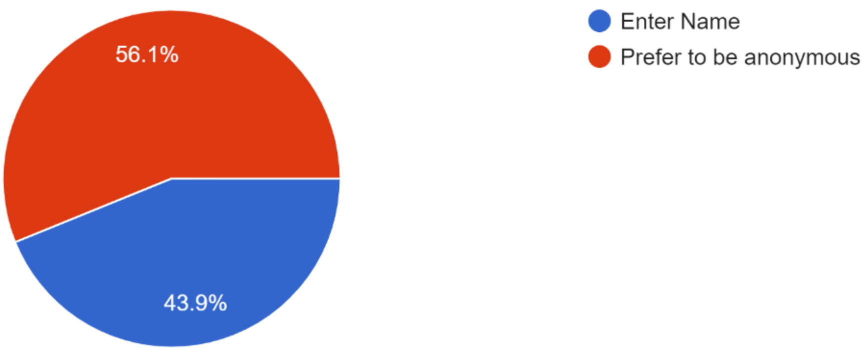


Figure 3:: Registered vs Anonymous Users

(ii) Gender Distribution

From the 57 responses received, the gender distribution of respondents was 40 male and 17 female which represents 70% and 30% respectively. This is represented in figure 4

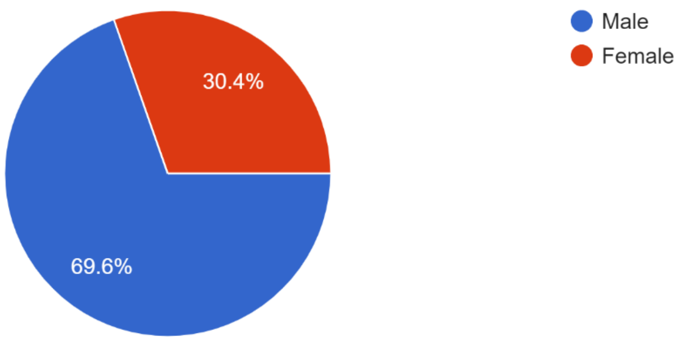


Figure 4: Gender distribution

(iii)Age groups

From the 57 responses received, one respondent was in the category of 18-24 years, 11 people were in the category of 25-34 years, 43 respondents were in the category of 35-54 years and 2 participants were in the age category of 55 and above. Hence, most respondents were in the age category of 35-54 at 43 respondents (68%) followed by those in 25-34 age distribution at 11 respondents representing 18% as shown in figure 5.

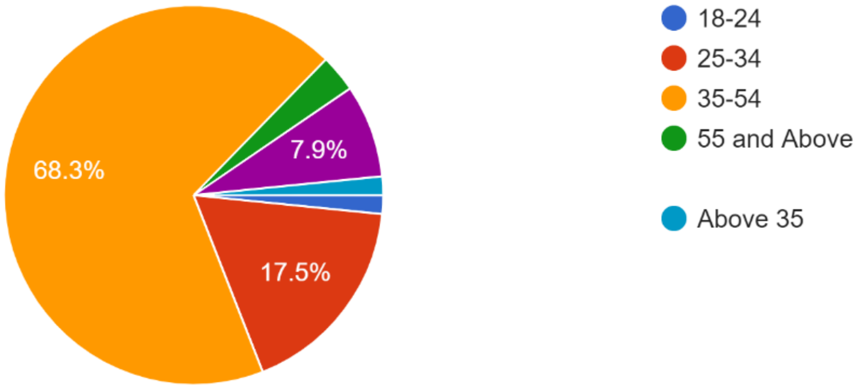


Figure 5: Age group distribution

(iv)Social Media Usage

A wealth of knowledge was received from 57 professions who included; Uganda Police Force respondents at 12 (19%),ICT industry at 10 respondents (16%), Engineering respondents at 6 (10%), Banking sector respondents at 2 (3%), Education respondents at 3 (5%), Civil Society Organization respondents at 3 (5%), Advocacy respondents at 2 (3%), Medical practitioner respondents at 2 (3%), ICT Research respondents at 2 (3%) and other categories of respondents at 1 (1%) such as Forestry, Audit, Procurement, Accounting & Consultants

Results show that 56 respondents which represents 98% use social media as illustrated in figure 5, regardless of their profession and age category and 25 respondents who are the majority users, spent a minimum of 1-2 hours daily on social media representing 40% followed by 16 respondents who spend 3-5 hours daily representing 25% and 10 respondents (16%) that spend 5–10 hours. This is illustrated in figure 6.

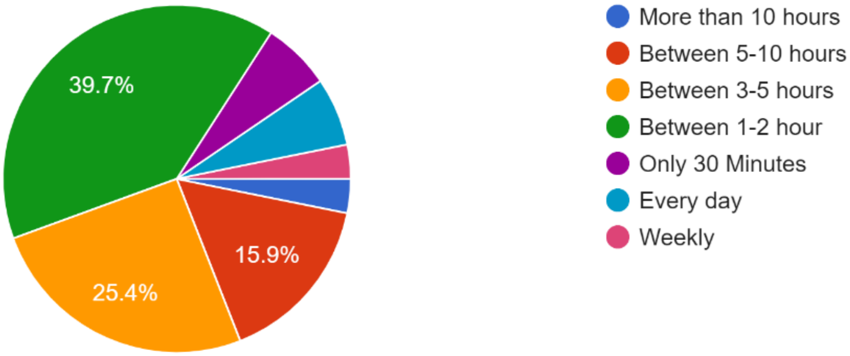


Figure 6 : No. of hours spent on social media

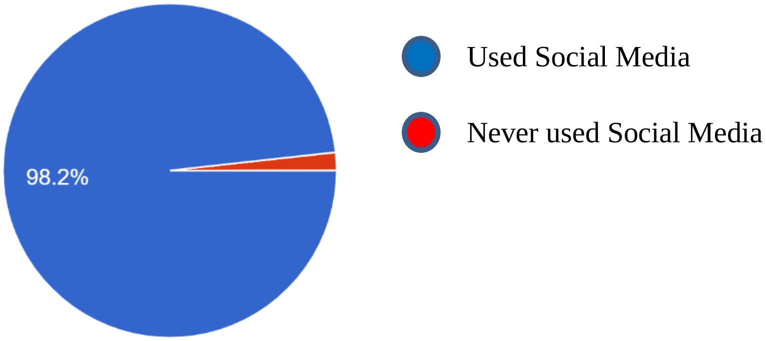


Figure 7: Social Media Usage

(v) Preference of social media platforms.

On the most preferred social media platform, 47 respondents (83%) selected WhatsApp as their best social media platform, followed by Twitter with 5 respondents at 9%, Facebook at 3 respondents (5%) and LinkedIn at 2 respondents (4%). This is illustrated in figure 8.

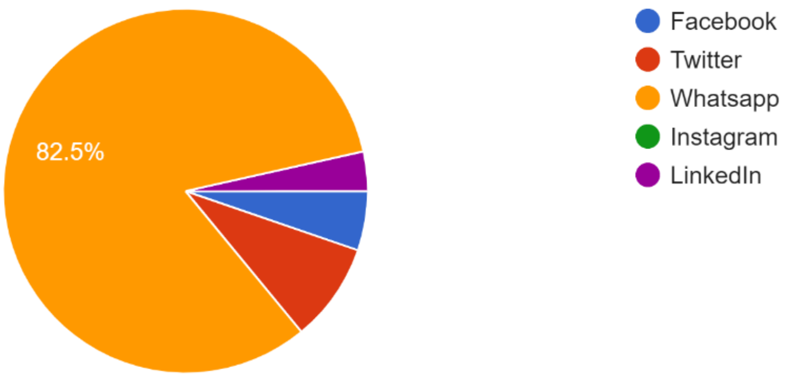


Figure 8: Preferred social media platform

(vi) Security features on social media platforms

From the research findings, it was noted that a good number of users had ever used security options on their favorite social media platforms. Findings show that out of the 57 respondents, 40 which represents 69% had ever used them, whereas 18 respondents representing 31% were not knowledgable about the security features of those plaforms as shown in figure 9.

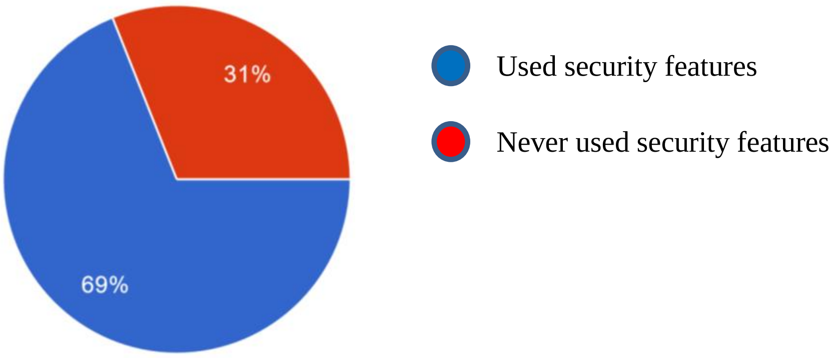
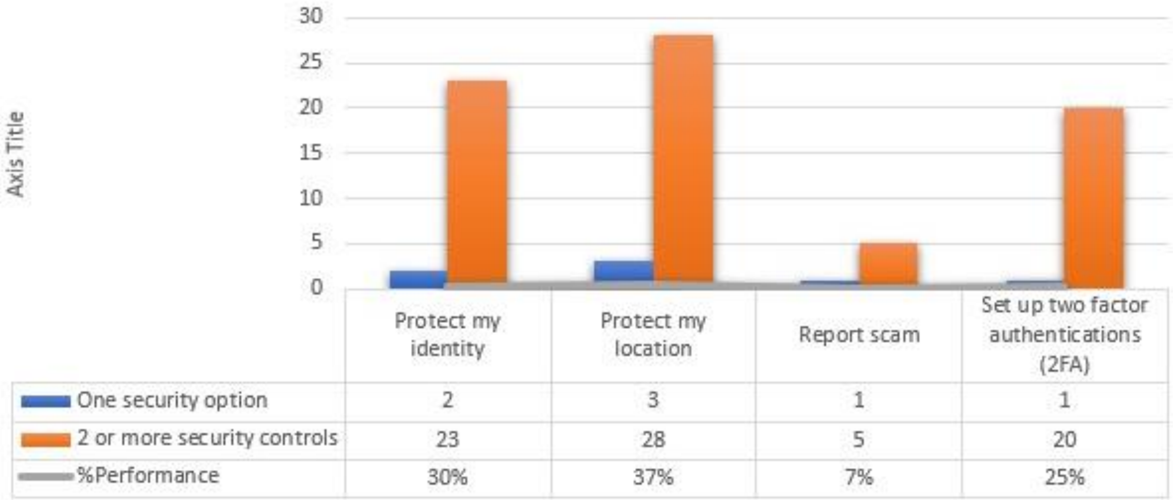


Figure 9: Social media security preference options

Among those who were knowledgable about security features of social media platforms, 25 participants (63%) used the secuity options to protect their identity, followed by 31 participants (78%) desired to protect their location, 9 repsondents (23%), reported spam, 21 participants (53%) were able to setup 2 factor authentication and others did a variety of actions including spam and privacy protection, and enabling of virtual private networks or incognito mode to mask their addresses. This is illustrated in figure 10 .



	Protect my identity	Protect my location	Report scam	Set up two factor authentications (2FA)
🟦 One security option	2	3	1	1
🟧 2 or more security controls	23	28	5	20
▬ %Performance	30%	37%	7%	25%

Figure 10: Security options utilized in social media platforms

(vii) Social media threat or crime

The questionnaire further sought to find out if the respondents had been victims of social media threats and crime. Findings show that out of 39 respondents, 16, equivalent to 41% of the respondents had ever been victims whereas 23 which is equivalent to 59% of respondents had never been victims. The distribution of attacks included electronic fraud, cyber harassment, some participants acknowledged that they had instances of revenge pornography from their former loved ones or friends and cyber stalking. It was observed that phishing was the highest crime followed by electronic fraud and cyber harassment. This is illustrated in figure 11 and 12.

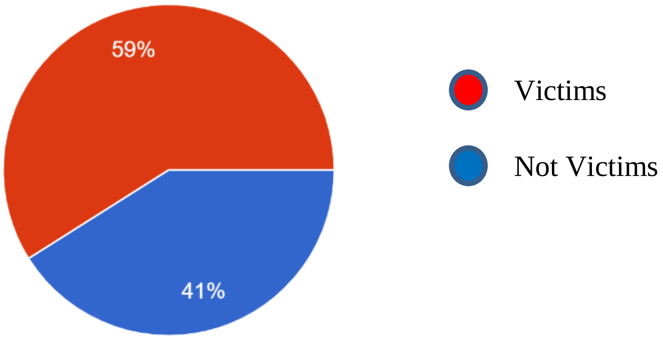


Figure 11: Distribution of social media crime and threats

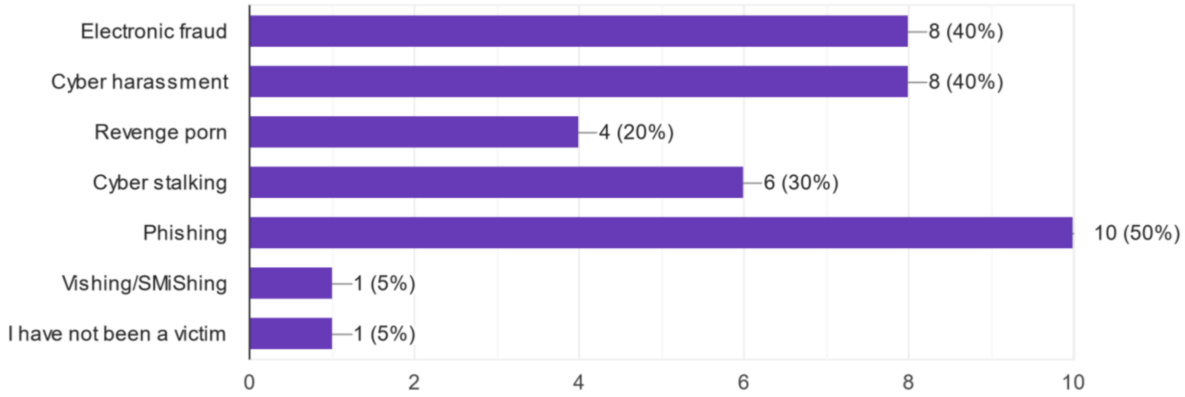


Figure 12: Category of social media threat reporting and crime awareness

(viii) Awareness about social media threats and security updates

Further analysis was done to find out the respondents' awareness of social media threats and crime. Results show that out of 57 respondents, 12 which represents 21% were not aware of social media threats and crimes, whereas 45 respondents representing 79% were knowledgeable as show in figure 13.

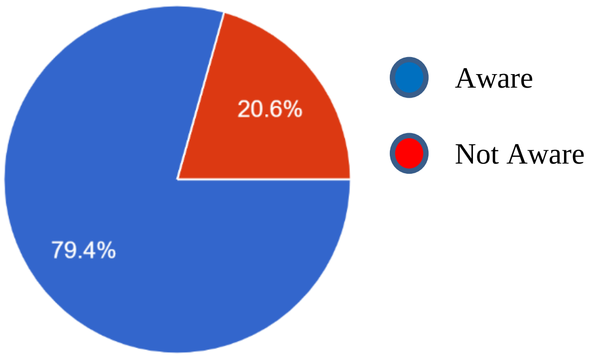


Figure 13 : Awareness of social media threats and crimes

The questionnaire further analyzed how often respondents got advice whenever there were new social media threats and crimes. Results show that out of the 63 respondents, 17 representing

27% never get advised at all whenever there are new social media challenges, 10 respondents which represents 16% get advised within a few days, 14 respondents representing 22% get updates whenever they access the internet, and 12 respondents representing 19% got advice whenever they visit the social media platforms. This is illustrated in the figure 14.

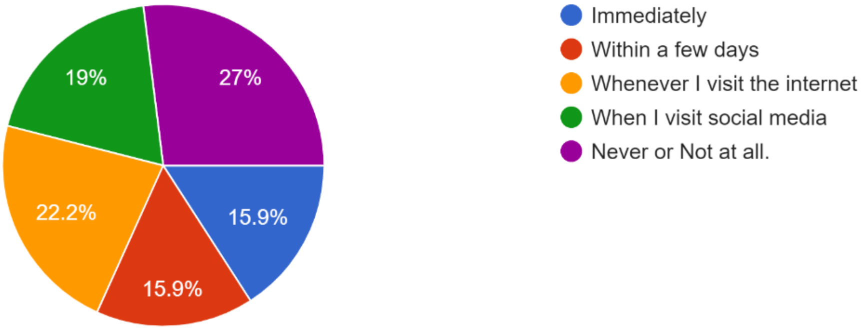


Figure 14: Response time to social media threats and crime

(ix) Rating of the security agencies and reporting of social media threats and crime.

The questionnaire further inquired from the respondents on how they rated the current security/regulation methods used by the different agencies namely; Uganda Police Force, Uganda Communications Commission, National Information Technology Authority, and Ministry of ICT & NG. The results indicated that 12 respondents rated the security/regulatory methods as poor (12%), 14 respondents rated them as fair (14%), 25 respondents rated them as average (45%) and 5 respondents rated them as excellent (5%) in illustrated in figure 15.

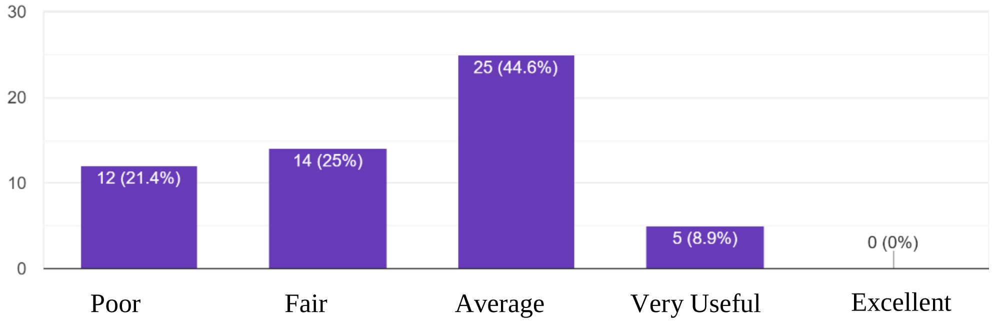


Figure 15: Rating of security/methods of awareness by agencies

Furthermore, efforts were made to find out whether respondents had ever reported a social media crime or threat to any of the security/regulatory agencies. Results show that out of 57 respondents, 48 which represents 84% had never reported a social media crime and only 9 respondents, representing 16% had ever reported. This is a clear indicator of the lack of trust, satisfaction and awareness in the current approach. This is illustrated in figure 16

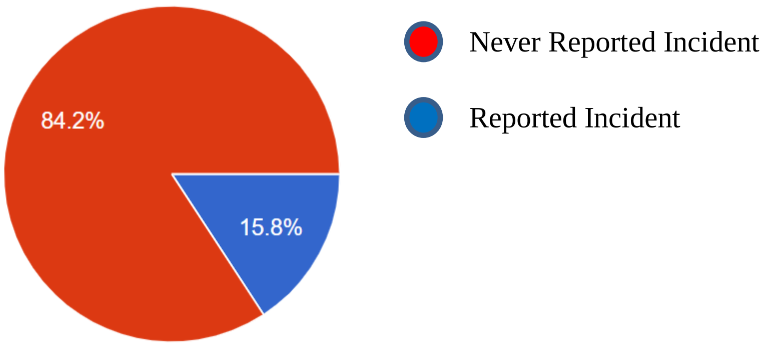


Figure 16: Percentage of social media threat or crime reported

It was noted that those who had recorded financial losses were ranging from as low as one hundred thousand shilling (100,000 Ugx) to over a million shillings (1,000,000 Ugx). However, the findings revealed that out of 9 respondents, 5 representing 56% had never lost any funds, 2 representing 22% has lost less than 100,000 Ugx, 1 respondent representing 11% had lost between 500,000 to 1,000,000 Ugx and 1 respondent representing 11% had lost more than 1,000,000 Ugx. The rest had occasioned some losses due social media threats and crimes as illustrated in the figure 17.

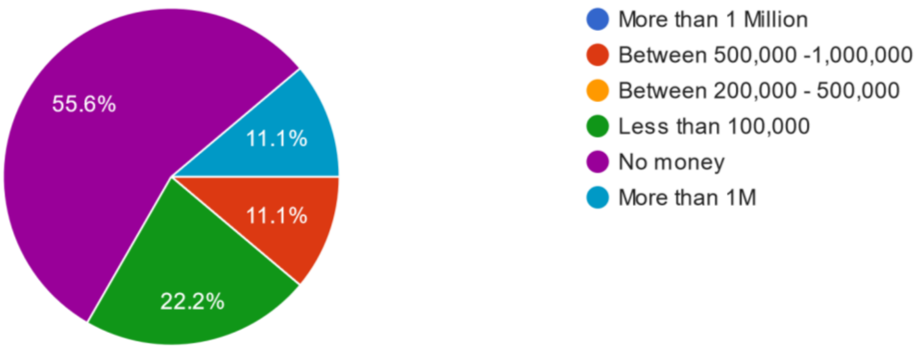


Figure 17: Financial loss occasioned from social media threats or crime.

It was further established that out of 7 respondents, 3 representing 43% faced victimization as a result social media threats and crime, 2 respondents representing 29% experienced a breach of their privacy, 1 respondent lost funds as well as 1 also lost a job each at 14% respectively as illustrated in figure 18.

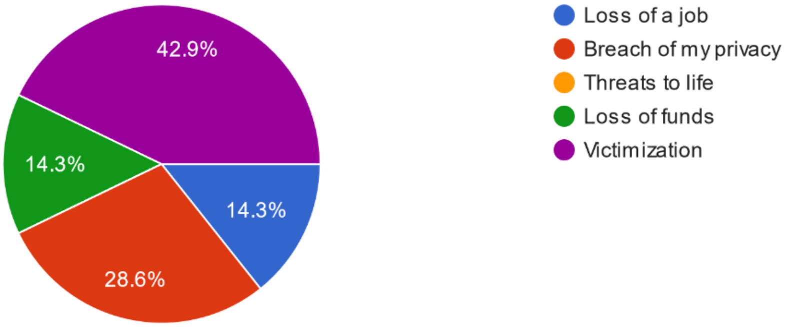


Figure 18: Effects of social media threats and crime

(x) Awareness of national laws that regulate social media.

It was noted that out of 56 respondents, 31 which represents 63% were aware of at least one of the national laws and regulations that control social media, whereas 19 respondents representing 37% were not aware of any social media laws and regulations as illustrated in figure 18. The most known law is the Computer Misuse Act. Twenty-two (22) respondents representing 39% had never had social media policies in their organizations, whereas 34 respondents representing 61% had social media policies in their institutions. This is illustrated in figure 19.

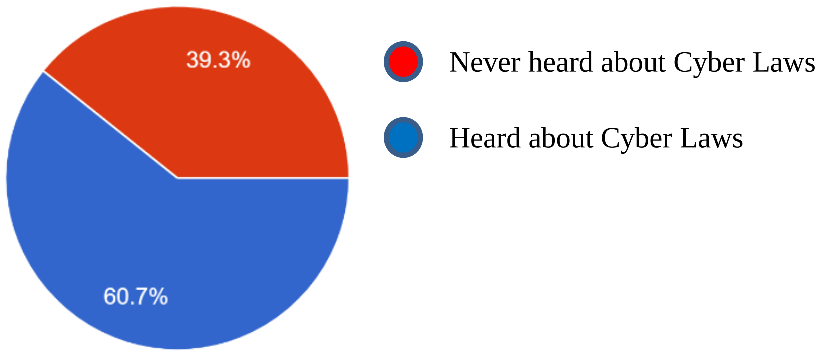


Figure 19: Knowledge about social media laws of Uganda

It was further revealed that out of 61 respondents, 38 representing 62% had a social media policy at their work places while 23 respondents representing 38% did not have any social media policy at all as illustrated in Figure 20.

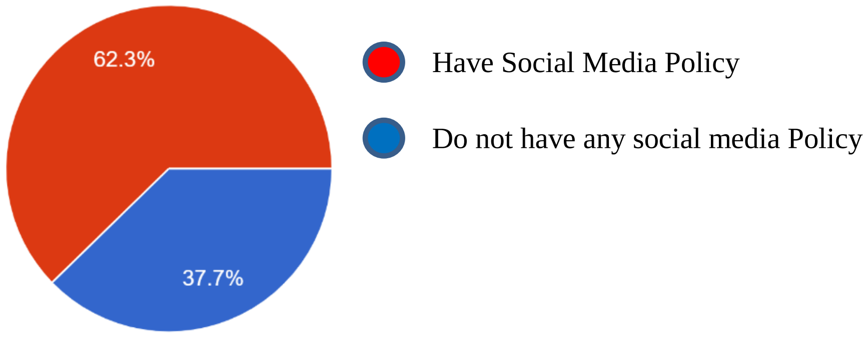


Figure 20: Organizations with social media Policy

(xi) Social Media Security Tips

Further inquiry was done to find out how often the respondents received security tips on social media threats and crime. It was found out that 57 respondents, 15 representing 26% received updates once a week, 8 respondents which is 14% represented updates of once a year, 11 respondents, which represents 19% received updates once a month and the majority who are 23 representing 40% confirmed that they never always received such updates as illustrated in the figure 21.

This is evident with awareness received from Uganda Police Force during the quarterly and annual press conferences. However, that is often not sufficient since not all persons listen or watch the press conference sessions. UCC, NITA and the Ministry of ICT & NG, also often share security awareness tips on social media platforms such as Twitter. In addition, UCC Consumer Affairs team has of late started a social media hash tag campaign dubbed as *#Donotbeconned* and #tonfera Furthermore, it was observed that Telecom companies normally did so through the use Short Message Service (SMS) alerts during promotions to prevent fraud, call tunes during subscriber calls and social media platforms like Twitter and Facebook.

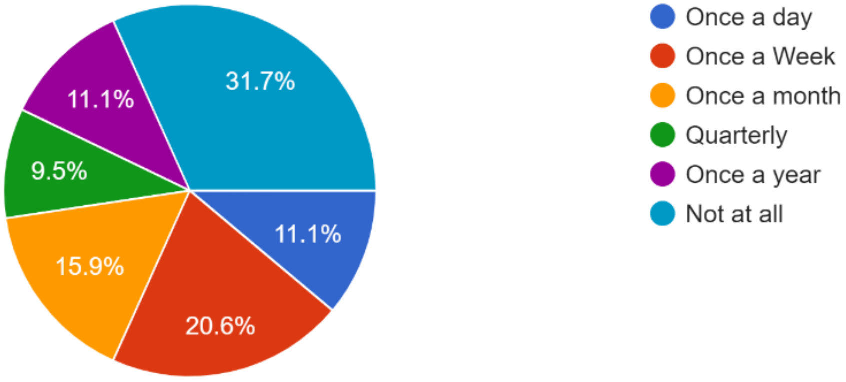


Figure 21: Frequency of social media threats and crime awareness

(xii) Desired System Functionality

The questionnaire further sought to find out the kind of functionality respondents would desire to have in the system. Results showed that out of 57 respondents, 27 agreed to the option of having the system with reports showing analytics about social media threats & crime representing 47%, 27 respondents agreed to the option of having location tracking and visualization of location with high crime concertation rates representing 47%, 27 respondents agreed to have the option of trend analysis and reporting which represents

47%, 27 respondents agreed to add the option of language translation representing 47%, 27 respondents agree to the option of integrating the system with other social media reporting systems representing 47% and finally 27 respondents also agreed to have the option of enabling registered and anonymous users reporting threats, crimes and tips which represents 47%., This is illustrated in the figure 22 under the various sub categories of desired system functionalities.

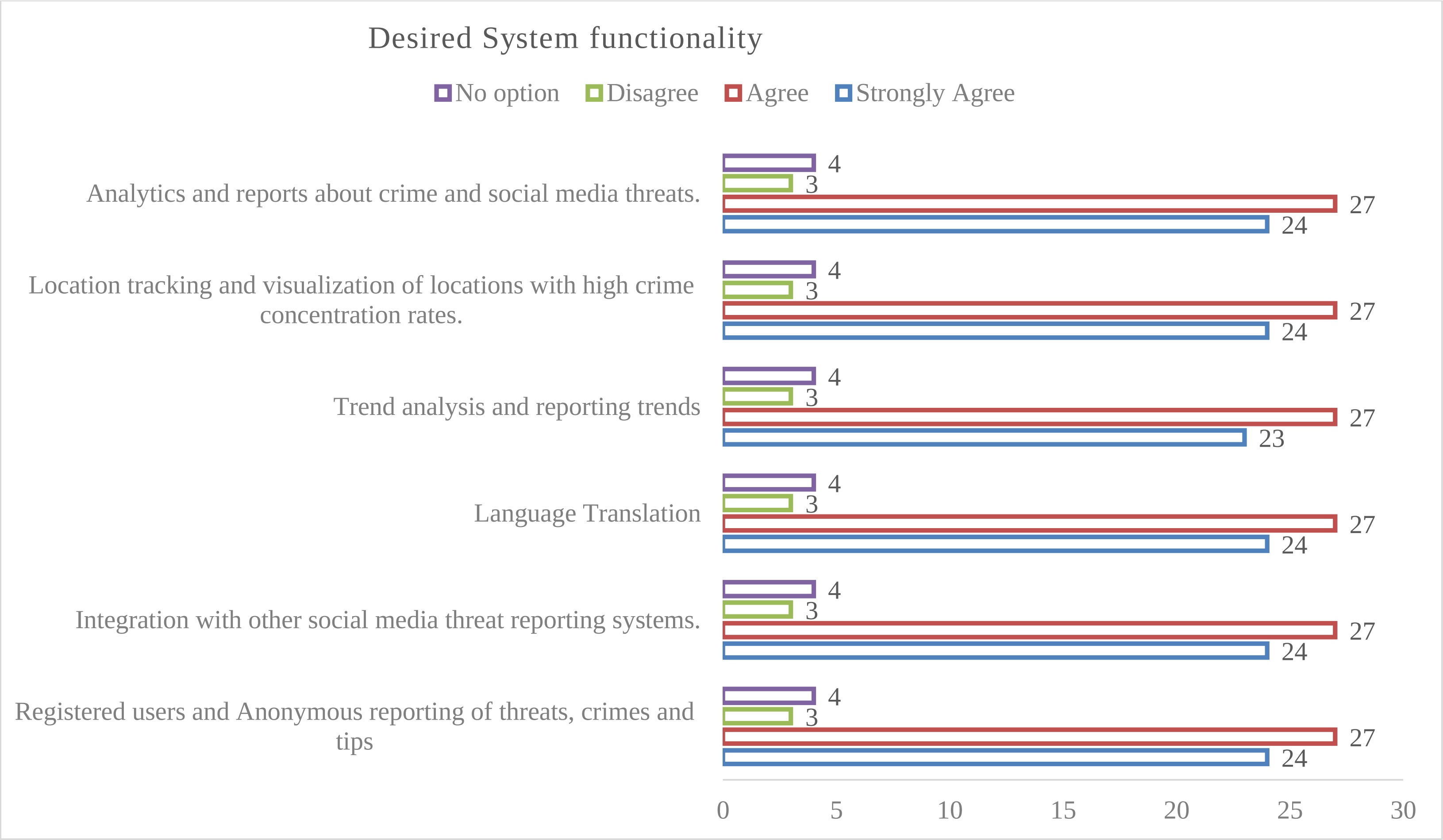


Figure 22: Desired system functionalities

(xiii) Language Translation

Further inquiry was done to find out whether the respondents desired to have a language translation plugin to the social media threats reporting and crime awareness system. It established that out of the 57 respondents, 27 representing 48% agreed to having language translation, 20 respondents which is 35% of the respondents represented those that strongly agree, 06 respondents, which represents 11% had no option and 03 representing 5% strongly disagreed and finally 01 respondent representing 2% disagreed as illustrated in the figure 23.

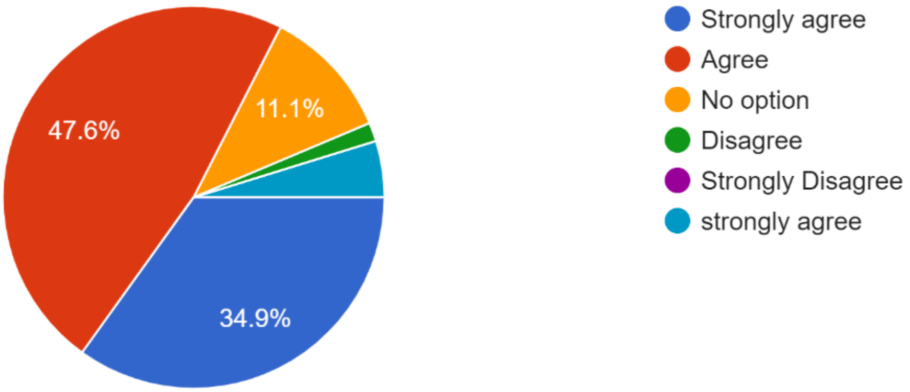


Figure 23: Language translation

3.3.2 Findings from the Focus Group Discussions

Four categories of users were interviewed during the FGDs who included; Information Technology and Telecommunication Sector practitioners, Civil Society Organizations, Business Community and the Justice Law and Order Sector (Law Enforcement and the Office of the Director of Public Prosecution). The categories were represented by the following organizations: Collaboration on ICT Policy in East and Southern Africa (CIPESA), Women of Uganda Network (WOUGNET), Elohim Exporters Limited, Archers technology Solutions Limited, Uganda Police Force (UPF), Office of the Directorate of Public Prosecution (ODPP), National Information Technology Authority of Uganda (NITAU), Ministry of Finance Planning and Economic Development (MoFPED), Global System for

Mobile Communication Association (GSMA) and Mobile Telecom Network - Uganda (MTN Uganda).

The objective of this engagement was to enlist the following information from the respondents.

(i) Common social media threats and crimes in Uganda.
(ii) Strategies currently used to disseminate information about social media threats and crimes.
(iii) Roles and activities of different players in the prevention and fight against social media threats and crimes in Uganda.
(iv) Measures that have been put in place to prevent and fight social media threats and crime for the business community.
(v) Legal provisions about social media threats and crimes in Uganda.
(vi) Procedures for enforcement and prosecution of social media threats and crimes.
(vii) The regulatory framework for addressing social media threats and crime in Uganda.
(viii) How awareness about social media threats and crimes in Uganda can be increased.
(ix) The possible challenges in dealing with social media threats and crimes in Uganda.
(x) What to be included as part of the solution in the proposed system.

The data collected from the focus group discussions was correlated in order to determine the requirements for the system.

3.3.3 Analysis of responses from the Focus Group Discussions

Sub sections (a) to (j) presents the views and opinions gathered from focus group discussions. It involved reviewing and synthesizing of information gathered from respondents as well as the recommendations from the discussion.

a) Common Social Media Threats and Crime in Uganda

It was noted during the discussions that the common social media threats and crimes as enumerated by the research done by WOUGNET, a Civil Society Organization (CSO), focusing on women at work were online violence on social media platforms such as Facebook, Twitter and WhatsApp through acts such as non-consensual sharing of intimate images (revenge porn), online harassment which most often culminated into sexual harassment as a threat and a crime, cyber stalking, identity thefts and electronic fraud.

Furthermore, NITAU and MTN Uganda (Telecom Sector) agreed to the fact that there was an increase in misinformation and disinformation or fake news, social engineering techniques, electronic fraud and obtaining money by false pretenses in the telecom sector. In addition, the Uganda Police Force presented unauthorized access, defamation, offensive communication, impersonation, money laundering and cyber harassment as the most common social media threats and crimes in Uganda.

b) Categorization and Legal Provisions of Social Media Crimes Reported

Law enforcement (the Uganda Police Force) and the Directorate of Public Prosecution noted that social media crimes were mainly categorized under the Computer Misuse Act 2011 contrary to section 23, 24, 25, and 26, which highlight child pornography, cyber harassment, offensive communication, and cyber stalking respectively (NITAU, 2011). The Penal Code Act also provides for Criminal libel, threatening violence, and inciting violence in section 83. In addition, according to the Anti-terrorism Act 2002 (Parliament of Uganda, 2002), section 9 highlights promoting terrorism using social media - publishing and disseminating news or materials that promote terrorism. This is described as radicalization, recruitment, funding, and violent extremism. Additionally, the Domestic Violence Act of 2010 provides for forms of abuse using social media such as emotional, verbal or psychological abuse to repeated insults, ridicule or name calling wherever there is a domestic issue. Finally, the Data Protection and Privacy Act 2019 (NITAU, 2020), section 35 highlights unlawful obtaining or disclosure of personal data and section 36 covers unlawful destruction of personal data (NITAU, 2020).

c) Strategies currently used to disseminate information about social media threats and crimes.

Participants noted that strategies currently used include training and creation of standards and policies on acceptable online behaviour by Civil Society Organizations such as CIPESA and WOUGNET Uganda Police Force, NITAU, GSMA, DPP and MTN Uganda. However, it was observed that such trainings needed to focus on education/mindset change in terms of the benefits of social media as opposed to the negative effect. In addition, the training is not regular and targets a small portion of the populace thus making it less effective. Therefore, such trainings ought to be incorporated into the training curricula of all education institutions as a means of being effective. This was described as digital literacy through targeted and deliberate education of platform users, development of Artificial Intelligence (AI) tools by some of the service providers as interventions to address social media crime and threats.

It was observed by MTN Uganda that the use of Artificial Intelligence tools in their core network has provided a notable decline in Authorized Push Payment (APP) fraud. This kind of fraud occurs when a person or business is tricked either through an SMS or voice call, typically by social engineering attacks involving impersonation into sending money to a fraudster posing as a genuine payee/beneficiary. Nonetheless, there were still pockets of fraud due to lack of awareness of the social engineering perpetration techniques of fraudsters. The participants from the GSMA and NITAU underscored the role played by the government education systems and collaboration with other players such as development partners and civil society organizations. However, this requires joint synergy in order to achieve wider awareness on digital safety and rights empowerment of all users.

d) Roles and activities of different players in the prevention and fight against social media threats and crime in Uganda

The DPP, UPF and NITA-U informed the discussion about the significant role played in the enforcement of related Laws, Policies and Prosecution of offenders, Regulation of the technology platforms in Uganda and advocacy for social inclusion in all aspects. However, the complexity of social media threats and crime require concerted efforts from all players and stakeholders. It was noted that whilst the laws are in place, the means and capacity to enforce them is still at a low scale hence the need for more resources to deal with the eminent threats of such platforms.

e) Measures that have been put in place to prevent and fight social media threats and crime for the business community/private sector.

CIPESA and Archers Technology Solutions Limited informed the discussion that facilitating individual responsibility for social media users is pivotal for the business community. This includes among others, the reduction of online personal information, the use of two factor authentication, not sharing passwords or credit card information with unauthorized parties and the review of privacy settings for social media accounts.

In the same vein, the discussion agreed that Law enforcement agencies and the Information Technology governance authority, need to strength their capability to respond to social media threats and crime with a view to developing an enterprise incident response plan, and creating public awareness of the services therein.

The meeting noted that some efforts were already in place such as Toll-free numbers (0800199399 or 999 – Uganda Police Force Emergency response and 0800222777 – Uganda Communications Commission Consumer Affairs Support Desk), and the Computer Emergency Response Team (CERT), but little was being felt in terms of the efforts or strides made so far.

f) Procedures for Enforcement and Prosecution of Social Media Threats and Crime

It was noted that reporting to the Uganda Police Force, Regulatory Authorities such as NITA-U and UCC is normally the starting point for addressing such threats and crime, and then the matter is escalated to the Electronic Counter Measures Department and Forensics Services Directorate at CID Headquarters and Naguru respectively for the UPF specifically. However, most of the social media crimes and offences were never reported due to victim privacy issues and at times delays or non-responsiveness or delay by the UPF during investigations.

The Telecom sector (MTN Uganda) has a call center where subscribers can report incidents and action is taken. However, it was noted that this was not enough since the victims may take long to recover the losses.

g) The Regulatory Framework for Addressing Social Media Crime in Uganda

It was stated that NITA-U created guidelines for social media use by all Ministries, Departments and Agencies with legal provisions to address social media threats and crimes. The Uganda Communication Commission and other global associations like the International Telecommunication Union (ITU) and Global System for Mobile Communication Association (GSMA) are also responsible for regulating the social media spaces. However, with the rise of online content providers and consumers, such regulations are becoming difficult to enforce and as such some of the platforms have become avenues for abuse by unscrupulous users.

h) How awareness about social media threats and crimes in Uganda can be increased.

It was noted that whilst awareness was being done by CIPESA and WOUGNET through their various research reports available online it was not an inclusive method since it targets a specific group of persons leaving out the most vulnerable groups like the elderly and rural youth that use these platforms with low levels of digital literacy. It was therefore agreed, that awareness should also be intensively carried out by the UPF, DPP, MTN Uganda and NITA-U through digital literacy, and deliberate knowledge sharing sessions. In addition, all Ministries, Departments, and Agencies (MDAs) of government need to budget for social media sensitization and awareness.

i) Possible challenges in dealing with social media threats and crimes

The UPF stated that most of the victims of crime do not report due to lack of awareness or for fear of victimization and stigmatization. Furthermore, it was noted by UPF and DPP that at times such crimes are committed by persons who are outside Uganda's jurisdiction which makes it difficult to investigate and prosecute. In addition, UPF and DPP stated that part of the digital evidence for social media cases required for court trial is stored by the platform owners and content providers in cloud servers. This renders the investigation process cumbersome when requesting for such evidence through the available Mutual Legal Assistance Channels.

Other challenges mentioned by the participants included: the disbandment of the Pornography Control Committee (PCC) which drastically reduced the role of government in the fight against online forms of pornography, low levels of digital literacy, inadequate knowledge about the laws and inadequate funding towards awareness and sensitization by government.

j) Functionalities of the web-based system for reporting and creating awareness about social media threats and crime

From the assessment above, it is evident that there is an awareness gap that requires to be filled by creating awareness about social media related threats and crimes, in order to reduce or prevent the incidents of more people from being victims of social media threats and crime. It was also noted that the desired web-based system for reporting and creating awareness about social media threats and crime system will;

(i) Improve awareness among the general public and

(ii) Analyse the generated data about incidents in the entire country and generate reports.

(iii) Incorporate the community standards and policies of social media platforms so as to ensure consumer protection and redress.

(iv) Provide content about the different attack surfaces, emerging trends and whistle blowing mechanisms.

The UPF, DPP, Archers Technology Solution Limited and Elohim Exporters noted the need to use the solution as a content provider for sensitization and awareness as well as generating statistics for decision making and depicting what is happening in society. NITAU and GSMA noted that the solution should leverage on the freely available APIs of social media platforms such as Twitter to analyze information in terms of attack surfaces or communication to perform predictive analysis of emerging trends.

3.4 Ethical Issues

The web-based system for reporting and creating awareness about social media threats and crime project was undertaken in accordance to the of the Data Protection and Privacy Laws of Uganda, the General Data Protection Regulations and the Community Standards.

Information obtained was only used for this research study. Where necessary, the data streamed was anonymized to hide individual account names. Data gathered was secured against use or disclosure beyond the research study.

The project equally followed the National Council for Science & Technology guidelines on research involving humans as well as the Makerere University research ethics guidelines as contained in the Research and Innovations Policy. Lastly, for emphasis, while dealing with private data of individual social media users, the Data Protection and Privacy Act 2019 and the

African Union Convention on Cyber Security and Personal Data Protection were key guiding documents.

3.5 Conclusion

By and large, the social media awareness and crime reporting system was successful through the use of a number of techniques, which included; requirements gathering through interviews, questionnaires and focus group discussions, design by UML, DFDs, Implementation through light weight technologies and then testing and validation through UATs of the different stakeholders. The next chapter, discussed about how the web-based system for reporting and creating awareness about social media threats and crime functions.

CHAPTER FOUR: SYSTEM ANALYSIS, DESIGN & IMPLEMENTATION

4.0 System Analysis

This chapter presents the analysis, design and summary of findings of the web-based system for reporting and creating awareness about social media threats and crime based on the information gathered from the use of both qualitative (Focus Group Discussions) and quantitative (questionnaire) data collection exercises. This provided the basis for functional and non-functional (performance and reliability) requirements for building the system.

4.1 System Design

In order to achieve the second objective of designing a web-based system for reporting and creating awareness about social media threats and crime in Uganda, simplified representations were used to depict the requirements that were obtained from the questionnaire, focus group discussions as well as the system & literature review. These included; Unified Modeling Language (UML), Context Diagram (CD), Data Flow Diagram (DFD), and Entity Relationship Diagram (ERD).

Based on the problem analysis, an object-oriented model of a web-based system for reporting and creating awareness about social media threats and crime was designed to implement the identified requirements. In this case, a web-based system for reporting and creating awareness about social media threats and crime was divided into basic components and modules, and classes were identified from these modules. According to the requirement relationship between classes, sub-classes within class, abstraction behavior of the class and common behavior of the classes were identified. Functions of the classes were then designed for each basic task.

Object oriented design is not simply features added to support a programming language or even an application. It views the enterprise as a community of agents, termed objects. Each object is responsible for a specific task. Object-oriented design strategy was used for the conceptual design. With this approach, the executing system was made up of interacting objects that maintain their own local state and provide operations on that state information (Tupper, 2011).

For the data structure design, two methodologies used to create a data model: the Entity-Relationship (ER) approach and the Object Model. The Entity-Relationship (ER) approach was used for this project because of its simplicity in communicating the data structure required by the database to the end user.

4.1.1 Context Diagram

The Context Diagram, also known as Level-0 Data Flow Diagram (DFD), was used to display the web-based system for reporting and creating awareness about social media threats and crime under consideration as a single high-level process and then the relationship that the system has with other external entities, system processes and data flows namely; Users (registered and anonymous), System administrators, System repository and the data flows such as; Threat reporting, awareness campaigns, news, locations maps, etc. In other words, it was the visual representation of the relationship between data and business processes.

The Context diagram was selected as an inception design model due to the enumerated benefits;

(i) It showed the scope and boundaries of a system at a glance including the other systems that interface with it.

(ii) There was no need for technical knowledge to understand the diagram

(iii) It’s was easy to expand by adding different levels of DFDs

(iv) It profited a wide audience including stakeholders, business analyst, data analysts and developers. These included but are not limited to Civil Society Organizations, Justice Law and Order Sector, Telecom Operators, Students, Financial Technology (FINTECH) Enthusiasts and the ICT Regulators.

4.1.2 Data Flow Diagram

The Data-Flow Diagram (DFD) which forms part of the components of the Structured-Systems Analysis and Design Method (SSADM) was used visualize the movement (flow) of data through the web-based system for reporting and creating awareness about social media threats and crime. That is to say, where data comes from, where it goes and how it gets stored.

It was used to describe the processes that were involved in the system, to transfer data from the input, to the file storage up to the generating of reports.

This approach was selected because it is one of the design industrial practices by Information Technology professionals and Systems Analysts for documenting and showing users how data moves between different processes in an Information System

DFD is process centric and thus was able to depict the four (4) main components of the web-based system for reporting and creating awareness about social media threats and crime. Namely;

(i) Processes which included user authentication, threat reporting, reporting generation and community standards publication.

(ii) External Entities which were the users namely: anonymous, registered and system administrators.

(iii) Data Stores (repository) which were the databases such as social media threats & crime, user profiles, social media awareness news & publications.

(iv) Data Flows (curved or straight line with arrowhead indicating flow direction) such as threat reporting, system login, viewing threat & crime locations, submission of perpetration techniques and uploading of publication.

4.1.3 Unified Modeling Language (UML)

UML was selected for the design of the web-based system for reporting and creating awareness about social media threats and crime because of its ability to visually represent a system along with its main actors, roles, actions, artifacts or classes. This made it easy to better understand and document the system.

The UML contains diagrams, and therefore we chose to opt for the Use Case Diagram (UCD) as the means of demonstrating the behavioural component of the software Design. That is, the actors communicating with the system through tasks.

The following were some of the use cases that we modeled:

(i) System administrators responsible for registrations of new users, user authentication (login), viewing of social media threat and crime awareness news and the generation of statistical reports with a crime distribution map.

(ii) Registered users such as law enforcement, students, CSO, business sector and general public. This category was responsible for general use of the system through system login, reporting of social media threats and crimes, and viewing of reports or awareness news.

4.1.4 Entity Relationship Diagram (ERD)

An Entity Relationship Diagram (ERD) is basically a snapshot or brief of various data structures. It is also a type of flowchart that illustrates how "entities" such as people, objects or concepts relate to each other within a system. It is a visual representation of different entities within a system and how they relate to each other.

I therefore opted for the use of an ERD because it can be used to design or debug relational databases in software engineering, business information systems, education and research arena. This approach therefore, provided a design platform for the public facing information system known as the web-based system for reporting and creating awareness about social media threats and crime.

ERDs thrive on simplicity through the use of symbols such as rectangles, diamonds, ovals and connecting lines to depict the interconnection of entities, relationships and their attributes. The rationale of using an ERD was its capability to: provide visual representation of the design, model data stored in databases, effective communication, simplicity and high flexibility.

4.2 System Development

The web-based system for reporting and creating awareness about social media threats and crime prototype was developed through the use of Object-Oriented Programming. By making use of abstraction (*the process of combining many functions into one*), inheritance (*technique that involves a child class inheriting functionality from a parent or super class*) and polymorphism (*exhibited by child classes running the same inherited method that returns* *different values*) the whole system was integrated to produce the desired output (Davis C. , 2020).

In order to achieve the objective of developing and implementing the web-based system for reporting and creating awareness about social media threats and crime in Uganda, various tools and technology were deployed based as enumerated.

4.2.1 Django framework.

(i) Django is a free, python-based, open-source web development framework that facilitates clean and rational designing of websites driven by databases.

(ii) It enjoys community support: Django enjoys the support of a huge and very professional community of developers.

(iii) It is compatible with DevOps which is an enabler to resolving any development issues faster with enhanced operational support.

(iv) Django religiously follows the 'KISS' principle which is "Keep It Short and Simple". In Django, it simply means that the code must be brief, easily understandable, and methods should not exceed more than 50-60 lines. Similarly, 'DRY' stands for "Don't Repeat Yourself", which means that the software patterns that occur quite often can be replaced with abstractions.

(v) Django comes with everything inbuilt. It has all the features which are required to build a web application from scratch.

(vi) It does not require any other external solution which makes it independent and complete.

(vii) Django as it is powerful enough to build a full-fledged API in just two or three lines of code.

4.2.2 JavaScript Object Notation (JSON)

(i) It was used for data exchange and integration with the existing social media systems.

(ii) JSON syntax is very easy to use. Its syntax is text, very small and light weighted hence making its execution response faster. Hence easy-to-parse data format which also makes it rather responsive.

(iii) The syntax of JSON is quite simple and self-describing because even the applications that don’t know which type of data to expect can interpret JSON

(iv) It acts as an enabler to data sharing. It was used to establish a connection between front-end and back-end languages for sharing data.

(v) It has got extensible browser support due to its independent data format. Therefore, it is supported by most browsers. That is to say, almost all programming languages have functions or libraries that support JSON.

4.2.3 HTML 5

(i) This was used to layout mappings and roles as well as to provide more security data persistence.

(ii) HTML5 provides support for multimedia because the tags for audio and video are treated as if they were images.

(iii) HTML5 has short and crisp syntax and comes with smart and improved security features hence it became very easy to write and manage HTML5 code

(iv) HTML5 is cross-platform and cross-device which means there is no need of writing different code for different browsers and devices hence saving a lot of time and cost.

(v) HTML5 has a flashy local storage feature that is between the regular cookies and client-side databases. It allows storage across a number of windows which improves security and performance, as well as knowing that the data will stay even once the browser is closed.

4.2.4 JavaScript

(i) It was used for validation messages and cleaning of data.

(ii) Java Script accelerates programme execution by eliminating the wait time for server connections and seamlessly integrates with other programming languages.

(iii) Java Script supports data validation within the browser itself rather than being forwarded to the server because it’s a client-side script.

4.2.5 MySQL.

(i) MySQL was used as the database management system because of it is able to create databases and manage their security.

(ii) It enables multiple data views. That is to say, different users of the database can be given different views of the structure and content of the database.

(iii) SQL is Open Source; therefore, it has free Databases (DBs) from MySQL, MariaDB and PostgreSQL which can be used at low costs.

(iv) SQL has got an Interactive language that can be used to talk to databases and get answers to complex questions in seconds.

(v) SQL enabled the connection of front-end computers (clients) and back-end databases (servers). Thus, supporting the client-server architecture.

(vi) It has got a faster query processing power. Large amount of data will be retrieved quickly and efficiently through operations such as; Insertion, deletion and manipulation of data.

(vii) It’s a portable language due to the fact that it can be used in programs on Personal Computers, Servers and Laptops independent of any platform (Operating System).

4.3 Testing and validating the system

In order to achieve the fourth objective of testing and validating the web-based system for reporting and creating awareness about social media threats and crime in Uganda, I embarked on a couple of approaches. A dry run was conducted with some of the potential users of the system, namely; Civil Society Organizations (CSO), Non-Governmental Organizations, Financial Technology Firms (FINTECH), Inspectorate of Government, Judiciary, Office of the Director of Public Prosecution, Uganda Police Force, University Students, Telecommunication Companies and the Uganda Communications Commission, the Communication Regulator. Actual execution of the system (production) and comparing the results against the expected results was undertaken through conducting User Acceptance Tests (UAT). This involved Component Testing, where each component in an application was done separately, errors found were fixed and the test which revealed the bug repeated after the bug fix. The UAT was aimed at proving that all requirements (performance and reliability) were met rather trying to find errors. See attached the annexure of the test results as annexure C & D

These approaches were geared towards conducting a User Acceptance Test (UAT) as a mechanism for generating feedback to the production before going Live. The UAT was successfully done using two approaches namely;

4.3.1 Focus Group Discussion

The FGD drew participants from Law Enforcement, Telecom sector, Civil Society Organization and ICT regulators in Uganda. The discussion generated the following feedback;

(i) The Civil Society Organizations and particularly the Women of Uganda Network (WoUGNET) recommended the inclusion of a Toll-free number as a means of reporting so as to consider all manner of persons.

(ii) All the stakeholders recommended for the inclusion addition of reporting center of social media threats and crime other than the Uganda Police Force. The discussion resolved to add the Financial Intelligence Authority, Uganda Communications Commission and a social media security advisor.

(iii) During the discussion, the stakeholders pointed out the need for reporter (end user) interaction with the Agency receiving the complaint. Therefore, an interactive mechanism was added that keeps the complainant/report in touch with the Agency handling the reported social media crime or threat.

(iv) The Telecom sector and Law enforcement stakeholders proposed that the system should be able to indicate the priority level of each reported incident of social media threats and crime. This was incorporated at a click for the user to select either; emergency, high priority or normal. This will in turn guide the recipient center to define its response time and resources to deploy.

(v) One of the stakeholders, in particular CIPESA and WoUGNET recommended for the inclusion of local languages (Kiswahili & Luganda) as part of the system since it is a public facing information system and some of the users are from the rural set up or even may not be conversant with the English language. This was considered and incorporated.

4.3.2 Online questionnaire

The respondents were drawn from the following sectors: Civil Society Organisations (CSO), Non-Governmental Organisations, Financial Technology Firms (FINTECH), Inspectorate of Government, Judiciary, Office of the Director of Public Prosecution, Uganda Police Force, University Students, Telecommunication Companies and the Uganda Communications Commission.

The -mentioned stakeholders were selected due to the role and responsibility they playing in addressing social media threats and crime or are providing technology driven platforms that have users who are prone to social media threats and crime.

The results from the questionnaire depicted what the user experience while interacting with the system.

(i) The users proposed for a more interactive and robust system with improved color and font themes.

(ii) The majority of respondents recommended for the use of Unstructured Supplementary Service Data (USSD) for submission of social media threats and crime. This is still work in progress

(iii) That safety and awareness tips or news should be more prominent on the home page along with the statistical data.

(iv) The inclusion of local language translator into the system to cater for the Bantu and Kiswahili users

In conclusion, albeit the cited areas for improvement, the stakeholders during both the FGD and the online questionnaire underscored the value addition and usefulness of the web-based system for reporting and creating awareness about social media threats and crime, namely;

(i) Its timely due of the increased incidents of social media threats and crimes.

(ii) It reduces on the reporting time of visiting a physical police station.

(iii) The system creates awareness on social media threats and has also provided platform for reporting and receiving feedback.

(iv) The system is device portable and has language translation option makes it the most preferred tool for social media threat reporting and crime awareness.

4.4 Hosting and Deployment

In order to deploy the system, I adopted the use of cloud-hosted services to deploy and manage the developed application on a Linux server. As earlier mentioned, MySQL was the Database Management System. Secure File Transfer Protocol (SFTP) was used for remote deployment. The web version of the web-based system for reporting and creating awareness about social media threats and crime is hosted on Ubuntu Linux digital ocean platform server (https://socialmedia.archersug.com/).; Apache lamp stack was used as the web-server and Linux as the operating system. I used the Google Map server, an SSH client for remote management and trouble-shooting. File transfer protocol (FTP) was used for remote deployment of the system. All these technologies offered robust, secure and agile capabilities.

4.5 System Requirements

The web-based system for reporting and creating awareness about social media threats and crime has both functional and non-functional requirements;

4.5.1 Functional Requirements

This section includes the definition of the functions and features of the web-based system for reporting and creating awareness about social media threats and crime in Uganda.

a) Functions of the system

(i) Enable users to report social media crime and threats as either registered or anonymous users of the system. This was derived from results of both the questionnaire and the focus group discussion where the Civil Society Organisations, Telecom Regulators and University students preferred inclusion of an option of anonymous reporting in order to preserve privacy of the reporters who may be drawn from either and the general public or organizations such as National Information Technology Authority of -Uganda (NITAU), Uganda Communications Commission (UCC), Global System for Mobile Association (GSMA), Non-Governmental Organizations (NGO), Uganda Police Force (UPF), Business community, among others.

(ii) Create and disseminate awareness news from a summary of threats and perpetration techniques submitted by users as well as existing reports from various professional bodies. This aspect was premised on the fact that the different agencies such as the Telecom sector and Civil Society Organizations were also providing consumer protection awareness and digital safety. Therefore, stakeholders who participated in the FGD suggested leveraging the same approach to provide continuous broadcast of social media safety tips to the general public.

(iii) Tracking of social media threat and crime locations as submitted by registered and anonymous users. These participants of the questionnaire and FDG who included NITAU, UCC, GSM, NGOs, UPF & business community agreed to the fact that the system ought to be interactive thus creating a track mechanism of the reported social media threats and crimes. Therefore, the use email as a chat platform of feedback was recommended so as to give real time response to the submitted social media threats on the platform. It was further noted by the participants from the Telecom sector that different action centers needed to be created in order to receive the various threats and crime.

(iv) The system should be able to show threat landscape of the social media threat perpetration techniques used by attackers. The system should be able to track threats and crimes reported by giving a detailed analysis of attack trends and periodic analysis in the specified location. From results of the questionnaire and FGD, representatives from Law enforcement and CSOs like CIPESA, recommended the inclusion of statistical data representation since both were already involved in the generation of the Annual Crime and Road Safety Reports as well as formulation of different International ICT Policies. They suggested that the system should provide social media threat and crime pattern analysis in accordance to the regions/districts of Uganda and category.

(v) The system should have guidelines and manuals that guide on how to use the platform. This should cover: general security tips on online safety, social networking sites standards and procedures, International and domestic laws that govern social media. These guidelines should combine ethics and professional standards put in place as guidelines for effective utilization of social media platforms as well as the social media threat awareness and crime reporting system. This was derived from the inputs of the Civil Society Organisations (CIPESA and WOUGNET), and Justice and Order Sector participants during the Focus Group Discussion. They argued that the system should have an eLearning feature where relevant laws and publications about social media threats, crimes and laws are profiled.

(vi) The system should provide for local and regional language translation. From the questionnaire and FGD results, majority of the participants mainly from the CSO, JLOS, Telecom and Business community underscored the fact that not all users understood the technical language used for social media threats and crime reporting. Therefore, an online google translator needs to be embedded into the system to translate English to other languages such as Luganda, Kiswahili, French, Arabic to mention but a few.

4.5.2 Non-Functional Requirements

These requirements describe the general properties of a web-based system for reporting and creating awareness about social media threats and crime. They are also known as quality attributes of the system.

a) Performance and scalability**.** The system will be able to return results in the shortest time possible and enhance access to social media threat and crime information.

b) Portability and compatibility**.** The system will be able to support all Operating Systems across any hardware and uses light weight technologies that have got low usage of system resources.

c) Reliability, maintainability, availability**.** The web-based system for reporting and creating awareness about social media threats and crime shall be reliable, easy to maintain and available over the internet.

d) Security. The system particularly for registered users, will be accessed through a login account. The application will have a security certificate to minimize on any forms of attacks such as cross-site scripting or SQL injection attacks

4.5.3 Hardware and Software Requirements

(i) Hardware

(a) Computer Processor of speed 3.0 Gigahertz. The computer processor clock speed will determine how quickly the central processing unit (CPU) can retrieve and interpret instructions (Input and Output). This will enable the computer accessing the system to multi-task faster.

(b) Random Access Memory (RAM) of 8GB as minimum. This will enable the computer to retrieve and read data for processing tasks such as retrieval of social media awareness news and crime maps. It reduces the risk of a major system crash due to overload.

(c) Sufficient hard disk of 500 Gigabytes space to store the large volumes of data into the SQL database and publication or social media awareness news downloads.

(d) Up and downlink of at most 20Mbps bandwidth. The internet speed capacity should be able to permit swift access to the web pages of the application and enable caching of pages for real time retrieval. This shall be provided by a compatible switch/router

(e) Firewall security: The system shall be secure from authorized traffic by using a pfSense router firewall.

(f) High-Definition Desktop monitor screen and power backup. The HD screen will provide clear display output of the system for the viewers. Since the system will display social media threat and crime maps and graphs. The power back up will facility business continuity in case of major power failures.

(ii) Software

(a) Operating systems-Windows (Vista, 7, 8,10, and 11). The mentioned operating system has got plugins that are compatible with the developed system. It offers user friendly Graphical User Interface (GUI), Multimedia support and upgradable with the latest security feature releases from Microsoft.

(b) The Webserver used is WAMP server. WAMP stands for Windows Apache, MySQL and PHP. It provides a virtual server on the computer that enables the testing of features without any consequences since it's localized and can be hosted on the local development machine.

(c) The Database Engine is MySQL because; it has got a faster query processing power, multiple views and a portable language that can be used across various windows operating system platforms.

(d) Internet explorer, Mozilla Firefox or Google Chrome web browsers. These browsers are supported by multiple operating systems, including those for mobile devices.

4.6 Systems Design

This section describes the design of the different components of the web-based system for reporting and creating awareness about social media threats and crime including user interfaces and flow of data, and data storage and retrieval covering both the physical and logical design. The key models presented include Context Diagram (CD), Use Case Diagram (UCD), Datta Flow Diagram (DFD) and Entity Relation Diagram (ERD)

4.6.1 Context Diagram

A context diagram was used to show how external entities interact with the internal system. In other words, it is used to depict the scope and boundaries of a system at a glance including the other systems that interface with it if any. The system administrator who is an ICT Law enforcement officer, has the right to create user accounts and delete them. As illustrated in figure 24, registered users and guests can report and view threat details.

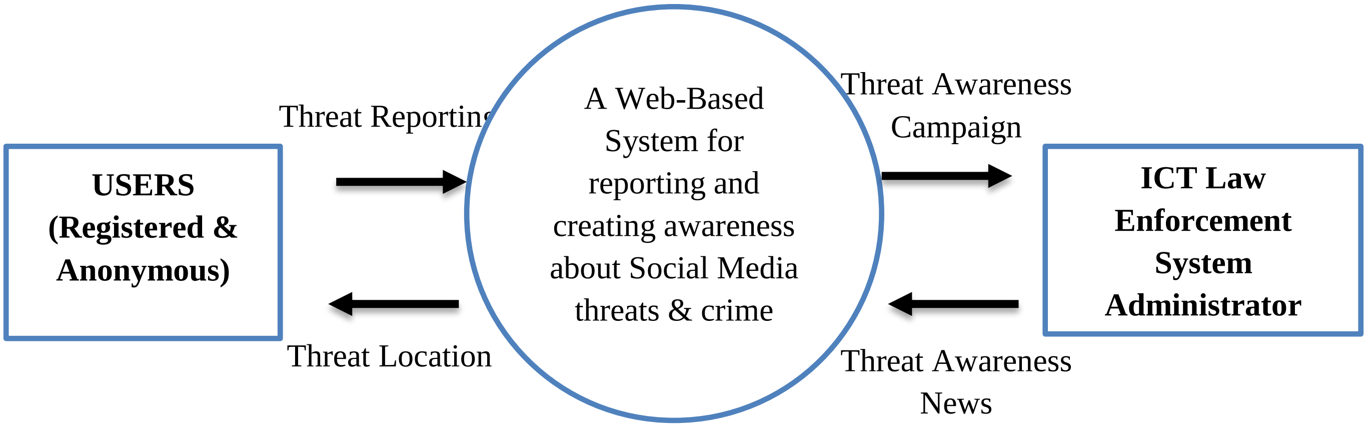

Threat Reporting
A Web-Based System for reporting and creating awareness about Social Media threats & crime
Threat Awareness Campaign
USERS (Registered & Anonymous)
ICT Law Enforcement System Administrator
Threat Location
Threat Awareness News

Figure 24: Context diagram for the web-based system for reporting and creating awareness about social media threats and crime

As represented in the context diagram, a user is categorized as registered and non-registered ones that can report threats into the system and also query the database and view threat information, threat locations as well as perpetration techniques and awareness information. Such users include professional bodies such as NITAU, Uganda Police Force, the GSM network, regulators such as UCC, the business community as well as ordinary social media users. The system administrator can post threat awareness tips. Registered and Anonymous users are able to report a threat and also view reported threat from other users as well as threat awareness tips. The context diagram shows the registered and anonymous system users, and the systems administrator.

4.6.2 Use Case Diagram

A Use Case Diagram is a behavioural UML diagram type that is used to analyze the different user roles of a system under development. It enables one to visualize the different types of roles in a system and how those roles interact with the system.

The system users are systems administrators (ICT Law Enforcement), registered users, and Guests/unregistered/anonymous users. Registered users include those from professional bodies such NITAU, GSM Network, NGO, sector regulators such as UCC, crime prevention units such as the Uganda Police force, Business community, as well as registered social media users.

These are illustrated in the use case diagram by figures 24,25 and 26.

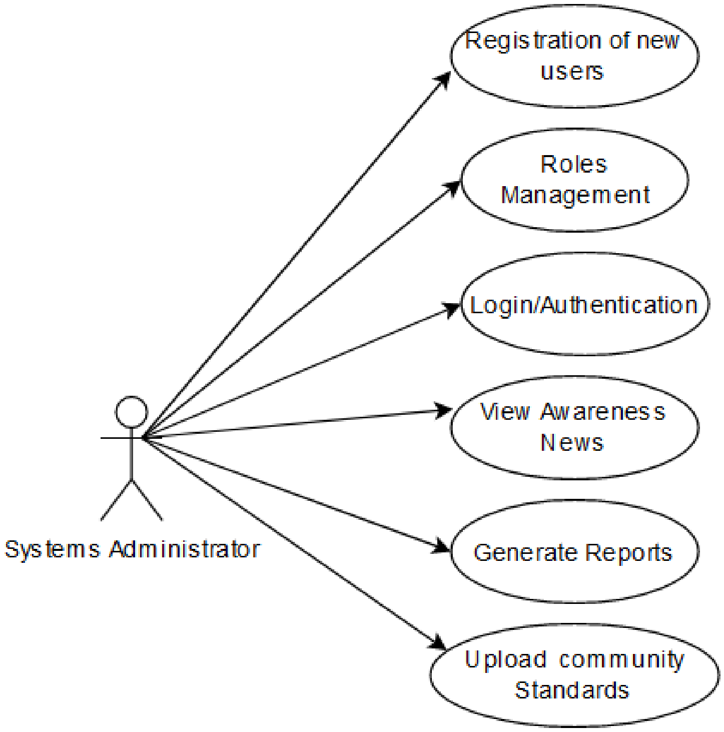


Figure 25: System administrator Use Case Diagram

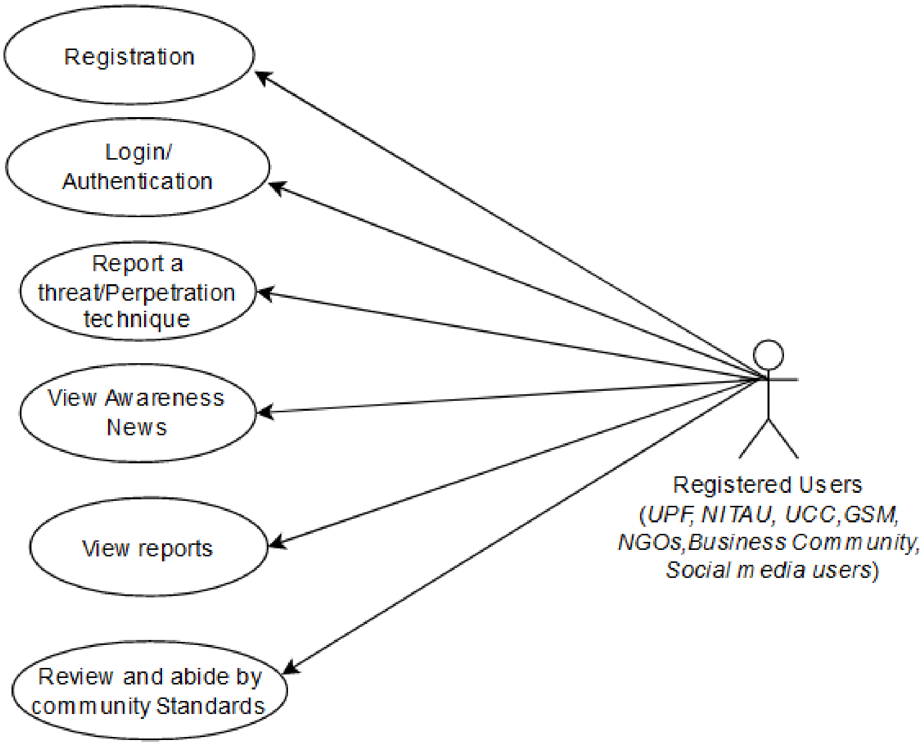

Registration
Login/ Authentication
Report a threat/Perpetration technique
View Awareness News
View reports
Review and abide by community Standards
Registered Users
(UPF, NITAU, UCC,GSM, NGOs,Business Community, Social media users)

Figure 26: Registered user use case diagram

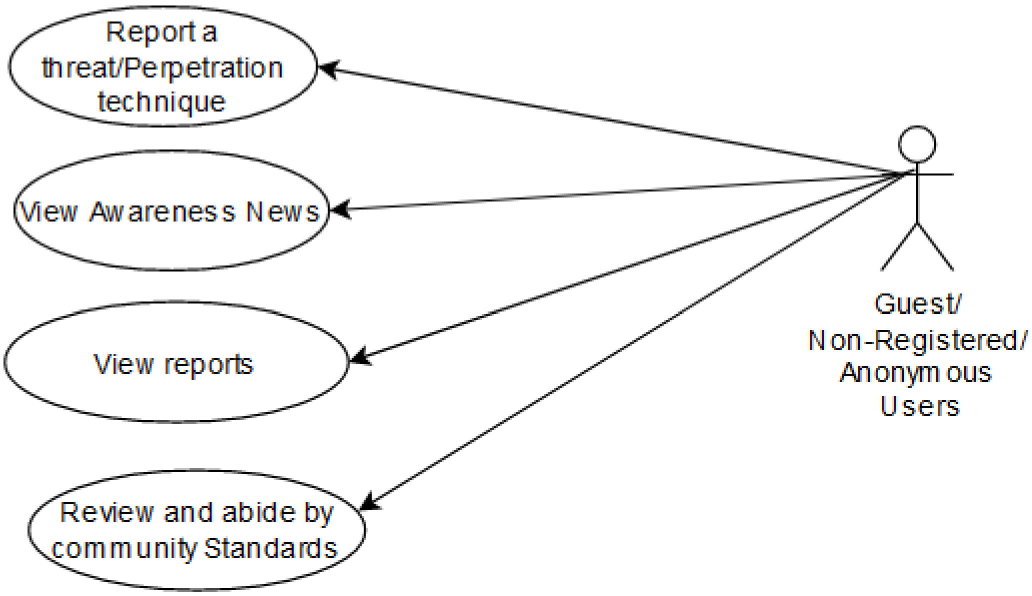

Report a threat/Perpetration technique
View Awareness News
View reports
Review and abide by community Standards
Guest/ Non-Registered/ Anonymous Users

Figure 27: Anonymous/non-registered user use case diagram

The Use Case diagram, explicitly outlines the different roles played by the different stakeholders in the system. These are described as;

a) Systems Administrator

The system administrator is the overall manager of the application, and he is able to manage all the roles in the system from registration, of users, roles management, capturing of awareness news, view of all reports in the system and upload of community standards. This is an ICT Law Enforcement Officer. This is illustrated in figure 24.

b) Registered users

These are the main data providers in the system. They are responsible for reporting crimes and threats, view awareness news and reports. These users include those from professional bodies such NITAU, GSM Network, NGO, sector regulators such as UCC, crime prevention units such as the Uganda Police force, Business community, as well as registered social media users. As illustrated in figure 25, they can register and login into the system, report threats, view reports from the system, review and abide by the existing community standards.

c) Anonymous users/Guest

These are also referred to non-registered users, they can report threats, view awareness news as well as report, view and abide by the existing community standards as illustrated in figure 27.

4.6.3 Data Flow Diagram

Data flow diagrams show the flow of information in and out of the web-based system for reporting and creating awareness about social media threats and crime. It clearly shows the flow of data within the system including the inputs, outputs, processes and data stores as illustrated in the DFD as shown in figure 26

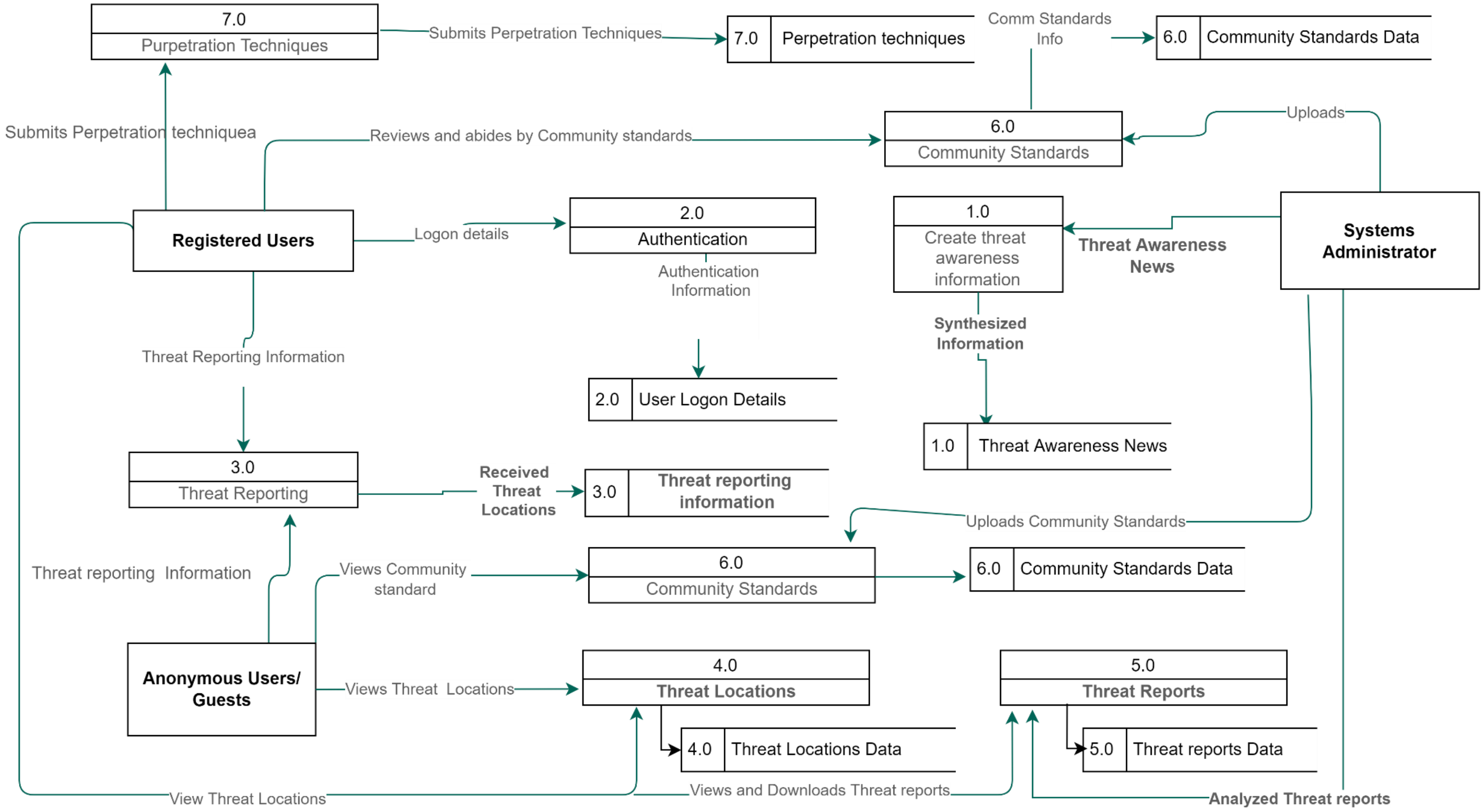
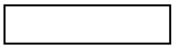
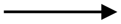
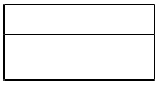


Figure 28: Data Flow Diagram for the web-based system for reporting and creating awareness about social media threats and crime

The data flow diagram shows the various processes used by the system users as illustrated in figure 27. It further shows the information accessed by the users and the processes that take place which include, input and output.

Table 3: Key for the data flow diagram

KEY

Name	**Symbol**	**Description**
External entity		Describes a user that interacts with the system.
Data Flow		This shows information flow in and out of the system.
Process		These are activities that retrieve or add information to the system.
Data Store		These are different storage areas in the system where processes alter this information.

Information flows as inputs, processes and outputs. Data stores represent storage files in the web-based system for reporting and creating awareness about social media threats and crime. Most of the actors that change data in the system include; System administrators, Anonymous and registered users.

a) Description of the Level One Data Flow Diagram

Figure 23, is the description of level one data flow diagram for all entities, actors and process that manipulate information in the web-based system for reporting and creating awareness about social media threats and crime in Uganda.

(i) Entities

This describes the user that interacts with the web-based system for reporting and creating awareness about social media threats and crime which include;

(a) **System Administrator;** The System administrator is authorized to create, delete and update user accounts that are considered as system users. This entity is also responsible for updating on threat awareness information.

(b) **Registered users;** A user who is considered as a user is an entity that views the social media threat reporting and crime awareness information from the system. A user can also create an account set and change his password and submit threat information into the system. Additionally, the user can also print a report for the status of his threats and crimes reported.

(ii) Data stores

This shows different data storage areas of the web-based system for reporting and creating awareness about social media threats and crime provided from different processes with the system.

(a) **Authentication details;** this includes all login information about users. This includes the login information such as username and password.

(b) **Threat and awareness information;** this is stored information about the threats and perpetration techniques available to the system users Services include types of threat reporting, awareness information and crime location.

(iii)Processes

This shows the different activities that are performed by the users with the web-based system for reporting and creating awareness about social media threats and crime. Processes are actions performed by different entities on the system so as to manipulate the data. These include delete, update, create and alter. The symbol above represents the flow of information in the system.

(a) **Authentication**: User is given access to the system using their user details. Details are sent to database for authentication purposes.

(b) **Registration of new users**. User is able to register their details before threat and crime reporting.

(c) **Threat and crime reporting**. The user is able to view all threats and crimes reported to the system. This can be done even for users who are not yet registered on the system.

(d) **View threat awareness information**. All details of the threats and awareness campaigns are uploaded by the systems administration, and the rest of the users are able to view captured information about threats and attack landscape.

(iv) **Data flow**

This shows the flow of information from an entity to a process and to a data store in the web-based system for reporting and creating awareness about social media threats and crime

(a) Logon Details; this represents the flow of logon details of the system users.

(b) Service details; the flow of the threat awareness service details when they are being accessed by the system users.

(c) Submit details; the flow of information submitted to the system.

(d) User details; the flow of the details of the system users when accessing the system. This is at the logon level during authentication.

(e) Registered user details; the flow of the user details when accessed by the system users depending on the rights assigned.

(f) Update threat information and attack landscape

4.7 Database Design

This section describes the methods that were used to model the database of the web-based system for reporting and creating awareness about social media threats and crime.

4.7.1 Entity Relationship Diagram

An entity relationship diagram was used to design the logical flow of information in the developed system. This is illustrated in figure 28.

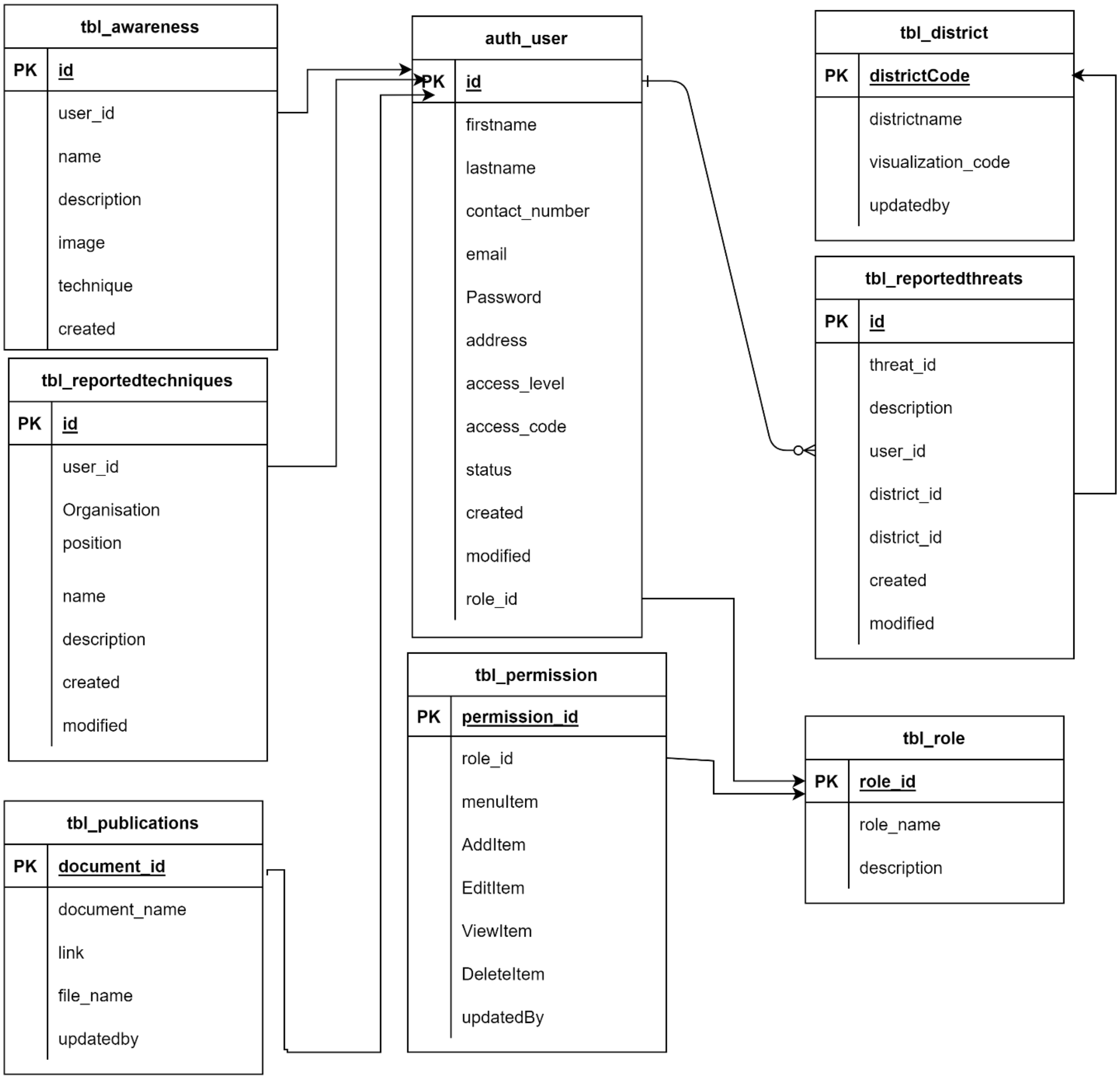


Figure 29: Entity relationship diagram

a) **tbl_awareness**; the entity stores social media awareness news of the different types of attacks and methods used.

b) **tbl_reportedthreats**; this entity stores information about social media related threats

c) **tbl_reportedtechniques;** the table stores social media perpetration techniques.

d) **auth_user**; in this entity is where access rights are granted to the users. The entity thus has a relationship with the user table.

e) **tbl_district**; This entity stores information about location about threats and crimes reported

f) **tbl_role**: This entity stores information about user roles in the system, and allows the system administrator to setup roles depending on the need.

g) **tbl_permission**: This entity allows the system administrator to assign different users permissions to the system, based on their user roles and what they are supposed to access as per the use case mapping and following the principle of least privilege.

This section defines the various entities and their attributes and data types. is the physical design of the database. Tables are broken down into User, registration, threat reporting and social media threat techniques. The required fields were selected, and unique identifiers known as primary keys selected. The entities are defined by Tables while attributes by columns in the physical database.

4.7.2 Table Structures for the Designed System

a) Database Name: db_socialmedia_v1

(i) Table: users

This table keeps details of the users on the system. It captures the user ID, the name of the user, the password, and the role and email address of the user. These are the details submitted by the users at the request to a user profile.

Table 4: User profile attributes

Column Name	Data Type	Type Size	Extra attributes	Description
Id	**integer**	**11**	**Primary Key**	
Firstname	varchar	32		first name of user
Lastname	varchar	32		Last name of the user
Email	varchar	64		Email address
Contact_number	varchar	64		Contact number
Address	text			Contact address
Password	varchar	30		The password for login
Access_level	text			Stores access code of the user
Access_code	**integer**	**11**	**Foreign Key**	**User's profile**
Status	varchar	30		Shows email address of user
Created	date			Stores the date when a record is created
Modified	date			Stores the date when a record is modified.

The Table user, records the users accessing the system. All user details are captured there and can be retrieved any time from the system. This varies from user identification *id* that is regarded as a primary key and uniquely identifies records in the table, its data type is an integer *int (11),* and name, password and email are declared as variable characters *varchar (32).* The role of every user is declared as a text because it captured a long text alpha numeric string that stores the user role in the system.

(ii) Table: tbl_reportedthreats

This table keeps details of threats reported by the different users. This is illustrated in the table below.

Table 5: Reported social media threats table attributes

Column Name	Data Type	Type Size	Extra attributes	Description
Id	**integer**	**11**	**Primary Key**	**Unique identifier**
threat_id	**varchar**	**50**	**Unique**	**Unique key**
description	date	50		description
user_id	integer	11		User identifier
district_id	varchar	50		District identifier
Created	date			Date created
Modified	date			Date modified

(iii)Table: tbl_reportedtechniques:

This gives details of techniques used by attackers. The user is able to access the different attack techniques used by attackers as illustrated below;

Table 6: Reported social media techniques table attributes

Column Name	Data Type	Type Size	Extra attributes	Description
Id	**integer**	**11**	**Primary Key**	**Composite key**
User_id	**integer**	**11**	**Primary Key**	**Composite key**
Organization	varchar	50		Organization Name
Position	varchar	50		position

Column Name	Data Type	Type Size	Extra attributes	Description
Name	varchar	50		Name of attack technique
description	text			Description of attack technique
Created	date			Date of creation
Modified	date			Date modified

(iv) Table: tbl_awareness:

This table keeps details of threat awareness that is given and posted by the system administrator onto the system, as a posted by the users of the system. The system captures all threat awareness information of users the threat and crime reporting information system.

Table 7: Social media awareness news table attributes

Column Name	Data Type	Type Size	Extra attributes	Description
Id	Integer	11	Primary Key	Awareness identifier
User_id	integer	11	Foreign Key	User identifier
Name	varchar	50		Name of awareness technique
description	varchar	255		Detailed description non an awareness technique
Image	varchar	512		Uploaded image
Technique	varchar	255		Attack technique
Created	date			Date of creation

(v) Table*:* tbl_district

This table captures the administrative units of the locations where threats are reported. The primary key in this table is the district Code which is a unique identifier for the data available in the system.

Table 8: District table attributes

Column Name	Data Type	Type Size	Extra attributes	Description
districtCode	integer	11	Primary Key	District Code, primary key
districtName	Varchar	50	Unique	District name
visual_code	varchar	50		Administration unit visualization code
updated by	varchar	50		Updated by

(vi)Table*:* tbl_role

This table captures the user roles expected in the system. The primary key in this table is the role_id which is a unique identifier for the data available in the system.

Table 9: Roles table attributes

Column Name	Data Type	Type Size	Extra attributes	Description
Role_id	integer	11	Primary Key	Role ID, primary key
Role_name	Varchar	50	Unique	Role name
description	varchar	100		Description

(vii) Table*:* tbl_permission

This table captures the user permissions expected for every user in the system, and the system functionalities they are supposed to access. in the system. The primary key in this table is the permission_id.

Table 10: Permissions table attributes

Column Name	Data Type	Type Size	Extra attributes	Description
permission_id	integer	11	Primary Key	Permission ID, primary key
Role_id	integer	50		Role name
menItem	varchar	100	Unique	Menu item
AddItem	boolean	1		Boolean
EditItem	boolean	1		Boolean
viewItem	boolean	1		Boolean
DeleteItem	boolean	1		Boolean
Updatedby	Varchar	50		Person who updated the permissions.

CHAPTER FIVE: SYSTEM MPLEMENTATION

5.0 Accessing the system

Navigation into the web-based system for reporting and creating awareness about social media threats and crime starts by accessing the link (https://www.socialmedia.archersug.com/) that loads the homepage in form of a dashboard that shows statistics of existing threats and attacks reported. This is illustrated in figure 30 as an extract of the display during the month of April 2022.

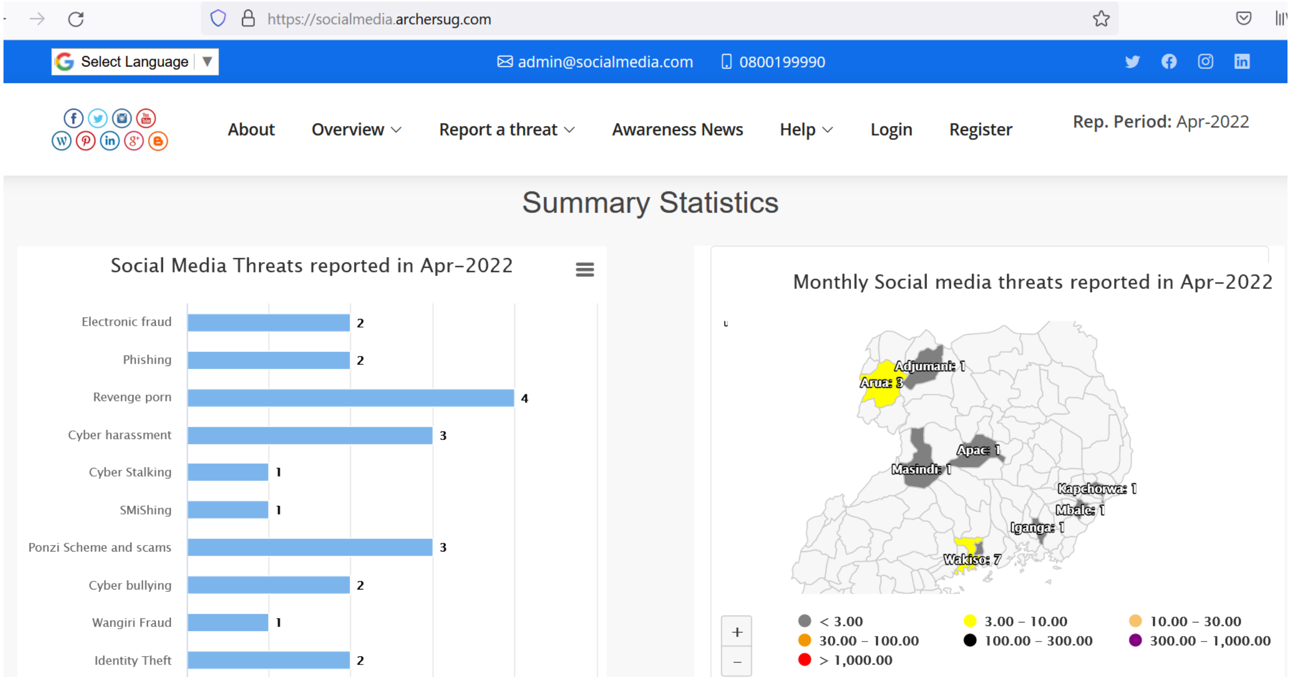
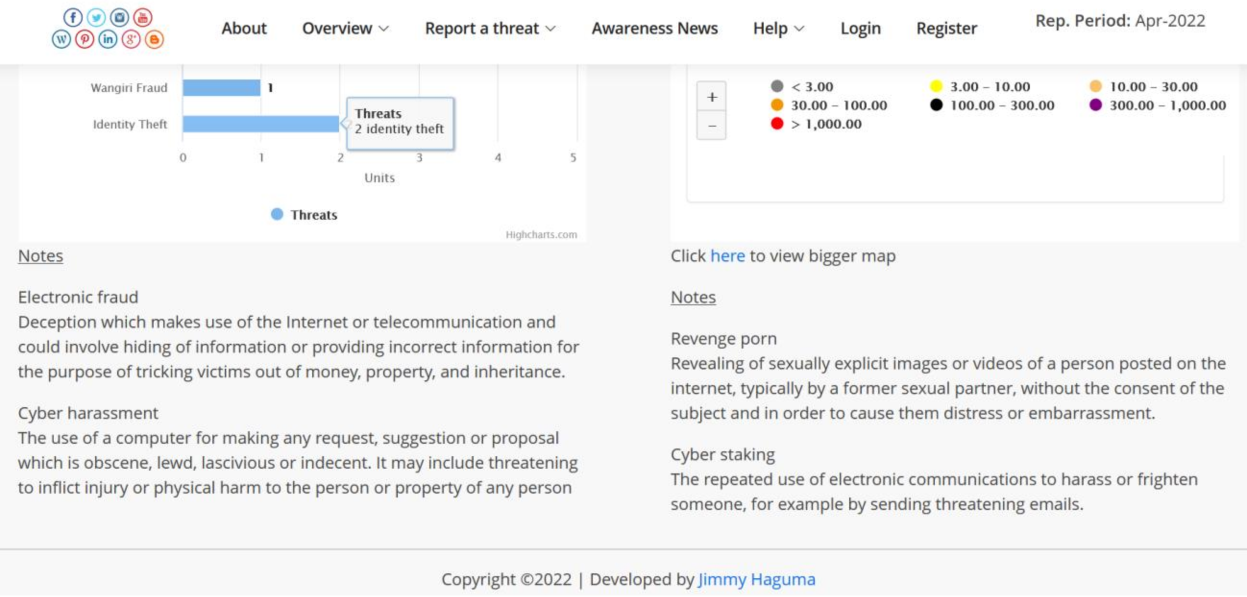


Figure 30: A snapshot of the summary statistics from the system

The Summary of statistics page has a number of menus that enables users both registered and anonymous to report any form of social media threat, view awareness news, seek for help on the use of the system and also register as illustrated in figure 31.



Notes

Electronic fraud
Deception which makes use of the Internet or telecommunication and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance.

Cyber harassment
The use of a computer for making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent. It may include threatening to inflict injury or physical harm to the person or property of any person

Click here to view bigger map

Notes

Revenge porn
Revealing of sexually explicit images or videos of a person posted on the internet, typically by a former sexual partner, without the consent of the subject and in order to cause them distress or embarrassment.

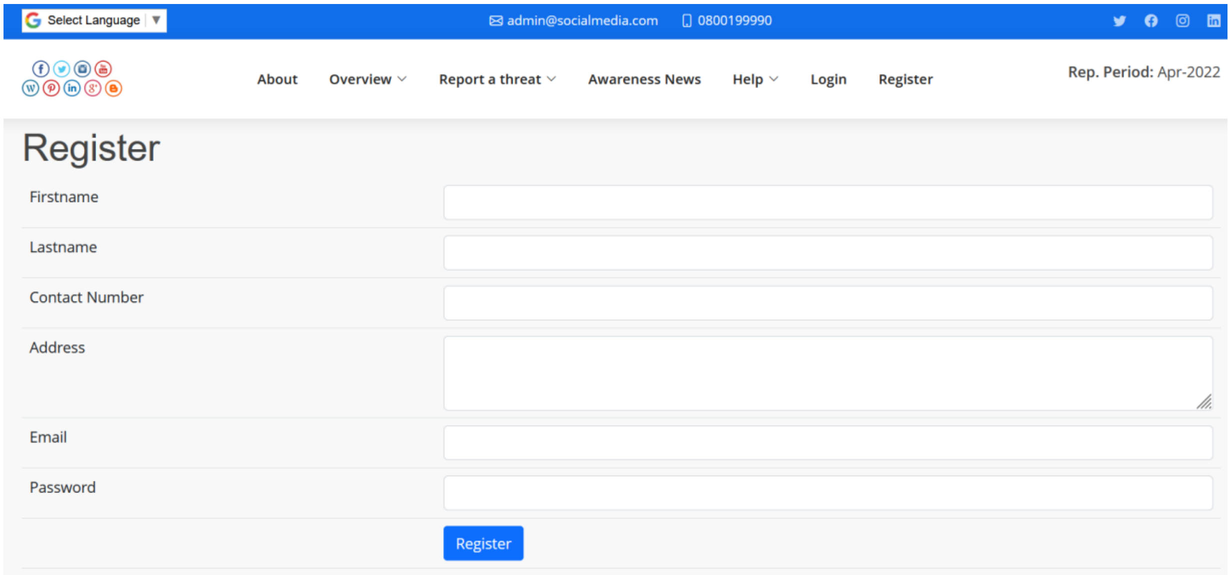
Cyber staking
The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.

Copyright ©2022 | Developed by Jimmy Haguma

Figure 31: Details display of the notes page

5.1 User Registration

From the registration menu, users are able to register their details prior to submission of social media threats. This covers the user’s email address and the desired password as shown in figure 32.



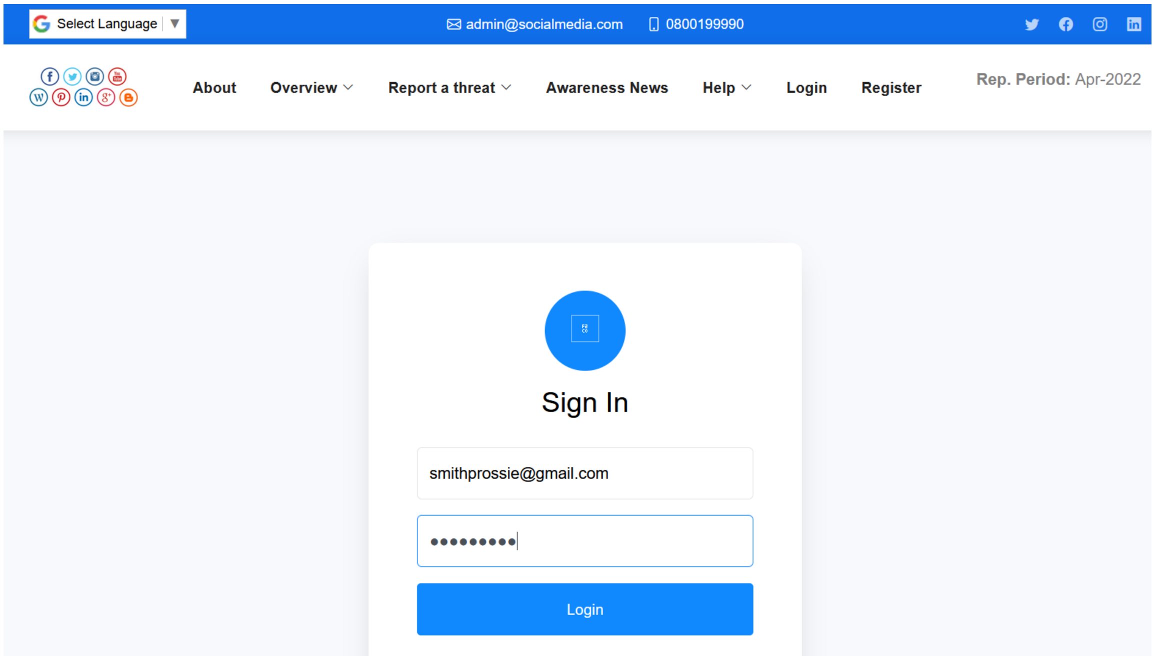
Register

Firstname	
Lastname	
Contact Number	
Address	
Email	
Password	
	Register

Figure 32: User registration form

5.2 User login

Once registration is completed, the next step is signing into the web-based system for reporting and creating awareness about social media threats and crime web-application as shown in figure 33.



Rep. Period: Apr-2022

smithprossie@gmail.com

•••••••••

Figure 33: User login process using email address

From figure 33, a user is required to fill in their login credentials to access the web-based system for reporting and creating awareness about social media threats and crime application. This is then followed by the process of reporting social media related threats to various categories of relevant bodies namely: Uganda Police Force, Uganda Communications Commission or Social media security advisor from the National Information Technology Authority of Uganda as shown in figure 36.

5.3 Password reset/forgot function

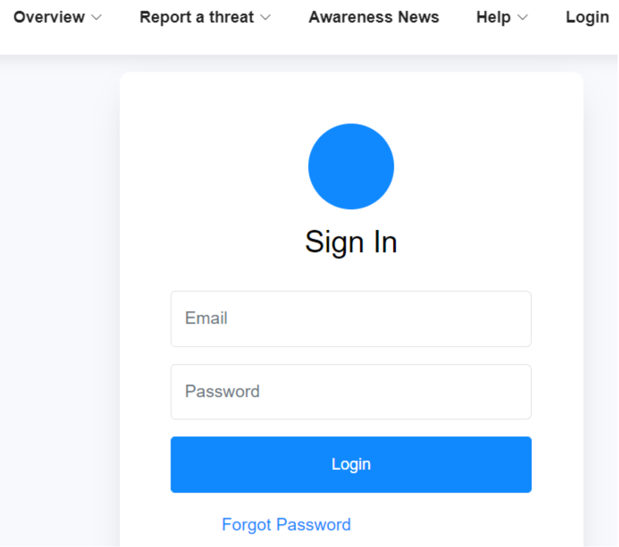
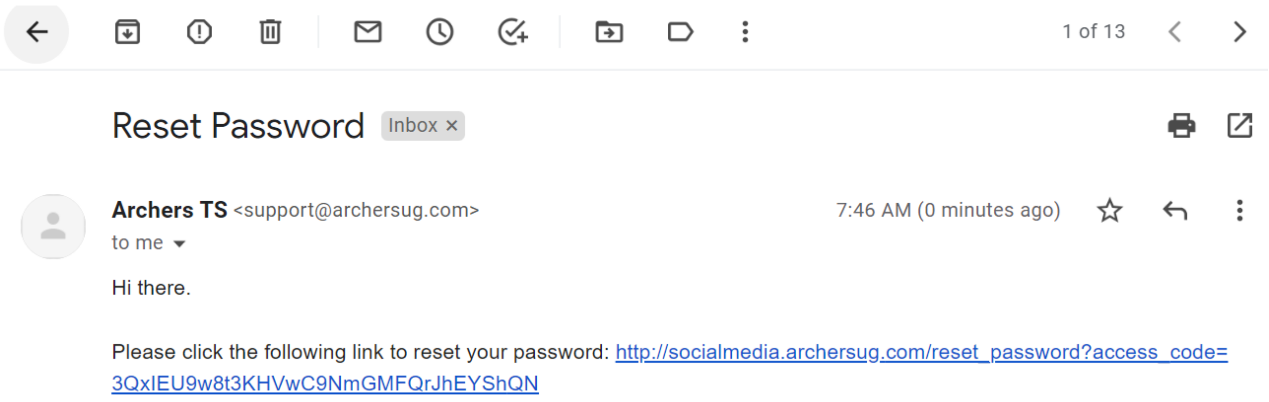


Figure 34: Forgot password display

Figure 34 shows the forgot password option. This option enables the user to reset their login credentials in case one has forgotten. This is further explained through the illustration in figure 35 with the reset password link.



Reset Password

Archers TS <support@archersug.com>
to me
7:46 AM (0 minutes ago)

Hi there.

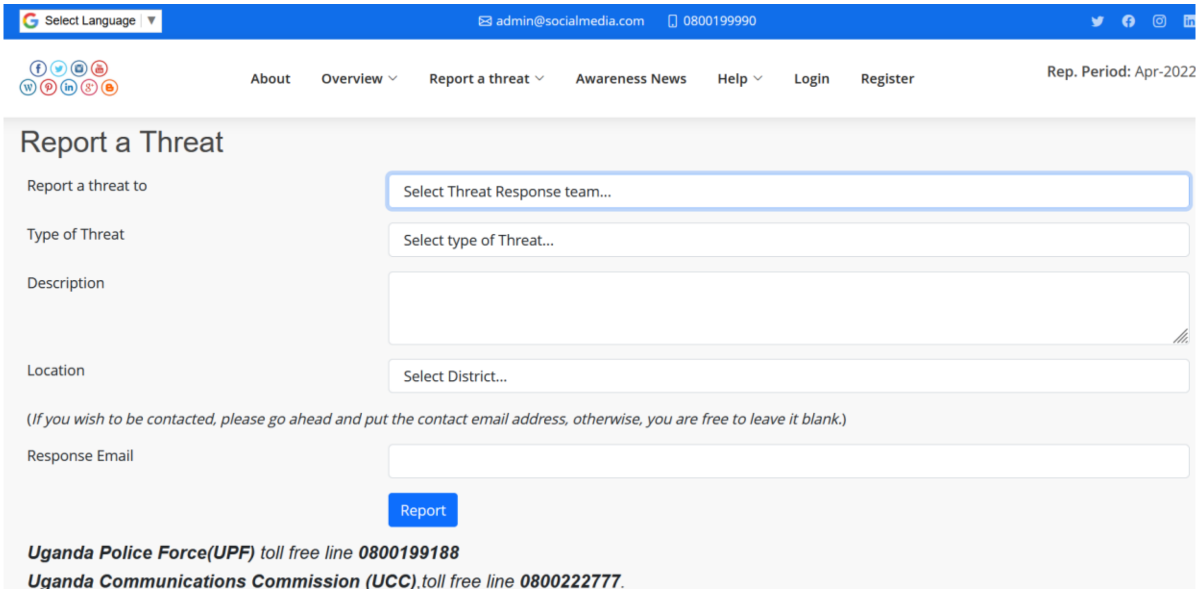
Please click the following link to reset your password: http://socialmedia.archersug.com/reset_password?access_code=3QxIEU9w8t3KHVwC9NmGMFQrJhEYShQN

Figure 35: Reset password link sent to user email

Figure 35, illustrates what happens if a user has forgotten their password and then opts for a reset. The reset function is display at the login prompt as forgot password. The reset will be sent to the email which is the username of the account user.

5.4 Social Media Threat Reporting function

This function enables the users to report social media threats to the relevant action centers namely: Uganda Police Force, Uganda Communications Commission or Social Media Security Advisor which is part the National Information Security Advisor Group (NISAG) which is an ad-hoc team of security experts based at the National Information Technology Authority of Uganda’s Computer Emergency Response Team (CERT)



Rep. Period: Apr-2022

Report a Threat

Report a threat to	Select Threat Response team...
Type of Threat	Select type of Threat...
Description	
Location	Select District...

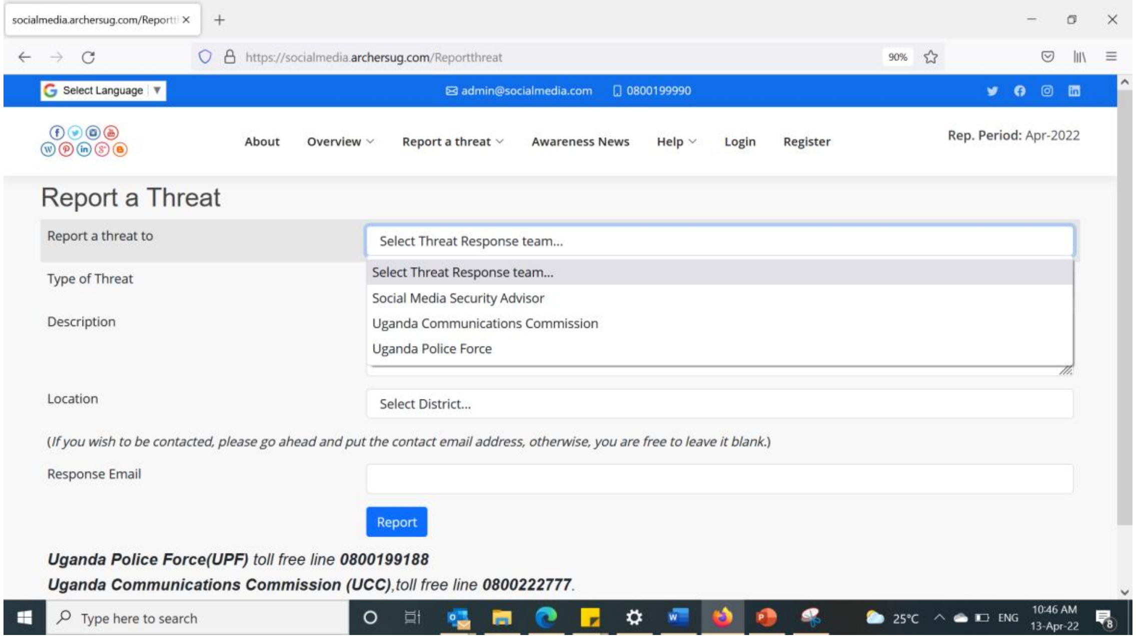
(If you wish to be contacted, please go ahead and put the contact email address, otherwise, you are free to leave it blank.)

Response Email

Uganda Police Force(UPF) *toll free line* ***0800199188***

Uganda Communications Commission (UCC)*,toll free line* ***0800222777****.*

Figure 36: Social media threat reporting



Rep. Period: Apr-2022

Report a Threat

Report a threat to	Select Threat Response team...
Type of Threat	Select Threat Response team... Social Media Security Advisor Uganda Communications Commission Uganda Police Force
Description	
Location	Select District...

(If you wish to be contacted, please go ahead and put the contact email address, otherwise, you are free to leave it blank.)

Response Email

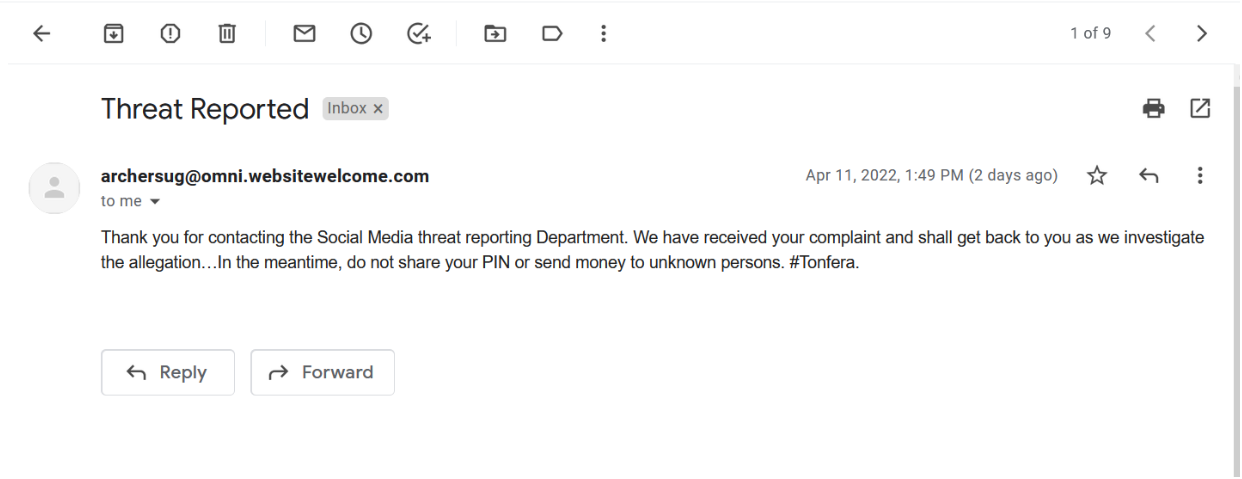
Uganda Police Force(UPF) *toll free line* ***0800199188***

Uganda Communications Commission (UCC)*,toll free line* ***0800222777****.*

Figure 37: Social Media Threat Reporting Action Centers

5.5 Automated system email alert

Once the user has reported any form of threat, they will receive an automatic response from the system that contains information security tips. This is shown in figure 37.



archersug@omni.websitewelcome.com

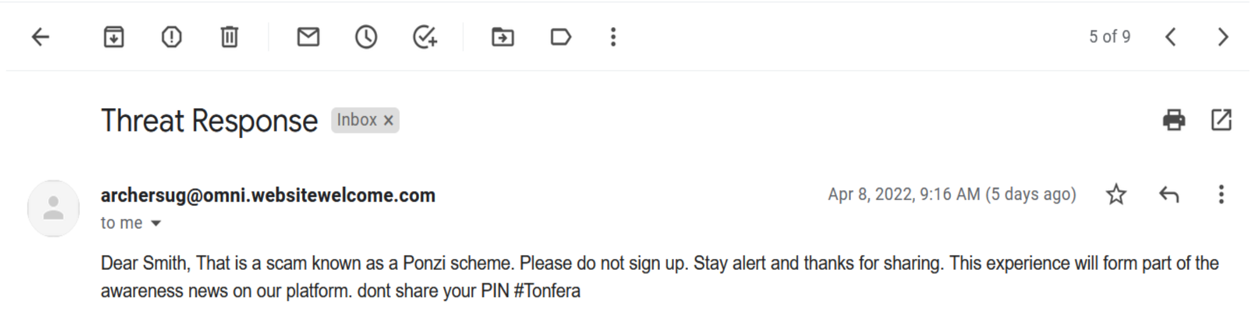
to me

Apr 11, 2022, 1:49 PM (2 days ago)

Thank you for contacting the Social Media threat reporting Department. We have received your complaint and shall get back to you as we investigate the allegation…In the meantime, do not share your PIN or send money to unknown persons. #Tonfera.

Figure 38: Automated email with security tip

Upon receipt of the reported threat, the target entity will respond to the user by giving relevant guidance or possible action or safer measures for the case of the threat reported to a social media security advisor. This is illustrated in the email extract from a user known as Smith in the figure 39.



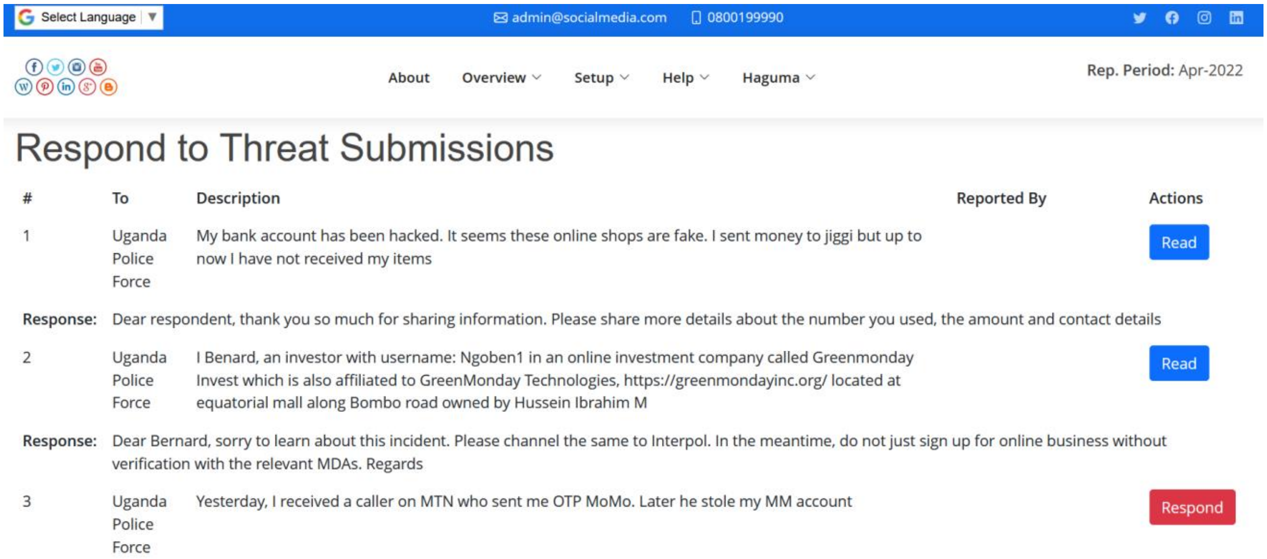
archersug@omni.websitewelcome.com

to me

Apr 8, 2022, 9:16 AM (5 days ago)

Dear Smith, That is a scam known as a Ponzi scheme. Please do not sign up. Stay alert and thanks for sharing. This experience will form part of the awareness news on our platform. dont share your PIN #Tonfera

Figure 39: System admin response to reported threat



Respond to Threat Submissions

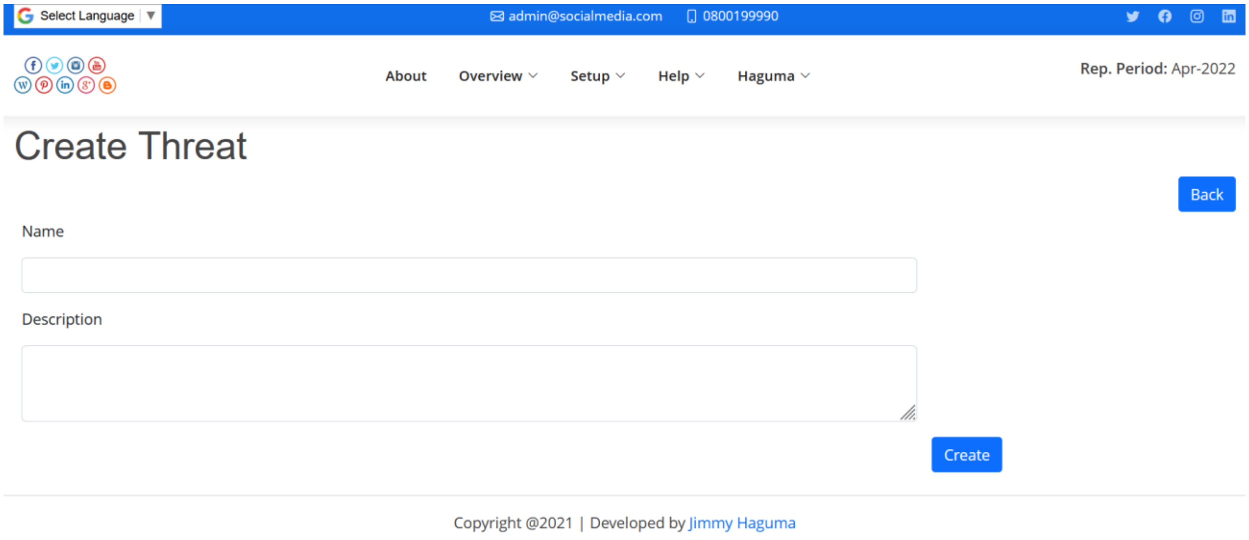
#	To	Description	Reported By	Actions
1	Uganda Police Force	My bank account has been hacked. It seems these online shops are fake. I sent money to jiggi but up to now I have not received my items		Read
Response:	Dear respondent, thank you so much for sharing information. Please share more details about the number you used, the amount and contact details			
2	Uganda Police Force	I Benard, an investor with username: Ngoben1 in an online investment company called Greenmonday Invest which is also affiliated to GreenMonday Technologies, https://greenmondayinc.org/ located at equatorial mall along Bombo road owned by Hussein Ibrahim M		Read
Response:	Dear Bernard, sorry to learn about this incident. Please channel the same to Interpol. In the meantime, do not just sign up for online business without verification with the relevant MDAs. Regards			
3	Uganda Police Force	Yesterday, I received a caller on MTN who sent me OTP MoMo. Later he stole my MM account		Respond

Figure 40: System admin portal for reported social media threats and crime

Figure 40, shows the admin portal dashboard of the reported social media threats and crimes. It is from this portal that the user receives feedback as response to the incidents reported and also from the same content the relevant action center will act to investigate the reported cases. These action centers include Law enforcement, Social Media Security Advisory, Uganda Communication Commission or the Financial Intelligence Authority based on what the user has indicated at the point of reporting the crime.

5.6 Viewing of the Social Media Threat and Crime perpetration technique

Once a threat is created in the system by the administrator, the next step is to provide a brief description of the kind of threat. This is done in reference to attacks reported and are entered into the system as shown in figure 41 and 42.



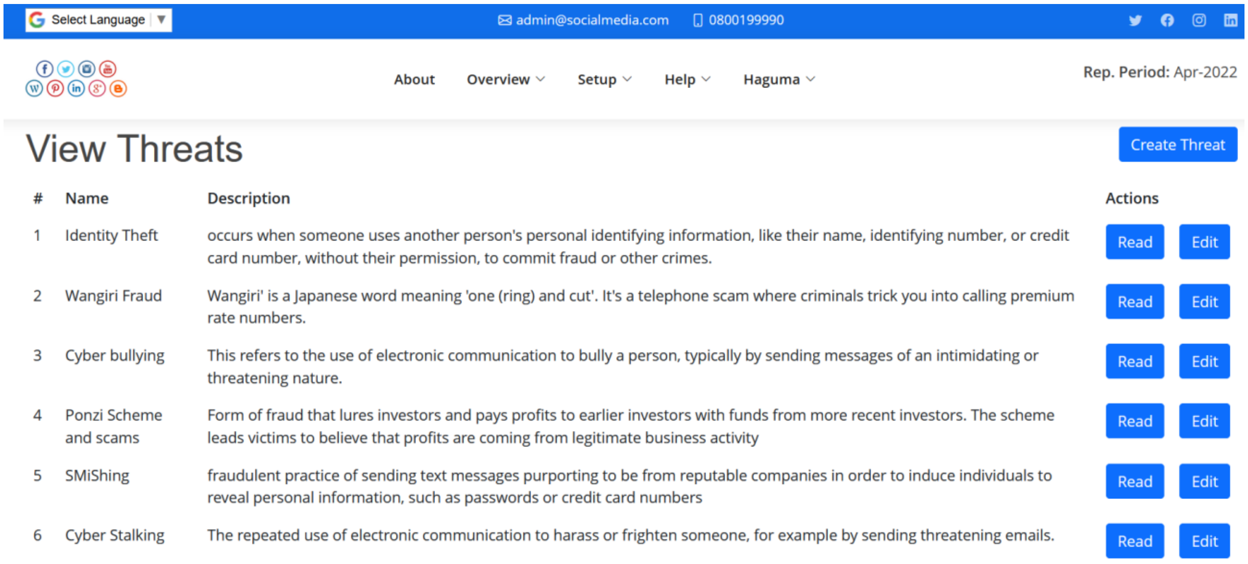
Create Threat

Name

Description

Copyright @2021 | Developed by Jimmy Haguma

Figure 41: Admin portal showing the social media threat and crime perpetration techniques



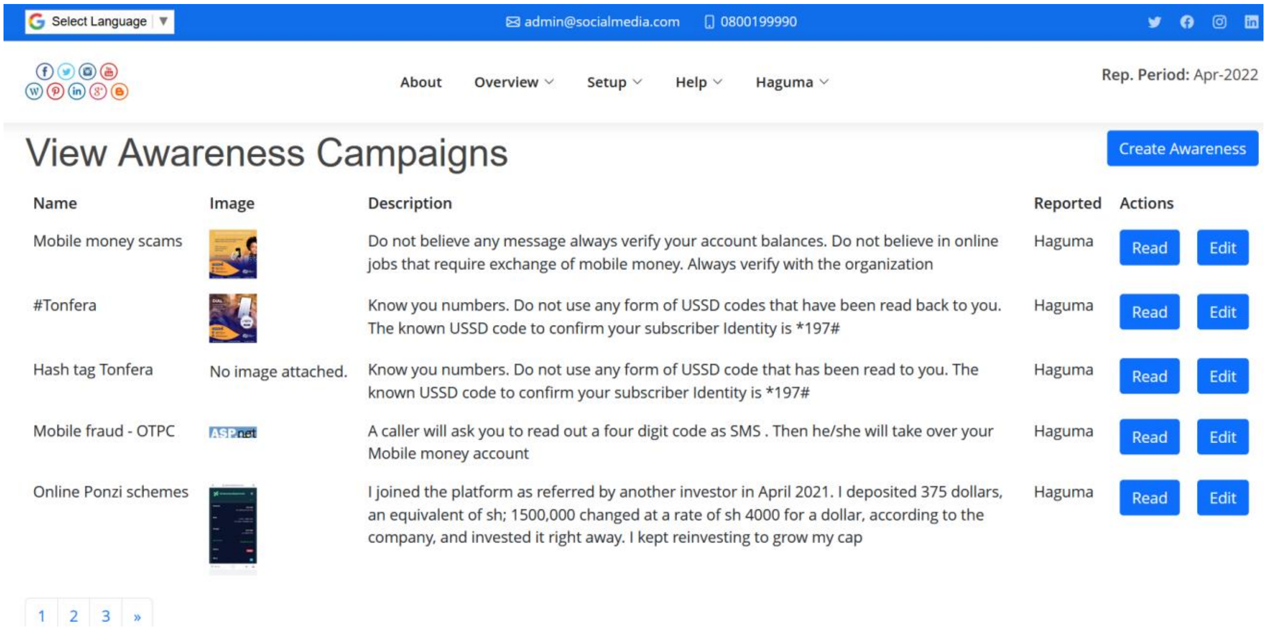
View Threats

#	Name	Description	Actions
1	Identity Theft	occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.	Read Edit
2	Wangiri Fraud	Wangiri' is a Japanese word meaning 'one (ring) and cut'. It's a telephone scam where criminals trick you into calling premium rate numbers.	Read Edit
3	Cyber bullying	This refers to the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.	Read Edit
4	Ponzi Scheme and scams	Form of fraud that lures investors and pays profits to earlier investors with funds from more recent investors. The scheme leads victims to believe that profits are coming from legitimate business activity	Read Edit
5	SMiShing	fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers	Read Edit
6	Cyber Stalking	The repeated use of electronic communication to harass or frighten someone, for example by sending threatening emails.	Read Edit

Figure 42: Admin portal for creating a system threat

5.7 Creating and disseminating of social media awareness news/information

This involves publishing information or content submitted by users in threat reports, coupled with publicly available information on the laws, frameworks and technology trends by the system administrator, to be able to share awareness news. This is illustrated in figure 43.



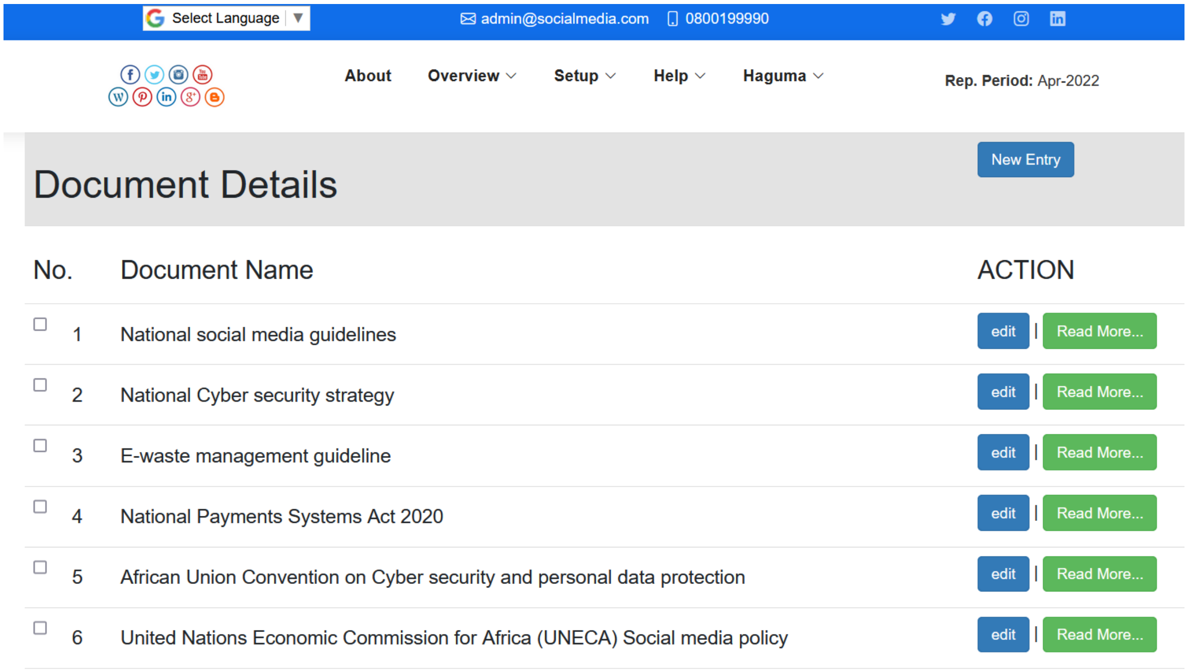
View Awareness Campaigns

Name	Image	Description	Reported	Actions
Mobile money scams		Do not believe any message always verify your account balances. Do not believe in online jobs that require exchange of mobile money. Always verify with the organization	Haguma	Read Edit
#Tonfera		Know you numbers. Do not use any form of USSD codes that have been read back to you. The known USSD code to confirm your subscriber Identity is *197#	Haguma	Read Edit
Hash tag Tonfera	No image attached.	Know you numbers. Do not use any form of USSD code that has been read to you. The known USSD code to confirm your subscriber Identity is *197#	Haguma	Read Edit
Mobile fraud - OTPC		A caller will ask you to read out a four digit code as SMS . Then he/she will take over your Mobile money account	Haguma	Read Edit
Online Ponzi schemes		I joined the platform as referred by another investor in April 2021. I deposited 375 dollars, an equivalent of sh; 1500,000 changed at a rate of sh 4000 for a dollar, according to the company, and invested it right away. I kept reinvesting to grow my cap	Haguma	Read Edit

Figure 43: System Admin portal for creating social media awareness news

5.8 Using the System Help function

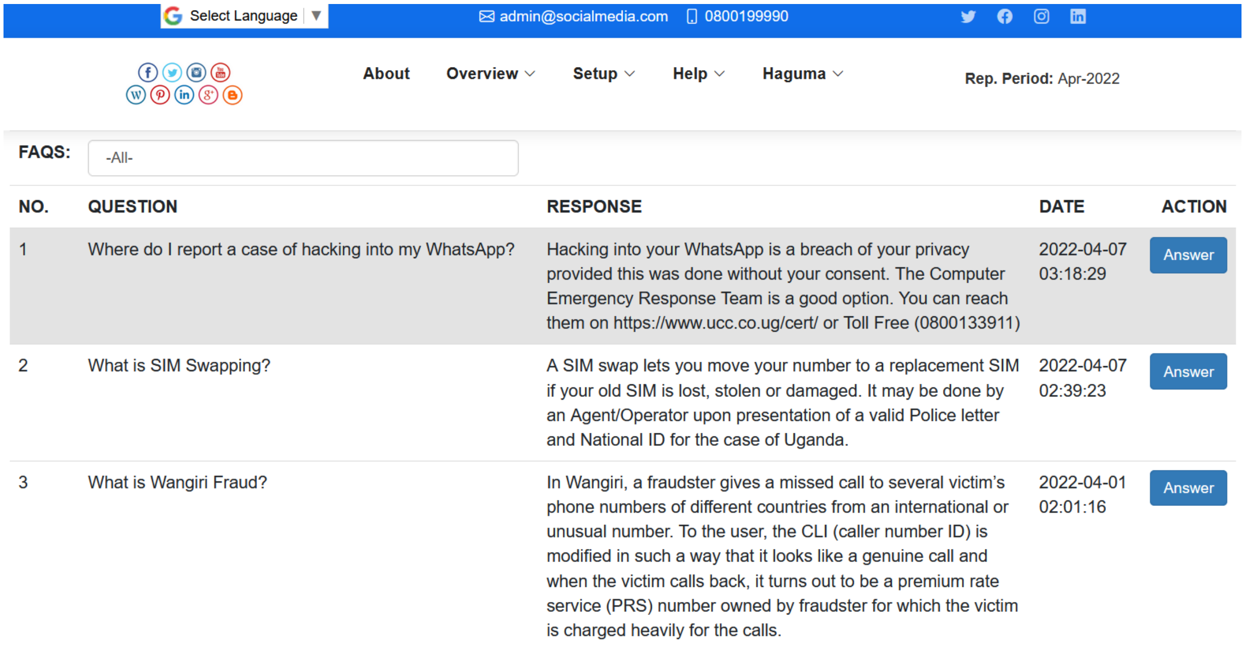
The system has provisions of support to the user(s) who may wish to view or pose the Frequently Asked Questions (FAQs) and read the system user guide. This therefore makes the system interactive enhances the user experience. This is illustrated in figures 44, 45 and 46.



Document Details

	No.	Document Name	ACTION
□	1	National social media guidelines	edit | Read More...
□	2	National Cyber security strategy	edit | Read More...
□	3	E-waste management guideline	edit | Read More...
□	4	National Payments Systems Act 2020	edit | Read More...
□	5	African Union Convention on Cyber security and personal data protection	edit | Read More...
□	6	United Nations Economic Commission for Africa (UNECA) Social media policy	edit | Read More...

Figure 44: System as a content provider/repository



FAQS: -All-

NO.	QUESTION	RESPONSE	DATE	ACTION
1	Where do I report a case of hacking into my WhatsApp?	Hacking into your WhatsApp is a breach of your privacy provided this was done without your consent. The Computer Emergency Response Team is a good option. You can reach them on https://www.ucc.co.ug/cert/ or Toll Free (0800133911)	2022-04-07 03:18:29	Answer
2	What is SIM Swapping?	A SIM swap lets you move your number to a replacement SIM if your old SIM is lost, stolen or damaged. It may be done by an Agent/Operator upon presentation of a valid Police letter and National ID for the case of Uganda.	2022-04-07 02:39:23	Answer
3	What is Wangiri Fraud?	In Wangiri, a fraudster gives a missed call to several victim's phone numbers of different countries from an international or unusual number. To the user, the CLI (caller number ID) is modified in such a way that it looks like a genuine call and when the victim calls back, it turns out to be a premium rate service (PRS) number owned by fraudster for which the victim is charged heavily for the calls.	2022-04-01 02:01:16	Answer

Figure 45: Frequently Asked Questions and Responses

The system manual is a walk-through guide that is available on the help menu as illustrated in figure 45. It has been compiled to enable users have a high-level view of the system functionalities namely; How to register as a user, resetting of user accounts, generating report about social media threats and crime, how to use the publication option as an e-library and how to access the awareness news as part of the social media campaigns.

SOCIAL MEDIA THREAT MANAGEMENT INFORMATION SYSTEM USER_MANUAL

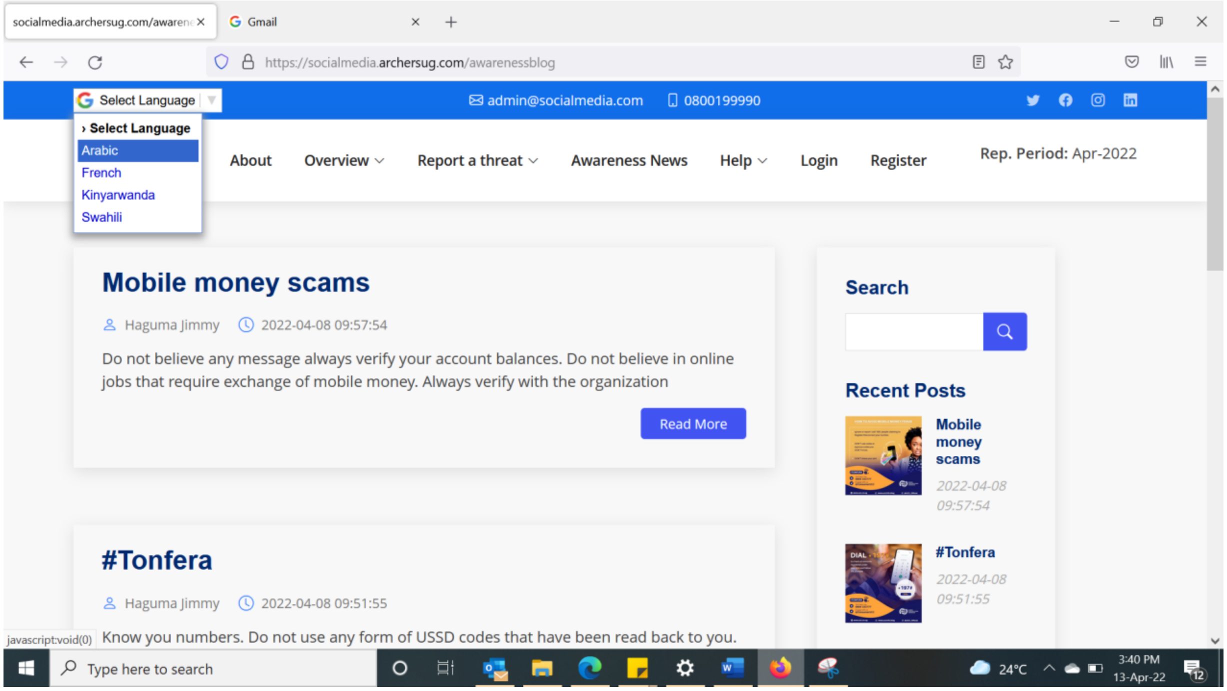
Prepared by

Jimmy Haguma

Figure 46: Snap shot of the System Manual

5.9 Using the Language translation option

The web-based system for reporting and creating awareness about social media threats and crime has been designed to provide language translation into Arabic, Swahili, French and Kinyarwanda in order to cater for different categories of people in Uganda and the diaspora as shown in the figures 47,48 and 49.



Mobile money scams

Haguma Jimmy 2022-04-08 09:57:54

Do not believe any message always verify your account balances. Do not believe in online jobs that require exchange of mobile money. Always verify with the organization

#Tonfera

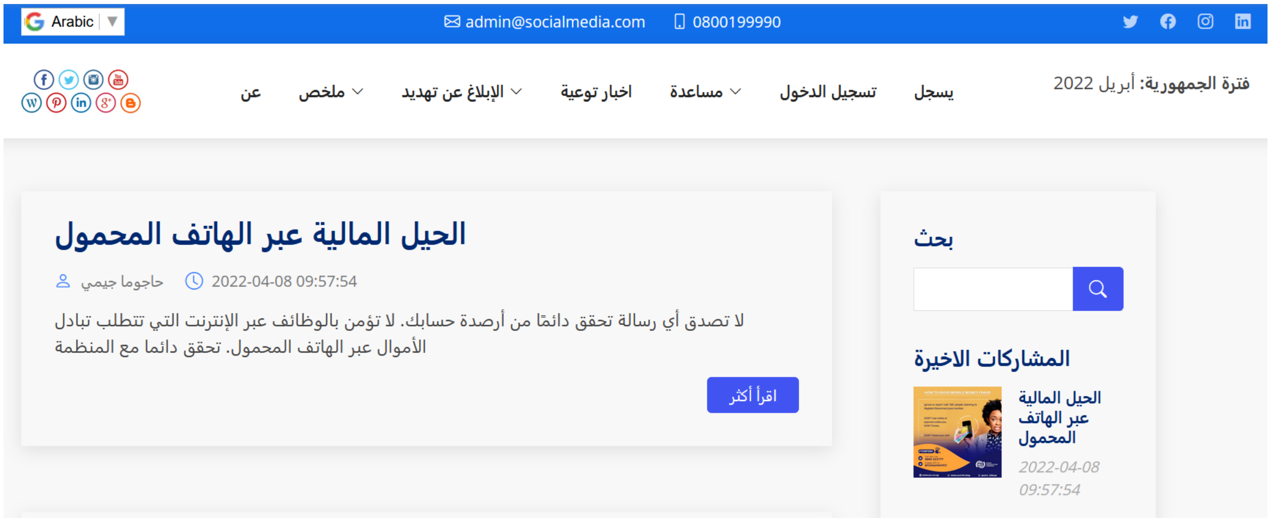
Haguma Jimmy 2022-04-08 09:51:55

Know you numbers. Do not use any form of USSD codes that have been read back to you.

Mobile money scams 2022-04-08 09:57:54

#Tonfera 2022-04-08 09:51:55

Figure 47: System Language translation Menu



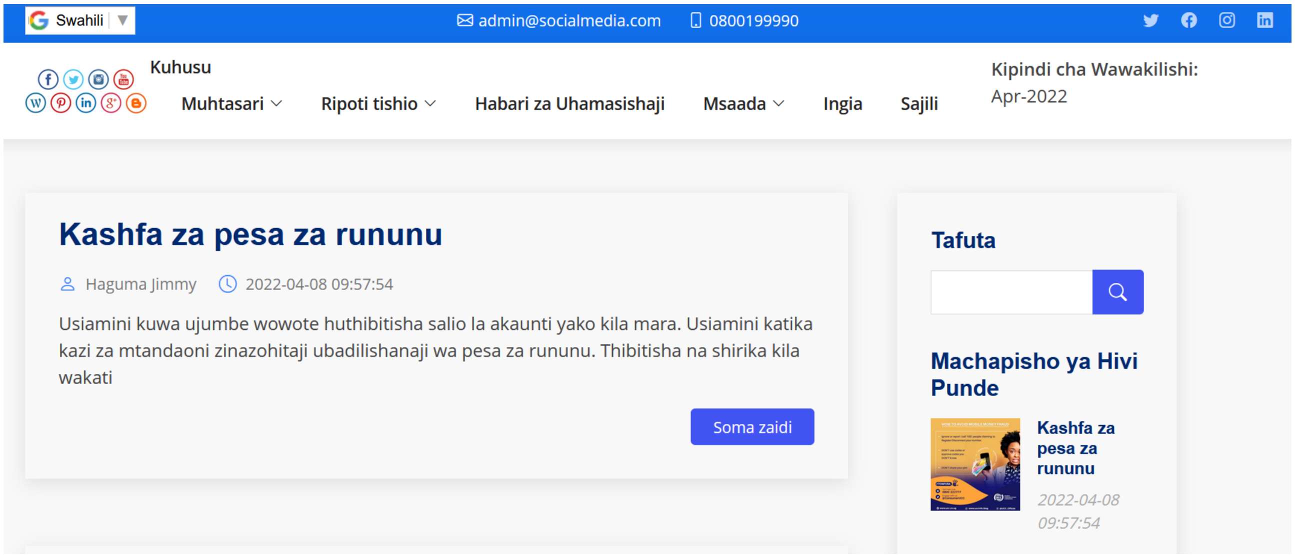
الحيل المالية عبر الهاتف المحمول

حاجوما جيمي 2022-04-08 09:57:54

لا تصدق أي رسالة تحقق دائمًا من أرصدة حسابك. لا تؤمن بالوظائف عبر الإنترنت التي تتطلب تبادل
الأموال عبر الهاتف المحمول. تحقق دائما مع المنظمة

الحيل المالية عبر الهاتف المحمول 2022-04-08 09:57:54

Figure 48: System translated into Arabic language



Kashfa za pesa za rununu

Haguma Jimmy 2022-04-08 09:57:54

Usiamini kuwa ujumbe wowote huthibitisha salio la akaunti yako kila mara. Usiamini katika kazi za mtandaoni zinazohitaji ubadilishanaji wa pesa za rununu. Thibitisha na shirika kila wakati

Figure 49: System translated into Kiswahili language

5.10 Social media threats and crime reports

Generation of social media threat and crime awareness reports is another output from the data captured in the system. The different reports are generated based on the type of threats reported, perpetration techniques, region/district where the incident occurred, period (month) when it happen/occurred as well the awareness campaigns conducted. Further analysis can be done through plotting such data to show the distribution of threats in the country on a map. This is illustrated in figure 49.

In addition, the system is able to generate a vertical bar graph for the month of April 2022, November 2022 monthly statistics of the threats so far reported and filtered statistics from January to November 2022 as illustrated in figure 50, 51 and 52 respectively.

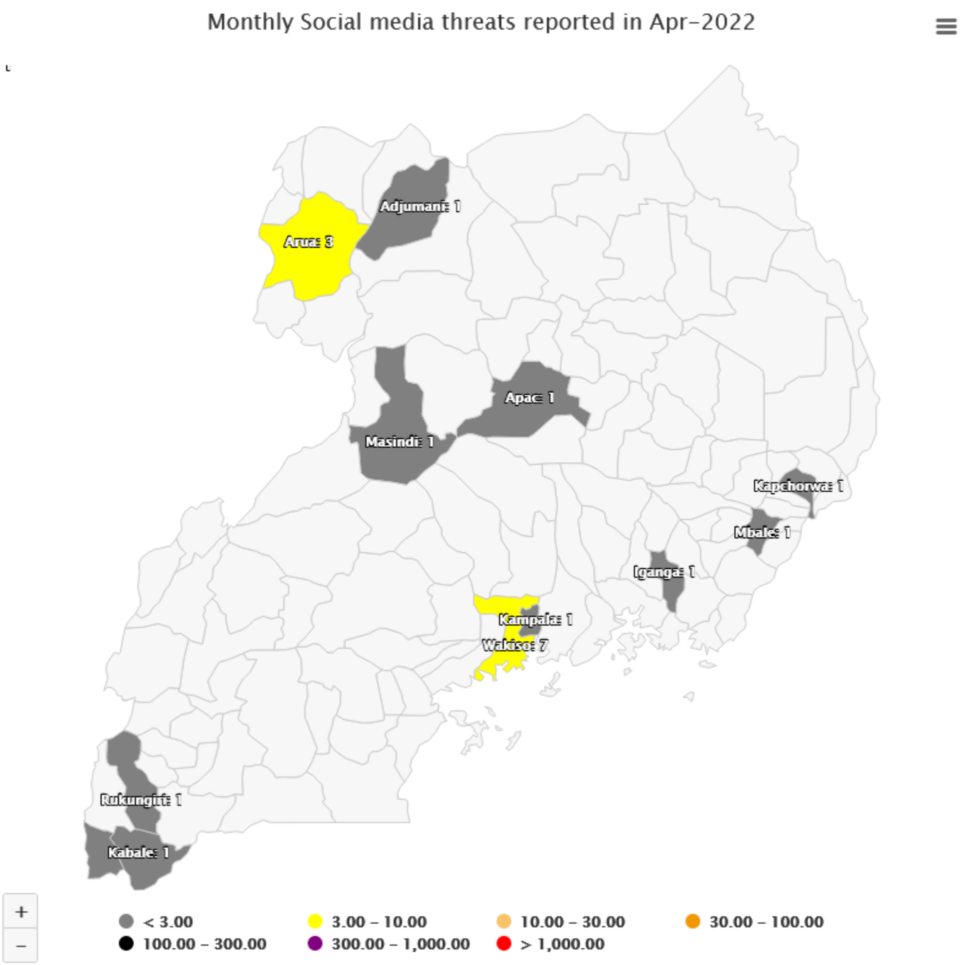


Figure 50: Social media threat and crime location map for April 2022

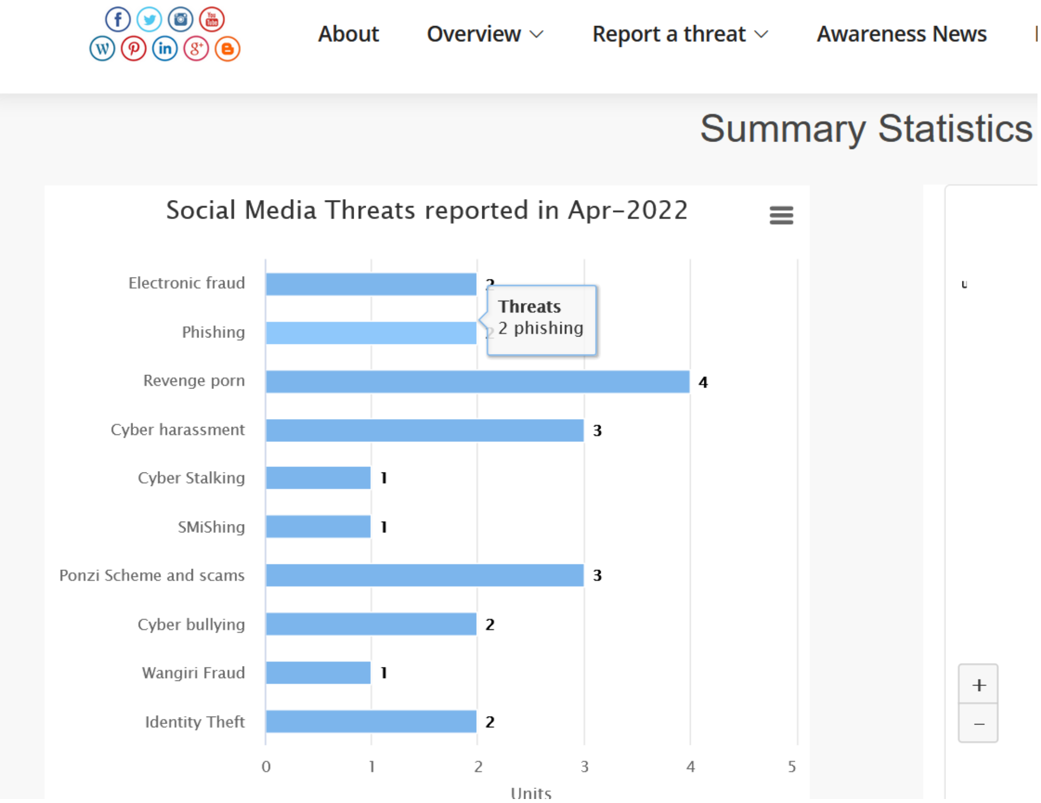
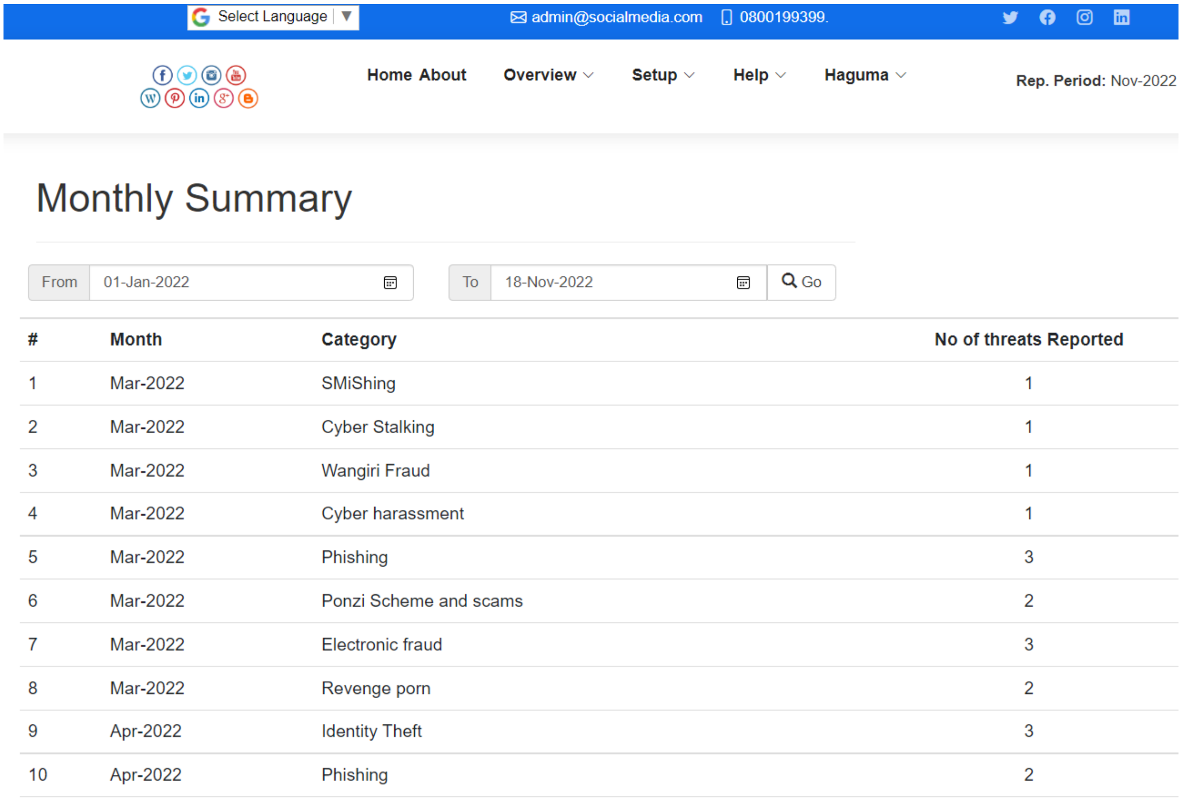


Figure 51: Vertical bar graph showing the monthly reported social media threats and crime



Rep. Period: Nov-2022

Monthly Summary

From 01-Jan-2022

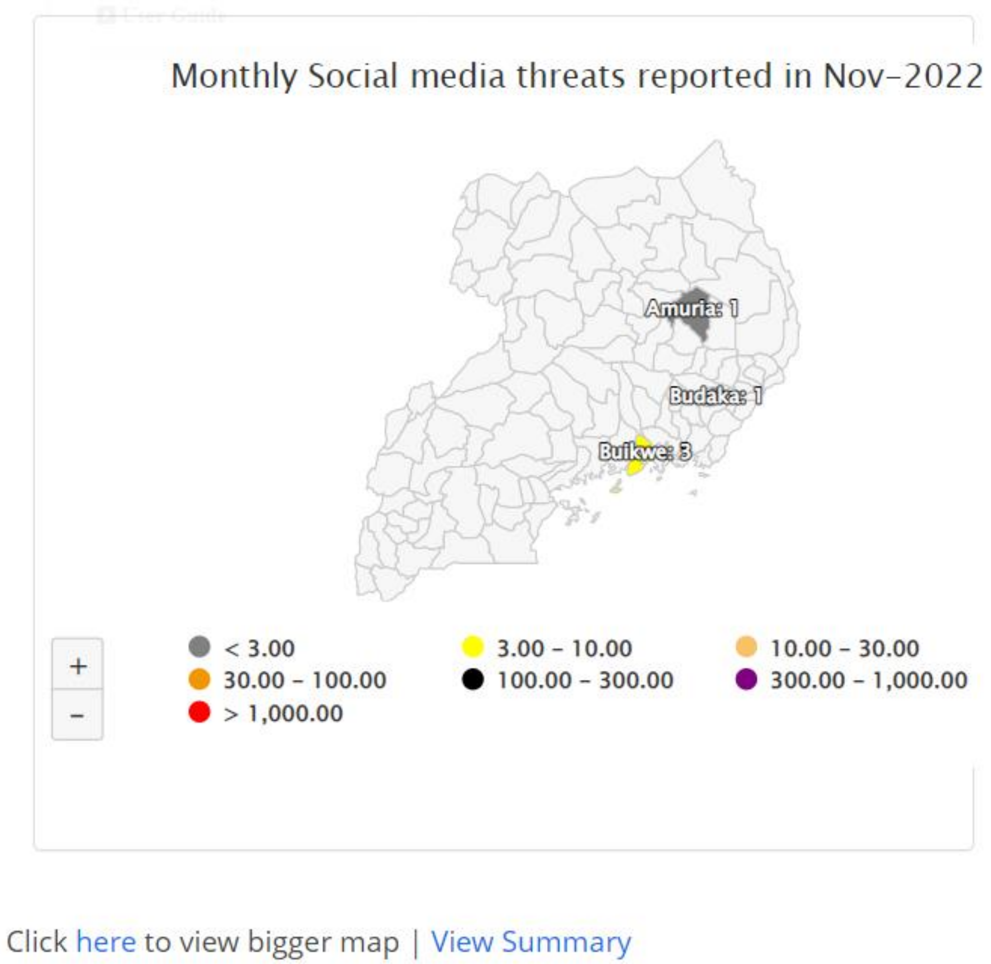
To 18-Nov-2022

#	Month	Category	No of threats Reported
1	Mar-2022	SMiShing	1
2	Mar-2022	Cyber Stalking	1
3	Mar-2022	Wangiri Fraud	1
4	Mar-2022	Cyber harassment	1
5	Mar-2022	Phishing	3
6	Mar-2022	Ponzi Scheme and scams	2
7	Mar-2022	Electronic fraud	3
8	Mar-2022	Revenge porn	2
9	Apr-2022	Identity Theft	3
10	Apr-2022	Phishing	2

Figure 52: Filtered monthly statistics from Jan - Nov 2022

5.11 Social media threat and crime map

The system automatically maps the reported incidents as per the location submitted by the users. The end product is a threat and crime map indicating the total reporting incidents as per the district monthly. This is illustrated in the figure 53



Monthly Social media threats reported in Nov-2022

Click here to view bigger map | View Summary

Figure 53: Social Media threat and Crime Map

CHAPTER SIX: SYSTEM TESTING AND VALIDATION

6.0 Introduction

This chapter presents the results obtained from the testing and validation of the web-based system for reporting and creating awareness about social media threats and crime. Participants were drawn various stakeholders namely; Law Enforcement (Uganda Police Force), Judiciary, Office of the Director of Public Prosecutions, Civil Society Organisations (CIPESA and WOUGNET), Uganda Communication Commission (UCC), National Information Technology Authority – Uganda (NITAU), Banking Sector (Housing Finance and DFCU), Education consultant – JDO Foundation (USA), Non-Governmental Organization (ARC - Allied), Business Community (Elohim Exporters), Financial Technology Services Providers Association Secretariat (FITSPA), Telecom Operators (Airtel and MTN Uganda) and University students as general users - Uganda Christian University (UCU).

The testing and validation of the system was conducted through a User Acceptance Test (UAT). A UAT is normally the last step in the software development life cycle the includes quality assurance testing of the functionalities and performance of the developed system so as to ensure that it meets the end user requirements.

This test was conducted using specific test business processes questions that were administered through an online questionnaire that was shared with a target group. This included key stakeholders like the Civil Society Organisation, Justice Law and Order Sector (JLOS), Telecom Sector, Bank and Financial Sector and the University Students. Therefore, the UAT improved on the system business processes.

The exercise was conducted using both the quantitative (google form questionnaire) and qualitative (Virtual Focus group Discussion). The exercise sought to obtain feedback on functionality, general outlook, usefulness and areas of improvement of the system.

6.1 Results from the questionnaire

The questionnaire was developed using google forms and was accessed on URL https://forms.gle/qCKDVpVn9HTYkvii9. It targeted over 30 participants and as of 17th May 2022, 22 participants had successfully submitted their feedback as enumerated.

6.1.1 Ability to report social media threats/crime without entering username and password (Anonymously)

Out of the 22 participants, 20 (91%) were able to report a social media threat anonymously which meets the system desired functionality and only 2 (9%) failed because they were not interested in using the reporting function of the system as shown by the pie-chart in figure 54.

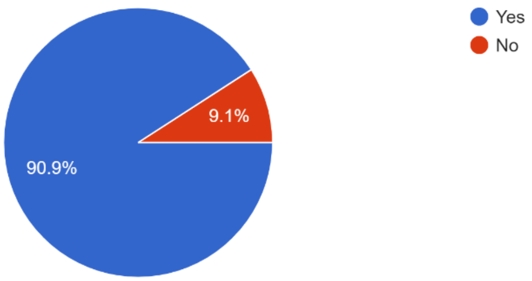


Figure 54: User reporting of social media threats and crime Anonymous.

6.1.2 Registration of users

All the 22 participants representing 100% successfully registered as users on the system.

6.1.3 Log on and reporting a threat/crime to the relevant authorities

Out of 22 participants, 19 representing 86%, were able to login and successfully report a threat and crime using their registered user accounts whereas only 3 (14%) were unable because they opted to remain anonymous. This is shown by the pie-chart in figure 55.

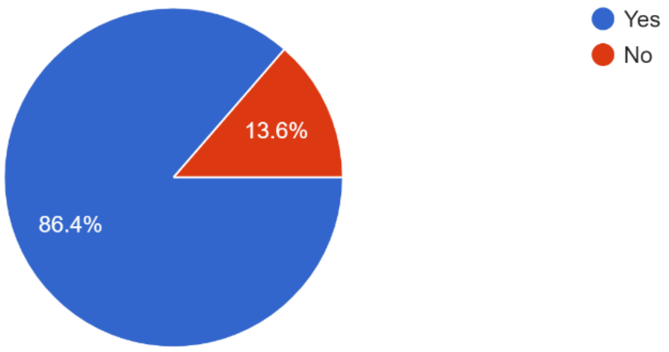


Figure 55: User login and social media threat and crime reporting

6.1.4 Ability to reset a password

Out of 22 participants that tested the system, 18 participants, representing 86% successfully reset their account passwords and were able to access the system. Only 4 failed which denotes 14% and this was due to the use of email addresses that they had also forgot their passwords and thus code not access the reset link as illustrated by the pie-chart in figure 56.

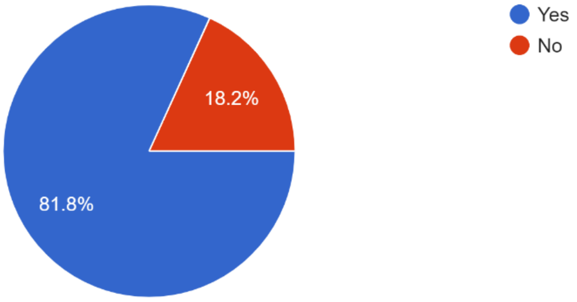


Figure 56: Password reset functionality

6.1.5 Ability for users to view published awareness news

Out of the 22 participants, 21 (96%) were able to view published awareness news while 01 (1%) failed to view it. This is shown by the pie chart in figure 57.

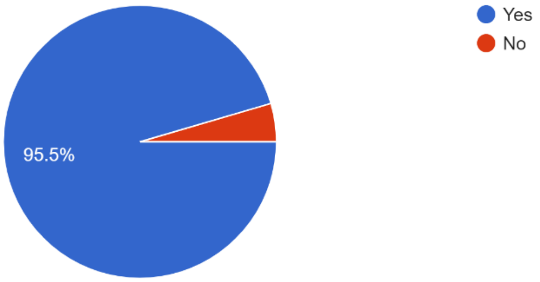


Figure 57: User access to published security awareness news

6.1.6 Ability to access security guidelines/tips for basic or general social media users

Out of 22 participants, 21 (96%) were able to view the security guideline/tips and awareness news compared to only 1 (4%) that were did not succeed as illustrated in figure 58.

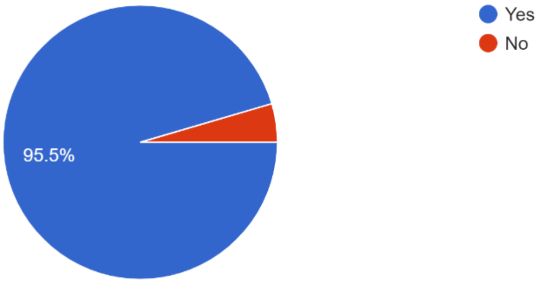


Figure 58: Security guidelines/tips or awareness news

6.1.7 Ability to tell the locations/districts where threats and crimes have been reported

All the 22 participants were able to tell all the location/districts on the social media threat and crime map as shown in the figure 59.

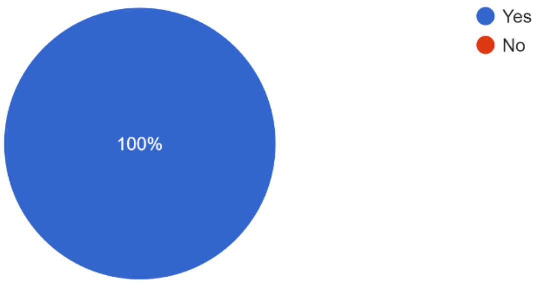


Figure 59: Social media threat and crime map

6.1.8 Ability to use a different language to read the content on the system

14 participants representing 64% were able to use the different language navigation tool on the system whereas 8 (36%) could not use or find it as illustrated in figure 60.

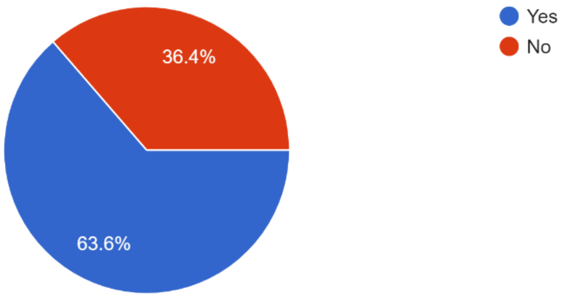


Figure 60: Language translation functionality

6.1.9 Getting feedback upon lodging of complaints

Out of the 22 respondents, 13 (59%) were able to get feedback upon reporting of a complaint because they were able to provide feedback email whereas 9 (41%) did not receive any feedback as shown in figure 61.

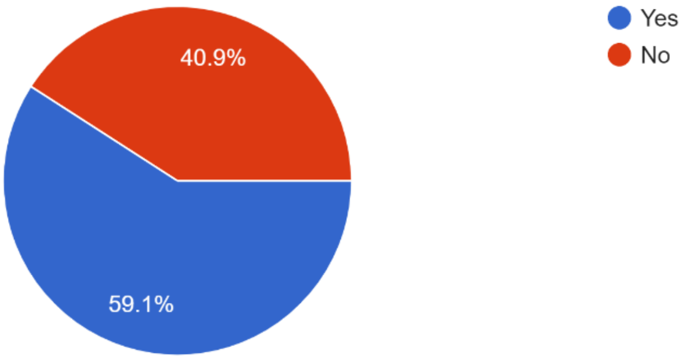


Figure 61: Feedback assessment from the system

6.1.10 Ability to generate social media incident reports

Out of 22, 17 (77%) respondents successfully generated social media incident reports whereas 5 (23%) could not as illustrated by the pie-chart in figure 62.

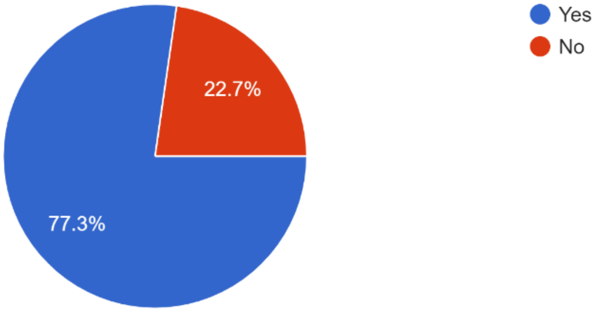


Figure 62: Generation of social media incident reports

6.1.11 Testing the usefulness of the system

Out of the 22 respondents, the system was found to be very useful by 14 respondents representing 64%, 3 respondents (14%) found the system to answer all their requirements, 4 participants (18%) found the system to be at average usefulness and 1 respondent (5%) found to the system to some extent useful. This is illustrated by the bar-graph in figure 63

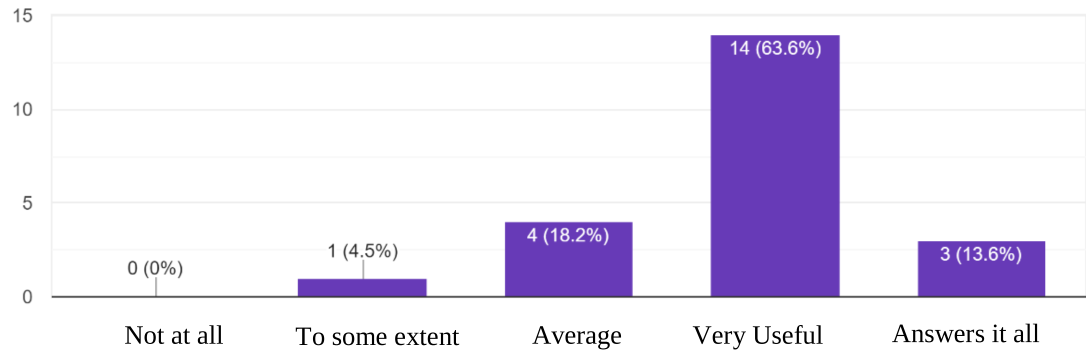


Figure 63: System rate of usefulness

6.1.12 Testing the ease of use and response time of the system

In terms of ease of use and response time, out of the 22 respondents, the system was rated as excellent by 8 respondents (36%) compared to Good by 7 respondents (32%) and Very Good by 7 respondents (32%) as illustrated by the bar-graph in figure 64.

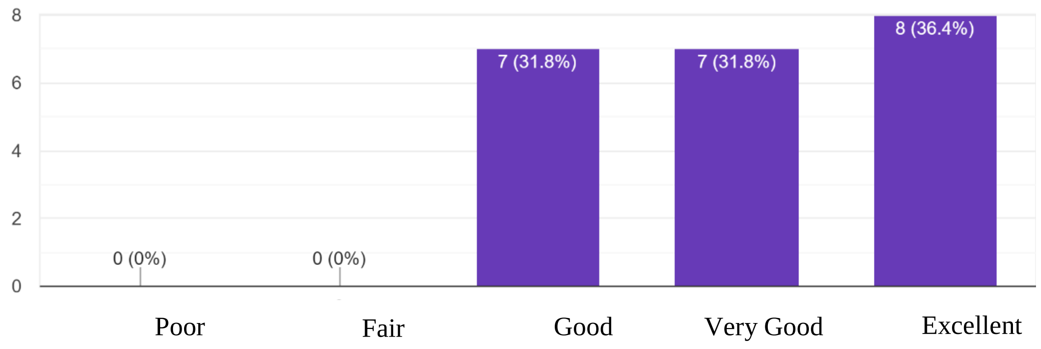


Figure 64: The rate of ease of use and response time

6.1.13 Testing the content value of the system

In terms of content on the platform, the system was rated as very good to the users by 10 respondents (46%), Excellent content by 7 respondents (32%), Good by 4 respondents (18%) and Fair by 1 respondent (5%). This is illustrated by the bar-graph in figure 65.

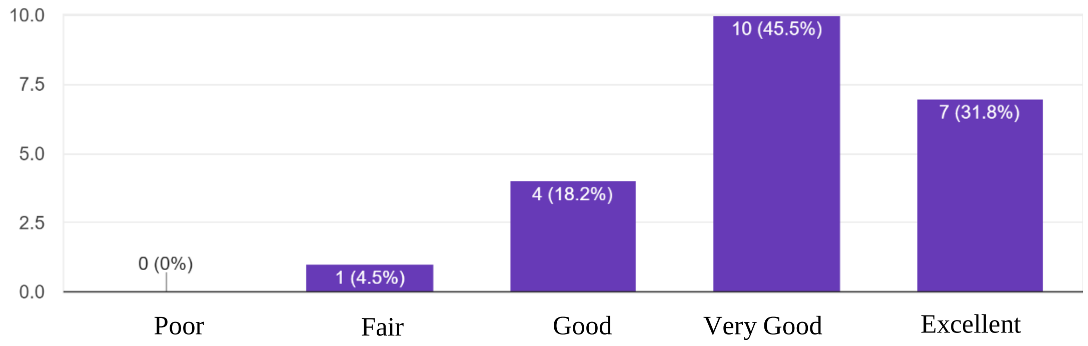


Figure 65: Testing the content of the system

6.2 Results from the Focus Group Discussion

The Focus Group Discussion was held on the 11th of May 2022 and it attracted 10 participants that were drawn from various stakeholders namely: FITSPA (Financial Technology Service Providers Association), Banking (DFCU), Civil Society Organisation (CIPESA and WOUGNET), Uganda Police Force – Investigations & Training Directorates, Students – Uganda Christian University (Mukono Campus), Medical sector (AAR) and the Business Community (Sunrise Investment Club). The meeting provided general feedback about the platform and its purpose as enumerated;

a) The participants underscored the fact that the solution is useful, provides timely feedback and is easy to use. For example, the participant from WOUGNET said, "this is timely, as an organisation we have been doing research on the effects and challenges of none-consensual sharing of intimate images among women."

b) Participants from the Bank sector and Financial Information Technology Service Providers Association (FITSPA) noted that the Innovation is highly relevant because there is an increased wave of in the number of social media threats and crimes in particular to the financial sector. Mrs Zianah Muddu, from the secretariat of FITSPA said, "the greatest weakness is users that are not informed about the tricks and methods that fraudsters are using. I love the fact that you have created awareness news. We shall gladly share content with you."

c) The students and business community applauded the fact that the system makes data collection, analysis and report generation very simple since it provides real time statistical information.

d) All the participants concurred with the opportunity to report social media threats and crime online, which is an aspect that creates room for timely reporting of the incidences compared to going to a typical police station to lodge a complaint.

e) All the participants observed that the system was interactive thus creating user satisfaction. For example, the FAQ section that allows users to also ask questions and get responses that form an information bank for all users.

f) The participants from the Uganda Police and Banking sector noted that the system is very good and timely due the growing incidences of social media crimes. The electronic aspect makes it perfect to also include victims in the different parts of the world.

g) All the participants appreciated the fact that the system creates awareness to the masses through the news published on the platform. Majority of people fall victims because they lack information about the problem at hand.

h) The participants shared the following views about the improvement of the system as represented in the table

Table 11: Feedback from the Focus Group Discussion and suggested improvements.

S/N	PROPOSED AREAS OF IMPROVEMENT AS FEEDBACK
1.	Change the theme color to ease navigations
2.	Add more graphics such as multimedia for illustrations that can depict what message is being communicated.
3.	Validate all the forms to minimize blank data entries
4.	System should be integrated with feature/basic phones
5.	More information needs to be included such as the freedom and rights of victims
6.	More crime options should be created which include others to be specified by the

S/N	PROPOSED AREAS OF IMPROVEMENT AS FEEDBACK
	user.
7.	Specifications of registration should be clear whether to new emails or current emails?
8.	Both the page for registration and password reset return a fresh page for that item even if you have finished the business of that page. It can confuse a user that what they just done (register or reset password) may have not work, even if a completion message is displayed.
9.	The buttons on the 'Report a threat' page ('Read' and 'Edit') merge into each other
10.	Change the word guidelines under HELP menu to publications.
11.	Fraud cases should be given immediate attention before victims lose lots of money.
12.	Safety and security tips should feature more prominently on the home page alongside the summary statistics
13.	Incorporate Luganda among the language options since it is a widely spoken.
14.	Include helplines in case someone needs real time support
15.	After registration the system should go to the login page NOT registration again with a login link which is hidden almost.
16.	Include social media threats and crime monthly statistical filter option
17.	Provide a telephone number as another option for reporting feedback to the user.
18.	Increase the number of centers to receive the complaint. For example, Financial Intelligence Authority and others
19.	Include the purpose of the system, target area, objectives and possible outcomes.
20.	While reporting a threat, the user should be able to classify the incident in order of priority. For example; a. Emergency b. High priority c. Normal
21.	Display all the menus with icons without sub menus
22.	Integrate the system with social media platforms such as Facebook and Twitter.
23.	Incorporate a feedback option from the users about their experience with the system
24.	Include a fact checker link for users to verify online content. *This can be done by benchmarking the use of Uganda Communications Commission Fact Checker tool.*
25.	Improve on the background of the map to make it conspicuous

6.3 Suggested improvements and status of implementation

Following the testing and validation exercise that was performed using both the questionnaire and Focus group Discussion, find the summary of suggested improvements and the status of implementing matrix.

Table 12: Validation analysis matrix of the test results

S/N	PROPOSED AREAS OF IMPROVEMENT AS FEEDBACK	STATUS/COMMENT
1.	Change the theme color to ease navigations, display all the menus with icons without sub menus and Improve on the background of the map to make it conspicuous	Completed
2.	Validate all the forms to minimize blank data entries	Done
3.	System should be integrated with feature/basic phones	This is for future implementation by using USSD codes
4.	More information needs to be included such as the freedom and rights of victims	Noted for Change
5.	More crime options should be created which include others to be specified by the user.	Done
6.	Specifications of registration should be clear whether to new emails or current emails?	Resolved. This should be for email where the user has access in order to retrieve the system feedback
7.	The buttons on the 'Report a threat' page ('Read' and 'Edit') merge into each other	Resolved
8.	Change the word guidelines under HELP menu to publications.	Resolved
9.	Fraud cases should be given immediate attention before victims lose lots of money.	This is honest feedback but may not be actionable here.
10.	Safety and security tips should feature more prominently on the home page alongside the summary statistics	Noted for Change
11.	Incorporate Luganda among the language options since it is a widely spoken.	Done
12.	Include helplines in case someone needs real time support	Done
13.	After registration the system should go to the login page NOT registration again with a login link which is hidden almost.	Done

S/N	PROPOSED AREAS OF IMPROVEMENT AS FEEDBACK	STATUS/COMMENT
14.	Include social media threats and crime monthly statistical filter option	Done
15.	Provide telephone number as another option for reporting feedback to the user.	Has been resolved
16.	Increase the number of centers to receive the complaint. For example, Financial Intelligence Authority and others	Done
17.	Include the purpose of the system, target area, objectives and possible outcomes.	Noted for inclusion
18.	While reporting a threat, the user should be able to classify the incident in order of priority. For example; d. Emergency e. High priority f. Normal	Noted for future consideration
19.	Integrate the system with social media platforms such as Facebook and Twitter.	Noted for future consideration
20.	Incorporate a feedback option from the users about their experience with the system	Noted for further consideration
21.	Include a fact checker link for users to verify online content. *This can be done by benchmarking the use of Uganda Communications Commission Fact Checker tool.*	Noted for further consideration

CHAPTER SEVEN: CONCLUSION, RECOMMENDATIONS, AND FUTURE WORK

7.0 Conclusion

The web-based system for reporting and creating awareness about social media threats and crime was developed as an ideal solution for reporting of social media threats and crime by the general public to different actors namely: Uganda Police Force, ICT Regulators, FINTECH Companies, Civil Society Organisations, Judiciary, Office of the Director of Public Prosecution, Telecom Service Providers, Internet Service Providers and the Business Community. It is also an enabler for tracking of social media related threats and concentration of those crimes per location in Uganda.

Therefore, the voluntary reporting of such social media threats and crime incidences, makes it one of the content providers for awareness about social media threats and crime, and will definitely influence decision making in terms of resource deployment in various fronts in the fight against such crimes in Uganda.

7.1 Recommendations

This section integrates the recommendations generated from the Questionnaire and Focus Group Discussion during testing and validation. These include;

a) The system should be accommodative to people using feature phones since at the moment it is limited to smart devices only. This can be achieved through the use of Unstructured Supplementary Service Data (USSD) codes.

b) Electronic Fraud cases should be given immediate attention before victims lose lots of money. This calls for integration of the platform with the telecom operator mobile money complaints solutions to enable timely and effective response to registered complainants.

c) The system needs to be integrated with a fact checker link for users to verify authenticity or correctness of online posts. Reference can be given to the Uganda Communications Commission Consumer Affairs Fact Checking process initiative using https://consumer.ucc.co.ug/faqs/

d) The line MDAs and Civil Society Organizations that advocate for social justice need to support the initiative to achieve the desired end state of social media awareness as a preventive mechanism to fight against social media threats and crime in Uganda.

e) The Uganda Police Force and general public need to adopt the use of the web-based system for reporting and creating awareness about social media threats and crime which will help in dissemination of information about social media threats and crime in the region and will help to facilitate investigation and prosecution.

7.2 Future work

The system has been developed as a prototype and has demonstrated benefits to the Justice Law and Order Sector, FINTECH Community, General users, Telecom Service Providers and Education/Academia. This section therefore, details some of the possible future work for the improvement of the system.

a) The system will need to adopt and adapt to the use of Unstructured Supplementary Service Data (USSD) codes for users that have basic phones, and are at risk of telecommunication related threats and crime.

b) Integration of the system with other complaint handling systems, such the Consumer Protection system and the Fact Checker Platforms for misinformation and disinformation at the Uganda Communications Commission and the Telecom Service Providers will be an extra bonus.

c) In order achieve the comprehensive reporting and adequate feedback for the system, it will be prudent to set up a team of social media investigators and field response teams that should follow up the complainants submitted and bring the suspects to book in accordance with the Computer Misuse Act of 2022 and other related laws of Uganda.

d) For effective roll out of the system, it will importance to create partnerships at multistakeholder level. This will include the social justice practitioners and advocates with the Civil Society space in Uganda and other development partners. The roll out shall be two-fold namely: Mass sensitization through print and audio-visual media channels as well as supporting or enabling tools such as computers/laptops with access to interest as criminal justice centers and place of learning for users to use the systems.

8.0 ANNEXURE

8.1 Annex A:

FOCUS GROUP DISCUSSION TOOL FOR WEB-BASED SYSTEM FOR REPORTING AND CREATING AWARENESS ABOUT SOCIAL MEDIA THREATS AND CRIME IN UGANDA

Objective of the study: *To develop a web-based system for reporting and creating awareness about social media threats and crime in Uganda.*

PREAMBLE

The total number of social media users worldwide is now projected to reach 3.6 billion by 2021 (Clement, 2020). The dramatic rise in use of social media sites such as Facebook, Twitter and YouTube in the last decade has also led to a marked increase in criminal activities and offences on such interactive spaces (InfoSec, 2020). Social media crimes include; spamming, social engineering, ransomware, phishing attacks, extortion, perpetration of kidnaps, rape, murder, suicide and electronic fraud (Soomro, 2019). However, social media crimes cannot be sufficiently investigated using traditional case management approaches, because the scene of social media crime is often virtual or borderless since all or part of the transaction occurs on the online community space in multiple jurisdictions and the offenders at times use anonymous identities which often makes it difficult for law enforcement to verify (Abdalla, 2014).

This coupled with the cost expenditure in-terms of investigative resources (Piest, Gramatikov, & Muller, 2016) in storing and processing of huge personal data as well as the digital forensic techniques employed to achieve results (Patton, 2017) makes the social media investigation cumbersome. Furthermore, the geo-politics of big data owners may make it difficult for the Justice Law and Order Sectors in individual States to administer Justice in cases of breach by the social media platforms (Kurbalija, 2017). Therefore, there is great need for a web-based system for reporting and creating awareness about social media threats and crime in Uganda.

The objective of this discussion is to enlist the following from the respondents;

(i) Collect requirements for a web-based system for reporting and creating awareness about social media threats and crime in Uganda.

(ii) Develop a web-based system for reporting and creating awareness about social media threats and crime in Uganda.

FOCUS GROUP DISCUSSION QUESTIONS

Participants introduce themselves at the beginning/Self introduction covering name, organization, position

1. What do you know about social media exploitation and crime?
2. What are the various forms of social media crimes that you know?
3. Please briefly share your experience if you or someone you know has ever been a victim of social media misinformation or crime (*do not mention name*) and how the issue was handled?
4. Uganda assented to the cyber laws in 2010 and the Data Protection and Privacy law in 2019. How is your organization/company using them in the fight against social media crime?
5. In 2015, Uganda launched the Uganda Computer Emergency Response Team, UG-CERT. What does this group do?
6. How was your experience when you reported any social media related fraud or breach of trust to law enforcement or any concerned organization?
7. What are some of the methods that have been used to disseminate information about how to remain safe while using social media applications?
8. What role is the Uganda Police Force playing in terms of handling and dealing with social media fraud?
9. If you are to report any form of social media fraud, would you prefer to be anonymous or otherwise? If so, why?
10. How is social media crime managed by;
    - Your organization and
    - Law enforcement agencies
11. What are you views about developing of an Information System that can create awareness on social media threats and crime?
12. What functionalities and outputs would you like to be included as part of the information system mentioned in question?

INFORMATION OF INTEREST FROM STAKEHOLDERS

SN	INSTITUTION	INFORMATION OF INTERNET
1.	Civil Society Organization a. CIPESA b. WOUGNET	(i) Understanding social media threats, crime and the efforts to fight it. (ii) The functionalities and outputs of the proposed system. (iii) Strategies of disseminating information about social media threats and crimes
2.	Law Enforcement a. UPF	(i) Understanding the legal provision about social media crimes (ii) Appreciating the capabilities of the investigation mechanisms (iii) Acquaint the meeting about the technical competences of the human resources to handle social media crimes
3.	ICT Regulators a. NITAU b. UCC	(i) Appreciate the regulatory framework in place to address social media crimes (ii) Collect views on the functionalities and outputs of the proposed systems (iii) Acquaint the meeting with the future prospects of dealing with the social media threats and crime
4.	Prosecution a. DPP	(i) Appreciate the prosecution mechanisms in place to fight social media crime (ii) Appreciate the technical capabilities of the prosecution sector in handling such crimes. (iii) Collect information about the functionalities and outputs of the proposed system
5.	Telecom Sector	(i) Appreciate the extent social media threats and crime

	a. MTN b. Airtel	to the sector (ii) Acquaint the meeting with the efforts in place to fight the crime (iii) Collect information about the functionalities and outputs of the proposed system
6.	Finance, Planning and Economic Development a. MoFPED	(i) Understand the role of the sector in the fight against social media crimes (ii) Collect information about the functionalities and outputs of the proposed system
7.	Business Community a. Exporters	(i) Obtain views about the extent of social media threats and crimes (ii) Collect insights into the business risks posed by social media threats and crimes (iii) Collect information about the functionalities and outputs of the proposed system

8.2 Annex B:

WEB-BASED SYSTEM FOR REPORTING AND CREATING AWARENESS ABOUT SOCIAL MEDIA THREATS AND CRIME QUESTIONNAIRE

A: General Information

1. Name
2. Age
3. Contact
4. Organization
5. What is your age group?
   a. 18-25
   b. 25-35
   c. 35-55
   d. 55 and
6. What is your profession?
   a. Security
   b. Law enforcement
   c. ICT
   d. Engineering
   e. Banking
   f. Education
   g. Advocacy
   h. Business
   i. Medical
   j. Civil Society
   k. Others (*Please specify*)
7. Do you use social media platforms? Yes/No

8. If yes, how much time to you spend daily on social media
   a. More than 10 hours
   b. Between 10 -5 hours

c. Between 5- 3 hours
d. Between 2 -1 hour
e. Only 30 mins

9. Rate your preferred social media platform? (On a scale of 1-5)
   a. Facebook
   b. Twitter
   c. WhatsApp
   d. Instagram
   e. LinkedIn
10. Have you ever used the security options available on these platforms? Yes/No

11. If yes, what actions did you perform

    a. Protect my identity
    b. Protect my location
    c. Report scam
    d. Set up two factor authentications (2FA)
12. Have you ever been a victim of any form of social media threat or crime? Yes/No
13. If so, what type? *(You can tick as many as you wish)*
    a. Cyber stalking
    b. Cyber harassment
    c. Revenge porn
    d. Electronic fraud
    e. Identity theft
    f. Offensive communication
    g. Phishing
    h. Vishing/SMiShing
    i. Others *(Please specify)*

B: Social media threat reporting and crime awareness

14. Are you familiar with social media threats and crime?

15. Do you know of any form of social media threat reporting and crime awareness methods? (Specify please)
16. How do you rate the rate the current methods by the different agencies? (use scale of 1-5
    a. Uganda Police Force
    b. Uganda Communications Commission
    c. National Information Technology Authority
    d. Ministry of ICT & NG
17. Have you ever reported by social media threat or crime? Yes/No
18. If yes, how can you rate the perform or services you received? (Scale of 1-5)
    a. Uganda Police Force
    b. Uganda Communications Commission
    c. National Information Technology Authority
    d. Ministry of ICT & NG

19. How much loss did you incur as a result of the threat or crime?
    a. More than 1M
    b. Between 1M to 500k
    c. Between 500k to 200k
    d. Less than 100k
    e. No money
20. What were some of the resultant effects as result of the threat or crime?
    a. Loss of a job
    b. Breach of my privacy
    c. Threats to life
    d. Loss of funds
    e. Victimization

C: Social media regulations

21. Do you know of any national laws that regulate social media?
22. Does your organization have social media policies and regulations?
23. How often do you receive information security tips?

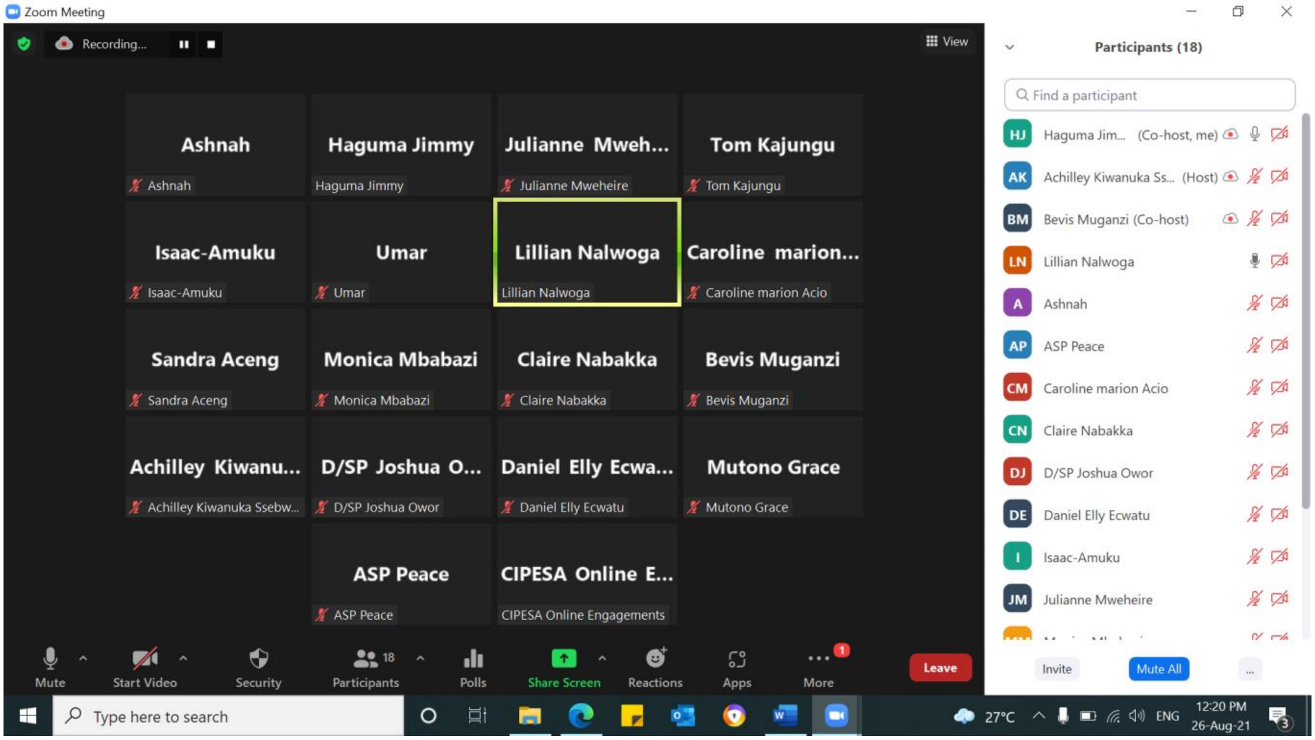
a. Every day
b. Once a week
c. Once a month
d. Once in a year
e. Never

D: Web-based system for reporting and creating awareness about social media threats and crime

24. As a planned or target user of the social media system, please score the system requirements that you desire for the solution. What is your view about the services to be provided by the social media awareness and threat reporting system?

8.3 Annex C:

VIRTUAL (ZOOM MEETING) FOCUS GROUP DISCUSSION ATTENDANCE



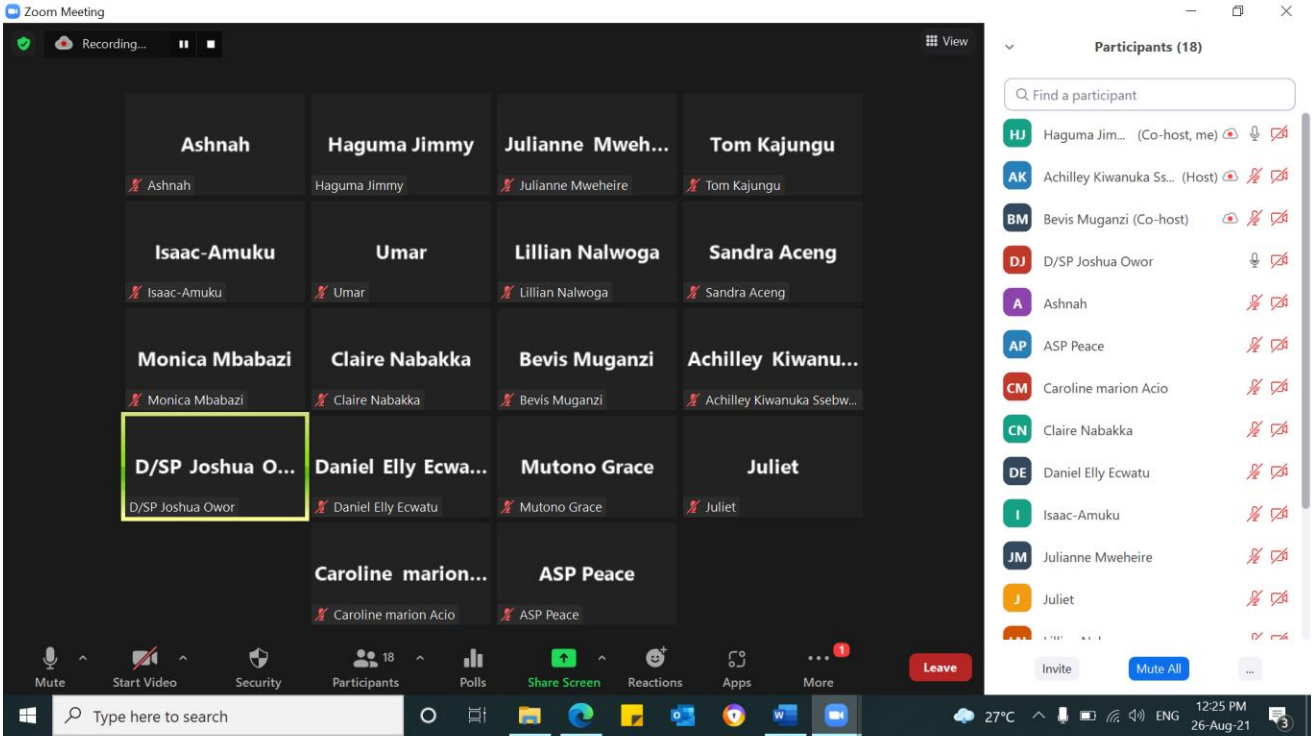
Zoom Meeting

Ashnah | Haguma Jimmy | Julianne Mweheire | Tom Kajungu
Isaac-Amuku | Umar | Lillian Nalwoga | Caroline marion Acio
Sandra Aceng | Monica Mbabazi | Claire Nabakka | Bevis Muganzi
Achilley Kiwanuka Ssebw... | D/SP Joshua Owor | Daniel Elly Ecwatu | Mutono Grace
ASP Peace | CIPESA Online Engagements

Participants (18)

- Haguma Jim... (Co-host, me)
- Achilley Kiwanuka Ss... (Host)
- Bevis Muganzi (Co-host)
- Lillian Nalwoga
- Ashnah
- ASP Peace
- Caroline marion Acio
- Claire Nabakka
- D/SP Joshua Owor
- Daniel Elly Ecwatu
- Isaac-Amuku
- Julianne Mweheire

12:20 PM 26-Aug-21



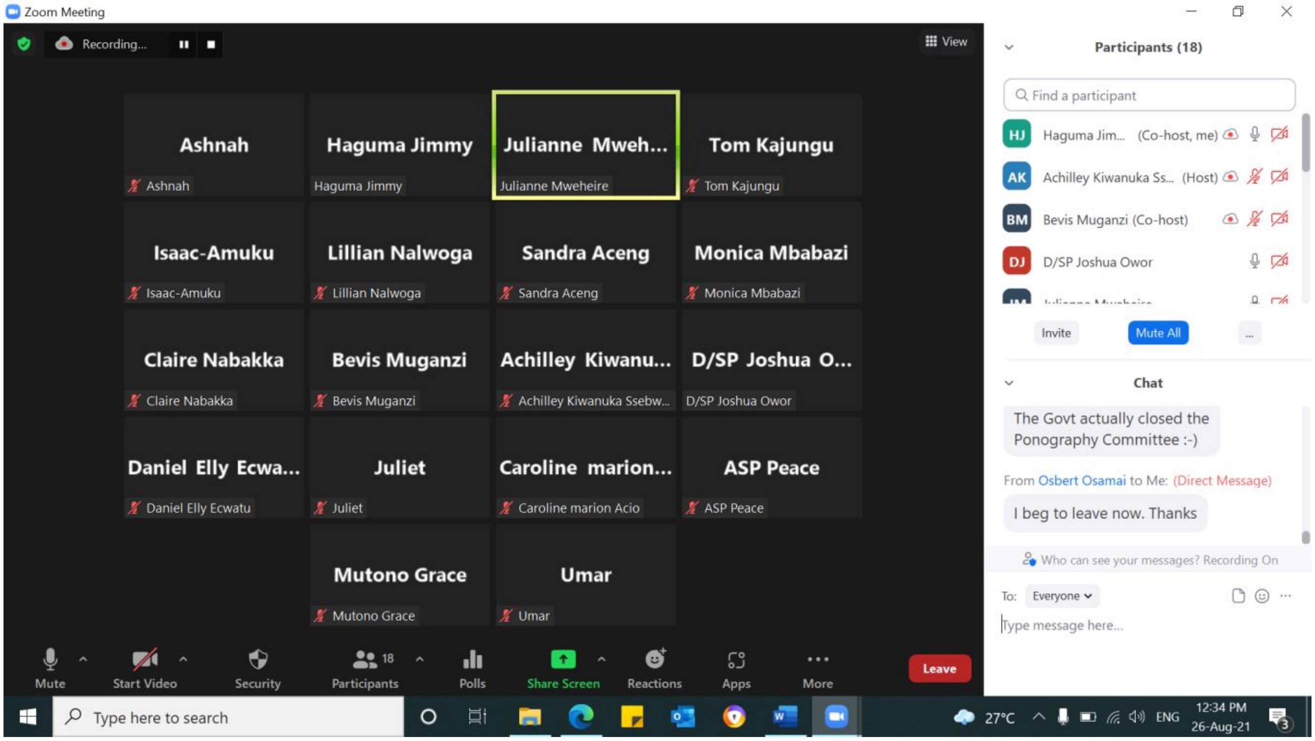
Zoom Meeting

Ashnah | Haguma Jimmy | Julianne Mweheire | Tom Kajungu
Isaac-Amuku | Umar | Lillian Nalwoga | Sandra Aceng
Monica Mbabazi | Claire Nabakka | Bevis Muganzi | Achilley Kiwanuka Ssebw...
D/SP Joshua Owor | Daniel Elly Ecwatu | Mutono Grace | Juliet
Caroline marion Acio | ASP Peace

Participants (18)

- Haguma Jim... (Co-host, me)
- Achilley Kiwanuka Ss... (Host)
- Bevis Muganzi (Co-host)
- D/SP Joshua Owor
- Ashnah
- ASP Peace
- Caroline marion Acio
- Claire Nabakka
- Daniel Elly Ecwatu
- Isaac-Amuku
- Julianne Mweheire
- Juliet

12:25 PM 26-Aug-21



The Govt actually closed the Ponography Committee :-)

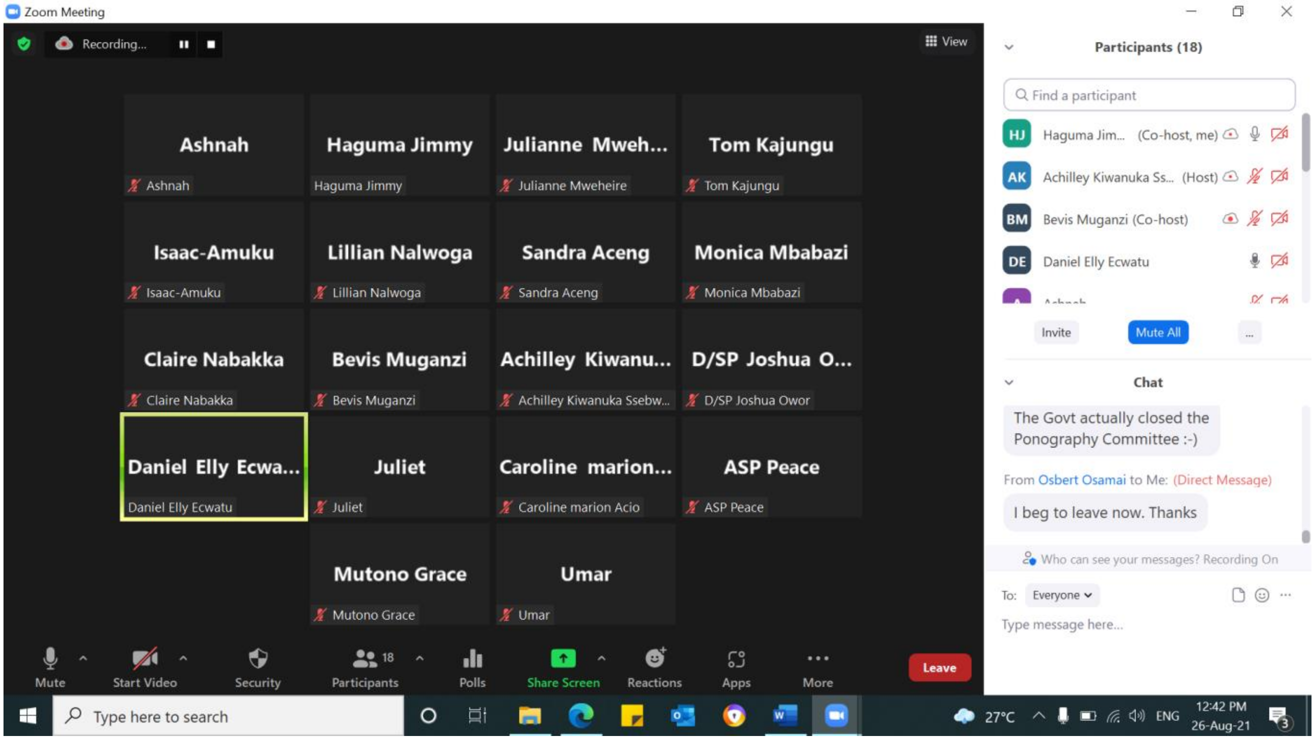
From Osbert Osamai to Me: (Direct Message)

I beg to leave now. Thanks

Who can see your messages? Recording On

To: Everyone

Type message here...



The Govt actually closed the Ponography Committee :-)

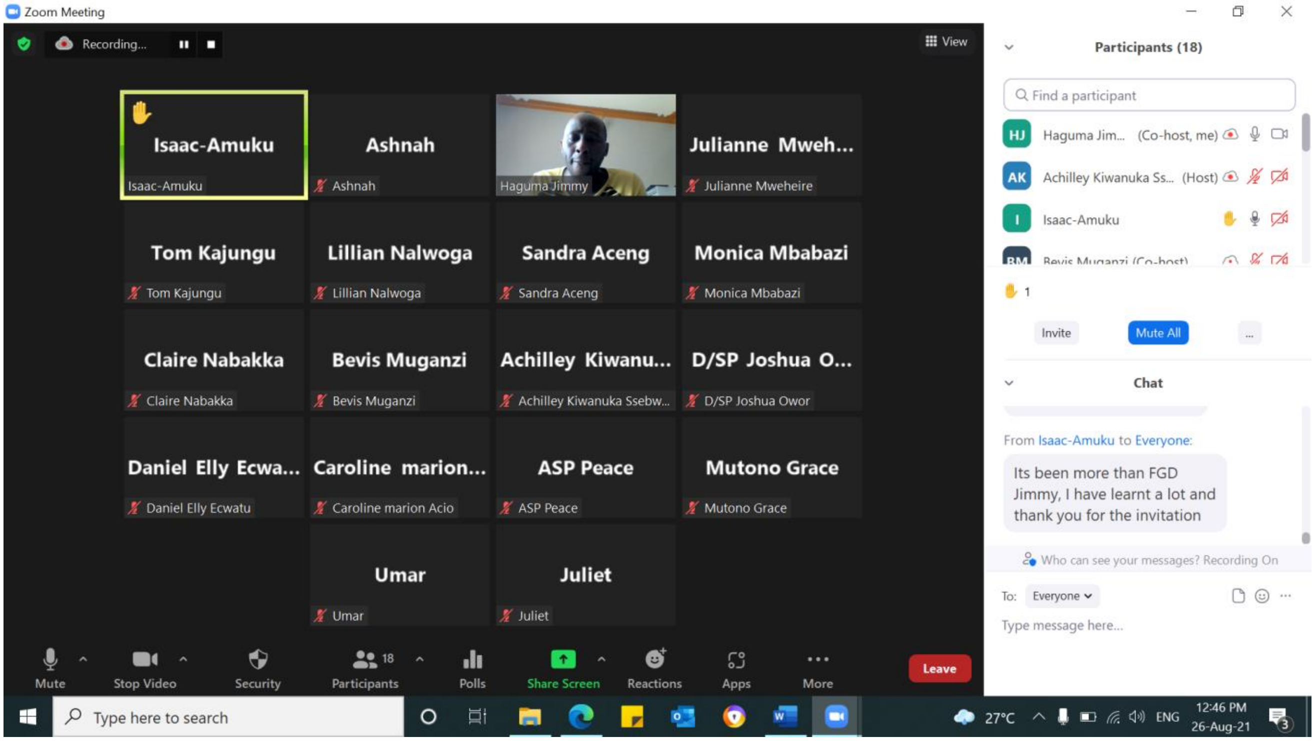
From Osbert Osamai to Me: (Direct Message)

I beg to leave now. Thanks

Who can see your messages? Recording On

To: Everyone

Type message here...



From Isaac-Amuku to Everyone:

Its been more than FGD Jimmy, I have learnt a lot and thank you for the invitation

Figure 66: Virtual Focus Group Discussion Sessions

8.4 Annex D

QUESTIONNAIRE FOR TESTING AND VALIDATION OF WEB-BASED SYSTEM FOR SOCIAL MEDIA THREAT REPORTING AND CRIME AWARENESS

PREAMBLE

Dear Respondent;

The advent of social media has created faster means of information sharing such as microblogging which in turn has massively changed the communication landscape. Government agencies and Civil Society Organizations in Uganda and the diaspora have resorted to the use social media platforms such as Facebook and Twitter in a bid to engage with the public in an efficient and cost-effective manner.

However, this advancement has brought a dramatic shift from what it means to ‘chat’ and ‘socialize’ with other people to a whole range of social media threats and crimes. These include but are not limited to offensive communication, cyber stalking, phishing, non-consensual sharing of intimate images, identity thefts, spreading of fake/false news to electronic fraud.

The perpetrators of such crime, often exploit the gaps in technology design and the deficiencies or low levels of awareness about social media security principles and practices among users. This coupled with being technologically advanced and the prolific market for new tools, acts as an enabler for them to stay ahead of law enforcement agencies.

It is against this background, that a web-based platform for threat reporting and crime awareness has been developed, in order to endeavor to address the gaps in criminal investigations, and accelerate the awareness drive on social media safety and security.

The web-based system for reporting and creating awareness about social media threats and crime has been tailored to support reporting of social media threats & crime as well as awareness among the Public, the Justice, Law and Order Sector, Business Community, ICT Regulatory Agencies, the financial sector and as a tool for publishing social media safety and security tips in Uganda and across the globe.

FUNCTIONS AND FEATURES OF THE SYSTEM

The purpose of this questionnaire is to enable reporting of social media threats, and provide periodical social media threat and crime statistics. It also profiles the latest social media crimes and threats nationally and globally.

The system is available at**:** https://www.socialmedia.archersug.com/

QUESTIONNAIRE

This will be distributed to 25 respondents outside those who will participated in the FGD who will share their feedback.

1. Testing Functionality

a) Are you able to report social threats/crime while anonymous? Yes/NO
b) Are you able to register as a user? Yes/NO
c) If yes, did you successfully login and report a threat/crime to the relevant authorities? Yes/NO
d) In case you forgot your password, are you able to reset it and still access the system? Yes/NO
e) Whilst an anonymous or registered user, were you able to view the published awareness news? Yes/NO
f) Does the system provide for any form of security guidelines/tips for basic or general social media users? Yes/NO
g) Are you able to tell the locations/districts where threats and crimes have been reported? Yes/NO
h) Are you able to use a different language to read the content on the system? Yes/NO
i) Did you get feedback upon lodging of your complaint? Yes/NO
j) Are you able to generate social media incident reports? Yes/NO

2. Testing usefulness of system

a) To what extent does the system meet the general purpose? (Scale of 1 to 5)
1-Not at all, 2 - To some extent, 3 – Average, 4 - Very useful, 5- Answers it all

b) Rate ease of use of the platform in terms of; (Scale of 1 to 5):

1 - Poor, 2 – Fair, 3 - Good, 4 – Very Good, 5 - Excellent

i. Time response,
ii. Content

iii. Display/Graphics used
iv. Navigation

c) Rate the relevance of the system to social media threat and crime awareness. Please explain your answer.

d) Provide suggests towards improving the system?

8.5 Annex E

FOCUS GROUP DISCUSSION TOOL FOR TESTING AND VALIDATION OF WEB-BASED SYSTEM FOR SOCIAL MEDIA THREAT REPORTING AND CRIME AWARENESS

The discussion will target key persons in the following categories;

a) Civil society Organizations
b) Business community
c) Justice Law and Order Sector. Namely; Uganda Police Force, Office of the Director of Public Prosecution and the Judiciary
d) Telecom operators
e) Education sector
f) Banking sector
g) General social media users

NOTE:

Participants will first be given the system link to go through the system and use it to:

a) Familiarize themselves with the system and its purpose
b) Report social media crime and threats they've heard of/encountered lately
c) Access social media and threat statistics
d) Access latest social media crime and threat news
e) Access, read and use the Frequently Asked Questions (FAQs)

1. **are the questions to be answered individually after participants have gone through and made an attempt to use the system.**

(i) Have you been able to report a social media threat/crime? If not, briefly explain why not
(ii) Did you access latest social media threat and crime statistics? If not, briefly explain why not
(iii) Did you access latest social media crime and threat news in Uganda and globally? If not, briefly explain why not
(iv) Are you able to access, read and use the Frequently Asked Questions (FAQ)? If not, briefly explain why not
(v) To what extent does the system meet the general and intended purpose?
(vi) How easy was it for you to use and navigate the system?
(vii) Suggest ways the system can be improved to effectively meet its purpose?

2. **Questions during the FGD after participants have responded to individual questions**

(i) How easy is the system to use and navigate? (Very easy, easy, neutral, not easy, very difficult)

(ii) Explain the basis of your answer in question (i) .

(iii) Rate the usefulness of the system in social media crime and threat reporting and awareness (very useful, useful, neutral, not useful, not sure)

(iv) Explain the basis of your answer in question (ii) .

(v) What functionalities should be added to the system to make it a better and more effective web-based system for reporting and creating awareness about social media threats and crime?

(vi) What current functionalities should be improved?

(vii) What functionalities are not necessary and should be removed?

(viii) Provide suggestions for general improvement of the system to make it a better and more effective social media threat and crime reporting and awareness system

(ix) Suggestions for successful implementation and wide utilization of the system including key players and their roles.

(x) Institutions that are ready to play one or more roles in its implementation and utilization and which roles, by who and when

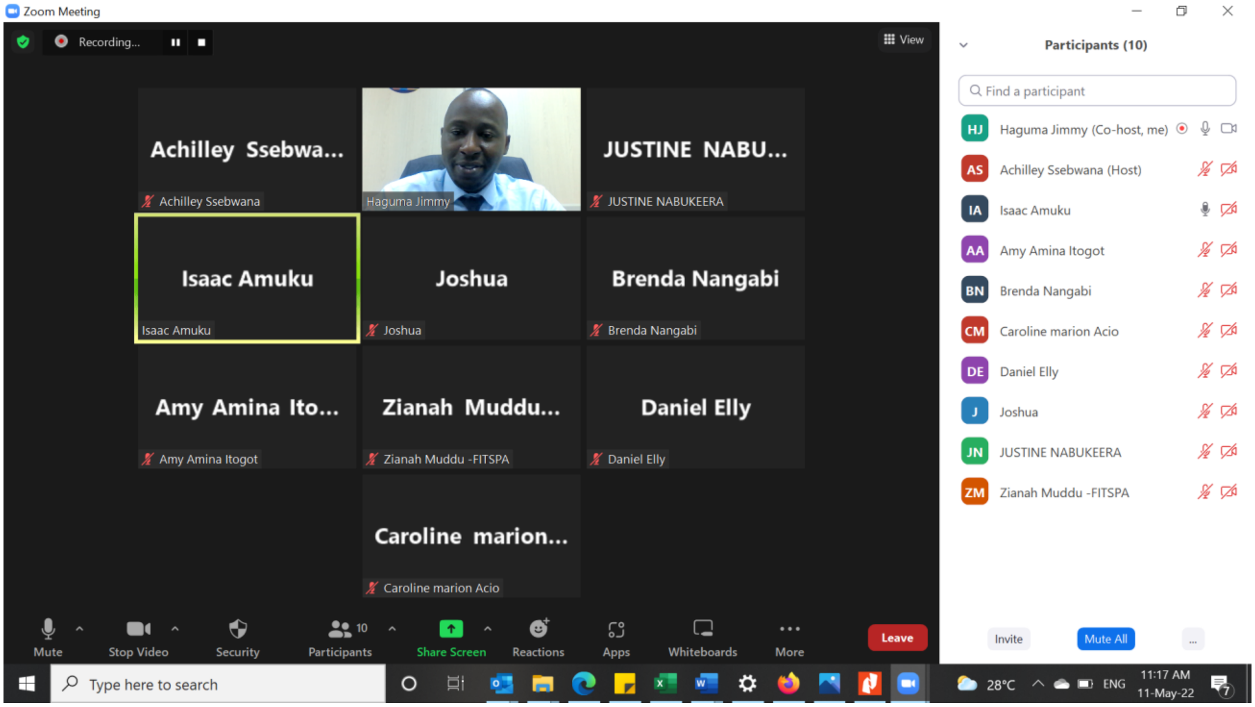
(xi) Anticipated challenges of implementation and utilization of the system

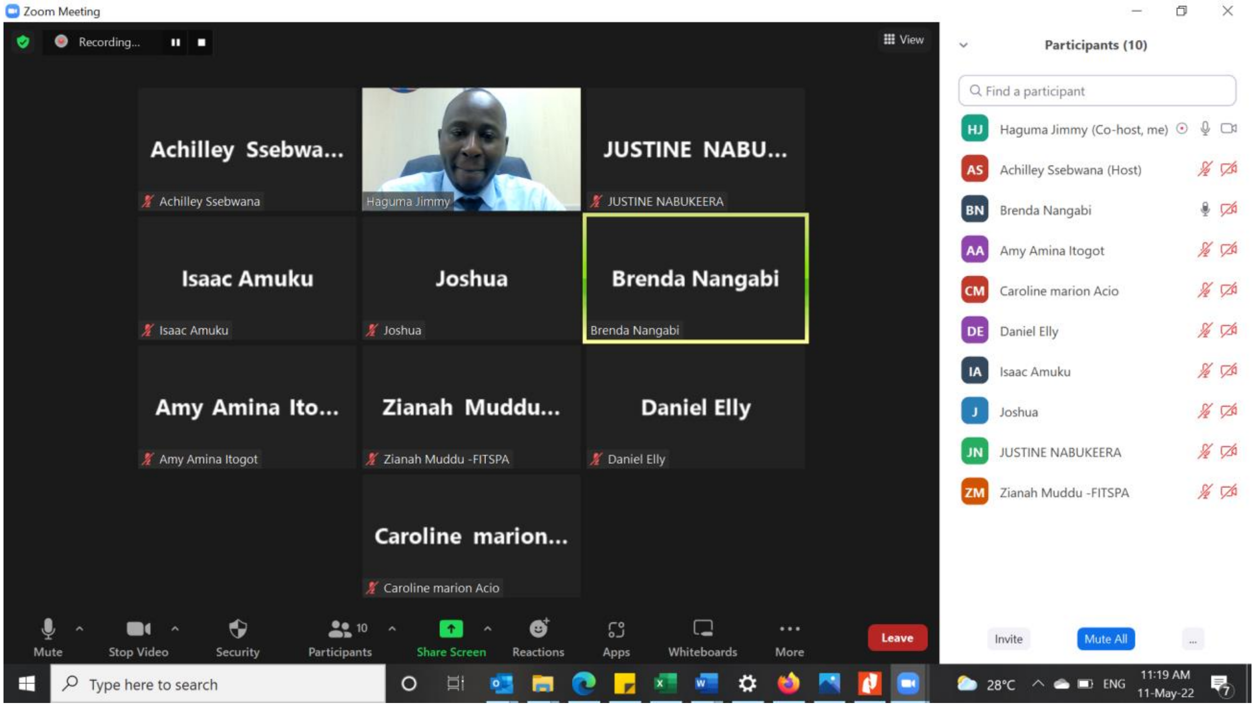
(xii) Potential solutions to the challenges

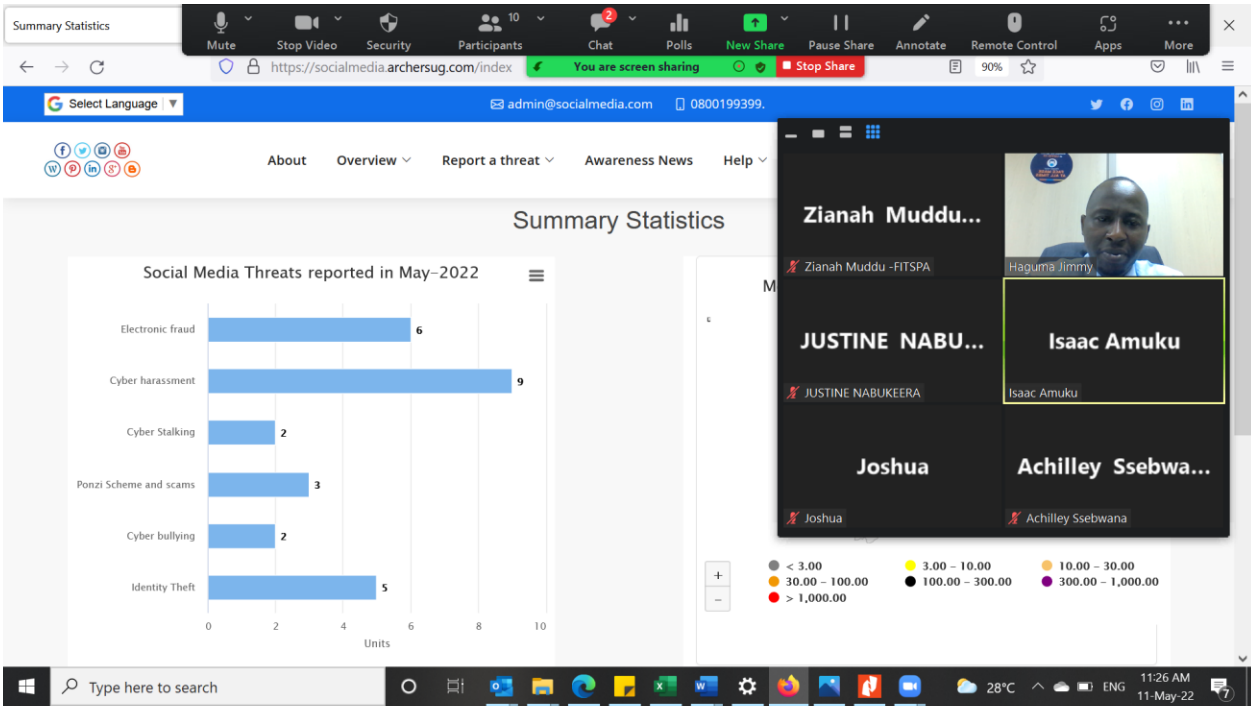
(xiii) Provide any other relevant comments/feedback.

8.6 Annex F

SNAP SHOTS OF THE VIRTUAL (ZOOM MEETING) FOCUS GROUP DISCUSSION DURING TESTING AND VALIDATION OF THE SOCIAL MEDIA THREAT REPORTING & CRIME AWARENESS SYSTEM



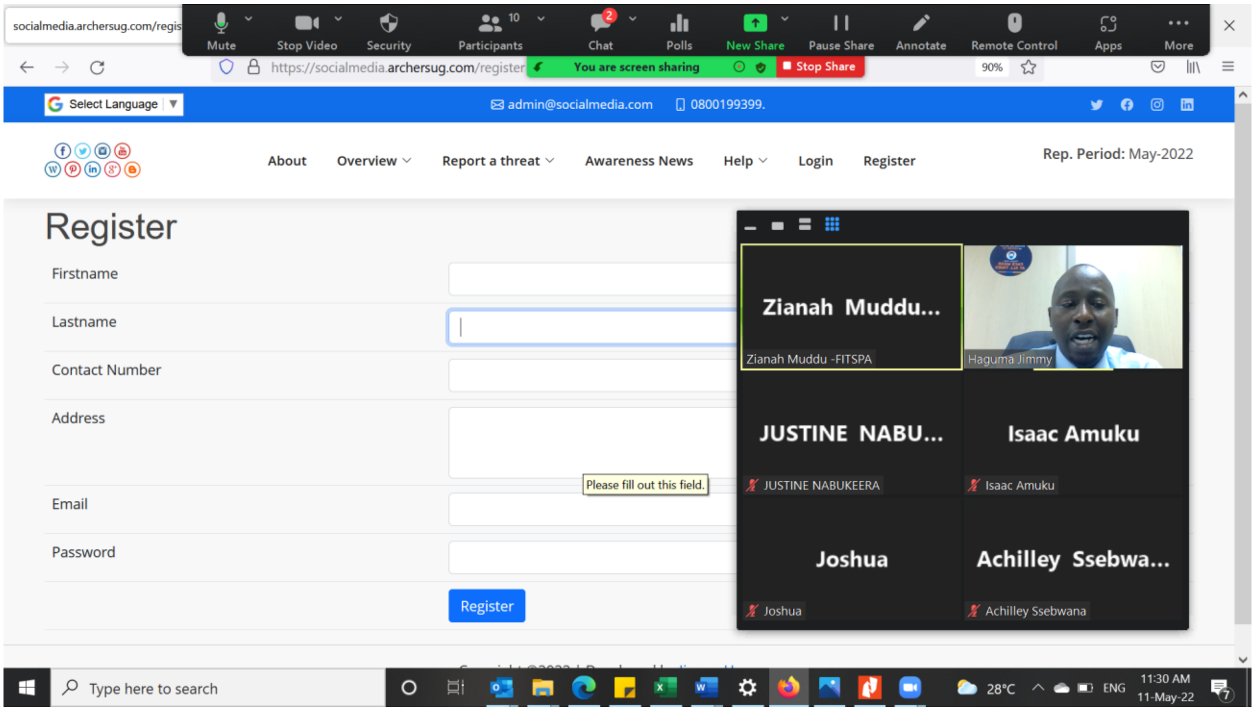




Summary Statistics

Social Media Threats reported in May-2022

	Units
Electronic fraud	6
Cyber harassment	9
Cyber Stalking	2
Ponzi Scheme and scams	3
Cyber bullying	2
Identity Theft	5



Rep. Period: May-2022

Register

Firstname

Lastname

Contact Number

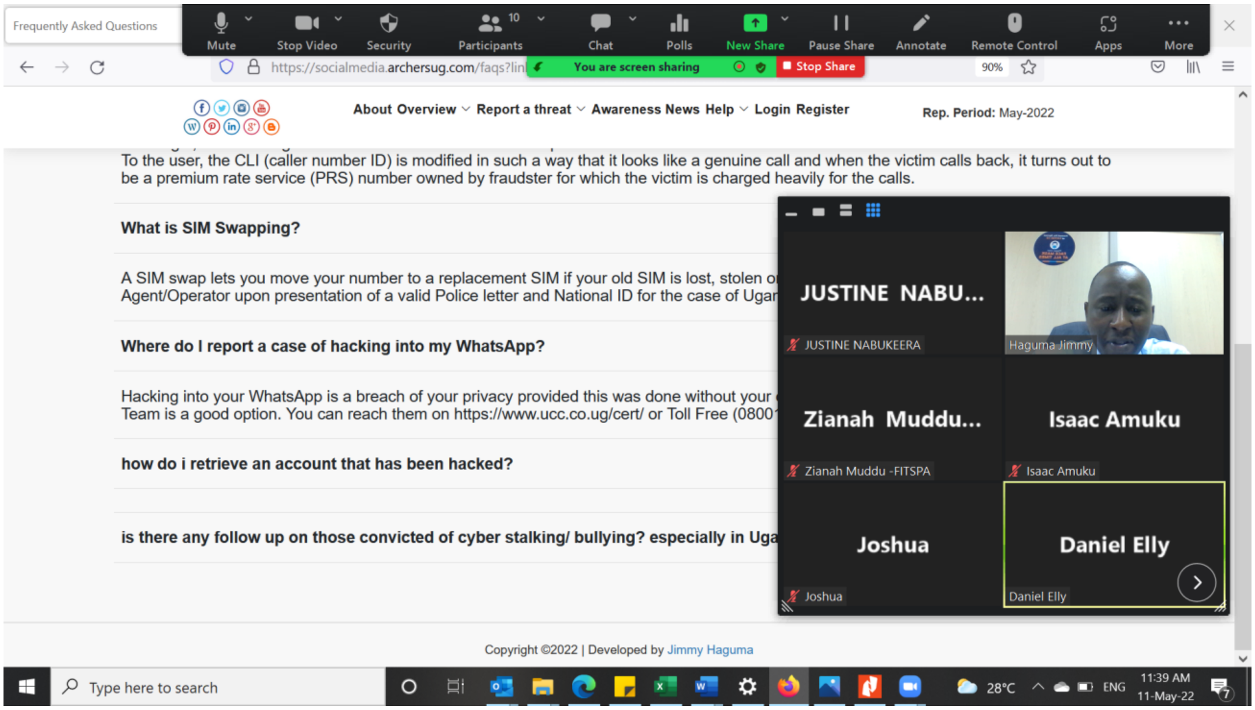
Address

Email

Password

Please fill out this field.

Register



Rep. Period: May-2022

To the user, the CLI (caller number ID) is modified in such a way that it looks like a genuine call and when the victim calls back, it turns out to be a premium rate service (PRS) number owned by fraudster for which the victim is charged heavily for the calls.

What is SIM Swapping?

A SIM swap lets you move your number to a replacement SIM if your old SIM is lost, stolen o Agent/Operator upon presentation of a valid Police letter and National ID for the case of Ugar

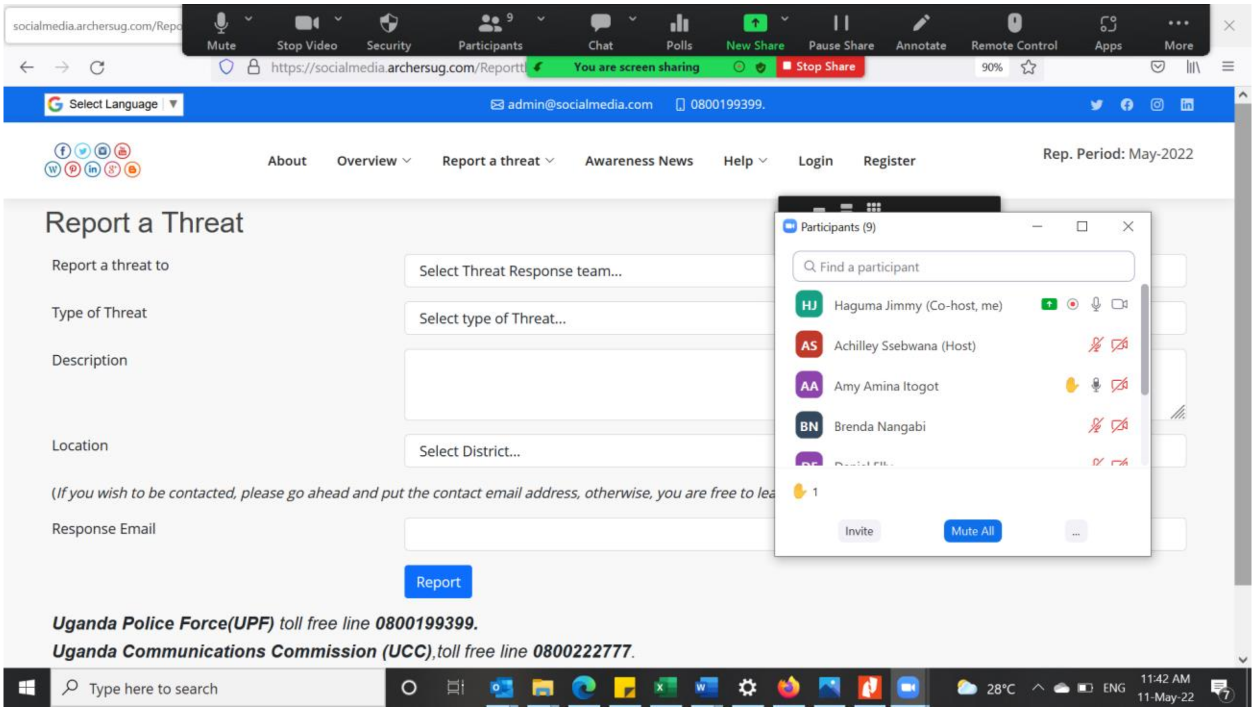
Where do I report a case of hacking into my WhatsApp?

Hacking into your WhatsApp is a breach of your privacy provided this was done without your Team is a good option. You can reach them on https://www.ucc.co.ug/cert/ or Toll Free (0800

how do i retrieve an account that has been hacked?

is there any follow up on those convicted of cyber stalking/ bullying? especially in Uga

Copyright ©2022 | Developed by Jimmy Haguma



Rep. Period: May-2022

Report a Threat

Report a threat to	Select Threat Response team...
Type of Threat	Select type of Threat...
Description	
Location	Select District...

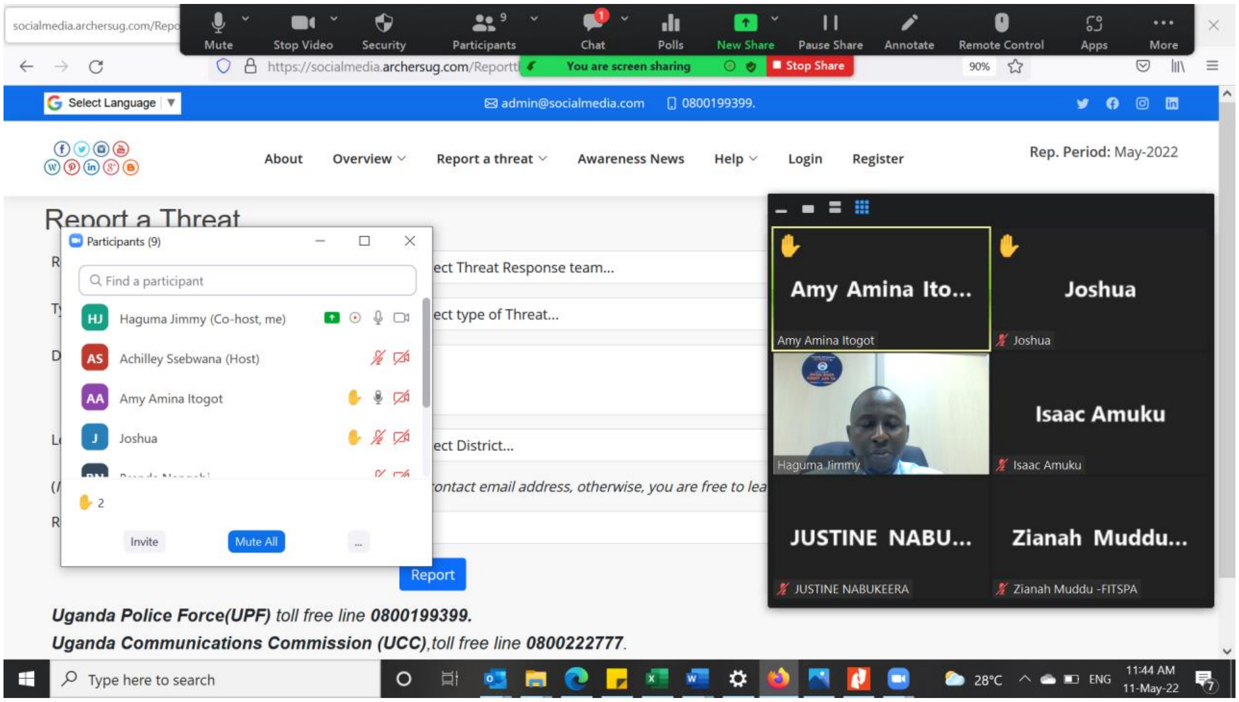
(*If you wish to be contacted, please go ahead and put the contact email address, otherwise, you are free to lea*

Response Email

Report

Uganda Police Force(UPF) *toll free line* ***0800199399.***

Uganda Communications Commission (UCC)*,toll free line* ***0800222777****.*



Rep. Period: May-2022

Report a Threat

Select Threat Response team...

Select type of Threat...

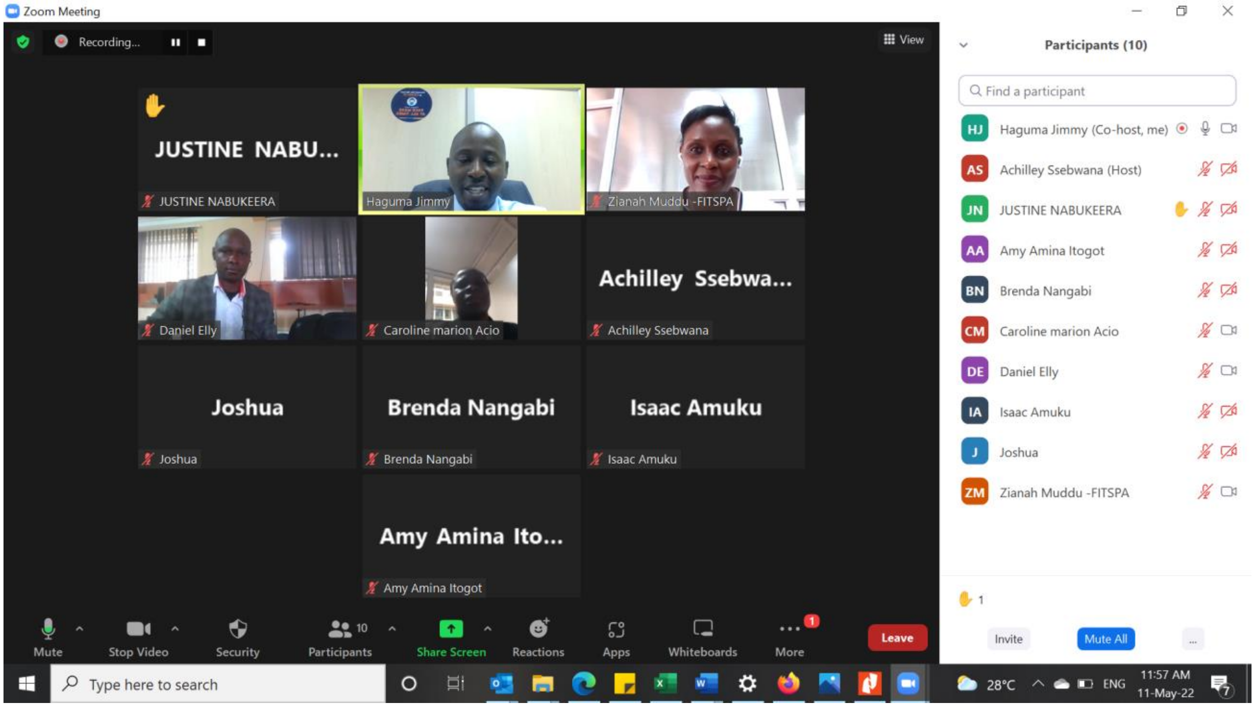
Select District...

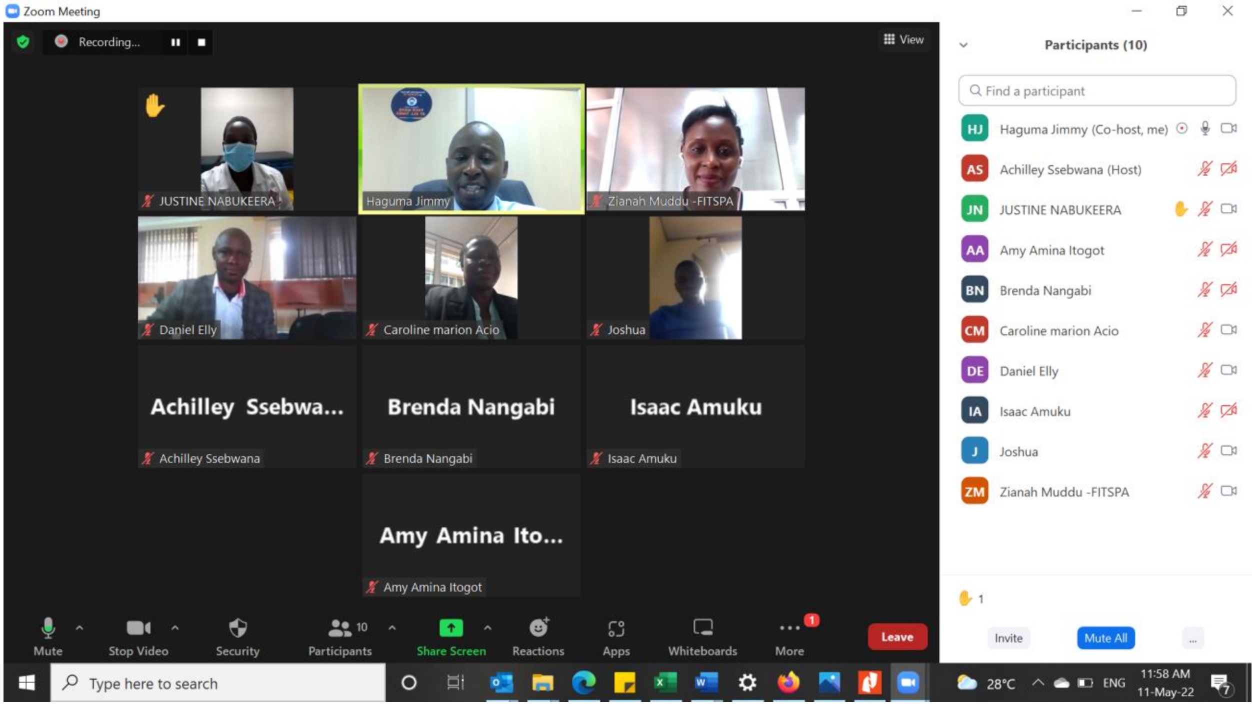
contact email address, otherwise, you are free to lea

Report

Uganda Police Force(UPF) *toll free line* ***0800199399.***

Uganda Communications Commission (UCC),*toll free line* ***0800222777***.

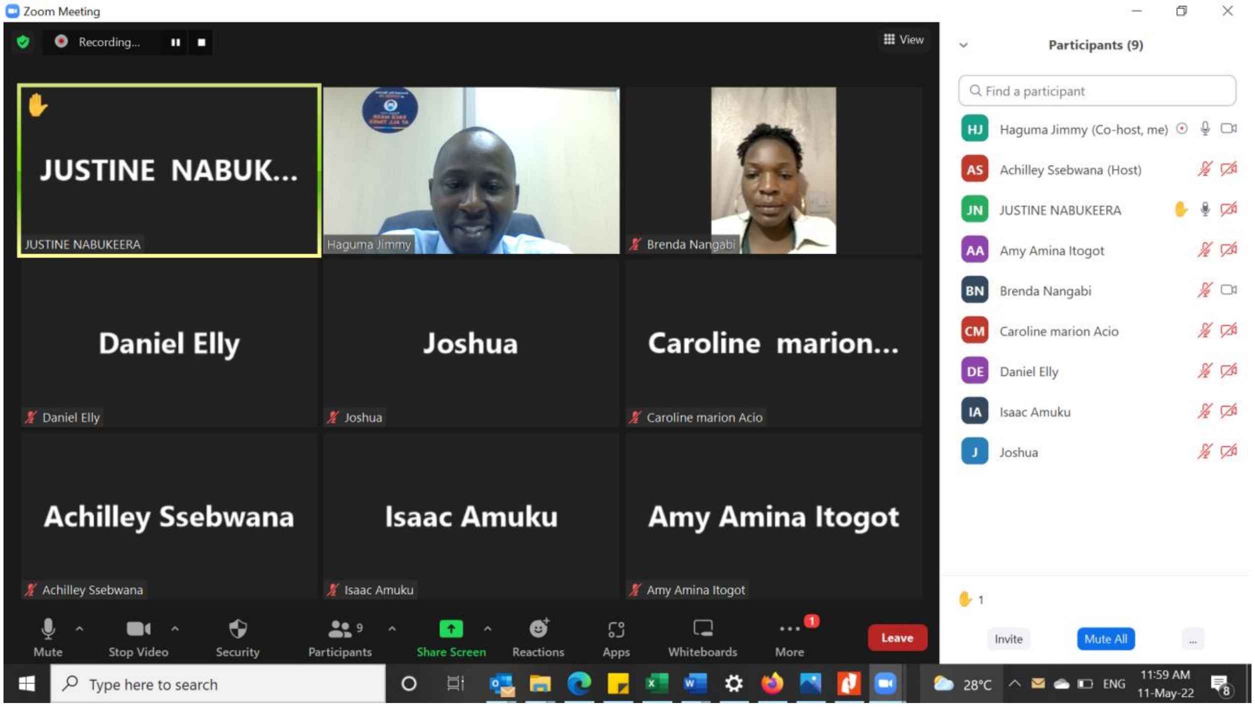




Participants (10)

Find a participant

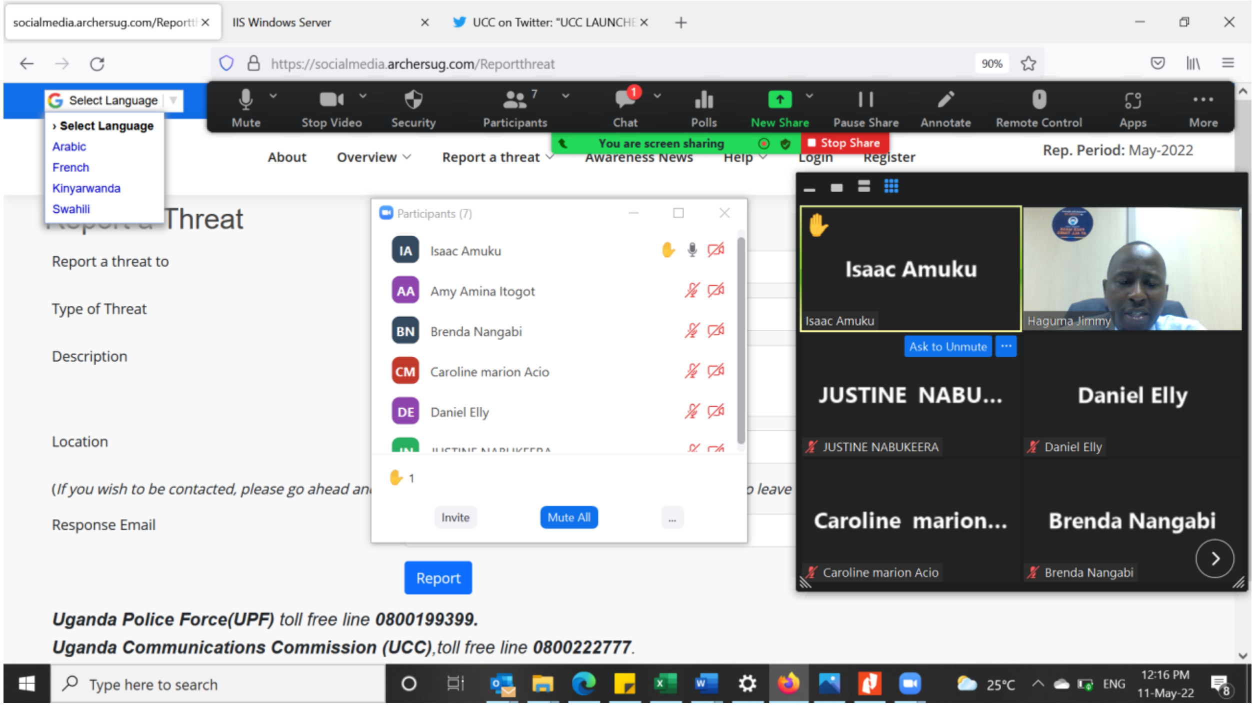
- HJ Haguma Jimmy (Co-host, me)
- AS Achilley Ssebwana (Host)
- JN JUSTINE NABUKEERA
- AA Amy Amina Itogot
- BN Brenda Nangabi
- CM Caroline marion Acio
- DE Daniel Elly
- IA Isaac Amuku
- J Joshua
- ZM Zianah Muddu -FITSPA



Participants (9)

Find a participant

- HJ Haguma Jimmy (Co-host, me)
- AS Achilley Ssebwana (Host)
- JN JUSTINE NABUKEERA
- AA Amy Amina Itogot
- BN Brenda Nangabi
- CM Caroline marion Acio
- DE Daniel Elly
- IA Isaac Amuku
- J Joshua



Rep. Period: May-2022

Report a Threat

Report a threat to

Type of Threat

Description

Location

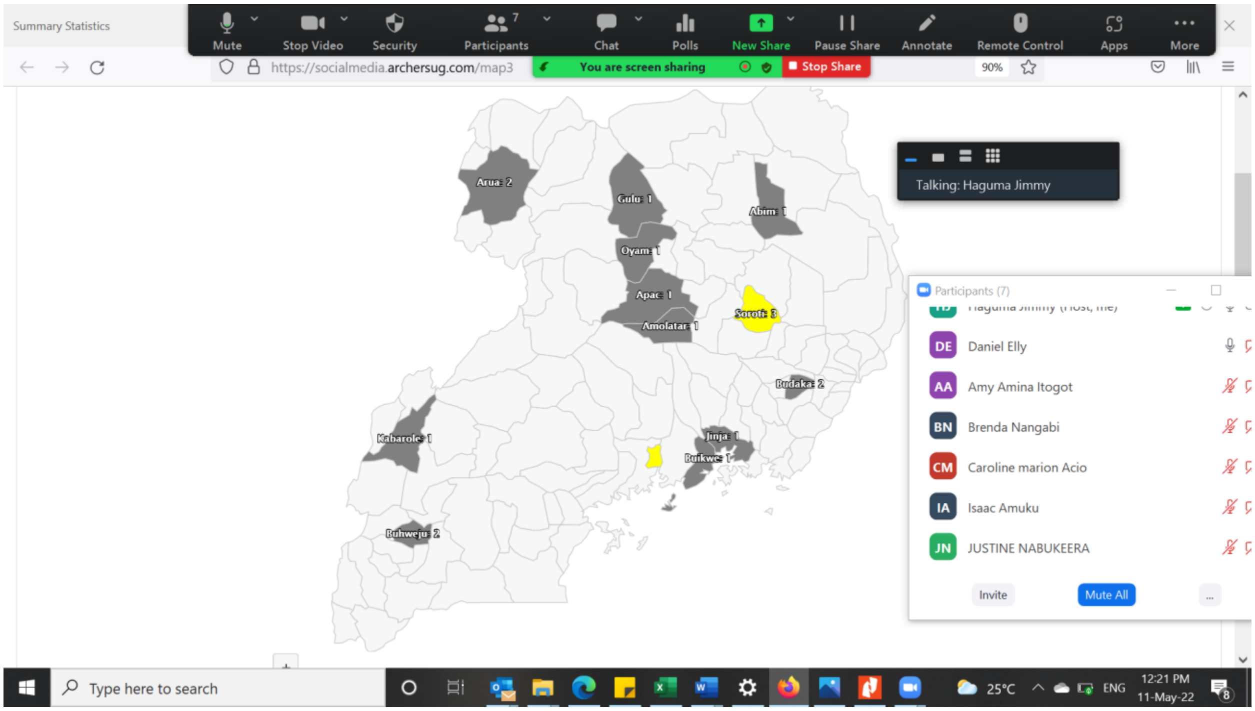
(*If you wish to be contacted, please go ahead an* ... *leave*

Response Email

Report

Uganda Police Force(UPF)** toll free line **0800199399.

***Uganda Communications Commission (UCC)**,toll free line **0800222777**.*



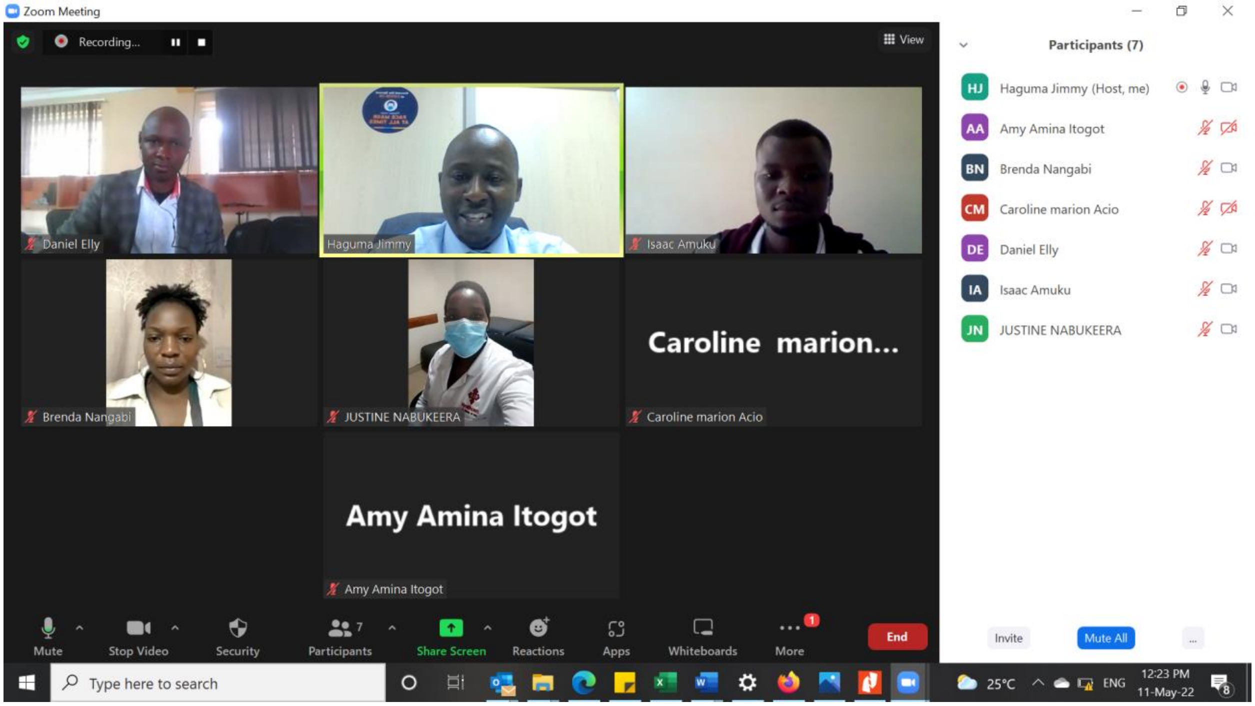


Figure 67: User Acceptance Testing Virtual Sessions with key stakeholders

8.0 REFERENCES

Friedman, L. (2014, April 22). *Benefits of Using Social Media*. Retrieved from https://www.linkedin.com: https://www.linkedin.com/pulse/20140422162738-44670464-5-benefits-of-using-social-media

Katherine, F., & George , T. E. (2019). Social Networks and Crime: Pitfalls and Promises for Advancing the Field. *Annual Review of Criminology*, 99-122.

PwC. (2020, September). *The National Payment Systems Act 2020.* Retrieved from Pwc: https://www.pwc.com/ug/en/assets/pdf/discussion-of-national-payment-systems-act-2020-slide-deck.pdf

Shikati, C. (2017, November 9). *Ways social media has changed our society*. Retrieved from What it takes: https://medium.com/w-i-t/ways-social-media-has-changed-our-society-38fd4d3e5ce8

Abdalla, A. a. (2014). *A Review of Using Online Social Networks for Investigative Activities.* Cham: Springer International Publishing.

Abulaish, M., & Haldar, N. A. (2018). Advances in Digital Forensics Frameworks and Tools: A Comparative Insight and Ranking. *International Journal of Digital Crime and Forensics*, 95-119.

Agena , M., Ojok , D., & Achol, T. (2019). *Social Media, Local Governance and Development in Uganda.* Kampala: Konard Adenauer Stiftung.

Agencies. (2020, September 8). *Uganda orders social media accounts with large following to register for monitoring*. Retrieved from The Citizen: https://www.thecitizen.co.tz/news/Uganda-orders-social-media-accounts-register-for-monitoring/1840360-5620714-vea62r/index.html

Ajayi, E. F. (2016). Challenges to enforcement of cyber crime laws and policy. *Journal of Internet and Information Systems*, 5-7.

Akram, W. (2018). A Study on Positive and Negative Effects of Social Media on Society. *International Journal of Computer Sciences and Engineering*, 136,491.

Alanezi, F. Y. (2016). SOCIAL MEDIA AS A TOOL FOR COMBATING CYBERCRIMES WITH SPECIAL REFERENCE TO SAUDI ARABIA. *Asia Pacific Journal for Advanced Business and Social Studies*, 610-624.

Amazouz , S. (2018, October 16). *African Forum on Cybercrime - African Union Convention on Cybersecurity and Personal Data Protection "Malabo Convention".* Addis-Ababa: African Union Commission. Retrieved from https://rm.coe.int/3148-afc2018-ws4-auc/16808e6875

Ampurire, P. (2020, June 17). *Two Arrested for Running Fake Facebook Account in Name of URA Commissioner General*. Retrieved from Soft Power: https://www.softpower.ug/two-arrested-for-running-fake-facebook-account-in-name-of-ura-commissioner-general/

Anderson , J., & Rainie, L. (2018, April 17). *Concerns about the future of people’s well-being*. Retrieved from Pew Research Center: https://www.pewresearch.org/internet/2018/04/17/concerns-about-the-future-of-peoples-well-being/

Anderson. (2019, Dec 29). *Theories of Crime: Classical, Biological, Sociological, Interactionist in SchoolWorkHelper.* Chicago: SchoolWorkHelper.

APC. (2019). *Securing human rights online in Africa through a strong and active "African Declaration on Internet Rights and Freedoms" network.* Johannesburg: Creative Commons Attribution 4.0 International .

Asongu, S. a.-M. (2019, September 09). Crime and Social Media. *Crime and Social Media*, pp. 1215-1233.

Awati, R. (2021, August 21). *cyberstalking*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/cyberstalking

Balhara, S. (2021, January 31). *Theories of causation of crime*. Retrieved from ipledges intelligent legal solutions: https://blog.ipleaders.in/theories-causation-crime/

BarefootLaw. (2019). *How Laws and regulations affect online activities.* Kampala: Barefootlaw.

Barrett, N. (2020). Social Media, Ethics and the Privacy Paradox. *IntechOpen*.

Berg, M. (2020, March 27). *What Does Hacking Mean?* Retrieved from Technopedia: https://www.techopedia.com/definition/26361/hacking

Bos, T. (2019). *Cyber Laws of Uganda - How laws and Regulations affect online activities in Uganda.* Kampala: Barefootlaw.

BreachLock, I. (2019, January 17). *Top 5 Open Source OSINT Tools*. Retrieved from BreachLock Inc: https://www.breachlock.com/top-5-open-source-osint-tools/

Bump, P. (2020, Febraury 18). *The 5 Types of Social Media, Pros & Cons of Each*. Retrieved from Hub spot Inc: https://blog.hubspot.com/marketing/which-social-networks-should-you-focus-on

Burstein, F. (2002). Information Management and Systems. In F. Burstein, *Research Methods for Students, Academics and Professionals* (pp. 147-158). Australia: Centre for Information Studies.

Caplinskas, M. (2015, February 24). *8 Simple Ways to Minimize Online Risk*. Retrieved from Entrepreneur: https://www.entrepreneur.com/article/243233

Chander, M. (2014). Social Media: Analysis of New Challenges and Opportunities for Indian Law Enforcement Agencies. *The Indian Police Journal*, 127-128.

CIPESA. (2018). *National Information Technology Survey 2017/18 Report.* Kampala: The Collaboration on International ICT Policy for East and Southern Africa.

Clement. (2020, February 14). *Global social networks ranked by number of users 2020*. Retrieved from Statista: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Clement, J. (2019, August 14). *Number of social network users worldwide from 2010 to 2021*. Retrieved from Statista: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Clement, J. (2020, July 15). *Number of social networking users worldwide in 2020, by region*. Retrieved September 13, 2020, from Stastica: https://www.statista.com/statistics/454772/number-social-media-user-worldwide-region/

Cohen, L. (2010, March 17). *6 Ways Law Enforcement Uses Social Media to Fight Crime*. Retrieved from Mashable: https://mashable.com/2010/03/17/law-enforcement-social-media/

Coolidge, T. (2022, May 17). *What are the Major Types of Cybercrime?* Retrieved from COOLIDGE LAW FIRM PLLC: https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/

Corporation, M. (2020, June 07). *Research strategy*. Retrieved June 07, 2020, from Mackenzie Corporation: https://www.mackenziecorp.com/phase-2-clearly-define-research-strategy/

Cox, K., Marcellino, W., & Bellasio, J. (2018, November 5). *Social media in Africa presents double-edged sword for security and development*. Retrieved from RAND Corporation: https://www.rand.org/randeurope/research/projects/social-media-in-africa.html

Creswell, J. W. (2018). Research design: qualitative, quantitative, and mixed methods approaches. 4th ed. Thousand Oaks, California. *Sage Publications*.

Cross, M. (2014). Beyond technology dealing with people - The Dark Side. In M. Cross, *Social Media Security* (pp. 161-191). Elsevier.

Curiel, P., Cresci, R., Muntean, S., & Ioana, C. (2020, April 02). Crime and its fear in social media. *Palgrave Communications*, pp. 20-43.

Curiel, R. P., Cresci, S., Muntean, C. I., & Bishop , S. R. (2020). Crime and its fear in social media. *Humanities and Social Sciences Communications*, 50-62.

Daily Nation. (2020, June 26). *17-year-old girl defiled by her Facebook lover, two others*. Retrieved from Daily Monitor: https://www.monitor.co.ug/News/National/17-year-old-girl-defiled-by-her-Facebook-lover-two-others/688334-5583252-111anpgz/index.html

Dalla, H. S., & Geeta. (2016). Cyber Crime – A Threat to Persons, Property, Government and Societies. *International Journal of Advanced Research in Computer Science and Software Engineering,*, 106-112.

Daniel, C. (2014). Cyber terrorism: Case studies. In C. Daniel, *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 165-174). Syngress.

David, S. (2020, May 29). *Trump signs executive order to narrow protections for social media platforms*. Retrieved from The Guardian: https://www.theguardian.com/us-news/2020/may/28/donald-trump-social-media-executive-order-twitter

Davis, C. (2020, September 13). *Encapsulation, Abstraction, Inheritance, and Polymorphism*. Retrieved from Medium: https://medium.com/@colebuildanddevelop/encapsulation-abstraction-inheritance-and-polymorphism-26aa98042d41

Davis, S. E. (2018). Objectification, Sexualization, and. *SAGE*, 1-9.

Derrick, K. (2016, August 31). *TVO case: Facebook attacks Uganda's record*. Retrieved August 31, 2016, from The Observer: https://observer.ug/news-headlines/46191-tvo-case-facebook-attacks-uganda-s-record

Dorris, B. (2020). *Report to the Nations 2020 - A global study on occupational fraud and Abuse.* Austin, Texas: Association of Certified Fraud Examiners.

Dr. Joseph, T. Wells. (2018). *Fraud Examiners Manual 2018 IInternal Edition.* Austin, Texas: Association of Certified Fraud Examiners.

Drury, A. (2020, September 6). *Social Media Definition*. Retrieved from Investopedia: https://www.investopedia.com/terms/s/social-media.asp

D'Urso, J. (2020, July 6). *How the coronavirus pandemic is changing social media*. Retrieved from Reuters Institute: https://reutersinstitute.politics.ox.ac.uk/risj-review/how-coronavirus-pandemic-changing-social-media

Elise , M. (2019, June 16). *The Pros and Cons of Social Networking*. Retrieved from Lifewire: https://www.lifewire.com/advantages-and-disadvantages-of-social-networking-3486020

Europol. (2022). *High-Tech crime*. Retrieved from Europol: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime/high-tech-crime

Feyisa, M., & Dawit , A. G. (2018). Perceived Benefits and Risks of Social Media: Ethiopian Secondary School Students' Perspectives. *Journal of Technology in Behavioral Science*, 294–300.

Filipo , S. (2013). Systematic Approaches to Digital Forensic Engineering (SADFE). *Digital forensic investigation in cloud computing environment: Impact on privacy* (pp. 2-7). West Lafayette: Center for Education and Research in Information Assurance and Security .

Finextra. (2020, April 30). *Increasing Resilence in colloborative Financial Services*. Retrieved from Finextra: https://www.finextra.com/newsarticle/35735/scammers-left-to-run-riot-on-social-media-which-finds

Finnberg, N. (2019, August 13). *How to Conduct Social Media Investigations and Remain Anonymous*. Retrieved from Security Boulevard: https://securityboulevard.com/2019/08/how-to-conduct-social-media-investigations-and-remain-anonymous/

France , L. R., & Verdie, C. (2016, October 5). *Kardashian heist: Police say social media made her a target*. Retrieved from CNN: Entertainment: https://edition.cnn.com/2016/10/04/entertainment/kim-kardashian-police-social-media/index.html

Gallo, B. (2015, July 17). *What happens when you text a tip to N.J. police?* Retrieved from Salem County - Prosecutor's Office: https://www.salemcountyprosecutor.org/what-happens-when-you-text-a-tip-to-n-j-police/

GlobalStats. (2020, March 1). *Social Media Stats Uganda*. Retrieved from Statcounter Global Stats: https://gs.statcounter.com/social-media-stats/all/uganda

Gregg, D. (2001). Information Systems Frontiers. In D. Gregg, *Understanding the Philosophical Underpinnings of Software Engineering Research in Information Systems* (pp. 169-183). Denver: Kluwer Academic Publishers.

Groot , J. D. (2020, September 30). *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*. Retrieved from Data Insider - Digital Guardian's Blog: https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

Halder, D. (2015, June 9). *Creating awareness of Online Victimization using Social Media: A Therapeutic Jurisprudential approach*. Retrieved from Therapeutic Jurisprudence in the Mainstream: https://mainstreamtj.wordpress.com/2015/06/09/creating-awareness-of-online-victimization-using-social-media-a-therapeutic-jurisprudential-approach/

Hameed, N., & Abid, A. (2018, December 19). *The role of social media in solving and committing crimes*. Retrieved from Arab News: https://www.arabnews.com/node/1422811/media

Hamrick, P. (2019, January 28). *Is Social Media Evidence Too Much For Criminal Investigators To Handle?* Retrieved from Nuix: https://www.nuix.com/blog/social-media-evidence-too-much-criminal-investigators-handle

Hollywood et al. (2018). Using Social Media and Social Network Analysis in Law Enforcement. *Creating a Research Agenda, Including Business Cases, Protections, and Technology Needs* (pp. 1-28). Washington, DC: RAND Corporation Inc.

IACP. (2013, January). *IACP CENTER FOR SOCIAL MEDIA*. Retrieved from iacpsocialmedia.org: http://www.iacpsocialmedia.org/getting-started/social-media-an-introduction/

ICT Policy Africa. (2019, September 24). *ICT Policy Africa Documents.* Retrieved from ICT Policy Africa: https://ictpolicyafrica.org/en/document/jny54lkvxho

IFIS. (2018, August 20). *IFIS*. Retrieved September 28, 2020, from IFIS: https://www.forensicsinstitute.org/cybercrime-in-uganda/

InfoSec. (2019). *Computer Forensics: Introduction To Social Network Forensics*. Retrieved June 06, 2019, from Infosec Institute: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/hybrid-and-emerging-technologies/social-network-forensics/#gref

InfoSec. (2020, May 28). *Introduction To Social Network Forensics*. Retrieved from Infosec Resources: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/hybrid-and-emerging-technologies/social-network-forensics/

ITU. (2019, December 20). *Committed to connecting the world*. Retrieved from Internatioanl Telecommunications Union Statistics: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Jain, S. (2018, March 8). *Types of Social Media Cybercrimes and How Women Should Deal With It*. Retrieved from Social Media and Digital Marketing blog: https://www.soravjain.com/cyber-security-for-women-in-social-media

JM Okoth, O. (2019). *Annual Crime Report - 2019.* Kampala: Uganda Police Force.

Jürgen , S. (2022, September 20). *Fighting intellectual property crime through global cooperation*. Retrieved from Interpol: https://www.interpol.int/en/News-and-Events/News/2022/Fighting-intellectual-property-crime-through-global-cooperation

Kairu, F. (2020, June 9). *How Uganda's New Director of Public Prosecutions Can Tackle Corruption and Illicit Financial Flows*. Retrieved from Global Financial Integrity: https://gfintegrity.org/how-ugandas-new-director-of-public-prosecutions-can-tackle-corruption-and-illicit-financial-flows/

Kamoga, J. (2017, August 18). *Uganda loses Shs 122bn annually to cyber attacks*. Retrieved from The Observer: https://observer.ug/news/headlines/54458-uganda-loses-shs-122bn-annually-to-cyber-attacks-says-report.html

Khode et al. (2015). Digital Forensic Tool for Decision Making in computer security domain. *INTERNATIONAL JOURNAL FOR RESEARCH IN EMERGING SCIENCE AND TECHNOLOGY*, 1-6.

Khoury, G. (2017, February 22). *5 Common Types of Social Media Crime*. Retrieved from FindLaw: https://blogs.findlaw.com/blotter/2017/02/5-common-types-of-social-media-crime.html

Kimbowa, J. (2018, January 3). *Nine ways you can be conned in 2018*. Retrieved from The Observer: https://observer.ug/lifestyle/56521-nine-ways-you-can-be-conned-in-2018.html

Koch, T. &. (2018). The impact of social media on recruitment: Are you LinkedIn?. *SA Journal of Human Resource Management.* , 16.

Koeze, E., & Popper, N. (2020, Apirl 7). *The Virus Changed the Way We Internet*. Retrieved from The New York Times: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html

Kortjan, N. (2013, November). *A Cyber Security Awareness and Education Framework for South Africa.* Retrieved from CORE: https://core.ac.uk/download/pdf/145053774.pdf

Kurbalija, J. (2017, May 9). *The impact of (big) data on geopolitics, negotiations, and the diplomatic modus operandi*. Retrieved from Diplo: https://www.diplomacy.edu/blog/impact-big-data-geopolitics-negotiations-and-diplomatic-modus-operandi

Kyatusimire, S. (2020, August 13). *URA Boss Ditches Facebook , Instagram over Frausters*. Retrieved from ChimpReports: https://chimpreports.com/ura-boss-ditches-facebook-instagram-over-fraudsters/

Lampe, K. v. (2011). The application of the framework of Situational Crime Prevention to ‘organized crime’. *Criminology and Criminal Justice*, 145-163.

Larsen, H. L., Blanco, J. M., Pastor, R. P., & Yager, R. R. (2017). *Using Open Data to Detect Organized Crime Threats - Factors Driving Future Crime.* Gewerbestrasse : Springer International Publishing.

LASPNET. (2017). *State of Access to Justice Report - 2017 Annual Trends Analysis.* Kampala: Legal Aid Service Providers' Network.

Lauren , F. (2014, April 22). *Benefits of Using Social Media*. Retrieved from Linkedin: https://www.linkedin.com/pulse/20140422162738-44670464-5-benefits-of-using-social-media

Leander Police Dept. (2020). *Tip411 Crime tips*. Retrieved from City of Leander Texas: https://www.leandertx.gov/police/page/tip411-crime-tips

Lee et al. (2019). International Journal of Cybersecurity Intelligence & Cybercrime. *A Test of Structural Model for Fear of Crime in*, 5-22.

Luisa, M., & Stasi. (2019). Competition and Regulation of Network Industries. *Social media platforms and content exposure: How to restore user control*, 86-110.

Lynch, J., & Nadine, B. (2020, February 5). *Social Media, Ethics and the Privacy Paradox*. Retrieved from IntechOpen.com: https://www.intechopen.com/books/security-and-privacy-from-a-legal-ethical-and-technical-perspective/social-media-ethics-and-the-privacy-paradox

Magelah, P. (2016). *State of Internet Freedom in Uganda.* Kampala: CIPESA.

Martin, M. (2022, December 24). *Software Development Life Cycle (SDLC) Phases & Models*. Retrieved from Guru99: https://www.guru99.com/software-development-life-cycle-tutorial.html#:~:text=What%20is%20SDLC%3F,defined%20time%20frame%20and%20cost.

McGovern, A., & Milivojevic, S. (2016, October 16). *Social media and crime: the good, the bad and the ugly*. Retrieved from The Conversation: https://theconversation.com/social-media-and-crime-the-good-the-bad-and-the-ugly-66397

McGuire, M. (2019, November 26). *Social Media: A Holiday Haven For Threat Actors*. Retrieved from The Cyber Feed: https://blog.cyberint.com/social-media-a-heaven-for-cyber-criminals

Ministry of ICT&NG. (2019, December 3). *The Electronics Signatures Act, 2011*. Retrieved from Ministry of ICT and National Guidance: https://ict.go.ug/2019/12/03/the-electronics-signatures-act-2011/

Mohney, G. (2017, April 18). *Murder on Facebook spotlights rise of 'performance crime' phenomenon on social media*. Retrieved from ABC news: https://abcnews.go.com/US/murder-facebook-spotlights-rise-performance-crime-phenomenon-social/story?id=46862306

MoICT&NG. (2019, December 3). *The Computer Misuse Act, 2011*. Retrieved from Ministry of ICT & National Guidance: https://ict.go.ug/2019/12/03/the-computer-misuse-act-2011/

Monitor, D. (2018, June 27). *Daily Monitor*. Retrieved June 05, 2020, from Daily Monitor: https://www.monitor.co.ug/News/National/Man-arrested-defrauding-Shs700000-IGP-fake-social-media-account/688334-4634106-14n26nd/index.html

Monitor, D. (2019, September 19). *Daily Monitor*. Retrieved from Daily Monitor: https://www.monitor.co.ug/News/National/Suspect-court-summon-First-Son--Marion-Mangeni/688334-5278726-12y0fjy/

Mostafa, H., & Jamal, E.-D. (2020). A social media adoption framework as pedagogical instruments in higher education classrooms. *E-Learning and Digital Media*, 2042-7530.

Mugasa, H. (2022). *National Information Technology Survey Report.* Kampala: NITAU.

Mukiza, C. N. (2019). *UGANDA BUREAU OF STATISTICS 2019 - STATISTICAL ABSTRACT.* Kampala: Uganda Bureau of Statistics. Retrieved 2019, from Uganda Bureau of Statistics: https://www.ubos.org/wp-content/uploads/publications/01_2019STATISTICAL_ABSTRACT_2019.pdf#page=113&zoom=100,0,685

Muliisa, H. (2019, May 31). *Chano8.* Retrieved September 27, 2020, from Chano8: https://chano8.com/kenyas-star-dj-fully-focus-to-spin-magic-at-the-johnnie-walker-highball-ultra-music-experience/

Mwesigwa, A. (2015, June 12). *UCC launches response team to curb cyber crime*. Retrieved from The Observer: https://www.observer.ug/business/38-business/25817-ucc-launches-response-team-to-curb-cyber-crime

Nabisubi, R. (2019, August 8). *Are women still depicted as the weaker sex online?* Retrieved from The New Vision: https://www.newvision.co.ug/news/1505116/world-warned-change-endanger-food-climate

Namutebi, A. (2021, August 11). *Suspected Airtel money hackers remanded*. Retrieved from New Vision: https://www.newvision.co.ug/category/news/suspected-airtel-money-hackers-remanded-111663

Nankinga, M. (2017, December 17). *Regional Forensic Referral Centre of Excellence Commissioned*. Retrieved from Uganda Police Force: https://www.upf.go.ug/regional-forensic-referral-centre-excellence-commissioned/

NapoleonCat. (2020, January 1). *Facebook users in Uganda January 2019*. Retrieved from NapoleonCat Stats: https://napoleoncat.com/stats/facebook-users-in-uganda/2019/01#:~:text=There%20were%202%20379%20000,user%20group%20(990%20000).

National CERT Uganda. (2020). *Uganda National Computer Emmergency Response Team*. Retrieved from Cert-Ug: https://www.cert.ug/

Nickols, F. (2020, April 5). *Thirteen Problem Solving Models.* Retrieved from University of Arkansas at Pine Bluff: https://www.uapb.edu/sites/www/Uploads/Assessment/webinar/session%203/13%20Problem%20Solving%20Models.pdf

NITAU. (2011, February 11). *Computer Misuse Act 2011.* Retrieved September 27, 2020, from National Information Technology Authority: https://www.nita.go.ug/publication/computer-misuse-act-2011-act-no-2-2011

NITAU. (2013, July). *Government of Uganda Social Media Guide.* Retrieved from NITAU: https://www.nita.go.ug/sites/default/files/publications/Government-of-Uganda-Social-Media-Guide.pdf

NITAU. (2016). *Cybersecurity Capacity Review of the Republic of Uganda.* Kampala: Global Cyber Security Capacity Center.

NITAU. (2020, April 24). *COVID-19 Cyber-Laws awareness*. Retrieved from NITA Uganda: https://www.nita.go.ug/media/covid-19-cyber-laws-awareness

Nouh, M. a. (2019). Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement. *Proceedings 2019 Workshop on Usable Security*.

Noyes, D. (2020, May 28). *The Top 20 Valuable Facebook Statistics – Updated May 2020*. Retrieved from Zephoria Digital Marketing: https://zephoria.com/top-15-valuable-facebook-statistics/

Ntezza, M. (2017, May 17). *Utilities Court launched in Kampala Amid Caution*. Retrieved from Chimpreports: https://chimpreports.com/utilities-court-launched-in-kampala-amid-caution/

Nunamaker, J., Chen, M., & Purdin, T. (2001). System Development in Information System Research. *Journal of Management Information System*, 89-106.

O'Neil, C., & Abuhamad, G. (2019). GATEWAY TO A NEW FUTURE OR A THREAT TO PRIVACY AND FREEDOM. *INTERNET, BIG DATA & ALGORITHMS* (pp. 17-20). 2019: The Aspen Institute Congressional Program.

Olupot, N. E. (2016, July 6). *Facebook Vs WhatsApp In Uganda*. Retrieved from PC Tech Magazine: https://pctechmag.com/2016/07/facebook-vs-whatsapp-in-uganda/

Palmer, A. (2019, November 13). *Facebook removed 3.2 billion fake accounts between April and September, more than twice as many as last year*. Retrieved from Cnbc: https://www.cnbc.com/2019/11/13/facebook-removed-3point2-billion-fake-accounts-between-apr-and-sept.html

Parliament of Uganda. (2002, February). *THE ANTI-TERRORISM ACT.* Kampala: Goverment of Uganda.

Pastor, R., & Larsen, H. L. (2017). Scanning of Open Data for Detection of Emerging Organized Crime Threats—The ePOOLICE Project. *Using Open Data to Detect Organized Crime Threats*, 47-71.

Patton, D.-W. B. (2017). Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations. *Sage*, 1-10.

Peters , I. (2019, May 2). *The Ethical Challenges and Opportunities of Social Media Use*. Retrieved from Institute of Business Ethics: https://www.ibe.org.uk/resource/the-ethical-challenges-and-opportunities-of-social-media-use.html

Piest, J., Gramatikov, M., & Muller, S. (2016). *Justice Needs in Uganda - Legal problems in daily life.* Kampala: ACORD Uganda and the Justice Law and Order Sector (JLOS).

Pinem, A., Hidayanto, A., Sandhyaduhita, P., Donie, A. P., & Phusavat, K. (2019). Social Media Strategy Framework Formulation and Implementation: A Case Study of Indonesian Government Organization. *Electronic Government, an International Journal.*, 10-15.

Roger , R. S. (2016). *Current Cybersecurity Best Practices - a Clear and Present Danger to Privacy.* Sophia Antipolis: ERCIM EEIG.

Rohilla, J. (2017). Role of Web 2.0 Technology in Social Media Marketing. *International Journal of Advance Research, Ideas and Innovations in Technology*, 18-28.

Rukwengye, B. (2019, August 22). *Storm brews over UCC online and social media registration rules*. Retrieved from African Center for Media Excellence: https://acme-ug.org/2019/08/22/storm-brews-over-ucc-online-and-social-media-registration-rules/

Sadulski, D. (2018, March 9). *Why Social Media Plays an Important Role in Law Enforcement*. Retrieved from Public Safety: https://inpublicsafety.com/2018/03/why-social-media-plays-an-important-role-in-law-enforcement/#:~:text=Many%20police%20departments%20across%20the,the%20community%20about%20current%20events.&text=For%20example%2C%20police%20post%20crime,citizens%20to%20re

Sam , H. (2019, January 22). *Top 9 Benefits of Social Media for Your Business*. Retrieved from Search Engine Journal: https://www.searchenginejournal.com/social-media-business-benefits/286139/#close

Sandie , O. (2018). *Combatting Cybercrime : Tools and Capacity Building for Emerging Economies.* Washington, DC: The World Bank and the United Nations.

Schwind, J., & Bayliss, L. (2020). Social Media Use in Emergency Response to Natural Disasters: A Systematic Review With a Public Health Perspective. *Disaster Medicine and Public Health Preparedness*, 139-149.

Scott , J., & Bonomo, E. (2017). *Crime Prevention in the 21st Century, 2017 - Learning from the Offenders' Perspective on Crime Prevention.* Atlanta: ISBN : 978-3-319-27791-2.

Sekyewa, E. R. (2019, October 8). *Peace and human security*. Retrieved from Digital Survelliance: https://www.dandc.eu/en/article/what-ugandan-authorities-are-doing-limit-impact-online-opposition-voices

Serianu. (2018). *Uganda cyber security report 2017.* Kampala: Serianu Limited.

Shareen , I., & Tariq, R. S. (2018). Identity Theft and Social Media. *International Journal of Computer Science and Network Security*, 45-48.

Shariati, A. (2017). Preventing Crime and Violence. In A. Shariati, *Situational Crime Prevention* (pp. 261-268). Research Gate.

Shelly , B. (2019, August 22). *Facebook, Twitter and the Digital Disinformation Mess*. Retrieved from The Washington Post: https://www.washingtonpost.com/business/facebook-twitter-and-the-digital-disinformation-mess/2019/08/21/6f432520-c44e-11e9-8bf7-cde2d9e09055_story.html

Simon , K. (2019). *The global state of digital in 2019.* London: Hootsuite & We Are Social.

Smith, K. (2019, June 1). *53 Incredible Facebook Statistics and Facts*. Retrieved from Brandwatch: https://www.brandwatch.com/blog/facebook-statistics/

Snyder, P., Kanich, C., Doerfler, P., & McCoy, D. (2017). Fifteen minutes of unwanted fame: detecting and characterizing doxing. *Proceedings of the 2017 Internet Measurement Conference* (pp. 434-444). London, UK: AMC.

SocialNet. (2020). *Social Media Forensics & Investigations*. Retrieved from Shadow Dragon: https://shadowdragon.io/socialnet/

Soomro, T. a. (2019, 05 03). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Applied Computer Systems*, 9-17.

Sqoop. (2019, June). *Sqoop*. Retrieved June 05, 2020, from Sqoop: https://www.sqoop.co.ug/201908/news/two-remanded-over-martha-kay-leaked-nudes.html

Stalans, L. J., & Finn, M. A. (2016). Understanding How the Internet Facilitates Crime and Deviance. *An International Journal of Evidence-based Research, Policy, and Practice*, 501-508.

Stasi, M. L. (2019, June 9). *Social media platforms and content exposure: How to restore users' control*. Retrieved from Competition and Regulation in Network Industries: https://journals.sagepub.com/doi/full/10.1177/1783591719847545

Stephen , W. (2020, May 13). *IT Security Vulnerability vs Threat vs Risk: What are the Differences?* Retrieved from bmc blogs: https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/

Thaddeus, H. (2014, September 01). *The Challenges of Preventing and Prosecuting Social Media Crimes.* Retrieved September 01, 2014, from Digital Commons-Law Pace Review: http://digitalcommons.pace.edu/plr/vol35/iss1/4

Timothy, A. (2021, August 21). *Understanding the Judicial Jurisdiction in Cyber-Crime Cases in Uganda*. Retrieved from Uganda Association of Prosecutors: https://uap.ug/understanding-the-judicial-jurisdiction-in-cyber-crime-cases-in-uganda/

Tip411. (2020, February 27). *Anonymous tips: Arlington Launches New Safety Alert, Tip System*. Retrieved from Tip411: https://home.tip411.com/tag/anonymous-tips

Tiry, E., Oglesby, A., & Kim, K. (2019). *Social Media Guidebook for Law Enforcement Agencies.* Washington, DC: Urban Institite.

Tombul , F., & Cakar , B. (2015). Police Use of Technology to fight aganist Crime. *European Scientific Journal*, 286-288.

Tran, T., & Bar-Tur, Y. (2020, March 26). *Social Media in Government: Benefits, Challenges, and How it's Used*. Retrieved from Hootsuite: https://blog.hootsuite.com/social-media-government/

Tupper, C. D. (2011). Object and Object/Relational Databases. In *Data Architecture,* (pp. 369-383). Chicago: Morgan Kaufmann.

UCC. (2017, September 14). *warning against irresponsible use of social and electronic communication platforms .* Retrieved from Uganda Communications Commission: https://www.ucc.co.ug/files/downloads/UCC_PUBLIC_NOTICE_AGAINST_IRRESPONSIBLE_USE_OF_SOCIAL_MEDIA%2014-09-2017.pdf

UCC. (2019, November 13). *New Communications Regulations have been gazetted*. Retrieved from Uganda Communications Commission Blog: https://uccinfo.blog/2019/11/13/new-communications-regulations-have-been-gazzetted/

UCC. (2019, May 13). *Uganda Communications Commission Blog*. Retrieved from UCC - Cyber Security capacity building: https://uccinfo.blog/2019/05/13/ucc-cyber-security-capacity-building/

UCC. (2020). *Complaint Handling Procedure*. Retrieved from Uganda Communications Commission: https://www.ucc.co.ug/complaint-handling-procedure/

UCC. (2021). *UCC - Market Performance Report 1Q21.* Kampala: Uganda Communication Commission.

Uganda, G. o. (2019, February 25). *https://ulii.org/system/files/legislation/act/.* Retrieved from Uganda Legal Information Institute: https://ulii.org/system/files/legislation/act/2019/1/THE%20DATA%20PROTECTION%20AND%20PRIVACY%20BILL%20-%20ASSENTED.pdf

UNODC. (2020, February). *Cybersecurity and Cybercrime Prevention - Practical Applications and Measures*. Retrieved from UNODC: The Doha Declaration: Promoting a culture of lawfulness : http://www.unodc.org/e4j/en/cybercrime/module-9/key-issues/situational-crime-prevention.html

UPF. (2018, June 27). Retrieved September 27, 2020, from Uganda Police Force: https://www.upf.go.ug/igp-impersonator-arrested/

UPF. (2019). *Cyber Barometer*. Retrieved from Uganda Police Force: https://www.upf.go.ug/cyber-barometer/

UPF. (2019). *Uganda police annual crime report 2019.* Kampala: UPF.

URN. (2018, December 10). *Dr Stella Nyanzi case fails to take off*. Retrieved December 10, 2018, from The Observer: https://observer.ug/news/headlines/59440-dr-stella-nyanzi-case-fails-to-take-off

Webb, G. (2019, June 18). *The Rising Risk of Social Media-Enabled Cyber Crime to the Enterprise and How to Defend Against It*. Retrieved from Martech Series: https://martechseries.com/mts-insights/guest-authors/rising-risk-social-media-enabled-cybercrime-enterprise-defend/

Wikipedia. (2020, June 05). Retrieved June 05, 2020, from Wkipedia: https://en.wikipedia.org/wiki/Cyberbullying

Wilfred, K. (2018, June 27). *IGP Impersonator Arrested* . Retrieved from Uganda Police Force: https://www.upf.go.ug/igp-impersonator-arrested/

William , C. (2015, March 30). *Law Enforcement Agencies (and Corporate Security) Benefit from Social Media Monitoring*. Retrieved from Social Media Monitoring_Glean info: https://glean.info/law-enforcement-agencies-and-corporate-security-benefit-from-social-media-monitoring/

World Bank. (2016). *Combatting Cybercrime: Tools and Capcity Building for Emerging Economies.* Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

Wright-Myrie, D., Charley, C., Walker, K., & Brown, M. (2016). Using social media to warn potential victims, and encourage youths to denounce crime and violence in Jamaica. *International Journal of Sociology and Anthropology*, 77-81.

Zakari, Z., & Harun, S. A. (2020). Cyber Defamation Awareness Among Adolescent: Case Studies in One Private Institution. *Journal of Physics: Conference Series*, 25-27.