An Investigation into End Users' Factors Leading to iPredators' Social Engineering Attacks in Cyberspace

[1]Ambrose Kinyanjui Muchonjo, [2]Prof. Gregory Wanyembi, [3]Dr. Cyrus Makori

[1,2,3] Mount Kenya University

Abstract: **Organisations and individuals have greatly embraced Information and Communication Technologies (ICTs) in their operations in order to reap the best of benefits from systems, networks, software platforms, and even Internet services. However, by organisations and users relying heavily on ICTs and cyberspace, challenges arises to ensure that critical data, information and files belonging to organisations and users are securely protected against unauthorized access, theft, modification or destruction by the iPredators whether in their storage servers or while in transit between user accounts or web servers. To maintain strong information technology and information security posture, huge investments are made on acquiring equipments, systems and technologies to secure data and Information assets. In spite of this, users and organisations continue to suffer huge losses due to compromised systems and networks arising from loss of user data and sensitive information through unauthorized access by iPredators. To avoid the risks involved while attempting to break into the highly secured computer systems and networks, the iPredators prefer deceiving the end users into diverting access information to them (iPredators) in order to circumvent computer security and execute attacks against the targets. This paper therefore sought to investigate the digital and online habits or activities by end users that make them most susceptible to iPredators' social engineering attacks. The researcher adopted the quantitive research design. A purposive sampling technique was adopted to identify the respondents who were to participate in the study's survey. Online survey technique was adopted by the study using structured questionnaire.**

Keywords: **iPredators, social engineering, digital technology end users.**

1. BACKGROUND TO THE STUDY

The cyberspace and digital technologies have become critical tools and platforms in driving the day to day activities of the digital society. The way people interacts socially and politically, transacts business, shares information, files and data is greatly dependent on use of digital technologies and cyberspace by the digital society especially the internet as a resource and platform (Alexander,2012);(Nuccitelli,2014). However, the high dependence by the society on internet and other Information and Communication technologies (ICTs) also exposes the society to cyber security threats and risks such as social engineering attacks, cyberbullying, cyberstalking, cyber hate, cyber terrorism all of which are digital/ cyber attacks perpetrated by iPredators. An iPredator is defined by Nuccitelli (2014) to refer to any person(s), group or agent who engages in digital and/or cyber exploitation, victimization, stalking, theft and disparagement of targets using the digital technologies and the cyberspace. The cyberspace and digital technology employed by iPredators as weapons of attacks have therefore moved crimes to a whole new level both locally and internationally. With only a few clicks targeting the victims' computer systems, large amount of money get lost daily to cyber criminals without trace or even without armed theft in banking halls being involved (Paula, et al., 2015). Similar arguments are made by Wainaina and Wanzala (2017) who observed that close to sum of Ksh. 10 billion was lost in 2015 by public and private sectors in Kenya to iPredators through social engineering attacks targeted on individuals and institutions. This was further confirmed by a report by Kaspersky Security that established that 39.7% of organisations and users in Kenya were being targeted with social engineering attacks (Kaspersky, 2015). Similar observations were also made by Wainaina and Wanzala (2017) who reported how four blue chip banks lost Ksh. 130 millions in December 2016 to iPredators who compromised the institutions' networks and information systems via social engineering attacks.

1.1 Statement of Problem:

Organisations and users are relying heavily on digital technologies and cyberspace in their operations for economic, social or political endeavours. Along with this, challenges arises to ensure that critical data, information and files belonging to organisations and users are securely protected against unauthorized access, theft, modification or destruction by the iPredators attempting to execute social engineering attacks on targets to commit crime. The iPredators prefer deceiving the end users as the weakest security links to these systems into diverting access information in order to bleach computer security and the execute attacks (Paula, et al., 2015);(Blackhat, 2015). Moreover,the human vulnerabilities in targets exploited during social engineers attacks lacks a single technical means to eliminate them completely (Luo, Brody, Seazzu, & Burd, 2011);(Wendy, Brian, & David ,2016) and (Nabie & Paul, 2016). This study therefore concerned itself with investigating the digital and online habits or activities by end users that make them most susceptible to iPredators' social engineering attacks

1.2 Objective of the study:

To investigate the digital and online habits or activities by end users that makes them most susceptible to iPredators' social engineering attacks.

1.3 Research Question:

What are the digital and online habits or activities by end users that make them most susceptible to iPredators' social engineering attacks?

1.4 Rationale and Justification of the Study:

The public and private sectors in Kenya continues to suffer huge financial losses through cyber crimes most of which are executed through social engineering approaches by local iPredators as well as international cyber criminals. Cases has been reported where social engineering malware attacks and techniques are employed for defrauding incidences by iPredators while aided by rogue employees to compromise systems thereby enabling the execution of the attacks against the targets. For instance, Alex Mutunga was charged in a Kenyan court on 21st March 2017 for allegedly using social engineering malware attacks to infiltrate Kenya Revenues Authority's (KRA) systems thereby defrauding the institution close to Ksh. 4 billion supposedly by collaborating with insiders who aided him in the planting the malware into the KRA's systems to facilitate the attacks (Kakah, 2017).

In addition, similar attacks were confirmed by Wainaina and Wanzala (2017) who while reporting for Daily Nation, a local print media in Kenya narrated how a KRA staff by the name Kiprop Langat working in the ICT department had been acting as a contact person for cybercrime syndicate run by Calvin Ogalo. In related incidences, it was further reported that Langat assisted the local iPredator to plant a laptop running a malware in KRA's network chambers connecting the unauthorized device to port 11 thereby facilitating Ogalo to have unrestricted access to the KRA servers thereby enabling the iPredator to defraud the institution hundreds of millions of shillings through the executed attacks.

2. LITERATURE REVIEW

The literature review presents, the theoretical framework, conceptual framework as well as some illustrations of notable cases relating to socially engineered attacks that has been targeting the private and public sector in Kenya in the recent past.

2.1 Theoretical Framework:

This study drew its ideas from two theories. The study therefore adopted ideas from the Space Transition Theory of Cyber Crimes by Jaishankar (2008) as well as the Routine Activity Theory. The Space Transition Theory argues that people tend to behave contrary to their true self while on cyberspace as compared to when on the physical space (Jaishankar, 2008). The iPredators tend to behave in a manner that is uncharacteristic of their true self during the planning and execution of social engineering attacks on targets online or via digital platforms as compared to their true self online.

The Routine Activity Theory (RAT) observes that crime happens during daily routines within a given society where a suitable target lacking a capable guardian interacts with a motivated digital offender (Cohen & Felson, 1979). Furthermore, the offenders possessing sophisticated technical skills while planning the attacks against unwitting targets on cyberspace further motivates such offenders to commit the crimes with little likelihood of identification and apprehension (Hutchings & Hayess, 2009). Furthermore, increasing the users' awareness in regard to potential digital attacks may go a long way in building the capacity of targets to become capable guardians in efforts of deflecting social engineering on them.

2.2 Social Engineering Attacks and the iPredators:

Chantler and Broudhust (2006) explains social engineering as the technique whereby an attacker manipulates a human target to deceitfully gain 'access information' to computer and information systems enabling the offender to steal critical data to later use it for malicious reasons against the victims, for financial or for personal gratifications. Most social engineering attacks are characterised by unique dynamics and stages which a well informed target would be able to spot while armed with relevant cyber security training and skills. Luo, Brondy, Seazzu, and Burd (2011) identifies the common stages involved during most social engineering attacks process as illustrated in figure 1.

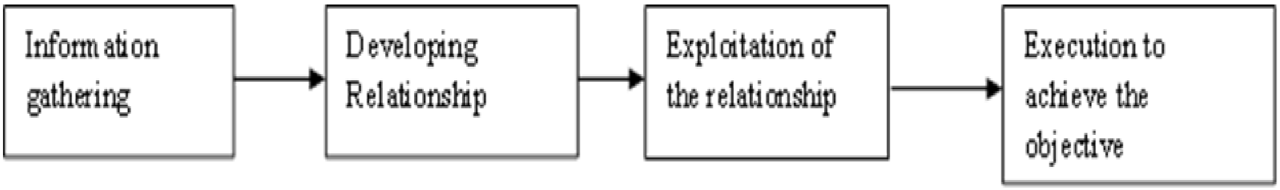

Information gathering
Developing Relationship
Exploitation of the relationship
Execution to achieve the objective

Figure 1: Social Engineering Process

Source: Luo, Brody, Seazzu, and Burd (2011)

2.3 Notable Incidences of Social engineering attacks in Kenya:

In Kenya, a number of iPredators' social engineering attacks related incidences had been reported to have affected the public and private sectors in Kenya in the recent past. Some of the notable cases and incidences relating to social engineering attacks reported as from the years 2014 to 2015 by Paula, et al. (2015) included: (1) 5000 Facebook users in Kenya faced with phishing attacks in December 2014, (2) The Ministry of devolution's system being compromised using stolen credentials facilitating fraudulent approval of tender requests resulting to huge loss of Kenyan taxpayers' money, (3) a Garissa county staff 's IFMIS password stolen and the systems used to authorize illegal payments, (4) Chinese cyber criminals arrested in Nairobi in possession of sophisticated hacking tools, and (5) electronic fraud involving an employee reported in one of local reputable bank. Furthermore, in the year 2017, the Daily Nation newspaper in Kenya reported how an established cybercrime syndicate had been operating in Kenya targeting individuals and institutions with cyber attacks leading to loss of hundreds of millions of shillings to the target victims. This was inclusive of: (1) One James Mwaniki who was reported to have been targeting Saccos with financial software infected with a 'back door' malware that allowed him to defraud the targets of millions of shillings, (2) a gang of local fraudsters reported of stealing teachers personal credentials allegedly by conspiring with corrupt Teachers Service commission staffs who reveals sensitive data belonging to victims thereby enabling the fraudsters to secure loans with local banks on account of their victims to tunes of Ksh. 2.8 million in Kiambu county alone and (3) the 4 billion shillings mega fraud scam from Kenya allegedly involving one Alex Mutunga who supposedly through executing machine based social engineering attacks was able to infiltrate Kenya Revenue Authority's (KRA's) system and commit the historital cybercrime in Kenya (Wainaina & Wanzala, 2017); (Kakah, 2017).

2.4 Conceptual Framework:

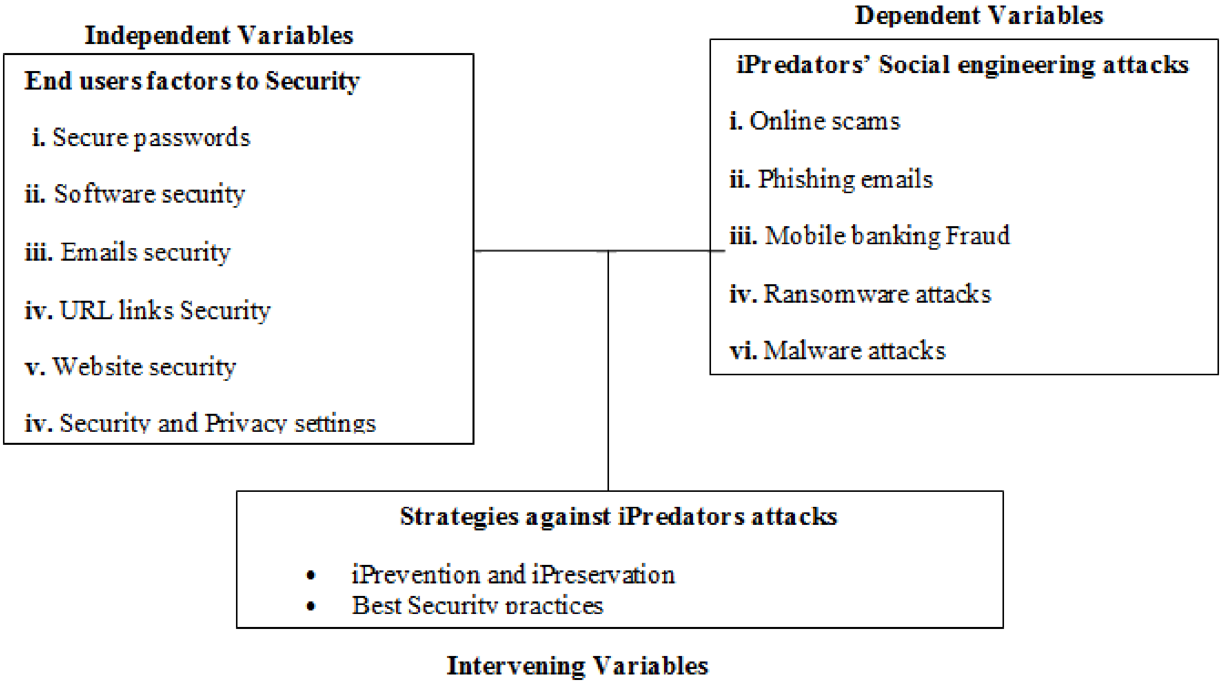


Figure 2: Conceptual Framework (Researcher, 2017)

2.5 iPredators and motivations behind iPredator Attacks:

As noted earlier, an iPredator is a person, group or nation that, directly or indirectly, engages in exploitation, victimization, coercion, stalking, theft or disparagement of others etc using ICTs. Accordingly, iPredators are driven by either of the following: deviant fantasies, desires for power and control, retribution, religious fanaticism, political reprisal, psychiatric illness, perceptual distortions, peer acceptance or personal and financial gain (Nuccitelli, 2014). Accordingly three criteria can be used to identify and qualify a potential iPredator including:

i. A self-awareness of causing harm to others, directly or indirectly, using ICT.

ii. The usages of ICT to obtain, tamper with, exchange and deliver harmful information.

iii. A general understanding of Cyberstealth while engaging in deviant activities such as profiling, identifying, locating, and stalking or engaging a target.

2.6 The preferred targets of iPredators:

According to Nuccitelli (2013) iPredators through practice and learning are able to develop a skill to experience an intuition to know what ICT user is very likely to become a successful target. Variety of potential target's characteristics can be investigated by the iPredator while profiling, stalking or casing a successful target to victimize (Nuccitelli, iPredator Bridge, 2013). Accordingly, the characteristics targets may inform an iPredator on the easiest target to victimize online:

i. The amount of personal information and frequencies of contact information a potential target discloses using ICT.

ii. The content of the information a potential target discloses using ICT and the amount of time he/she spends online.

iii. The lack of ICT safety measures a potential target institutes online.

iv. The potential targets willingness to discuss sensitive issues including sexual topics, financial information, their physical location, parental or adult monitoring of their ICT activities, experiences of distress at home, work, school and interpersonal or intrapersonal issues.

v. The type of information a potential target discloses on their social networking profiles and chartrooms (i.e.WhatsApp, Twitter, Facebook, MySpace, MyYearbook, LinkedIn etc.).

vi. The pattern of “likes” and “dislikes” an ICT user discloses on their social networking site profiles.

vii. Images and/or videos showing the potential target’s economic status, the layout of their residence or their material objects they or their loved ones own.

Accordingly, Nuccitelli (2013) observes that the prime targets sought by iPredators mostly are ICT users who lacking: ICT safety strategies and technology, heightened levels of awareness online, comprehensive digital citizenship practices and C3 plans.

3. RESEARCH METHODOLOGY

3.1 Research Design:

This study adopted a Quantitive research design. Quantitive research is defined by Aliaga and Gunderson (2006) to refer to a research design that is meant to lead to explanation of phenomena through collection of quantitive data that are to be analyzed numerically using statistical tool. Consequently, quantitive research tends to adopt descriptive research approach, explanatory as well as exploratory research approaches. These research approaches was expected to lead to creation of quantitive data.

3.2 Research Technique:

Research technique is defined by Kothari (2004) to refer to the instruments the researcher employs in carrying out research operations such as recording data, techniques of processing data as well as making observations. In this study, the researcher adopted the online survey technique whereby structured online questionnaire was prepared using Google forms and administered online to the respondents. The respondents participated in the survey online sending back the filled survey questionnaire to the researcher via their personal emails. Furthermore, relevant secondary data in regard to literature review was obtained through desktop study technique.

3.3 Target Population:

Cooper and Schindler (2000) defined the term target population to refer to total collection of elements about which findings and conclusions regarding a given research study are based on. This study drew its target population from the Kenyan public and private sectors digital technology end users.

3.4 Sample Size:

A sample size is defined by Bryman (2008) to refer to the portion of the population that has been selected by a researcher to lead to a given investigation. The total number of people that formed technology end users within the Kenyan public and private sectors was fairly unknown and whose actual size was thought to be relatively very large. Owing to this, the researcher adopted a formula suggested by Scott (2013) to determine an appropriate sample size for the study since it was argued that this particular formula fits well in research studies based on survey techniques. This formula proceeded as follows:

$\textit{Sample Size} = (\textit{Z-score})^2 \times \textit{StdDev} \times (1\text{-}\textit{StdDev}) / (\textit{margin of error})^2$

Z-score corresponds to researcher’s preferred confidence level. The most common confidence levels are usually 90%, 95%, and 99% confidence levels and whose Z scores are as follows:

90% confidence level, Z Score = 1.645,

95% confidence level, Z Score = 1.96 and,

for *99% confidence level* = **2.326**

StdDev refers to the Standard Deviation. A *StdDev of 0*.5 tend to offer a value that can lead to sample size that just sufficient and appropriate. The *margin of error* is a measure of the error by which the sample mean is allowed to be lower or above the population mean by the researcher mainly ranging between 1% to 10% (Scott, 2013)

In this study, a 99% confidence level was chosen by the researcher with a 0.5 standard deviation and a margin of error of +/- 7%. Consequently the sample size for the study evaluated as:

$\textit{Sample size} = ((2.326)^2 \times 0.5(0.5)) / (0.07)^2$

= (5.4103 × 0 .25) /0 .0049

=276.041

Therefore, ***276*** respondents were required for this study.

3.5 Sampling Technique:

This study adopted a purposive sampling technique. This technique was chosen in order to increase transferability as argued by (Teddlie & Fen Yu, 2007). Purposive sampling also allowed the researcher to obtain greater depth of information from a smaller number of carefully selected cases (Patton, 2002). Furthermore, purposive sampling technique also helped the researcher in selecting the respondents based on specific purposes they would serve in answering the research questions or certain unique information they were likely to offer to the researcher (Teddlie & Fen Yu, 2007); choices (Maxwell, 1997).

3.6 Description of Research Instrument:

In this study, the researcher used online survey technique using structured questionnaires to collect the primary data. The online questionnaires were administered through emails to the respondent's accounts or through URL links sent to the respondent's Facebook's Messenger application platforms or to the respondents' Whatsapp inboxes. This technique helped the researcher in obtaining data from respondents faster, cheaply as well as allowing the respondents to respond to research question at their own convenient time. Furthermore the researcher was able overcome geographical barrier that could otherwise hinder the response rates from the respondents.

3.7 Validity and Reliability Online Questionnaire:

According to Wampold and Kivlighan (2008) pilot testing may be used to measure the validity and reliability of a research tool. Consequently the researcher piloted the study's questionnaire for three weeks whereby the responses were checked for reliability and validity. The validity of the questionnaire was further strengthened by improving the quality of questions in the questionnaire based on the feedback the researcher received online from the respondents. A response rate of 54% was achieved during the piloting stage. To establish the reliability of the questionnaire, internal consistency among the questions in the research tool was examined to ensure that they derived similar responses from the respondents in terms of how they responded to certain questions during the piloting study as compared to how they responded to same questions in the main study's survey. The responses to questions in the survey during the pilot study by purposefully selected respondents as compared to their responses during the main study survey revealed consistencies confirming the reliability of the questionnaire used.

3.8 Ethical Considerations:

The research followed the ethical principles that in regard to research codes of ethics seeking to ensure that the quality and integrity of the research was upheld while also seeking to protect respondents from any potential unethical practices. The respondents were informed about the reasons for the research. The study in particular followed the codes of ethics as stipulated by the National Commission for Science Technology and Innovation (NACOSTI). In addition, the principle of voluntary participation and informed consent at free will was respected with adhered to ensure that due confidentiality and anonymity of the research respondents were protected.

4. DATA PRESENTATION, ANALYSIS, AND DISCUSSION

This section involved the presentation and analysis of research data. The results of analysis of the research data was presented in form of percentages, bar graphs, and Pie Charts.

4.1Data Presentation and Analysis:

According to Cooper and Schindler (2000) data analysis as a term to refer to the reduction of accumulated data to a manageable size, development of data summaries, as well as looking for patterns by using statistical tools. Analysis of data and the presentation the survey's data for this study was done using Google sheets app and Microsoft Excel application spreadsheet. Lastly, data summaries were presented in form of percentages, figures, pie charts and bar graphs. A descriptive analytical statics was therefore adopted. 270 online questionnaires were administered to the respondents with 225 respondents giving back valid responses. The response rate for the study was therefore 83.33 %. The outcome of the study's online survey was captured as illustrated in the sections 4.2 to 4.12.

4.1.1 Gender of respondents:

Based on the results from data collected, 158 males participated in the survey representing 69.9% of the respondents. The females who participated in the survey were 68 representing 30.1% of the respondents. This is reflected by figure 3.

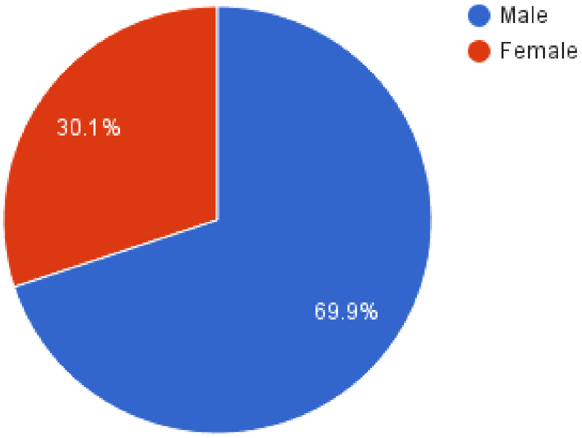


Figure 2: Respondent's Age

4.1.2 Geographical Location of Respondents

The distribution of respondents in the survey was a reflection of the eight administrative provinces in the republic of Kenya. Nairobi metropolitan and Central Kenya registered the majority of respondents in terms of numbers. To determine the province from which the respondent participated in survey from, the researcher considered the current town of residence of the respondent. This is illustrated by figure 4.

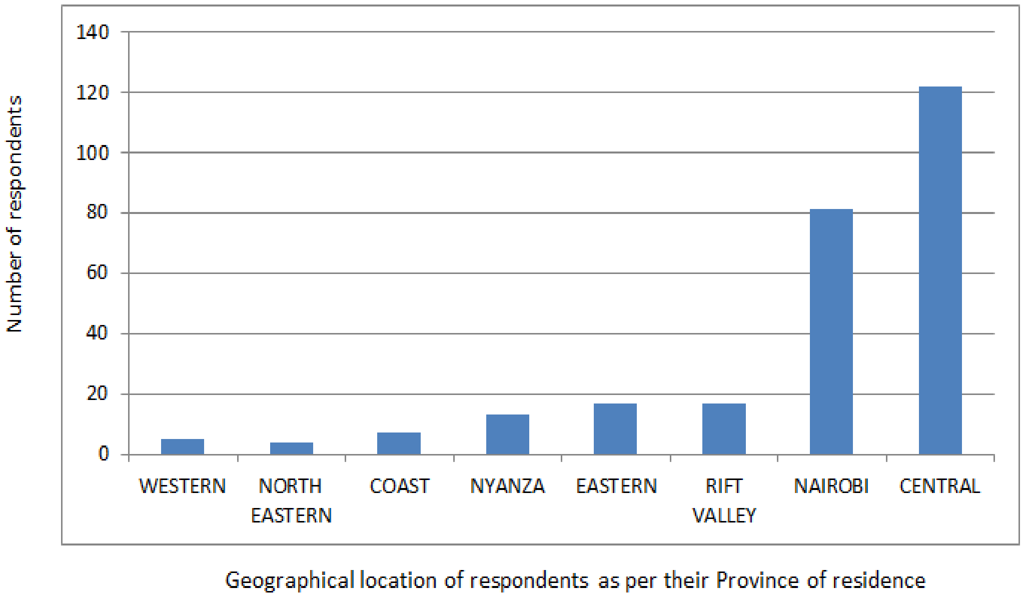


Figure 3: Location of the respondents

4.1.3 Distribution of respondents by age:

The respondents whose ages ranged between 25-35 years were majority participants in the survey with their number contributing to 58.8% of total number of respondents. Those between ages 21-25 represented 17% of total number of respondents while those between 40-55 years represented 11.7% of the number. The rest of age brackets had a representation of less than 10% of total number of respondents. From this statistics it is clear that majority of technology end users in Kenya lies between ages 21-40 years representing 85% of the users who normally active in online and digital activities. This illustrated by the figure 5.

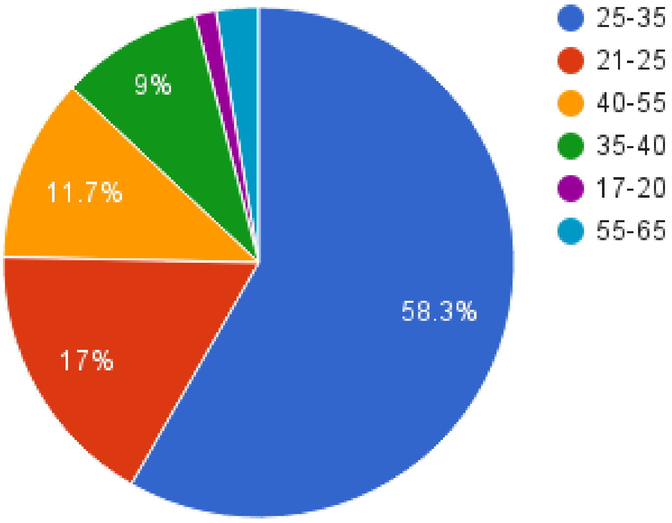
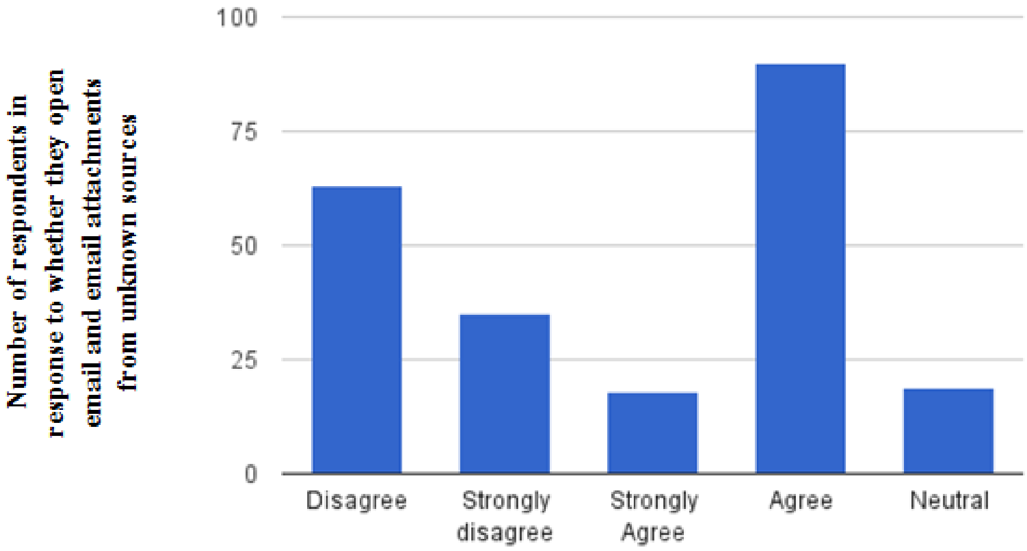


Figure 4: Distribution of respondents by age

4.1.4 Respondents and the email security:

Seeking to establish whether the respondents usually open emails and emails attachment sent to from unknown sources, 15.6% of the respondents strongly disagreed with the statement while 28% of the disagreed with the statement. In addition, 7.5% of the respondents remained neutral to the statement. Therefore, those who either strongly agreed or agreed that they usually open emails and email attachments from unknown sources represented 48% of the respondents. The figure 6 illustrates this.



.

Figure 5: Respondents and the security of email accounts

4.1.5 Respondents and how they manage passwords:

Seeking to establish whether the respondents have ever shared their user accounts passwords with others, 6.6% of the respondents strongly agreed with the statement and 35.4% of the respondents agreed with the statement. 48% of the respondents either strongly disagreed or disagreed with the statement. Only less than 10% of the respondents remained neutral to the statement. Figure 7 illustrates this.

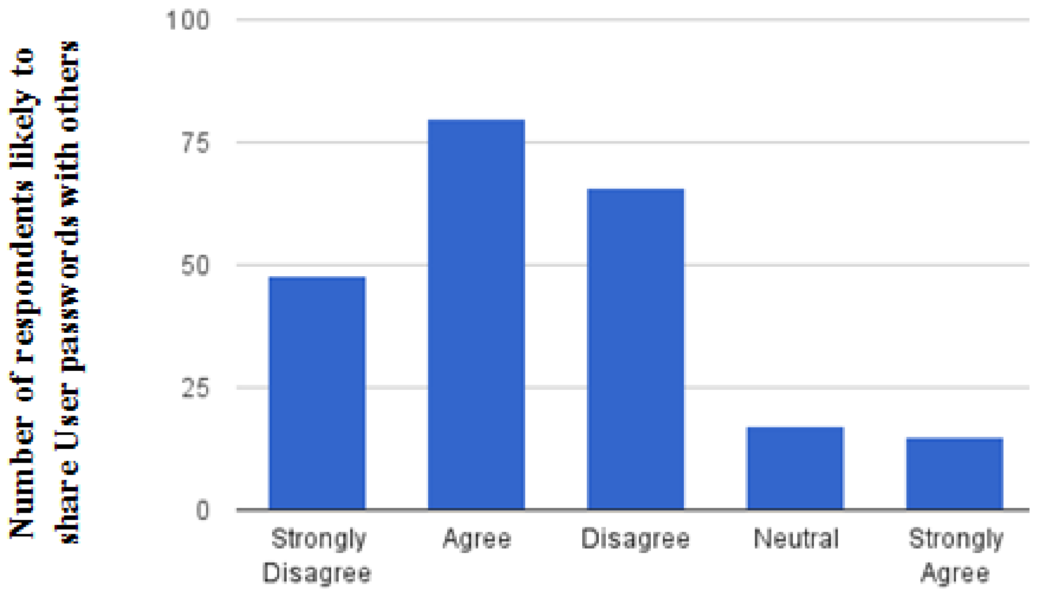


Figure 6: Respondents and how they manage user account passwords

4.1.6 Respondents and how they handle URL links:

Seeking to establish whether the respondents ever clicks on URL links sent even when they don't know their source, 9% of the respondents strongly agreed with the statement with 46.4% of the respondents agreeing with the statement. Only 7.7% of the respondents remained neutral to the statement. The figure 8 illustrates this.

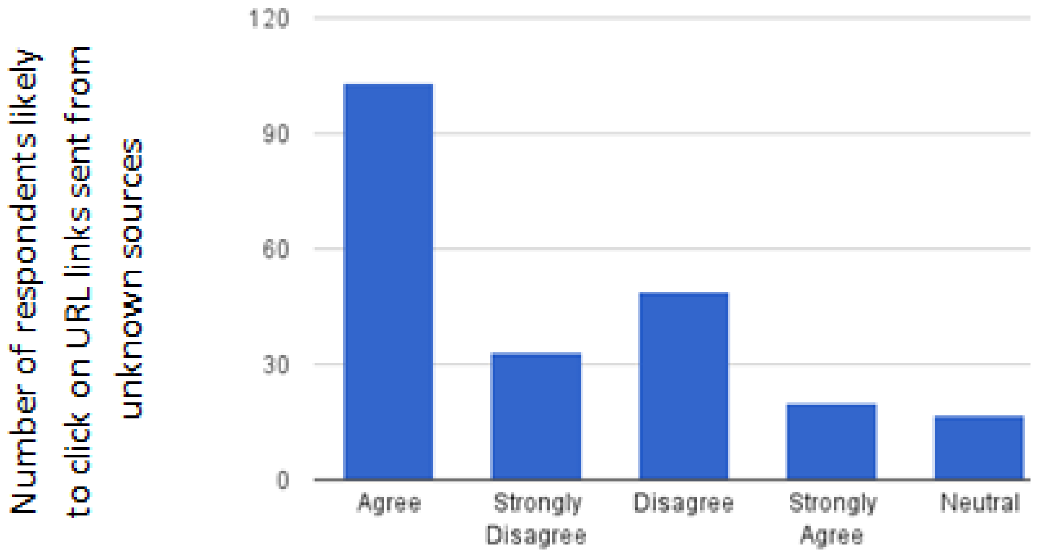


Figure 7: Whether respondents clicks on suspicious URL links

4.1.7 Respondents and handling of Spam emails:

Seeking to establish whether the respondents ever open or respond to spam emails the data results revealed that 4% of the respondents strongly agreed that they often open or respond to spam emails. 24.1% of the respondents also agreed with the statement. 59% of the respondents either strongly disagreed or disagreed with the statement with only 12.9% of the respondents remaining neutral to the statement. The figure 9 illustrates this.

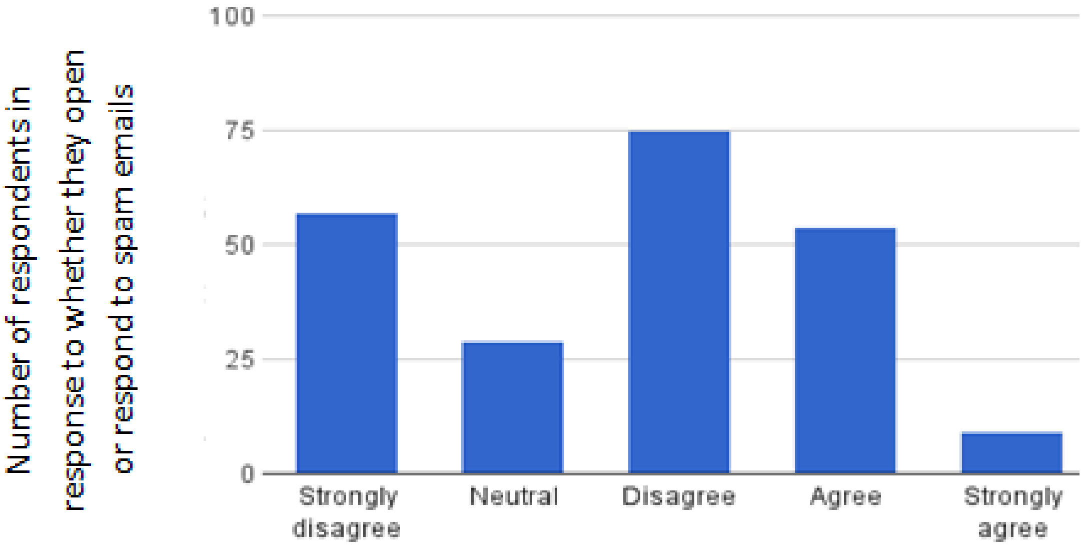


Figure 8: How respondents handle spam emails

4.1.8 Handling of Pop-Ups by respondents on their user accounts

Posed with a question whether the respondents ever enters personal credentials on pop-ups appearing on their platforms and requesting them to authenticate to have their app improved or to have a technical hitch with their accounts fixed, 2.2% of the respondents strongly agreed with the statement while 24% of them agreed with the statement. The survey also revealed that 71.4% of the respondents either strongly disagreed or disagreed with the statement. 12.4% of the respondents chose to remain neutral to the statement as illustrated by figure 10.

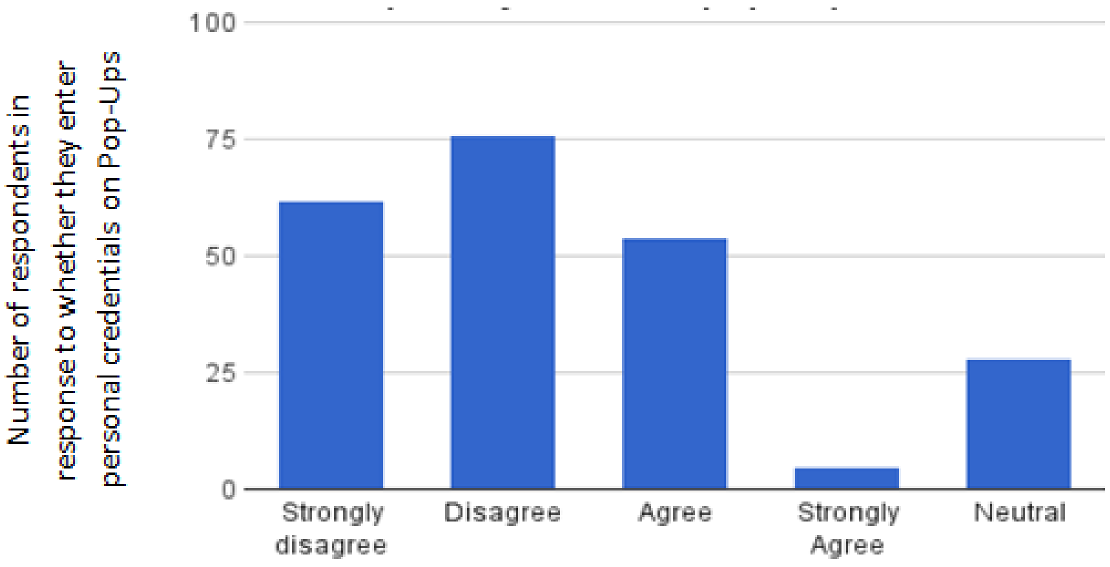


Figure 9: How Respondents handle personal credentials

4.1.9 Respondents and use of email filtering software

Requested to indicate whether they posses or make use of email filtering software, 7.1% of the respondents strongly agreed with the statement with 23.2% of the respondents also agreeing with the statement. 54.56% of respondents either strongly disagreed or disagreed with the statement of ever possessing or making use of email filtering software. 34 15.2% of the respondents chose to remain neutral to the statement. The figure 11 illustrates this.

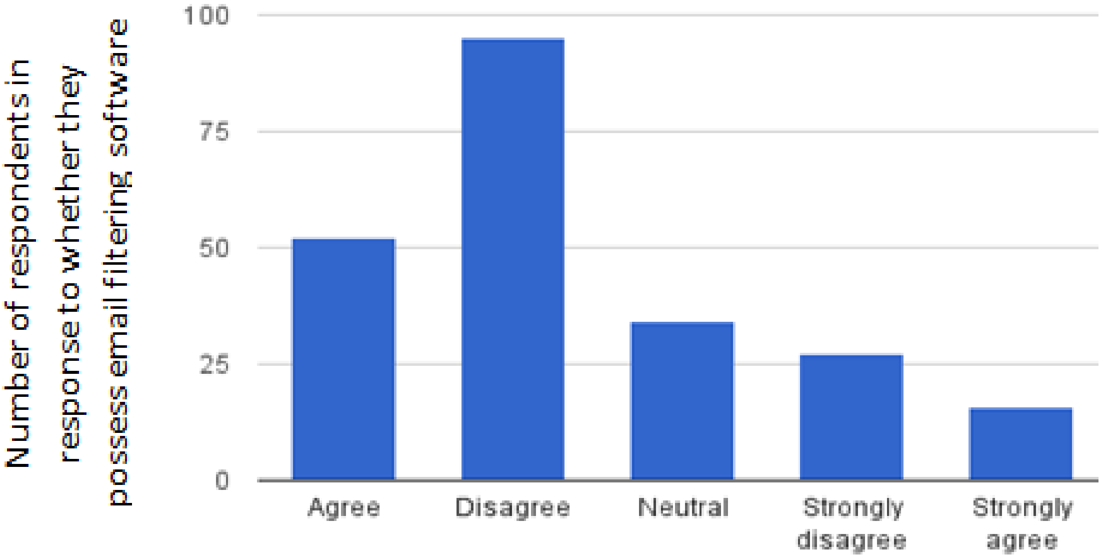


Figure 10: Whether respondents use email filtering software

4.1.10 Respondents and use of Patched and updated Programs software:

Seeking to establish whether the respondents always use patched and updated software programs or run updated antivirus software definition in all their devices, 16.5% of the respondents strongly agreed with the statement while 31.3% of them agreed with the statement. 29% of the respondents either strongly disagreed or disagreed with the statement. 23.2% of the respondents chose to remain neutral to the statement. This is illustrated by figure 12.

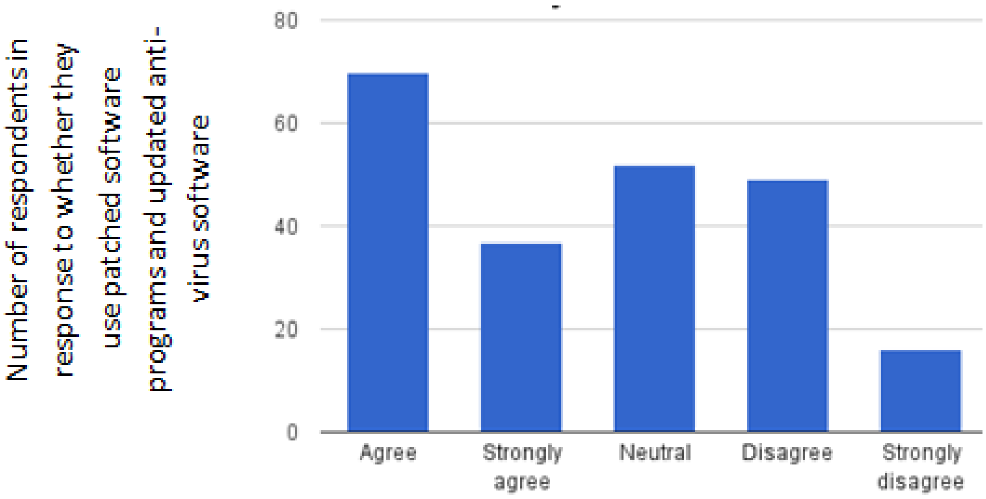


Figure 11: Whether the respondents use patched and updated software programs

4.1.11 Respondents Diligence in Observing Website Platform Security

Posed with a question to establish whether the respondents are often keen checking out for the security lock on browsers they are surfing from, 14.7% of the respondents strongly agreed with the statement with 24% of the respondents also agreeing with the statement. 43.5% of the respondents either strongly disagreed or disagreed with the statement of always checking out for the security lock on browsers before transacting online. 17.8% of the users chose to remain neutral to the statement. This is illustrated by figure 13.

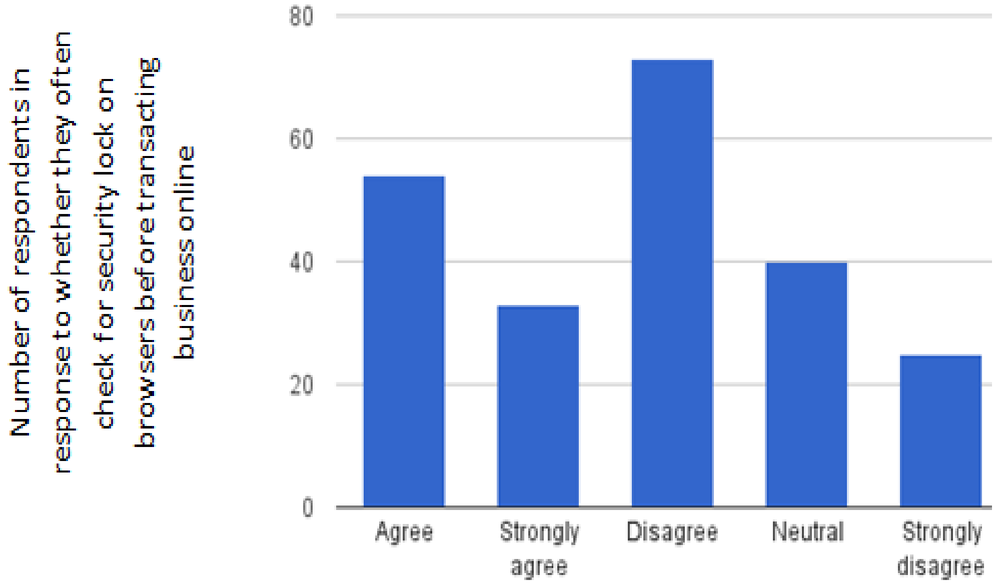


Figure 12: Respondents keenness on in checking for security locks on websites

4.1.12 Respondents and how they manages security and privacy settings

Seeking to establish whether the respondents properly manage the security and privacy settings on their digital devices and apps to secure their personal information, 61.8% of the respondents either strongly agreed or agreed that they manage privacy and security settings properly with 26.3% of the respondents either strongly disagreeing or disagreeing with the statement. Only 12% of the respondents chose to remain neutral to the statement. This is illustrated by figure 14.

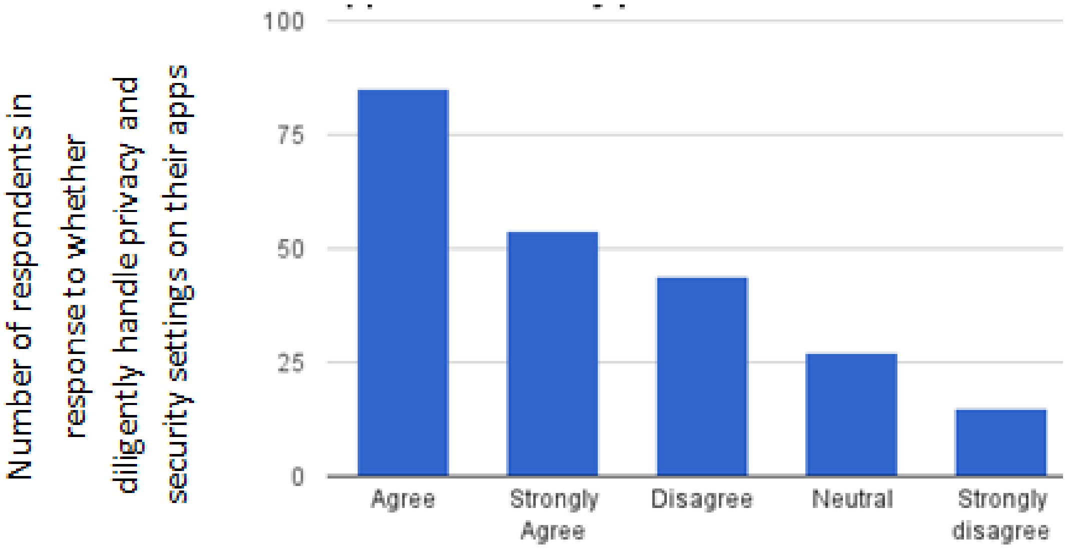


Figure 13: Whether respondents manage privacy and security settings properly

4.1.13 Respondents and online scam attacks

Posed with a question whether they have ever been faced with online scam, 37 respondents representing 16.4% of users strongly agreed with the statement that they have ever been faced with online scam while 109 respondents representing 48.2% of users agreed with the statement. Those who strongly disagreed with the statement were 26 respondents representing 11.5% users and those who disagreed with the statement were 30 representing 13.3% users. Those who chose to remain neutral were 24 respondents representing 10.6% users as illustrated by figure 15.

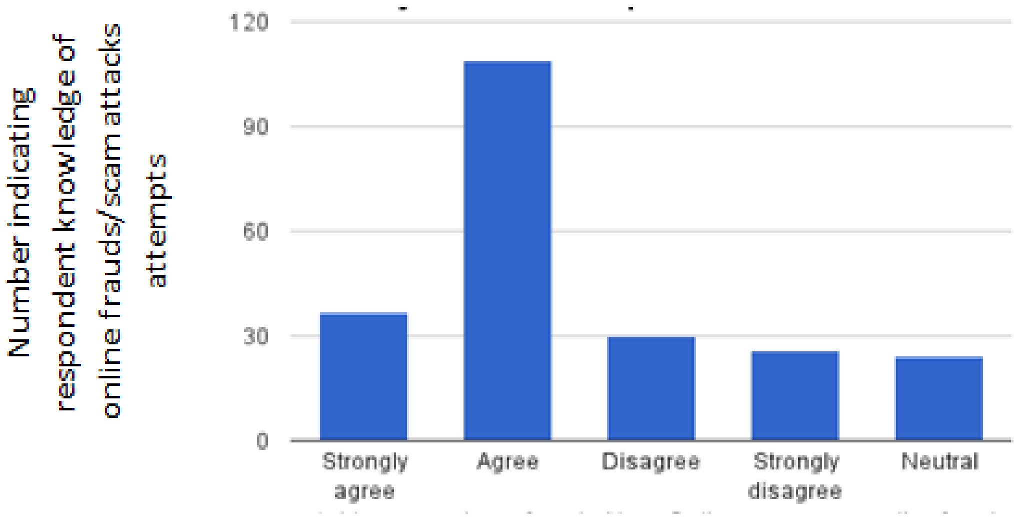


Figure 14: Respondents' awareness on online scams

4.1.14 Respondents and Mobile banking fraud attempts:

Posed with statement to establish whether they have ever been faced with attempt of mobile money banking fraud such as being conned of money from my M-Pesa or Airtel money accounts and the like, 92 respondents representing 40.7% of users agreed with the statement that they have ever been faced with a form of mobile banking fraud while 66 respondents representing 29.2% of users strongly agreed with the statement. Those who strongly disagreed with the statement were 22 respondents representing 9.7% of the users while those who disagreed with the statement were 30 representing 13.3% of the users. 16 respondents representing 7.1% of users remained neutral to the statement as illustrated by the figure 16.

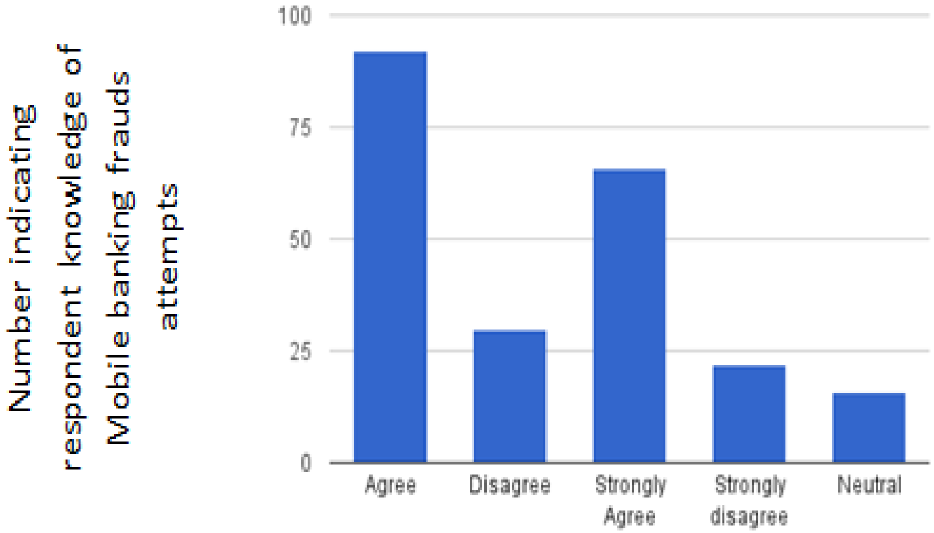


Figure 15: Respondents' awareness of Mobile banking frauds

4.1.15 Respondents and Malware attacks on their devices:

Requested to establish whether they have ever been faced with viruses, worms and Trojan attacks on their devices, 85 respondents representing 37.9% of the users strongly agreed with the statement that they have been faced with a form of such attacks while 108 respondents representing 42.8% of users agreed with the statement. Those who disagreed with the statement were 8 respondents representing only 3.6% of the users while those who strongly disagreed with the statement were 12 representing 5.4% of the users. Those who chose to be neutral to the statement were 11 representing 4.9% of the users as illustrated by figure 17.

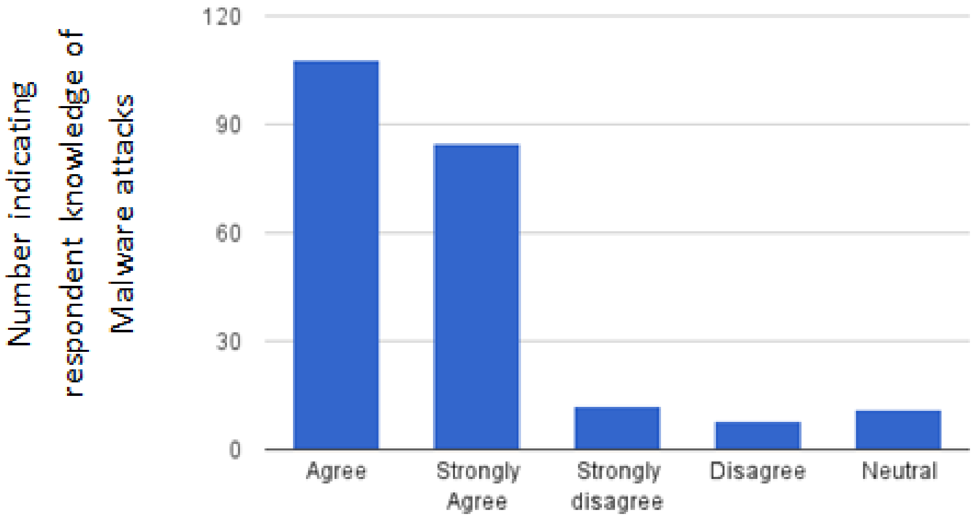


Figure 16: Respondents' awareness of malware attacks

4.1.16 Respondents and Phishing Attacks:

Requested to establish whether they have any knowledge of the workers or clients ever been faced with phishing attacks in their organisations, 27 respondents representing 12.1% of the users strongly agreed with the statement that they have ever witnessed clients or workers in their organisations been faced with Phishing attacks while 66 respondents representing 29.6% of users agreed with the statement. Those who disagreed with the statement were 45 respondents representing only 20.2% of the users while those who strongly disagreed with the statement were 27 representing 12.1% of the users. Those who chose to be neutral to the statement were 85 representing 38.1% of the users as illustrated by figure 18.

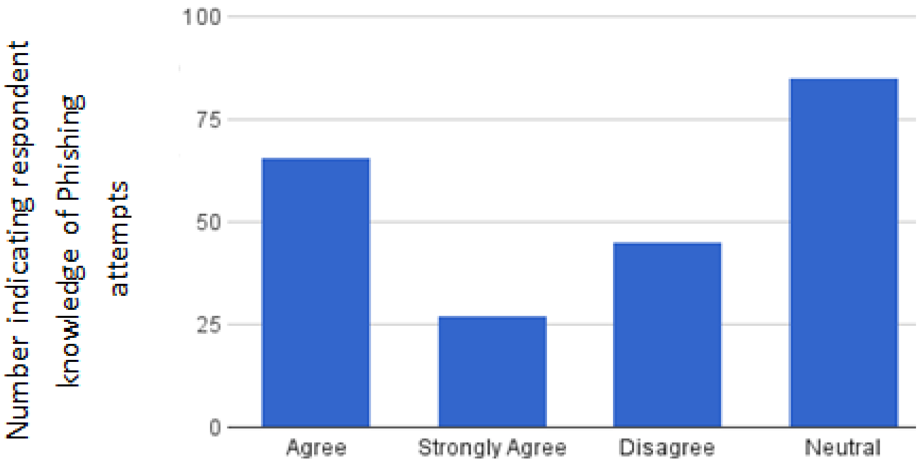


Figure 17: Respondents' awareness on Phishing attacks

4.1.17 Respondents and the Ransomware attacks attempts

Requested to establish whether they have ever been faced with Ransomware attacks, 12 respondents representing 5.3% of the users strongly agreed with the statement that they have been faced with such attacks while 46 respondents representing 20.4% of users agreed with the statement. Those who disagreed with the statement were 49 respondents representing only 21.7% of the users while those who strongly disagreed with the statement were 34 representing 15% of the users. Those who chose to remain neutral to the statement were 85 representing 37.6% of the users as illustrated by figure 19.

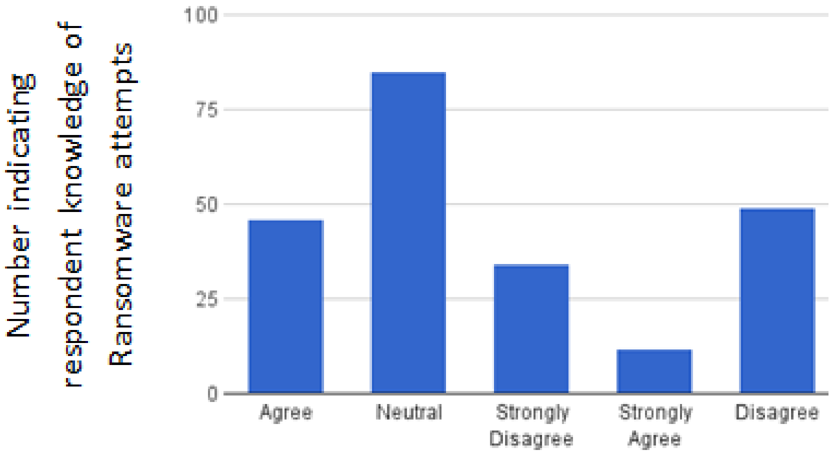


Figure 18: Respondents' awareness of Ransomware attacks

4.2. Respondents and the Sextotion attempts:

Posed with a statement intended to establish whether they ever have been faced with Sextotion attack, 41 respondents representing 18.2% of the users strongly agreed with the statement that they have been faced with an attempt of such attacks while 79 respondents representing 35.1% of users agreed with the statement. Those who disagreed with the statement were 44 respondents representing only 19.6% of the users while those who strongly disagreed with the statement were 32 representing 14.2% of the users. Those who chose to remain neutral to the statement were 29 representing only 14.2% of the users. This is illustrated by figure 20.

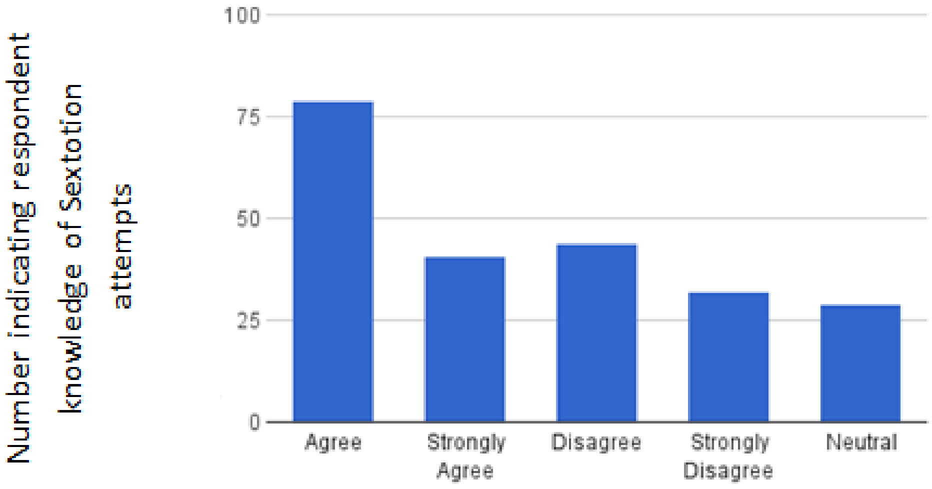


Figure 19: Respondent's awareness on Sextotion attacks

4.3 Discussion:

This section discusses the results of analyzed data collected through the online survey to illustrate how the end users online activities contributes to likelihood of them being faced with potential iPredators' social engineering attacks.

First, it emerged from the study that 48% of the respondents indeed do opens emails and email attachments from unknown sources. It also emerged that 43.6% of respondents are cautious not to open suspicious email and email attachments from unknown sources. This indicates that quite higher number of users who are not diligent in handling emails is likely to be faced with social engineering attacks executed via emails carrying infected files or folders than those users who would rather avoid opening such emails and emailing attachments. Furthermore, the study revealed that 28.1% of the respondents often open Spam mails from their email accounts against 58.9% of the users who would not. The targets who present themselves as lacking skills of instituting email security best practices are the prime choices the iPredators target with social engineering attacks, phishing attacks and other forms online scams.

Furthermore, the study also established that 42% of the users diligently manage their user accounts passwords securely. In contrast, 50.4% of users did not institute the use of secure passwords on their devices as a way of discouraging potential digital intrusion or attacks by the iPredators. This indicates that quite a large number of users due to lack of digital and cyber security skills in regard to use of secure passwords are likely to be exposed to risk of iPredators' social engineering attempts on their user accounts.

Regarding to how respondents handle URLs on their platforms, the study established only 37% of the respondents who remain cautious to avoid clicking on URLs from unknown sources against 55.4% of respondents who often click on URLs links even from unverified sources putting themselves at high risk of potentially being redirected to social engineering and scams websites making them most susceptible to fall prey of iPredators' social engineering attacks.

In regard to how the respondents handles personal credentials especially while required to login using pop-up on their platforms, the study revealed that 26.2% of the users a are likely to enter their personal credentials on such pop-ups even when they have not verified that that such requests are coming from authentic and genuine sources as compared to 61.4% of the users who would take caution not to. The iPredators are fond of using pop windows to trick unsuspecting users to enter their personal credentials mostly using fake websites eventually stealing such credentials to compromise the accounts of their victims thereby successfully executing social engineering attacks against the targets. Furthermore, the study also established that 43.5% of the users are usually not cautious to confirm the security lock on website they are surfing from potentially exposing themselves to risk of falling prey of iPredators' social engineering attacks. Website security is a critical cybersecurity skill to be observed by all end users to help spot and avoid potential iPredators' social engineering sites.

Furthermore, the study established that only 30.3% of the respondents use or possessed email filtering software against 54.56% of the respondents who never used email filtering software on their email accounts. Email filtering software is essential in detecting spam emails which are choice techniques for iPredators in executing social engineering attacks against target. This implies that roughly 55% of users who don't use email filtering software in their user accounts potentially put such users at high risks of been targeted with spam emails and email attachments carrying malware files potentially putting them at risks of Phishing attacks and Malware attacks.

In addition, the study revealed that roughly 29% of the users are never diligent in using patched and updated software programs whether such software are operating systems, application software or anti-virus definition software. Failure of users to diligently use patched and updated program software potentially create security vulnerabilities that can be exploited by iPredators seeking to execute social engineering attacks against them.

Finally, the study revealed that 61.8% of the users properly manage the privacy and security settings on their devices and apps to discourage unauthorized access of their personal credentials by iPredators. The study further established that 26.3% of the respondents are not aware of the importance of managing the security and privacy settings on their devices or apps as way discouraging unauthorized access into their devices or information systems by iPredators bent on attempting attacks on them. This potentially put such users at risks of falling victims of iPredators' social engineering attacks attempts.

Lastly, owing to end users' digital habits or activities that presented them as lacking iPrevention and iPreservation skills against iPredators' social engineering attacks due to their poor or negligence to observe cyber and digital security practices and ethics while interacting with ICTs, the study established that: 64.4 % of the users at one point had ever been victims of online scams, 69.9% of the users had been faced with mobile banking fraud, 86.1% of the users also having ever been faced with Malware social engineering attacks, with 41% of the users reporting to have been ever been faced with attempts of phishing attacks, 25.8% of the users having being faced with Ransomware attack and 53.3% of the users having been faced or witnessed attempts of some form of Sextotion attacks during their online activities.

4.4 Proposing a digital defense mechanism against iPredators' social engineering attacks in cyberspace:

The iPredators employs various Social engineering techniques or approaches while planning and executing attacks against targets and therefore the way the target handles digital technologies or behaves online becomes critical in deflecting possible attacks. To shield themselves from potential attacks by the iPredators, this paper adopts Nuccitelli (2013) for digital self defense against potential iPredators' social engineering attacks.

Under the concept of iPrevention every digital and cyber user must remain conscious of the need to observe cyber ethics, cybersafety, and cybersecurity (C3) practices to ensure their personal digital safety and the security of their digital assets while in realm of cyberspace. By diligently observing iPrevention, the target actually is involved in efforts of denying the iPredator(s) the benefit or reward that they would have gained by successfully executing the attacks. Moreover, through iPrevention, the target(s) tends to increase risks on part of the iPredator thereby discouraging the iPredator activities in the cyberspace.

On the other hand, iPreservation as attacks deflection mechanism simply implies that all digital and cyber users diligently ascribe to the practice of instituting iPrevention against potential cyber attacks including social engineering attacks. According to Nuccitelli (2013) iPreservation is an innate state of self-survival manifesting in end users whenever interacting via digital devices or participating in cyber activities for social, business purposes or otherwise. Consequently, the practice of iPreservation therefore serve to trigger appropriate internal responses in human targets prompting them to act accordingly and appropriately to shield themselves from any possible digital or cyber attacks such as the iPredators' social engineering attacks.

The practice of an end user instituting iPreservation may involve the targets asking key questions to suspected social engineer that only authentic personnel in the given organisation would respond to correctly and accurately. As a result, this will prevent an iPredator disguising as an authority to juniors or end users deceiving them to give out access information to systems that can enable the attacks. For instance, since the social engineers have tendency to cloud targets with too much information or triggering anxiety in them in efforts to make them have little time to think logically or challenge the demand of the iPredator, a target who is instituting iPreservation is likely to opt to uphold to a call back policy or hold by call policy with the suspected iPredator. Through such an iPreservation strategy, the end user will have enough time to think logically and even consult with other personnel regarding the suspected security incidence relating to social engineering attacks. Should the incidence be confirmed a case of attempted social engineering attack, the target would have responded appropriately thereby successfully deflecting the attack.

Digital self defense therefore results from users carefully observing sustained levels of iPrevention and iPreservation practices that require all end users to diligently observe security best practices and controls for deflecting attacks at personal level. These controls and best security practices may include: (1) ensuring that they use strong passwords to protect their devices and software applications, (2) Regularly having their system and application software programs patched and updated regularly, (3) Using updated anti-virus software to scan, detect and clean their devices from malware attacks, (4) quickly reporting abuse for instance online banking fraud attacks, mobile banking fraud attacks, phishing attempt to authorities (5) Diligently handling privacy and security settings on all apps and their devices to discourage unauthorized access by social engineers, (6) Using disposable email accounts, concealing email address, avoiding opening emails and email attachments from suspicious and unknown sources, using email filters and firewalls to prevent unauthorized access to personal data through infected URLs, files attachments or Spam mails and (7) Due diligent while handling USB drives especially when they are from unknown or unauthorized sources since social engineers could have loaded them with infected files meant to compromises the organisation's information infrastructure.

5. CONCLUSION

The study established that a number of digital and cyber activities by end users may contribute to likelihood of exposing them to iPredators' social engineering attacks. The study identified the following factors as the one that contribute greatly to end users exposing themselves to social engineering attacks:

i. Failure to institute secure passwords and poor login procedures

ii. Poor observance of software security

iii. Poor handling of URL links, email and email attachments

iv. Failure to observe website security practices

v. Poor management of security and privacy settings on apps and computing devices

The most common types or forms of social engineering targeting private and public sector as revealed by the study were found to include among other attacks: online scams, phishing attacks, mobile banking fraud, Ransomware attacks and Malware attacks.

6. RECOMMENDATION

The researcher recommends that further study need to be done leading to development of models, frameworks or other tools for addressing the problem of iPredators' social engineering attacks targeting users and organization both locally and globally.

REFERENCES

[1] Alexander, K. (2012). National Cyber Security Framework Manual. Pretoria: Van Schaik Publishers.

[2] Aliaga and Gunderson (2006). Interactive Statistics. Upper Saddle River, N.J.: Pearson Prentice Hall.

[3] Blackhat. (2015). Blackhat Attendee survey: Time to rethink enterprise IT security. Chicago: Blackhat.

[4] Bryman, A. (2008). "Of methods and methodology", Qualitative Research in Organizations and Management: An International Journal, Vol.3 Issue 2: University of Leicester

[5] Chantler, A., & Broudhust, R. (2006). *Social Engineering and Crime Prevention in the Cyberspace*. Uk: Technical Report, Justice, Queensland University.

[6] Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588-608. Retrieved 14th July 2015 from http://www.jstor.org/stable/2094589

[7] Cooper, D, and Schindler, P. (2000), Business research methods, seventh edition New York: Irwin/ McGraw- Hill

[8] Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

[9] Kakah, M. (2017, March 21). Man in court over loss of KRA Sh. 4bn. Retrieved March 22, 2017, from nation.co.ke: http://www.nation.co.ke/news/Man-in-court-over-loss-of-KRA-Sh4bn-/1056-3859206-rllk4a/

[10] Kaspersky. (2015). Kaspersky security bulletin 2015. New York: Kaspersky lab.

[11] Kothari, C. R. (2004). Research Methodology : Methods & Techniques. New Delhi: New Age International (P) Ltd.

[12] Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering: the neglected human factor for information security management. Idaho; Information Resources Management Journal.

[13] Maxwell, J. (1997). Designing a qualitative study.Thousand Oaks, CA: Sage.

[14] Nabie, Y. C., & Paul, J. S. (2016). Cybersecurity: Risks,vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research .

[15] Nuccitelli, M. D. (2014). iPredator. Retrieved May 12, 2015, from www.iPredator.co: https://www.ipredator.co/inside-cybercriminal-minds/

[16] Patton, M. Q. (2002). Qualitative research and evaluation methods (3rd ed.). Thousand Oaks, CA: Sage Publications.

[17] Paula, M., Carol, M., Kelvin, K., Martin, M., Barbara, S., Daniel, N.(2015). Kenya Cybersecurity Report 2015. NAIROBI: SERIANU.

[18] Scott, S. (2013, April 8). Qualtrics. Retrieved July 28, 2016, from Qualtrics.com: http://www.qualtrics.com/blog/determining-Sample-Size/

[19] Teddlie, C. & Fen Yu (2007). Mixed Methods Sampling: A Typology With Examples. Thousand Oaks, CA: Sage.

[20] Wainaina, E., & Wanzala, O. (2017, March 9). Police burst ring of hackers. Retrieved March 22, 2017, from nation.ke.co.ke: http://www.nation.co.ke/news/policeburstringofhackers/10563842558formatxhtmlc2vor2

[21] Wampold, B. E., & Kivlighan, D. M., Jr. (2008). *Research design in counseling*. (4rd Ed.). Belmont, CA: Thomson Brooks

[22] Wendy, F., Brian, L., & David, M. (2016). Anatomy of Social engineering attacks Exploiting Human Behaviour. New York: Price Waterhouse Coopers.