A SECURITY RISK SCALE TO ENHANCE PHISHING DETECTION

ROBERT METHOD KARAMAGI

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN COMPUTER SCIENCE (MSCS)

DEPARTMENT OF ICT AND MATHEMATICS OF

THE OPEN UNIVERSITY OF TANZANIA

2023

CERTIFICATION

The undersigned certifies that he has read and hereby recommends for acceptance, by The Open University of Tanzania, a dissertation entitled, **A Security Risk Scale to Enhance Phishing Detection,** in partial fulfilment of the requirements for the award of the Degree of Master of Science in Computer Science (MSCS).

……………………..…………

Dr. Said Ally

(Supervisor)

……………………..…………

Date

COPYRIGHT

DECLARATION

I, **Robert Method Karamagi** declare that the work presented in this dissertation is original. It has never been presented to any other University or Institution. Where other people's works have been used, references have been provided. It is in this regard that I declare this work as originally mine. It is hereby presented in partial fulfillment of the requirement for the Degree of **Master of Science in Computer Science (MSCS).**

……………………..…………

Signature

……………………..…………

Date

DEDICATION

I would like to dedicate this research to all victims of social engineering and phishing in Tanzania and across the world.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest appreciation to my research supervisor, **Dr. Said Ally**. He has supported me throughout each step and phase of this research, and continuously provided invaluable guidance to drive the research forward and develop it in all aspects.

I also thank **CRDB Bank Plc,** for providing me with the environment and resources to perform the research study.

I thank the panelists, discussants, and my lecturers, for all their comments and suggestions to improve this research.

ABSTRACT

Cybersecurity defense techniques have evolved with time, which has led to attackers needing to deploy more resources to break into systems. As humans are the weakest link to security, social engineering remains highly marketable for hackers to gain unauthorized entry into information systems. Due to the increased ease and need for communication globally, phishing has become the most common method threat actors use to trick victims into unintentionally submitting their data. There are many ways in which the victim may be convinced to believe in the false email and regard it as a legitimate one. In this study, an experimental test was conducted to determine the emotion that will result in significant user interaction when manipulated in a phishing email. Data was collected from 327 users inquiring about the rate they receive phishing emails and the probability of interacting with the phishing emails, based on the Likert scale. In this study, we have found that a major cause of successful phishing attacks where emotions are triggered, is manipulation of curiosity, fear, authority, and empathy emotions out of 10 social engineering techniques. A security risk scale to enhance phishing detection has been developed. The scale consists of critical, high, medium, and low severity levels of risk. To assist in solving this problem of susceptibility to phishing attacks by manipulation of emotions, it is recommended that organizations with mail servers train their staff on the use of this developed security risk scale and all its features in relation to phishing attacks triggered by emotions. This will resolve the ever-growing security problem of social engineering attacks through phishing emails.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
ANN	Artificial Neural Network
APA	American Psychological Association
APT	Advanced Persistent Threat
APWG	Anti-Phishing Working Group
ATM	Automated Teller Machine
AUC	African Union Commission
BEC	Business Email Compromise
BERT	Bidirectional Encoder Representation from Transformers
BIM	Behavior Intelligence Model
CAG	Controller and Auditor General
CBOW	Continuous Bag of Words
CCU	Cybercrime Unit
CEI	Cybersecurity Exposure Index
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team

CGAP	Consultative Group to Assist the Poor
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
CNN	Convolutional Neural Network
CPU	Central Processing Unit
CRDB	Cooperative and Rural Development Bank
DARTH	Decision Analysis in R for Technologies in Health
DBIR	Data Breach Investigations Report
DDoS	Distributed Denial of Service
DT	Decision Trees
EE	External Examiner
EPOCA	Electronic and Postal Communications Act
FBI	Federal Bureau of Investigators
GAN	Generative Adversarial Network
GCI	Global Cybersecurity Index
GCNN	Generative Convolutional Neural Network
gTLDs	Generic Top-Level Domains
HELPHED	Hybrid Ensemble Learning Phishing Email Detection

HLI	Higher Learning Institution
IAA	Institute of Accountancy Arusha
IBM	International Business Machines
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IG	Information Gain
IP	Internet Protocol
IQR	Interquartile Range
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
KCB	Kenya Commercial Bank
KNN	K-Nearest Neighbor
KnowBe4	Know Before
KRI	Key Risk Indicator
LDC	Least Developed Countries

LSTM	Long Short-Term Memory
MitM	Man in the Middle
ML	Machine Learning
MLP	Multi-layer Perceptron
MPSPM	Multidimensional Phishing Susceptibility Prediction Model
NAOT	National Audit Office of Tanzania
NB	Naïve Bayes’
NICTBB	National ICT Broadband Fiberoptic Backbone
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NN	Neural Network
OUT	Open University in Tanzania
PhD	Doctor of Philosophy
PLC	Public Limited Company
PoS	Part of Speech
PPP	Phish-prone™ Percentage
p-value	Probability Value

QR	Quick Response
RAM	Random Access Memory
RAT	Remote Access Trojan
RCNN	Recurrent Convolutional Neural Network
RF	Random Forest
RNN	Recurrent Neural Network
SACCOS	Savings and Credit Cooperative Societies
SDLC	Software Development Life Cycle
SGD	Stochastic Gradient Descent
SMS	Short Message Service
SN	Serial Number
SOC	Security Operating Center
SPSS	Statistical Package for Social Sciences
SQL	Structured Query Language
SQLi	Structured Query Language Injection
SSL	Secure Sockets Layer
SSN	Social Network Site

SVC	Support Vector Classifier
SVM	Support Vector Machine
TCRA	Tanzania Communications Regulatory Authority
TCU	Tanzania Commission for Universities
TF-IDF	Term Frequency-Inverse Document Frequency
TLR	Logistic Regression
TshPhish	Two Stage Hybrid Phishing Detection
TUMa	Tumaini University Makumira
TZ-CERT	Tanzania Computer Emergency Response Team
UoA	University of Arusha
URL	Uniform Resource Locator
VPN	Virtual Private Network
VRO	Virtual Risk Officer
Word2Vec	Word to Vector
XGBoost	eXtreme Gradient Boosting
XSS	Cross-Site Scripting

CHAPTER 1

INTRODUCTION

1.1 Background

Phishing is a social engineering technique where a malicious individual sends a fake message to a victim and requests them to perform some action, which without them knowing will help the evil attacker achieve their unethical mission such as stealing their login information or bank credit card details. (Rosenthal, 2021)

Rosenthal (2021) describes phishing as an attack that relies on tempering with the psychological aspect of the victims. It differs from attacks that need more sophistication such as a man in the middle (MitM) attack as discussed by Mallik et al. (2019) A man in the middle attack as the name suggests is where the attacker gets in the middle of the communication between a client and the server. Any communication between the client and the server will first pass through the attacker. The attacker then forwards the request to the intended destination. The attacker may listen to and manipulate the information when it reaches him or her. (Mallik et al., 2019)

Malicious acts such as phishing and spoofing advancing with new electronic systems integrations, as per the Tanzania Cybercrime Study Report of 2016, have constricted the e-commerce growth and led to costs of up to $85 million with projections to increase with developments in business process automation. (Msaki, 2019) The costs of malicious insider threats is estimated at $30 million a year. (Oreku, 2020)

Phishing remains a major threat in Tanzania as studies show that with time a majority of users will be first time internet users and unaware of the dangers and prevailing threats. (Bishel, 2022) Tanzania Computer Emergency Response Team (TZ-CERT) (2022) honeypots show that there have been over 70 million network attacks, 130 million malware attacks, and 2 million web attacks, in the period between January 2019 to March 2022. (TZ-CERT, 2022) The information shows that network attacks are doubling every year. There are more than 40 million malware attacks annually. Web attacks have also increased with time. With a dangerous attack surface observed, phishing is a threat that requires attention.

The survey performed by Msaki (2019) to evaluate the security risks that are perceived towards traditional retailers engaging in e-commerce, found that 90.65% of the respondents agreed and strongly agreed that the risk of hackers exists. Likewise, 70.54% that there is a risk of phishing is existent. 66.67% on the false personification risk, and 58% on the risk of insecurity. (Msaki, 2019)

Mswahili (2022) assessed the factors that promote the acceptance and use of mobile money interoperability services in Tanzania. Utilization of mobile money faced an eruptive increase from when it was introduced in 2008, making it a key instrument for accessing monetary services in the country. By the end of the second quarter of 2020, over 29 million mobile money accounts were actively registered in Tanzania with an average transaction volume of up to 4.1 billion US dollars. The findings from his study revealed that the resolution of security issues such as phishing attacks, identity theft, etc., positively influenced the usage of mobile money services. It is therefore essential that proper security measures against cyber-attacks and phishing be incorporated to advance from the growing risk. (Mswahili, 2022)

The research of Lissah et al. (2022) realized that cashless payment methods face hindrance due to the emerging security threats such as phishing, pharming, denial of service attacks, fraud, identity theft, etc., and as a result barriers are formed to the growth of cashless economy. (Lissah et al., 2022)

Salim (2022) assessed frauds occurring in mobile money transactions and its impact on Telecom Service Providers in Zanzibar. The findings presented showed that phishing, spoofing, and vishing were regular and continuously performed fraudulent actions that had marketing, financial, and legal impacts leading to losses in reputation, revenue, customers. (Salim, 2022) Mobile networks operators in Tanzania have recently observed a sharp rise in Short Message Service (SMS) phishing attacks. (Mambina et al., 2022)

Research by Kavishe (2021) examined that 627 cybercrime instances throughout 2007 to 2012 were reported in Tanzania. The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) documented 28 internet assaults that were launched from Tanzania to other target countries. The attack techniques included 13 spams, 7 phishing, 5 malware, and 3 web defacement. (Kavishe, 2021)

A survey performed by Ndibwile et al. (2018) uncovered an unsatisfactory awareness to phishing in Tanzania. 78% of the participants of their survey were likely to interact with an email from a source unknown to them. Their study also revealed that most of the participants in Tanzania i.e., 58% would seek cybersecurity knowledge on their own accord rather than through professional training services such as universities, schools, or at their workplace. (Ndibwile et al., 2018)

Panga et al. (2022) found that the socioeconomic and social culture affects the phishing knowledge of teenagers, by using a game and traditional method of assessment. Scholars in urban areas, foreigners, and private scholars had stronger knowledge to phishing than those from the rural areas and government schools. (Panga et al., 2022)

Mwabukojo (2020) pointed out how Tanzania has a diminished capacity to innovate which has led to a significant deficiency in science and technology within the nation. Some drivers mentioned include lack of capital, technology institutions, infrastructure, and political determination. These factors raise the risk of lacking the sufficient and needed sophisticated protection against cyber threats and phishing attacks. (Mwabukojo, 2020)

1.2 Statement of Problem

The introduction of machine learning and artificial intelligence into the cybersecurity regime have significantly improved the mechanisms to detect phishing emails. Modern techniques apply machine learning algorithms to train models to learn through large datasets, on how to predict and classify phishing emails. Natural language processing and text mining models have evolved to perceive the context in email messages and determine whether they are malicious ones or benign.

Despite the efforts made to accurately predict phishing emails using advanced machine learning models, a realization of the impact severity and risk posed by the detected phishing emails is yet to be uncovered. This is a problem because without a measurement of risk, security protection mechanisms are not implemented with a consideration of the threat levels and probable exposure.

1.3 Objectives

Main Objective

To develop a security risk scale to enhance phishing detection in mail systems.

Specific Objectives

1. To identify the factors affecting the effectiveness of phishing attempts through mail messages.

2. To design a security risk scale based on the relationships between phishing variables and the security risk.

3. To assess the performance level of the proposed security risk scale against results of a phishing attack performed at a bank.

1.4 Research Questions

Specific Objective 1

1. What are the factors that affect the effectiveness of phishing attempts through mail servers?

Specific Objective 2

2.What is the design of a security risk scale based on the relationships between phishing variables and the security risk?

Specific Objective 3

3. What is the performance level of the proposed security risk scale against results of a phishing attack performed at a bank?

1.5 Significance of the study

With evolving technology, cybercriminals are getting more sophisticated in their attacking mechanisms, and as a result, the cost of cyber-defenses are skyrocketing. As of 2023, the enterprise email phishing detection and prevention solutions charge at least $3 per user per month. The costs for blocking spam and phishing emails increase based on the number of incidents. Organizations aiming at optimizing their cybersecurity expenditures may focus their budget on defending the higher risk phishing emails revealed by the proposed email phishing security risk scale methodology.

A high-risk phishing email should be countered by stern cybersecurity protection, whereas for the cases of less risk phishing emails, the security management may channel defense efforts where greater risk exists.

This study provides risk input to the enterprise risk management program and defines the associated phishing key risk indicators (KRIs). The level of phishing risk may be objectively quantified giving organizations a notice in advance of potential phishing risks that could cause damage.

The risk scale may be used as a tool in the risk management framework. As described by Ullah et al. (2021) a framework helps to discover and manage the risks within the organization, as well as functionalize the risk management process. Employees may collaborate via the governance team to identify risks, analyze, evaluate, and monitor them, and eventually plan out responses for the risks. (Ullah et al., 2021)

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

Phishing is a form of social engineering, and an unethical act performed by malicious adversaries that aim to capture sensitive user information through manipulating human emotion. Most of the times, attackers use emails, instant messaging, etc. to get victims to navigate to evil links. Because new techniques are always being devised by the hackers, social engineering awareness and training serves the best means to prevent the phishing attacks. (Saxena et al., 2019) Spam is a dangerous phishing vector as users are sent so many unsolicited emails in their inbox, they catch the emotion of boredom or annoyance. The user will mainly wish for the spam messages to just stop coming. The hacker uses this to their advantage and provides them with an unsubscribe option or link to stop receiving the spam messages, however, the site it re-directs to is a malicious phishing site with potential malware and input forms to steal confidential data. (Karim et al., 2019) Social engineering is a non-technical type of attack, but it can be used in collaboration with technical attacks such a spyware, keyloggers, backdoors, remote access trojans (RATs), reverse shells, viruses, worms, rootkits etc. The essence of social engineering is about targeting the weakest element in an organization’s security, which is the human factor, as they can be hacked much easier in comparison to computers. (Abass, 2018) Spear phishing is a form of phishing attack that targets a single primary individual. The attacker focuses their attention to a single person or group and lures them into surrendering their secret data without them having a clue what is going on. (FireEye, 2018) (Bullee et al., 2017) Voice phishing or Vishing is another form of phishing where by the attacker makes a phone call to the victim and then tries to manipulate them over the phone in giving up confidential data. (Maseno, 2017) Whaling is a form of phishing that targets the high-profile individuals such as chief executive officers (CEOs), presidents, kings or queens etc. (Gupta et al., 2018) A keylogger is a form of spyware that can be either hardware or software based. Its sole purpose is to record all the keystrokes that are typed in by the user, without them knowing. (Parekh et al., 2020) A backdoor is a form of malware that functions to allow hackers to gain access to a machine without any approval, authorization, or authentication. (Loi & Olmsted, 2017) A remote access trojan is a type of backdoor that allows a hacker to remotely take full and unabated control over a device. (Valeros & Garcia, 2020) A reverse shell is a connection shell that is virtual and open to the attacker's machine that initiates from the victims' device. (Lu, 2019) Computer viruses are dangerous pieces of code that self-replicate by infecting other programs within its reach by injecting malicious code in them. (Kumar & Dey, 2019) Computer worms are malicious programs that replicate on their own without the need of interacting with any other file, and spread across machines in a network. (Jajoo, 2017) Rootkit are programs written primarily for evading detection while maintaining privileged access to the system. (Nadim et al., 2021)

2.1.1 Phishing in Tanzania

Internet developments

Bishel (2022) indicated the under-developed internet access in Tanzania. Satellite was the only means to access internet before 2009 making features such as connectivity and bandwidth affordable to only enterprises. Private citizens turned to internet cafeterias for feasibility. Survey data revealed that in 2008, only 6% of Tanzanians used internet, and 4% of the participants used it daily. It was only in 2009 where the first underwater fiber optic cable was installed to connect the world internet to Tanzania, and later in 2016, expanded to land connectivity through the National ICT Broadband Fiberoptic Backbone (NICTBB). Afrobarometer surveys exhibited that 89% of the respondents never used internet in 2011, 86% in 2014, 77% in 2016, and 72% in 2019. As of 2019, only 10% of the respondents used internet every day. (Bishel, 2022)

The usage of Internet in Tanzania is growing year by year. Statistics from the Tanzania Communications Regulatory Authority (TCRA) show that the estimated number of internet users have increased from 19,862,525 in 2016 to 29,858,759 in 2021 with a penetration rate of over 40% annually. Between September 2021 and March 2022, an average of not less than 148 petabytes of internet data traffic has been recorded in Tanzania. These statistics demonstrate an increasing attack surface for phishers and a need to develop robust security mechanisms. (TCRA, 2022)

Legal Aspects

Magalla and Mnyigumba (2021) reviewed legislations on cyberterrorism in Tanzania and noticed that the present legal statues are ineffective in the prosecution and opposition against cyberterrorism, with regards to the increasing cyber terrorist campaigns and challenges in tracking and charging the cybercriminals. The shortage of adhesive legal frameworks has in turn entertained cyberterrorists to perceive the government are incapable of legally apprehending them. (Magalla & Mnyigumba, 2021)

The Electronic and Postal Communications Act (EPOCA) enacted by the Tanzania Communications Regulatory Authority (TCRA) in 2010 had no consideration for protecting ICT users from cybercrime. (Olivia, 2022) Moreover, it took many years for cybercrime to be discussed in the parliament in Tanzania, and to be confirmed in the bills as a breach of law. (Ghelerter et al., 2022)

Tanzania came to pass cybersecurity laws resembling China in 2015. (Fick et al., 2022) The National Assembly of Tanzania enacted the Cybercrimes Act of 2015 to criminalize misdeeds against Information Systems and facilitate forensic investigations, electronic evidence collection, chain of custody, and usage. (Pallangyo, 2022) A report of the African Union Commission (AUC) and Symantec in 2016 pointed out Tanzania alongside 10 other countries in Africa (Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Uganda and Zambia) to have distinct laws and provisions established to combat cybercrime and control electronic evidence. (Kshetri, 2019a)

(Euphemia et al., 2019) (Van Vuuren et al., 2019) Additionally, complex dedication and involvement in cybersecurity strategies and schemes has progressed. (Pantserev, 2022)

Lubua and Pretorius (2019) investigated the failure of organizations in Tanzania to comply to the security standards and requirements of the International Organization for Standardization/International Electrotechnical Commission - ISO/IEC 27001 for information security management systems (ISMS) due to a deficiency in viable security policies. Stakeholder engagement in devising policies and periodic reviewing of the policies within 3-year intervals is performed by few organizations. Furthermore, top management authorization of the cybersecurity policies in use, is not necessarily adhered to. (Lubua & Pretorius, 2019)

Soutis (2020) assessed the role played by laws and regulations made by the government to drive e-banking in commercial banks in Tanzania to adapt. The study explored challenges such as effects of cybercrime on electronic banking. Issues such as phishing tailored to steal financial information using social engineering, malicious websites, and input forms, etc., pose as a serious threat. It was found that the protection given by the legal system was inadequate, and a state of trust for electronic banking could not be established, as a consequence corporations fail to equip themselves with the means to facilitate electronic transactions independently. (Soutis, 2020)

Cross (2021) highlighted politics as giving implication to ideas of the usage and policing of mobile phones and the internet along with the fact that useful insights for political negotiations regarding security and development may yield from exploring the ideas. (Cross, 2021)

A study by Malekela (2022) revealed an insufficiency in the legal framework on data protection and privacy in Tanzania. Despite the laws identifying when a respective legislation may gather and process personal data, they lack to convey the terms and procedures in which this data may be lawfully processed. The deficit of data protection laws brings forth risk of personal data being stolen and disclosed, moreover by phishers and cyber criminals. (Malekela, 2022)

Cybercrime

Magufuli (2019) inspected how communications regulations would affect content cybercrime prevention in Tanzania. The findings from the study showed that 75.8% of the respondents confirmed a sizeable rate of content cybercrimes in Tanzania. Online platforms and social media were seen to be the dominant sources of internet scams, hoaxes, and deceptive messages to steal money. TCRA signified that in 2019, 7091 cases of content cybercrimes were reported in Tanzania. However, TCRA faces a shortage in the capacity to productively counter the content cybercrime. Further constraining issues uncovered included deficiencies in public security awareness programs on content cybercrime consequences, short supply of resources such as labor force, capital, workspace, etc., absence of the latest technology to proactively initiate cybersecurity threat responses as well as a user-friendly institutional system, frail policies and legal frameworks, and a deficit in private sector engagements. (Magufuli, 2019)

As of 2011, studies revealed that only 40% of the banks in Tanzania alongside Kenya and Uganda were ready to defend themselves against cyberthreats. Similar surveys across banks in Tanzania and neighboring countries depicted issues such as hacking, poor security acumen of employees, and malicious insiders put the banks at high risk of exploitation by adversaries. (Kshetri, 2019b)

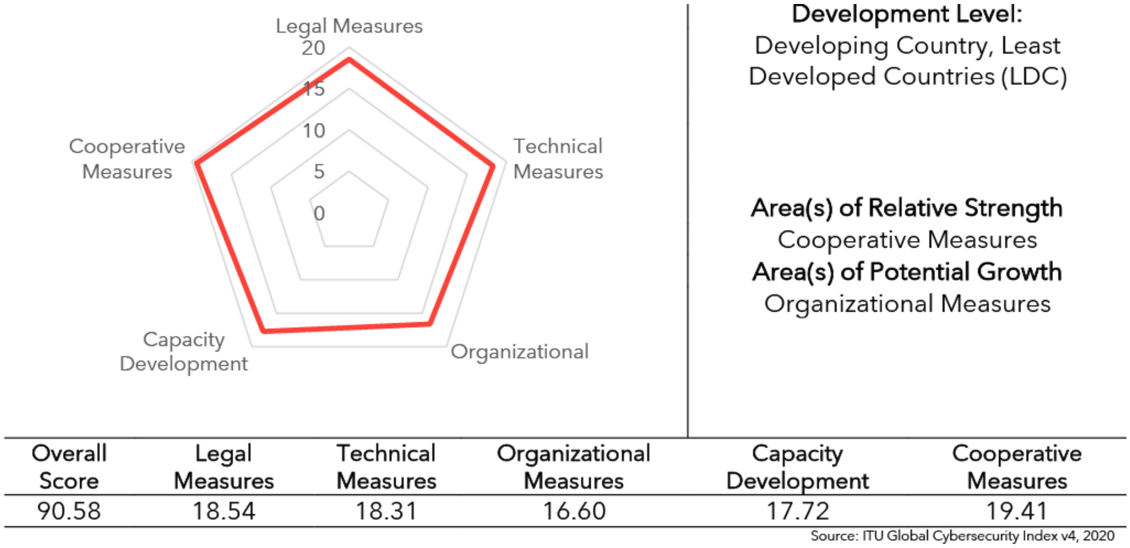
A survey conducted by the International Telecommunication Union (ITU) and Consultative Group to Assist the Poor (CGAP) in 2016, across 5200 mobile money users in Tanzania, Ghana, and Philippines, had 27% of Tanzanian respondents agreeing to have fallen victims of fraudulent or scam messages, while 17% of the interviewees claimed to have been extorted money in a fraud or scam. (Baur-Yazbeck et al., 2019)

Oreku (2020) observed that the cybersecurity violations in Tanzania are caused by social engineering attacks such as phishing, scams, identity theft, and unapproved access. Employees working together internally in collusion alongside hijacking attacks were seen to primarily facilitate embezzlement and financial fraud. The internet, as per the respondents was taken as the top source of intrusions, thenceforth collusion, pharming, and phishing. (Oreku, 2020)

As per Malale and Christopher (2022), abuse in information technology has led to the increase of cybercrime in Tanzania to the point it has become a common thing. Cyber robbery is on the rise, with hackers infiltrating user's private data and demanding ransoms. (Malale & Christopher, 2022)

Pallangyo (2022) observed that a deficiency in proactive cybercrime defense techniques when countering incidents and insufficient education on cybersecurity and cybercrime to the end users are factors that contribute to expeditious growth of cybercrime. (Pallangyo, 2022)

The Global Cybersecurity Index, which measures the global cybersecurity commitment of countries, in 2020 ranked Tanzania with an overall score of 90.58, second in Africa - behind Mauritius, and 37th worldwide. (ITU, 2020)



Development Level:
Developing Country, Least Developed Countries (LDC)

Area(s) of Relative Strength
Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
90.58	18.54	18.31	16.60	17.72	19.41

Source: ITU Global Cybersecurity Index v4, 2020

Figure 2. 1 Tanzania Global Cybersecurity Index Profile

Source: ITU Global Cybersecurity Index v4 (2020)

However, Tanzania is listed as the second country in Africa - behind Ethiopia, to exhibit the greatest cybersecurity threat by the Cybersecurity Exposure Index (CEI), which periodically surveys data of 108 countries across Europe, America, Asia-Pacific, and Africa and ranks the impact of cybercrime on the countries. The CEI score ranges from 0 to 1, with the higher score implying greater exposure. Tanzania has a CEI score of 0.731, ranking 10th in Africa and 72 across the globe. (Mphatheni & Maluleke, 2022)

Monetary Losses

Oreku's (2020) study depicted that the main reason behind the cyber-attacks in Tanzania is financial gain, supporting the observations of financial organizations, transaction processing institutions, savings and credit cooperative societies (SACCOS), etc., being key targets for the threat actors. (Oreku, 2020)

Tanzania has confronted losses amounting to $6 million on several cybercrime incidents triggering the establishment of Cybercrime Units (CCUs) and Computer Emergency Response Teams. (CERTs) (Bukht et al., 2020)

The estimated cost of cybercrime in Tanzania in 2017 summed up to $99 million with an estimated 300 certified professionals, as per the African Security Report of 2019. (Akinyetun, 2021) (Mtakati & Sengati, 2021a)

Collectively, more than $245 million, as indicated by Deloitte, has been lost since 2011 in financial organizations in Tanzania alongside Kenya, Rwanda, Uganda, and Zambia. (Interpol, 2021)

E-Commerce, Mobile and E-Banking

Mlelwa (2019) confirmed security to be a major concern for e-commerce expansion in Tanzania. Protection from fraudulent and unlawful online business is needed. Data needs to be secured in all aspects. There is a lack of proper funds, frameworks, policies, and adopted industry standards to ensure confidentiality and privacy of the data. (Mlelwa, 2019)

From the findings of Ntigwigwa, (2019) it can be seen that cybercrime in mobile money services in Tanzania originates from technical security loopholes. (Ntigwigwa, 2019)

Nuru (2020) surveyed mobile banking customers of Kenya Commercial Bank (KCB) in Tanzania. 44% of the respondents did not believe that due to the cyber security provided by the bank being very high, the technological risk is minimal. (Nuru, 2020)

Chanda's (2020) assessment of factors affecting customer's adoption to electronic banking services found that there is a negative perception from the customers since several cyberattacks and poorly secured systems have been a cause of fraud. Despite the increased means of convenient and highly available electronic banking products, customers fear for the loss of their funds, making them reluctant to digital investments. (Chanda, 2020)

Mpofu and Mhlanga (2022) looked into Tanzania’s hefty reliance on mobile money for both formal and informal transactions and issues on rural habitants being financially included in digital financial services as compared to those in urban regions. (Mpofu & Mhlanga, 2022)

Education sector

An analysis of cybersecurity threats in higher learning institutions in Tanzania by Kundy and Lyimo (2019) for the case of University Of Arusha (UoA) and Tumaini University Makumira (TUMa) revealed pitfalls in the cybersecurity strategy and organizational standards execution and compliance, information systems, employees, and security awareness. (Kundy & Lyimo, 2019)

Mshangi (2020) shed light on the absence of considering the security of information systems as technological advances are made in information and communication technology (ICT) with time. A survey of users in the education sector in Tanzania depicted that 12.8% of them encounter cyberattacks because of browsing infected websites and spam makes up 63.29% of the emails received by the users. For a period of less than a month in 2017, the education sector in Tanzania lay victim to several hacks on its websites and information systems. The attack targets included the website of the Open University of Tanzania (Mtakati & Sengati, 2021b), and University of Dar es Salaam, and TCU’s information system web application. As ICT progresses with time, the trends of hacking information systems in Tanzania’s cyberspace by exploitation of open security holes or vulnerabilities is increasing because the development and deployment of system's fail to incorporate security requirements sufficiently throughout all the stages of their software development life cycle. (SDLC) (Mshangi, 2020)

The Cybersecurity posture of Higher Learning Institutions (HLIs) in Tanzania was analyzed by Mtakati and Sengati (2021). A vast number of vulnerabilities exploitable by hackers were revealed by an audit on information systems directed by the Controller and Auditor General (CAG) of the National Audit Office of Tanzania (NAOT) from 2017 to 2019. However, HLIs have yet to address their readiness to cybersecurity. An analysis of the cybersecurity readiness of HLIs and organizations have not yet been performed by the Tanzania Commission for Universities (TCU) and the Tanzania Communications Regulatory Authority (TCRA) respectively. HLIs lack suitable cybersecurity provisions such as strategies, incident reporting, assessing third parties, threat information sources, and inter-institute collaboration making them vulnerable to attacks. (Mtakati & Sengati, 2021b)

Benard et al. (2021) similarly investigated effects of cybercrimes on social media usage among higher learning institution students in Tanzania. They realized the risk posed by many students who willingly offer a lot of useful information for hackers publicly on social media or email. Threats relating to cyberbullying, cyberstalking, hacking, spoofing, spam, and malware are on the rise and require control by policy governance. Investments in security training, awareness, and research are depleted. (Benard et al., 2021)

Lyimo (2022) unveiled that internal and external organizational factors influence the increase in information security vulnerabilities in Tanzania for the case of the Ministry of Education. Internal factors found involved unintentional employee errors, malicious employee threats, failure to identify and classify information assets and exposures on them, failure to realize the consequences of the vulnerabilities, insufficient awareness on information security, and shortfalls in security response mechanisms. External factors included system attacks from threat actors or disgruntled ex-employees, website or server defacement, remote attacks, organized crime, phishing, etc. (Lyimo, 2022)

Semlambo, Mfoi, et al. (2022) performed a case study on the Institute of Accountancy Arusha (IAA) to depict the threats and vulnerabilities related to information security systems of higher education institutes in Tanzania. They noticed the prime factors influencing information system security were human factors, security policies, work conditions, and demographics. (Semlambo, Mfoi, et al., 2022)

Mlyatu and Sanga (2023) conducted an experiment across 100 websites of African Universities where 30 of the 100 were websites of Tanzanian Universities accredited by the Tanzania Commission for Universities (TCU). They investigated if enforcing of security headers was done to help mitigate various cyberattacks such as cross-site scripting (XSS), click-jacking, session hijacking, structured query language (SQL) injection, etc. They found that 70% of the websites had no X-Content-Type-Options and X-Frame-Options headers, 90% had no Strict-Transport-Security header, 96% of the sites did not have a Referrer-Policy and Content-Security-Policy headers, and all the websites were missing a Permissions-Policy header. Such security misconfigurations observed provide a realization to the severe risk that lies across the landscape of web applications in Tanzania. Social engineering and phishing attacks that relay the misconfigured websites may result in serious exploits and losses. (Mlyatu & Sanga, 2023)

Security Awareness

Oreku (2020) highlighted a major challenge in Tanzania is constructing a nation that realizes the significance of information security. (Oreku, 2020) Challenges in forming cyber security awareness among employees were identified by Shaaban and Athumani (2020) being the employee preparedness, belief and steady sanctioning of technology. (Shaaban & Athumani, 2020)

The survey conducted by Mambile and Mbogoro (2020) disclosed that the public servants in Tanzania lack of awareness on cybercrimes, cyberlaws and their impacts. Out of the surveyed public servants, 76.02% of the respondents have continuous internet access to perform daily activities on information systems. The results signify a rapid digitization rate with real social impacts, raising the red flag for the necessity of cybercrime and cyberlaw awareness. However, the findings portrayed that most of the public servants vaguely know about cybercrime or do not have any idea at all. This situation presents great risk as the public servants are mostly incapable of fixing important safeguards for themselves. (Mambile & Mbogoro, 2020)

Schemes such as the Public Likes and D9 Ponzi in Tanzania are reasons for capital markets, central banks, security institutions, etc., to proactively alert the public on hoaxes that compromise security as well as enhance awareness initiatives where active bidirectional involvement is needed. (Wambalaba et al., 2021)

Lyimo and Kamugisha (2022) performed a study to analyze how employees in Tanzania are aware about the internet security. They found that the employees do not have sufficient knowledge on the approaches to keep themselves secure from internet threats. They also noted that compliance to online safety principles by the users was not satisfactory. (Lyimo & Kamugisha, 2022)

User Issues

Ndibwile et al. (2019) illustrated how respondents from Tanzania will neglect following or implementing security measures such as automatically updating their smartphones because of financial factors such as data charges which prove to be significant for users in a developing country. (Ndibwile et al., 2019)

Ndibwile's (2020) survey found that 67% of Tanzanian respondents understood that updating the operating system improved security. However, most respondents were not motivated by the impact of securing their systems, rather an improved interface (34%), and performance (22%). Download costs hindered 45% of the respondents. (Ndibwile, 2020)

In Msaki’s (2019) assessment of the challenges on e-commerce engagement for the case of selected traditional retailers, various views on cybercrime in Tanzania were observed. In the study, 35% of the respondents believed that technology is the root cause of cybercrime, as 71% were victims of money theft and other related offences. The study also revealed that impedance to e-commerce engagements is derived from critical trust issues. Other financial sectors alongside e-commerce, where mobile and electronic services were introduced, have fallen prone to vulnerabilities triggering money loss through the channels. (Msaki, 2019)

James and Mbogoro (2020) found that the perceived systems security among other factors affect the endorsement of depositing cash through automated teller machines (ATMs) of commercial banks in Tanzania by 40.2%. (James & Mbogoro, 2020)

2.1.2 Phishing across the world

William Sutton, dubbed as America’s most daring bank robber and jail breaker of his time, when interviewed as to why he robs banks, replied “because that’s where the money is”. His quote trended and evolved into Sutton’s law which states that, “When diagnosing, first consider the obvious.” (Wikipedia, 2022) To capture a hacker, we should try to think what the most successful hackers would think. Which is what makes Sutton’s logic quite interesting for our study. If we ask ourselves, “Why do adversaries perform email phishing?” Using Sutton’s law, we can come up with the reason that it is because that is where the targets are.

Research has revealed that a spear phishing email was the initial attack that resulted to 93% of successful cyber invasions universally. Email phishing constitutes to 96% of the types of phishing attacks, followed by 3% taken by malicious websites, and 1% being via the phone or vishing. (EasyDMARC, 2022a)

Threat analysis performed by Abnormal Security (2022) has revealed that email is the greatest malicious attack vector. As of the second half of 2022, attacks on business email compromise (BEC) have increased by 60% from the previous year at a similar time. Likewise, BEC has been the most economically damaging cyber offense since 2015. Email phishing cannot be neutralized by traditional email security tools, as they are content manipulative and apply principles of social engineering, rendering their detection impossible. Email is used globally for communications and the attacks are not costly, which in turn gives success to threat actors and motivation to continue using it as a tool for phishing. (Abnormal Security, 2022a)

The Anti-Phishing Working Group (APWG) (2022) Phishing Activity Trends Report has revealed that a total of 1,097,811 total phishing attacks were observed in the second quarter of 2022, which is a new record and the largest recorded as of the time. Hackers of business email compromise (BEC) attacks have requested an average of $109,467. (Anti-Phishing Working Group, 2022)

The X-Force Threat Intelligence Index 2022 report by IBM Security (2022) has highlighted that, in 2021 phishing attacks were the greatest cause of infection and compromise. Several incidents were remediated by IBM Security X-Force (2022), with most of them, i.e., 41% being phishing. (IBM Security, 2022)

Zscaler (2022) have identified Phishing as a Service (PhaaS) to be a new vector for increased surges in phishing in their 2022 ThreatLabz Phishing Report. Phishing has been simplified using open-source phishing frameworks and kits. People may be exploited easily as hackers of any skill level are resorting to offers in the dark web for pre-made phishing campaigns and resources. Expert adversaries maintain the software code and phishing tools for their following. (Zscaler, 2022)

Interisle Consulting Group's (2022) Annual Study of the Scope and Distribution of Phishing have released findings in their Phishing Landscape 2022 report that need to be given attention. The phishing attacks reported monthly have doubled, making it a 61% increase when measured over a period of one year. Reported domain names associated with phishing have increased by 72% over the same period, with malicious domain name registrations spiking up by 83%. (Aaron et al., 2022)

Agari and PhishLabs (2022) carried out an analysis on enterprises, their staff, and labels, for the period of the first quarter of 2022. They inspected over hundreds of thousands of phishing attacks targeting these organizations. Their study revealed that financial institutions are victims to the most phishing incidents, ranging up to 53.8% of all the recorded incidents during that window. The staging of 52% of the phishing sites was done on sites compromised prior to the phishing attack or on sites from a registered and paid for domain. Generic top-level domains (gTLDs) such as .com and .org, is where up to 66% of all the observed phishing sites were staged on. (PhishLabs, 2022)

Research on 550 organizations that fell victim to data breaches was performed by Ponemon Institute (2022) and sponsored by IBM Security® (2022). It was found that more than a single data breach existed for 83% of these organizations with an average total cost of a breach amounting to $4.35 million. There was no zero-trust architecture for 79% of organizations with critical infrastructure with the average cost of a data breach being $4.82 million. Cloud based breaches impacted 45% of the organizations. (Ponemon Institute & IBM Security, 2022a)

The 2022 Data Breach Investigations Report (DBIR) by Verizon (2022) points out external attacks to be the largest vector for compromises of data in comparison to any other source. The human factor persists to be the major driving force to breaches of information, constituting 82% of the breaches. Verizon (2022) found that despite the actual clicking on links in phishing emails is generally done by only 2.9% of the employees, hackers may still be well motivated to continue their attempts. Out of 1,154,259,736 personal records recorded to be breached, it means phishing would have been successful for 33,473,532 accounts. (Verizon, 2022)

Phishing is the cause of approximately 90% of data breaches. The US Federal Bureau of Investigation has projected phishing attacks to scale up by 400% annually. Around 57% of internet users have no security considerations or controls on their systems. Despite the online small businesses being aware of the consequences of data breaches, 71% do not have any operational data leak prevention controls. (EasyDMARC, 2022b)

Bolster (2022) gathered and analyzed data from over a billion sites, to uncover the patterns leading to counterfeit and phishing sites. The findings in the 2022 State of Phishing and Online Fraud Report reveal that the top brands to be phished were Microsoft (259,847), Facebook (94,078), Amazon (42,114), Apple (37,822), Adobe (34,037), and Netflix (16,439). The top hosting providers for malicious sites were Cloudflare (1,111,818), Google (501,682), Namecheap (380,270), Amazon (336,502), and Unified Layer (251,970). The top email services used for phishing campaigns were Gmail (73%), Yahoo (13%) and Outlook (3%). (Bolster, 2022)

Continuous conditioning of the human factor is an essential step in the prevention of phishing. This helps to keep individuals aware of trending threats that they are most likely going to encounter. Humans are considered a critical element in detecting and preventing phishing attacks. They may always be capable of discovering something not right in the email. (Cofense, 2022)

Proofpoint (2022), performed an in-depth study, mentioned in their 2022 State of the Phish Report, to explore user awareness, vulnerability, and phishing resilience. They conducted a survey to uncover misconceptions of end users with regards to emails. Proofpoint (2022) found that 62% of the employees surveyed, did not know that they cannot be defended by their service provider, from all harmful emails targeting their personal mail. 63% could not imagine how malicious files can be stored in the cloud, and how they could receive multiple emails from dangerous adversaries. 64% did not know that a hazardous risk may exist from internal emails. 70% lacked awareness about the security tools and technical controls put in place by their organization, not having the capability to defend them against all potentially threatening emails. (Proofpoint, 2022)

The organization's last line of defense is humans. When defending the organization, they may be regarded as the human firewall. KnowBe4 (2022) conducted a study to evaluate the effect of training employees on their susceptibility to phishing. They used a measure known as the Phish-prone™ Percentage (PPP) to quantify how vulnerable a user is to a phishing attack. Over 23.4 million phishing tests were run in three phases, against 9.5 million users from 30,173 organizations across 19 various industries. The first phase involved attacks on untrained users throughout all industries and sizes to find out their initial phishing prone percentage. The average initial PPP was 32.4%. The second phase involved providing security awareness training to the users first, then launching the simulated phishing attacks 90 days after the training. The PPP reduced to 17.6% which justifies training and awareness programs as a critical factor in preventing phishing. Phase three dealt with facilitating monthly training over the stretch of a year before the tests. The PPP was reduced significantly to 5% further supporting training as a method to achieve a rigid human firewall. (KnowBe4®, 2022a)

The volume and severity of email attacks shall continuously intensify. Mitigation of this threat shall need the intervention of behavioral artificial intelligence-based approaches. Strong baselines to evaluate the content, context, and identity need to be established.

(Abnormal Security, 2022b) An average savings in costs due to data breaches of $3.05 million results from organizations having full deployments of security artificial intelligence and automation. (Ponemon Institute & IBM Security, 2022b)

2.2 Related Works

2.2.1 Phishing Detection

Yang et al. (2019) used support vector machines (SVM) to classify between phishing and non-phishing emails. They analyzed the email-header structure, email-URL information, email-script function, and email psychological features to prepare a classification dataset. Fang et al. (2019) devised an improved recurrent convolutional neural network (RCNN) model with multilevel vectors and attention mechanism. They designed THEMIS - an email detection technique that simultaneously models the email header, email body, character, and word level. Oladimeji (2019) performed a comparative analysis of naïve bayes, K-nearest neighbor and support vector machine (SVM) algorithms to classify word embeddings in emails. Text processing of the email content was done by removal of noise (stop words), lexicon normalization (stemming and lemmatization), removal of non-words, word standardization. Castillo et al. (2020) created a word embedding model to analyze the textual content in emails and classified them using a backpropagation classical feed forward neural network with multiple hidden layers. Lee at al. (2020) detected phishing emails using the email content and context features from the email header. They fine-tuned a pre-trained bidirectional encoder representation from transformers (BERT) model by replacing half the transformer blocks with simple adapters. Abdelaziz et al. (2020) conducted natural language processing on emails to classify phishing using a multinomial naïve bayes (NB) classifier. They conducted lexical and semantic analysis of email content to create a bag of words model by removing special and single characters, multiple spaces, lemmatization, and conversion into lowercase. Verma et al. (2020) processed email content by removing stop words, punctuations, special characters, tokenization, stemming, part of speech tagging, language detection, and identification of semantic relations and applied natural language processing (NLP) and support vector machine (SVM) linear classification. AbuMansour and Alenizi (2020) implemented a hybrid feature selection method via information gain and a genetic algorithm. They compared k-nearest neighbors (KNN), naïve bayes, support vector machines (SVM) and decision trees (J48) to classify phishing. Ahmed et al. (2021) extracted features from the email header and hyperlinks using term frequency-inverse document frequency (TF-IDF) and information gain (IG). They detected phishing using a multi-layer perceptron (MLP) neural network model and random forest classifiers. Franchina et al. (2021) analyzed email metadata and content including the body to detect phishing. They carried out text mining and text analytics by text categorization, information extraction, clustering, and text summarization. Bagui et al. (2021) captured inherent characteristics of the email body by deep semantic analysis using a continuous bag of words (CBOW) model. They used a convolutional neural network (CNN) to classify phishing from word embeddings and one-hot encoding representation of words. Bountakas et al. (2021) extracted text features of pre-processed emails and undertook chi-square-based feature selection to reduce train time. They compared natural language processing models, namely TF-IDF, Word2Vec, and BERT and classification algorithms, namely Random Forest, Decision Tree, Logistic Regression, Gradient Boosting Trees, and Naïve Bayes to classify phishing. Bountakas and Xenakis (2022) took hybrid features from the email message body and email content such as headers, attachments, etc. and converted them to an input representation. They used stacking and soft voting ensemble learning algorithms separately to process the hybrid features in parallel. Decision trees were used to classify the content features and k-nearest neighbors for the text features. Muralidharan and Nissim (2022) analyzed all segments of the email, i.e., the header, body, and attachments by a deep learning framework. They classified phishing emails using an ensemble of deep learning classifiers comprising of CNN and BERT models with output from an Extreme Gradient Boosting (XGBoost) model. Korkmaz et al. (2022) developed a two-stage hybrid phishing detection model called TshPhish which inspects for malicious embedded URLs in an email, and the content of the email. A generative convolutional neural network (GCNN) model, which is a combination of a generative adversarial network (GAN) and convolutional neural network (CNN) models, was used to classify malicious embed URLs and a deep neural network (DNN) for content inspection. Noah et al. (2022) predicted phishing emails by analyzing the content such as subject line, email address and body. Their model was built upon stochastic gradient descent (SGD) and support vector classifiers (SVC). Chowdhury et al. (2022) constructed the DARTH framework to extract the email body text, embedded URLs, email metadata e.g., headers, and other features like attachments. They deployed multiple ensembles of multiple neural network models to classify the phishing emails.

Halgaš et al. (2020) transformed text and textual structure content features in the email into a sequence of symbol and word tokens and represented them as unique integers. A recurrent neural network (RNN) phishing classifier with long short-term memory (LSTM) layers was trained to classify the emails. Salahdine et al. (2022) extracted content features present in the email body and header to establish an artificial neural network (ANN) with two hidden layers, 100 neurons each, and rectified linear unit (ReLU) activation. Somesha and Alwyn (2022) extracted email header features from emails to create a dictionary via heuristic methods, such as tokenization and lemmatization. Vectorization of the features extracted was performed by word embedding and fed to a classifier. They compared various models and algorithms. They used TF-IDF, Count Vectorization, Word2Vec and FastText for the word embedding model and Random Forest, SVM, Logistic Regression, Decision Tree, and XGBoost for the classifier.

Table 2. 1: Comparison of Phishing Detection Techniques

SN	Reference	Paper	Solution	Technique	Achievements
1	(Z. Yang et al., 2019)	Phishing Email Detection Based on Hybrid Features	Support Vector Machines (SVM) was used to classify between phishing or non-phishing emails.	An analysis of the email-header structure, email-URL information, email-script function and email psychological features was conducted to prepare a classification dataset.	A 99% true-positive rate, 9% false-positive rate, 91.7% precision and 95% accuracy in detecting the phishing emails

2	(Fang et al., 2019)	Phishing Email Detection Using Improved RCNN Model with Multilevel Vectors and Attention Mechanism	An improved recurrent convolutional neural network (RCNN) model with multilevel vectors and attention mechanism.	THEMIS - an email detection technique that simultaneously models the email header, email body, character and word level.	An overall accuracy of 99.848% and false positive rate of 0.043%.
3	(Olayemi, 2019)	Text Analysis and Machine Learning Approach to Phished Email Detection	Naive Bayes, K-Nearest Neighbor and Support Vector Machine (SVM) algorithms compared to classify the word embeddings.	Text processing the email content - Removal of Noise (Stop Words), Lexicon Normalization (Stemming and Lemmatization), Removal of Non words, Word Standardization.	Naïve Bayes classification accuracy of 99.0%.
4	(Castillo et al., 2020)	Email Threat Detection Using Distinct Neural Network Approaches	Backpropagation through a classical feed forward network with multiple hidden layers.	Detection of phishing by creating a word embedding model to analyze the email textual content.	The first dry run accuracy of 95.68% and second dry run 91.85%. The model is capable of learning complex and non-linear relations between the inputs and outputs.
5	(Lee et al., 2020)	CatBERT: Context-Aware Tiny BERT for Detecting Social Engineering Emails	Fine tuning of a pre-trained Bidirectional Encoder Representations from Transformers (BERT) model by replacement of half the transformer	Email content and context features from the email header are learnt to detect phishing.	A detection rate of 87%. Resilience to word attacks such as random re-ordering, use of typos and synonyms.

			blocks with simple adapters.		
6	(Verma et al., 2020)	Email phishing: Text classification using natural language processing	Natural language processing (NLP) and Support Vector Machine (SVM) linear classifier	Email processing by removing stop words, punctuations, special characters, tokenization, stemming, part of speech tagging, language detection, and identification of semantic relations	SVM classification accuracy of 98.77%.
7	(Mansour & A. Alenizi, 2020)	Enhanced Classification Method for Phishing Emails Detection	K-Nearest Neighbors (KNN), Naïve Bayes, Support Vector Machine (SVM) and Decision Tree (J48) classification	Hybrid feature selection method via Information Gain and Genetic Algorithm	A 98.9% accuracy rate.
8	(Halgaš et al., 2020)	Catching the Phish: Detecting Phishing Attacks using Recurrent Neural Networks (RNNs)	Recurrent neural network (RNN) phishing classifier with Long Short-Term Memory (LSTM) layers	Text and textual structure content features in the email transformed into a sequence of symbol and word tokens and represented as unique integers	An accuracy of 98.91%, Precision of 98.74% and F-score of 98.63%. Flexibility to continuously classify new trends.
9	(Salahdine et al., 2021)	Phishing Attacks Detection: A Machine Learning-Based Approach	Artificial Neural Network (ANN) with two hidden layers, 100 neurons each, and Rectified Linear Unit (ReLU) activation	Extraction of content features present in the email body and header.	ANN classification accuracy of 94.5%

10	(Abdelaziz et al., 2021)	A Novel Phishing Email Detection Algorithm based on Multinomial Naive Bayes Classifier and Natural Language Processing	Natural language processing (NLP) and multinomial Naïve Bayes (NB) classifier	Lexical and semantic analysis of email content to create a bag of words model by removing special and single characters, multiple spaces, lemmatization, and conversion into lowercase	Accuracy of 96.03% for balanced datasets and 97.21% for imbalanced datasets
11	(Ahmed et al., 2021)	Effective Phishing Emails Detection Method	Multi-layer perceptron (MLP) neural network and Random Forest classifiers with feature selection by Term Frequency-Inverse Document Frequency (TF-IDF) and Information Gain (IG).	Extracts the header and hyperlinks in the email to detect phishing	An accuracy of 99.46% was obtained using 25 out of 36 of the best features selected by Information Gain (IG), and evaluated using 10-fold cross validation.
12	(Franchina et al., 2021)	Detecting phishing e-mails using Text Mining and features analysis	Text mining and text analytics by text categorization, information extraction, clustering, and text summarization.	Email metadata and content - including the body and subject are analyzed to detect phishing.	An accuracy of 99.2%.
13	(Bagui et al., 2021)	Machine Learning and Deep Learning for Phishing Email Classification using One-Hot Encoding	Convolutional Neural Network (CNN) with Word Embedding and One-Hot Encoding Representation of Words	Inherent characteristics of email body captured by deep semantic analysis using Continuous Bag of Words (CBOW)	Accuracy of 96.34%.

14	(Bountakas et al., 2021)	A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection	Natural Language Processing by TF-IDF, Word2Vec, and BERT. Classification by Random Forest, Decision Tree, Logistic Regression, Gradient Boosting Trees, and Naïve Bayes	Text feature extraction of a pre-processed email and chi-square-based feature selection to reduce train time.	An accuracy of 98.95% for Word2Vec with Random Forest for a balanced dataset, and 98.62% for Word2Vec with Logistic Regression for an imbalanced dataset.
15	(Korkmaz et al., 2022)	A Hybrid Phishing Detection System Using Deep Learning-based URL and Content Analysis	Generative Convolutional Neural Network (GCNN) - a combination of Generative Adversarial Network (GAN) and Convolutional Neural Network (CNN) models was used to classify malicious embed URLs and a deep neural network (DNN) for content inspection.	TshPhish - Two stage hybrid phishing detection - A hybrid model to inspect for malicious embedded URLs in an email, and content of the email.	97.68% accuracy for the URL-based GCNN model, 93.69% accuracy for the content based DNN, and 98.37% accuracy for the TshPhish model evaluated by 5-fold cross-validation.
16	(Noah et al., 2022)	PhisherCop: Developing an NLP-Based Automated Tool for Phishing Detection	Built upon Stochastic Gradient Descent classifier (SGD) and Support Vector Classifier (SVC).	Predicts a phishing email by analyzing the content such as subject line, email address and body.	An average accuracy of 96% was achieved.

17	(Chowdhury et al., 2022)	Phishing Detection Using Natural Language Processing and Machine Learning	Multiple ensembles of multiple neural network models.	DARTH framework used to extract the email body text, embedded URLs, email metadata e.g., headers, and other features e.g., attachments	A precision of 99.97%, f-score of 99.98%, and accuracy of 99.98%
18	(Somesha & Pais, 2022)	Classification of Phishing Email Using Word Embedding and Machine Learning Techniques	Word embedding by TF-IDF, Count Vectorization, Word2Vec and FastText. Classification by Random Forest, SVM, Logistic Regression, Decision Tree, and XG Boost	Email header features extracted from emails to create a dictionary via heuristic methods (tokenization and lemmatization). Vectorization performed by word embedding and fed to classifier.	An accuracy of 99.50% for FastText-Continuous Bag of Words (CBOW) with Random Forest classification.
19	(Bountakas & Xenakis, 2023)	HELPHED: Hybrid Ensemble Learning Phishing Email Detection	Stacking and Soft Voting Ensemble Learning algorithms were separately used to process the hybrid features in parallel. Decision Trees were used to classify the content features and k-nearest neighbors for the text features.	Hybrid features taken from the email message body and email content such a header, attachments, etc. were converted into an input representation.	The Soft voting ensemble learning method performed best with an f1-score of 0.9942, 99.43% accuracy, precision, and recall. A low training time of 0.0313seconds with 0.9714 area under the curve (AUC), and 0.967 Matthews correlation

					coefficient (MCC).
20	(Muralidharan & Nissim, 2023)	Improving malicious email detection through novel designated deep-learning architectures utilizing entire email	An ensemble of deep learning classifiers comprising of convolutional neural network (CNN) and Bidirectional Encoder Representations from Transformers (BERT) models with output from an XGBoost model.	All segments of the email, i.e., the header, body, and attachments are analyzed by the deep learning framework.	An area under the curve (AUC) value of 0.993 and a true positive rate (TPR) of 5%.

Source: References in Table (2019-2023)

2.2.2 Risk Scales

The Virtual Risk Officer (VRO) created by KnowBe4 (2022) is a dynamic user interaction-based risk scale. Various risk factors quantify the risk of a user or an organization. The VRO shows how possible it is to phish a user. (KnowBe4®, 2022b) The Tessian (2021) Human Layer Rik Hub provides risk scores to users and groups according to how they handle their emails. The risk score increases when a user makes an insecure action and reduces by secure ones. Present and past emails and identity data populate a behavior intelligence model (BIM) that dynamically creates a risk profile of the users in real-time. (Tessian®, 2021) Yang et al. (2022) performed a study to enable scaling of the phishing risk of a user by considering the effect of their personality using what they termed a multidimensional phishing susceptibility prediction model (MPSPM). (R. Yang et al., 2022) Affinity IT Security Services (2019) have a dynamic scale to compute the risk of an interacting user relatively. The users begin with a neutral score of 5. Ignoring a phishing attempt lowers the risk score by 1, whereas informing about it lessens the risk by 2. If a user clicks on a link in the phishing plot, the score on the scale increases by 1, and giving up sensitive data increases it by 2. (Affinity IT Security Services, 2019) LexisNexis' (2017) risk scale, Emailage, gives a rating of the risk of the email address that the user has received an email from. Different factors such as the domain of the email or the IP address are used to give judgement. (LexisNexis® Emailage®, 2022) Steves et al. (2020) measure phishing risk by observable characteristics in the email itself, such as the number of cues and the premise alignment. Cues are indicators in the email that would give away the identity of the hacker. E.g. a suspiscious looking attachment. The premise alignment is a spear-phishing factor that shows how the email content relates to the target's premises. e.g., knowledge of the target's work culture and context, responsibilities, expectations as a group, etc. Risk severity accounts for the challenge a user faces in detecting a phishing email. The less the number cues and the greater the premise alignment imply that it is harder for phishing to be detected. The risk is eventually greater.

Table 2. 2: Comparison of Risk Scales

SN	Author	Name of Risk Scale	Type of Risk Scale
1	KnowBe4® (2017)	Virtual Risk Officer (VRO)	User Personality and Interaction
2	LexisNexis® Risk Solutions (2017)	Emailage	Email Identity
3	Affinity IT Security Services (2019)	"Phishing Risk " scale	User Interaction
4	Steves et al. (2020)	NIST Phish Scale	Email Content
5	Tessian® (2021)	Tessian Human Layer Rik Hub	User Personality and Interaction
6	Yang et al. (2022)	Multidimensional Phishing Susceptibility Prediction Model (MPSPM)	User Personality

Source: (KnowBe4®, 2022b) (Tessian®, 2021) (R. Yang et al., 2022) (Affinity IT Security Services, 2019) (LexisNexis® Emailage®, 2022) (Steves et al., 2020)

2.3 Research Gap

Despite many interesting efforts made to efficiently detect phishing by examining the content of the email using artificial intelligence techniques, improvements may be made to further classify the detected phishing emails based on the emotional sentiment within its context and provide ratings of the risk posed by such a class of phishing emails. The risk scale proposed by Yang et al. (2022) deals with the personality of the user while that from Affinity IT Security Services (2019) works with how the user interacts with the email. KnowBe4 (2022) and Tessian (2021) risk scales combine the effects of user personality and user interaction with the phishing email to rate the risk. LexisNexis (2017) used the identity features of the email. Steves et al. (2020) analyzed the actual email content. All of the risk scales with the exception of Steves et al. (2020) focus on the user behaviour or the email address. This study proposes a scale to measure risk based on the content written by the hacker in the email. Although Steves et al. (2020) have proposed a similar type of scale, their technique has not critically dealt with emotional triggers in the email content. Since social engineering mainly aims at targeting human emotions, it is essential to lay focus on that aspect.

2.4 Conceptual framework

In the first case of our conceptual framework, we have two dependent categorical variables which are components of the phishing security risk. i.e., the probability of interacting with a phishing email, and the frequency of receiving a phishing email. The independent variable is a categorical variable i.e., the social engineering techniques or the phishing variable.

In the second case of our conceptual framework, we have six different independent categorical variables, i.e., demographics. They are namely, gender, age range, education level, professional status, nature of institution, and field of work. Like the first case, the two components of the phishing security risk, i.e., the probability of interacting with a phishing email, and the frequency of receiving a phishing email, are the two dependent categorical variables. The social engineering techniques or the phishing variable is a moderating categorical variable. It affects the relationship between the independent and dependent variables.

Relationships between categorical variables are determined using non-parametric tests.

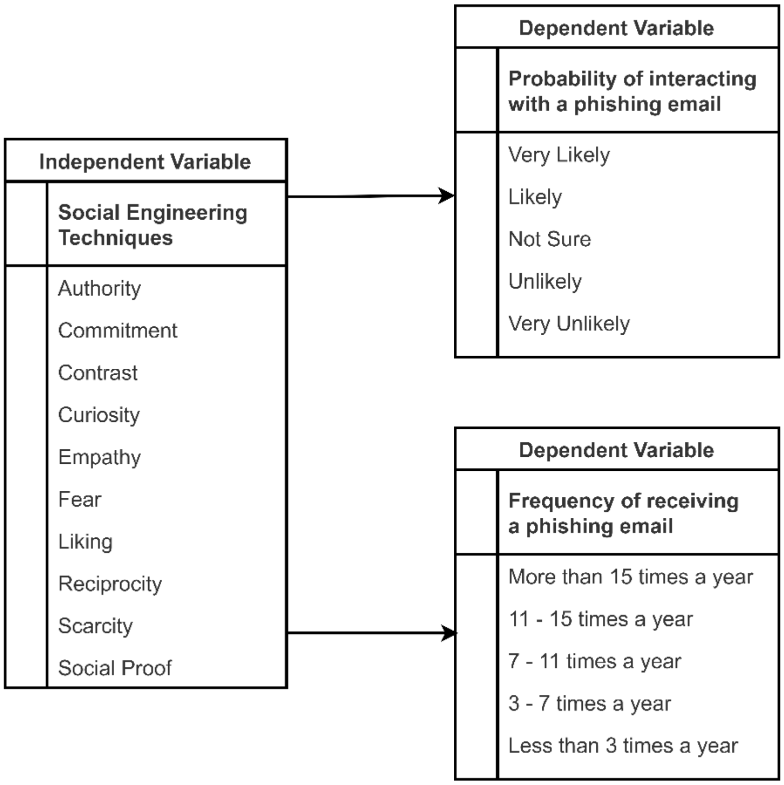


Figure 2. 2: Conceptual framework – Case I

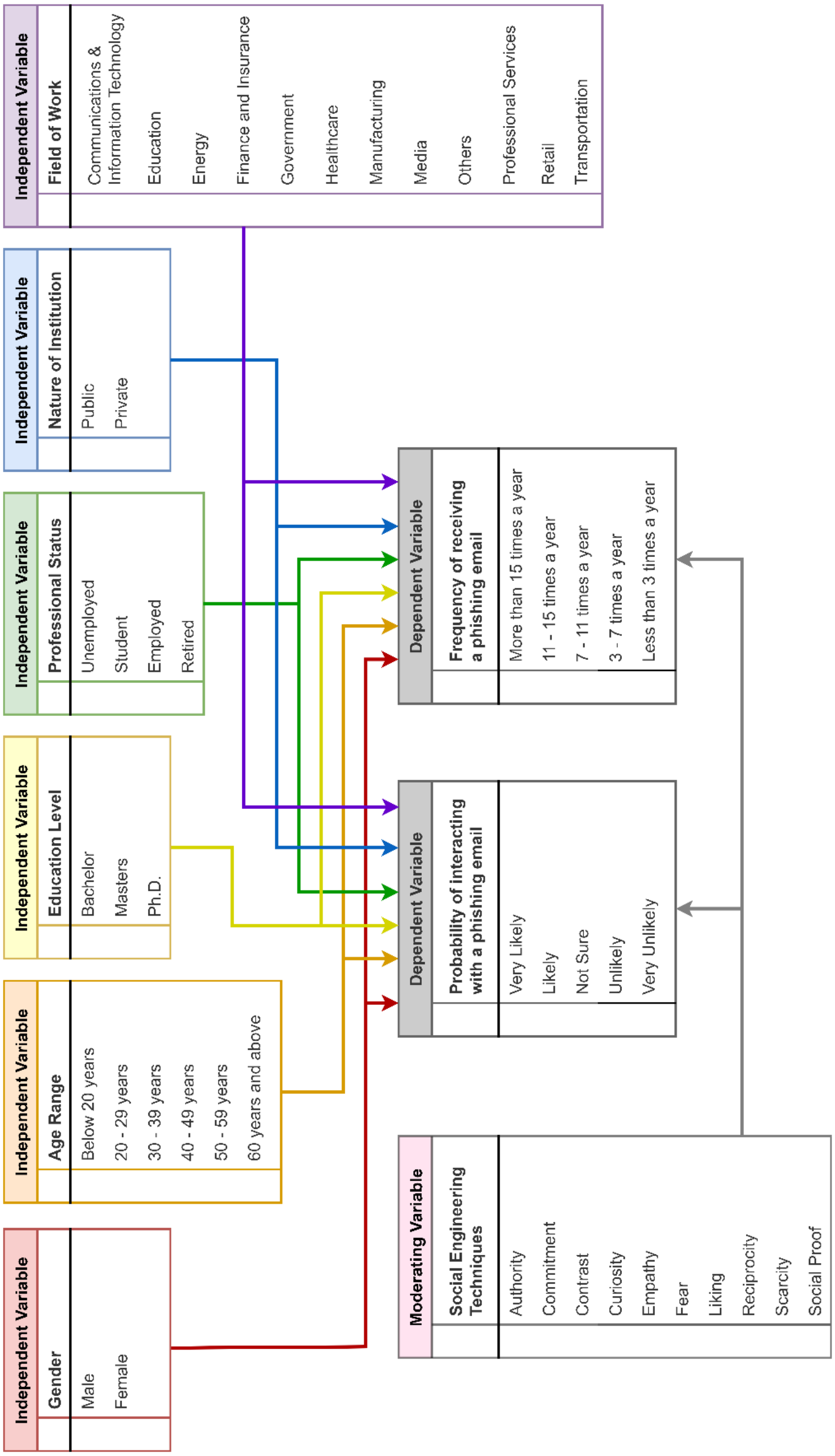


Figure 2. 3: Conceptual framework – Case II

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Research Philosophy

Positivism philosophy uses objective and quantitative methods for analysis. Al-Ababneh (2020) explains how positivism adds certainty to where knowledge is seen to be accurate and firmly grounded. He defines it as being used with regards to a posited thing, i.e., something given. He illustrates how it deals with observations made by scientific methods with a direct form of experience rather than speculation. Dawadi et al. (2021) explains how scientific discoveries are presented by positivism and how confidence in science and objectivity are portrayed. They discuss how statistical analysis, structured methodology and observations that can be quantified are needed. (Al-Ababneh, 2020) (Dawadi et al., 2021)

Interpretivism philosophy uses subjective and qualitative methods for analysis. Al-Ababneh (2020) talks of interpretivism philosophy contradicting the main aspects of positivism philosophy. He points out on how it focuses on subjective and descriptive means of developing knowledge. The interpretivism research paradigm uses qualitative tools such as observations, interviews, questionnaires, etc., to gain an understanding of the idea and elaborate the findings noticed. (Al-Ababneh, 2020) (Dawadi et al., 2021)

3.2 Research Approach

Al-Ababneh (2020) highlights two distinct approaches to research, namely, the deductive and inductive approaches. He explains how the deductive approach concentrates on building hypotheses and theory as well as describing relationships between variables. The research strategy that is designed deductively aims at testing the hypotheses. The positivist philosophy relates to the deductive approach. He emphasizes on the necessity to align the research philosophies with the approach used. An inductive approach deals with data collection and development of theories from data analysis. The interpretivist philosophy relates to the inductive approach. (Al-Ababneh, 2020)

Okoli (2021) explains deductive reasoning as the inference of a situation of a specific case from a general rule under study and deductive theorizing as the deriving of newly enhanced theories from a proposed theory. He describes inductive reasoning as drawing general rules from specific cases brought up and inductive theorizing as the creation of theory from non-theoretical phenomena. (Okoli, 2021)

3.3 Research Design

Research questions are transformed into projects by properly fitting the research design. The processes, methods, strategy, and sampling techniques may be selected from the research design. The objective of the research shall determine the selection of the design.

An exploratory study looks into things that occur, searches for new insights, asks questions, and creates thoughts and assumptions for research to come. It is used at times when the information on the topic is scarce or unavailable. Likewise, in situations where seldom research on the topic has been performed in the past to give a clearer picture of the research problem. Literature searches and interviews are among the main ways of performing an explorative study.

The descriptive study aims at describing various aspects of the phenomena across different levels and perspectives. It portrays the researched item with accuracy thus requiring enough information collected about it. Characteristics of variables are found out.

An explanatory study targets getting explanations, predictions on probable outcomes, or patterns exhibited by the researched item. It works at establishing relationships between variables or differences among the groups of the variables through testing of hypotheses. (Al-Ababneh, 2020)

3.4 Research Methods

Al-Ababneh (2020), Kandel (2020) and Dawadi et al. (2021) describe a mixed research methodology to be a method of collection and analysis of both quantitative and qualitative research data using both quantitative and qualitative research methods. It utilizes the strengths of both methodologies as it makes up for the limitations of each method. The two methods are used to answer complex research questions and provide insights from different perspectives that cannot be achieved by a single method alone. The mixed research method combines positivism and interpretivism research philosophies to provide breadth and depth respectively. (Kandel, 2020) (Dawadi et al., 2021) (Al-Ababneh, 2020)

Kandel (2020) elaborates on both quantitative and qualitative research methodologies. The analysis of numerical data using mathematical methods to explain a phenomenon is a quantitative research methodology. Variations being studied are quantified. Hypothesis and theories related to a particular phenomenon are developed to give answers on the relationships of variables. Quantitative research works with numbers and measurable items. On the contrary, qualitative research observes the things said and done by people for analysis and interpretation. It aims at building an understanding of the concepts and meaning of phenomena. Unlike the quantitative methodology that is objective, qualitative research methods are subjective and depend on data from, and experience of people through interviews, discussions, and the like. Some insights that cannot be elucidated with only quantitative data are shown by qualitative research. Exploration is performed to acquire an understanding of social problems. Kandel (2020) suggests that the world we live in, and the way things are in it, are understood better with the aid of qualitative research whose goal is to generate concepts to discern the nature of society. The quantitative methodology follows the positivism philosophy while the qualitative methodology grounds on the interpretivism philosophy.

Mwita (2022) outlines two types of data, namely primary and secondary data. He points out the differences between them. Primary data is firsthand data collected by a researcher for the first time through methods such as observing, interviews, discussions, and questionnaires. On the other hand, secondary data is data conveniently available for researchers through methods such as literature surveys and document analysis. Such data is collected by other individuals beforehand. (Mwita, 2022)

3.5 Research Strategy

Al-Ababneh (2020) explains how the research strategy is a generalized plan established to give responses to research questions. The strategy is intended to formulate the data collection methodology and organize the research objectives. He mentions various strategies such as surveys, experiments, case studies, etc. Strategy selection is dependent on factors such as the research objectives, philosophy, questions, and knowledge that exists.(Al-Ababneh, 2020)

An interpretivism research philosophy is used for the main objective that is based on the inductive research approach. A descriptive research design is used to illustrate the security risk scale that enhances phishing detection in mail systems. Primary data is collected by a qualitative research methodology through questionnaires to describe the security risk.

An interpretivism research philosophy is also used for specific objective 1 that is based on the inductive approach. An explorative study design is used to collect secondary data using a qualitative research methodology of literature searching to discover the factors that affect the effectiveness of phishing attempts through mail servers.

A positivism research philosophy is used for specific objective 2 that is based on a deductive research approach. An explanatory research study design is used to explain the design of the security risk scale based on the relationships between the phishing variables and the security risk. Primary data from the questionnaire survey results are used in the statistical tests. A quantitative research methodology is used to perform the non-parametric tests, i.e., Friedman Test and Kruskal-Wallis Test.

A positivism research philosophy is also used for specific objective 3 that is based on a deductive approach. An explanatory type of study design in used to explain how the performance of the proposed risk scale relates to the results of the phishing attack performed at the bank. Primary data is collected from the phishing test to be used in the performance measurement of the proposed risk scale. Quantitative research methods are used to compare the quantitative values derived from the proposed risk scale against the quantitative values that resulted from the phishing test.

Table 3.1 shows the summary of the research strategy that includes the research questions, philosophy, approaches, design, methods and types of data.

Table 3. 1: Summary of research strategy

Research Objective	Research Question	Research Philosophy	Research Approach	Research Design	Research Methods	Type of Data
Main Objective	What security risk scale may enhance phishing detection in mail systems?	Interpretivism	Inductive	Descriptive	Qualitative	Primary
Specific Objective 1	What are the factors that affect the effectiveness of phishing attempts through mail servers?	Interpretivism	Inductive	Explorative	Qualitative	Secondary
Specific Objective 2	What is the design of a security risk scale based on the relationships between phishing variables and the security risk?	Positivism	Deductive	Explanatory	Quantitative	Primary
Specific Objective 3	What is the performance level of the proposed security risk scale against results of a phishing attack performed at a bank?	Positivism	Deductive	Explanatory	Quantitative	Primary

3.6 Data Collection Techniques

Specific Objective 1

For our first specific objective of identifying the factors that affect the effectiveness of phishing attempts through mail servers, an exploratory research methodology is used to gather the data on the phishing factors, which may also be termed as the phishing social engineering techniques.

Specific Objective 2

For our second specific objective of designing a security risk scale based on the relationships between phishing variables and the security risk, a survey was performed to collect data from respondents on the likelihood that they may click a link in a specific class of phishing email and the frequency that they receive such a phishing email of the questioned class.

Specific Objective 3

For our third specific objective of determining the performance level of the proposed security risk scale against results of a phishing attack performed at a bank, a quantitative research methodology was used via simulated phishing attacks at CRDB Bank Plc using the KnowBe4 phishing simulator targeting the employees of the bank. Quantitative data was collected relating to the number of employees that opened the phishing email, the number of employees that clicked on a phishing link in the email, and the number of employees that reported the phishing email as an incident to the Security Operating Center (SOC)

Table 3. 2: Data Collection Techniques

Specific Objective	Data Collection Technique	Type of Data	Sampling Methodology
To identify the factors affecting the effectiveness of phishing attempts through mail messages.	Exploratory Research: Literature Survey	Secondary Data	Purposive Sampling
To design a security risk scale based on the relationships between phishing variables and the security risk.	Qualitative Research: Questionnaire	Primary Data	Purposive Sampling
To assess the performance level of the proposed security risk scale against results of a phishing attack performed at a bank.	Quantitative Research: Simulated Phishing attack	Primary Data	Convenience Sampling (CRDB Bank) Purposive Sampling (Social Engineering Techniques)

3.7 Sampling Methodology

Mulisa (2022) discusses sampling and its types. Sampling can be defined as the selection of units from an entire population that are a representation of the population from which they are selected. The aim behind the selection of samples is to gain insights into the whole population being studied and not only the samples selected from it. Sampling improves preciseness, reduces costs, and time consumed especially when the population is very large. All the characteristics of the population should be contained within the samples. There are two main types of sampling methodologies, namely probability sampling and non-probability sampling.

Probability sampling is also termed as random sampling. The possibility of the selection of a sample from a population is the same for each sample. In other words, there is an equal chance of any sample being selected from the population. The samples are selected randomly. The key assumptions when it comes to probability sampling are that each sample in the population has a non-zero chance of selection and that the selection of one sample has no relation to the selection of another. Often, quantitative research methodologies use probability sampling,

Non-probability sampling or non-random sampling refers to the selection of samples based on a particular reason. It is a judgmental and subjective form of sampling where the researcher uses their expertise to carefully select samples rich in data. It is commonly used in qualitative research or where the resources are limited. (Mulisa, 2022) Kim (2022) supports non-probability sampling to have merits of quick data collection, cost reductions, and ease of engagements with the sample cases. (Kim, 2022)

Purposive sampling as quoted by Staller (2021) and Denny and Weckesser (2022) is a non-probability sampling methodology where the samples are selected based on relevance to the research question and the objective of the study. Samples that provide a depth of view into the research are selected, as they are more informative. (Staller, 2021) (Denny & Weckesser, 2022)

Stratton (2021) and Denny and Weckesser (2022) describe convenience sampling as a non-probability sampling methodology where the samples are selected based on their availability to be a part of the study or accessibility to the researcher. The convenience sampling method is less costly, simple, and takes less time in comparison to other sampling methodologies. (Stratton, 2021) (Denny & Weckesser, 2022)

For the first objective of identifying the factors that affect the effectiveness of phishing attempts through mail messages, a purposive sampling methodology was selected to sample the secondary data collected from various literatures via an exploratory survey.

Similarly, the purposive sampling methodology was used for the second research objective of designing a security risk scale based on the relationships between phishing variables and the security risk as well. Primary data collected from the questionnaires was sampled purposively.

For the third research objective of assessing the performance level of the proposed security risk scale against results of a phishing attack performed at a bank, both purposive and convenience sampling methodologies were used. Convenience sampling was used to select the population and area of performing the simulated phishing attack. Primary data from CRDB Bank Plc employees was chosen as the convenience samples for the phishing test from the population of Dar es salaam, Tanzania. Purposive sampling was used to select the social engineering techniques to be used in the phishing attack test.

3.8 Population and Area of the Research

The questionnaire survey area covered both local and global reach through respondents from domestic and international countries on the online platforms. The population of the questionnaire survey respondents consisted of both male and females. The age range selected was 20 years and above. The minimum education level of respondents was the bachelor’s degree from any field. Both working and unemployed, students, and retired individuals were sampled. Various business and industrial sectors from both public and private institution where the respondents work was considered, such as communications & information technology, education, energy, finance and insurance, government, healthcare, manufacturing, media, professional services, retail, transportation, and others. Table 3.3 below shows the demographic information collected from the respondents that make up the population for the questionnaire survey.

Table 3. 3: Demographic Information

SN	Demographic	Groups of Respondents
1	Gender	• Male • Female
2	Age Range	• 20 – 29 years • 30 – 39 years • 40 – 49 years • 50 – 59 years • 60 years and above
3	Education Level	• Bachelor • Masters • Ph.D.
4	Professional Status	• Unemployed • Student • Employed • Retired
5	Nature of Institution	• Public/Government sector • Private sector
6	Field of Work	• Finance and Insurance • Manufacturing • Energy

		• Retail • Professional Services • Government • Healthcare • Media • Transportation • Education • Communications & Information Technology • Others

Oreku (2020) describes how financial organizations and transaction processing institutions are key targets of threat actors performing cybercrime in Tanzania. (Oreku, 2020) Mpofu and Mhlanga (2022) observed that Tanzania has a strong dependency on mobile money for official and non-official transactions with inclusions both rural and urban regions. (Mpofu & Mhlanga, 2022) Ntigwigwa (2019) points out mobile money services in Tanzania as a vector for cybercrime. (Ntigwigwa, 2019) The survey performed by Nuru (2020) on mobile banking customers revealed the belief in the presence technological risk despite of cybersecurity measures. (Nuru, 2020) Chanda (2020) assessed electronic banking services and found that fraud is present as a result of cyberattacks that in turn leaves customers with fear of losing their funds. (Chanda, 2020) The phishing activity trends report of quarter 4 of 2022, produced by the anti-phishing working group (APWG) in collaboration with their founding member OpSec Security, uncovered that phishing attacks against the financial sector that includes banks, are the highest targeted industry sector, with 27.7% of the phishing attacks. This is an increase from the previously recorded 23.2% in quarter 3 of 2022. (APWG, 2022) From this information it can be seen that the financial and banking sector in Tanzania and worldwide is a major area that cybercriminals are trying to exploit. The phishing experiment research area was conveniently sampled to be at CRDB Bank Plc Head Office in Dar es salaam, Tanzania, targeting the population of employees from different departments of the bank, as it is one of the largest commercial banks in Tanzania. (K. Mbura & Sekela, 2020) Demographic information collection of employees targeted in the phishing attack was not part of the scope of the phishing experiment. Figure 3.1 below shows the financial institutions as the most targeted industry sector in the fourth quarter of 2022.

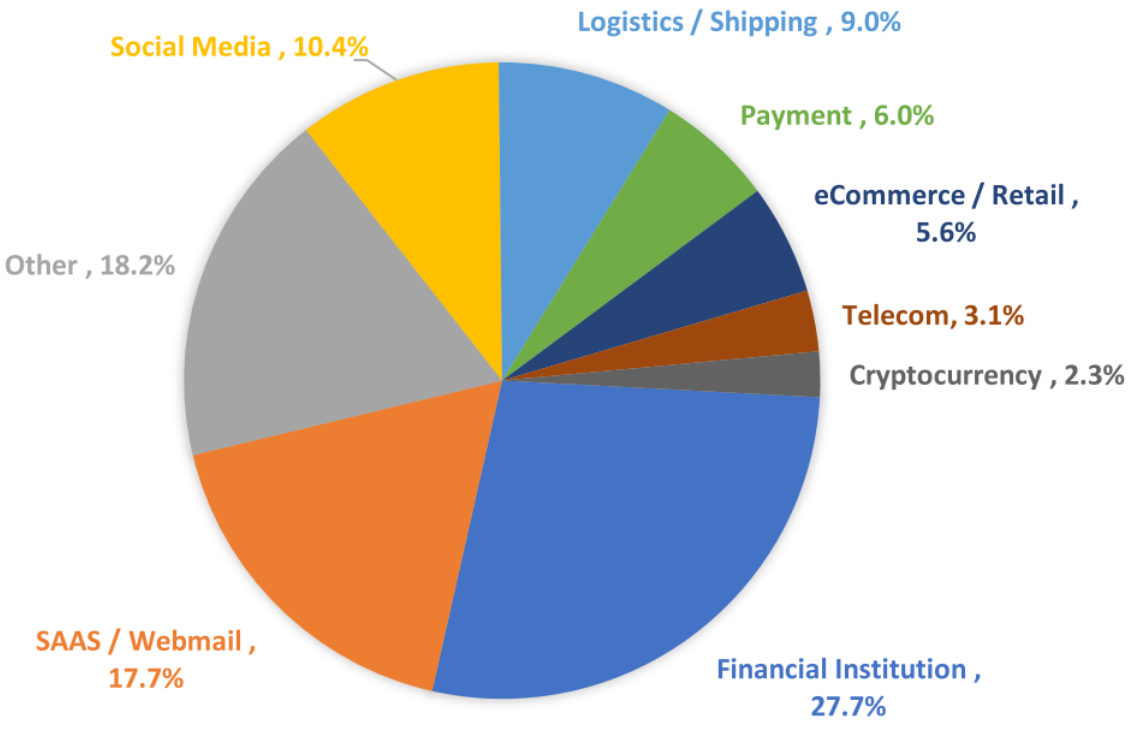


Figure 3. 1: Most targeted industry sectors in Quarter 4 of 2022

Source: APWG (2022)

3.9 Hypothesis and Testing Methodology

3.9.1 Variables

Kaliyadan and Kulkarni (2019) highlight variables and their types. A variable can be considered as a statistical data component that has a value that can vary in quantity or quality. It is a unique characteristic of an element in a population or its samples. Variables can be classified as quantitative or qualitative variables. Quantitative variables are those that vary in their quantity, for example the number of successful phishing hacks in a day. Likewise, qualitative variables vary in quality, for example the susceptibility of a user to being hacked by phishing emails.

Quantitative variables are classified into discrete quantitative variables and continuous quantitative variables. Discrete variables are taken as those that do not have any quantifiable values that can exist between a pair of two discrete values. On the contrary, continuous variables can have any values existing between two continuous values.

Qualitative variables are also called categorical variables. They can be classified into nominal and ordinal variables. Nominal variables are those that contain two categories or more but have no inherent order. E.g., the field of work of an individual. It could be Information Technology, Manufacturing, Retail, Healthcare, Education, etc. Dichotomous variables are a type of nominal variable that specifically contains two categories without rank or order. E.g., Gender which could be a male or female. Ordinal variables on the other hand contain two or more categories that have order or rank. E.g., Education Level where the bachelors are the lower rank, followed by masters, the higher rank, and Ph.D., the highest rank.

Variables may also be classified as dependent and independent variables. Dependent variables depend on the independent variables. The independent is the variable that can be manipulated to see how the dependent variable changes as a result. (Kaliyadan & Kulkarni, 2019)

Table 3. 4: Categorical dependent variables

Categorical Dependent Variables
Dependent Ordinal variable: Probability of interacting with a phishing email • Very unlikely (1) • Unlikely (2) • Not sure (3) • Likely (4) • Very likely (5) *Dependent Ordinal variable: Frequency of receiving a phishing email* • Less than 3 times a year (1) • 3 - 7 times a year (2) • 7 - 11 times a year (3) • 11 - 15 times a year (4) • More than 15 times a year (5)

Source: Field data (2022)

Table 3. 5: Categorical independent variables and the groups within them

Categorical Independent variables (Demographics)	**Groups within the Categorical Independent Variables**	**Type of Variable/Scale**
Gender	• Male • Female	Nominal Variable (Dichotomous)
Age Range	• 20 – 29 years • 30 – 39 years • 40 – 49 years • 50 – 59 years • 60 years and above	Ordinal Variable
Education Level	• Bachelor • Masters • Ph.D.	Ordinal Variable
Professional Status	• Unemployed • Student • Employed • Retired	Ordinal Variable
Nature of Institution	• Public/Government sector • Private sector	Nominal Variable (Dichotomous)
Field of Work	• Finance and Insurance • Manufacturing • Energy • Retail • Professional Services • Government • Healthcare • Media • Transportation • Education • Communications & Information Technology • Others	Nominal Variable

Source: Field data (2022)

Table 3. 6: Categorical independent variable (Social engineering techniques)

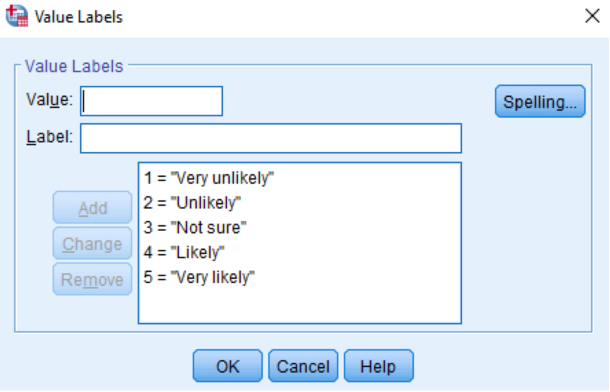
Categorical Independent variable (Social engineering techniques)
Authority
Commitment
Contrast
Curiosity
Empathy
Fear
Liking
Reciprocity
Scarcity
Social Proof

Source: Field data (2022)

3.9.2 Coding

Williams and Moser (2019) describe coding as key operation that assembles the data that is collected in qualitative research and performs organized classification and sorting to derive a meaning. Hidden concepts can be uncovered from the data through coding processes that allow data analytics and steps to achieve the research objectives. (Williams & Moser, 2019) The IBM© Statistical Package for Social Sciences (SPSS) uses "Value Labels" to code the variables that are assessed. In this study, integer number codes have been used to represent the various variables used so mathematical computations can be performed on them in IBM SPSS.

Figure 3.2 shows the coding methodology for the first dependent ordinal variable used in the research, i.e., the probability of a subject interacting with a phishing email.

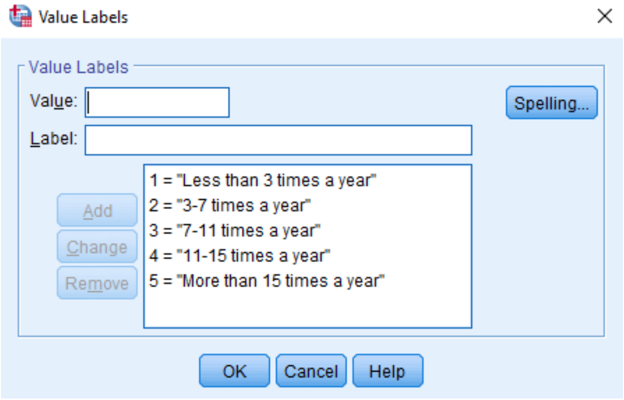


1 = "Very unlikely"
2 = "Unlikely"
3 = "Not sure"
4 = "Likely"
5 = "Very likely"

Figure 3. 2: Coding of the probability of a subject interacting with a phishing email

Source: IBM SPSS (2022)

Figure 3.3 shows the coding methodology for the second dependent ordinal variable used in the research, i.e., the frequency of a subject receiving a phishing email.

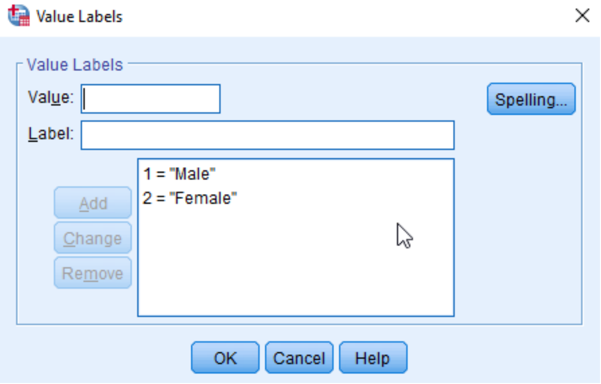


1 = "Less than 3 times a year"
2 = "3-7 times a year"
3 = "7-11 times a year"
4 = "11-15 times a year"
5 = "More than 15 times a year"

Figure 3. 3: Coding of the frequency of a subject receiving a phishing email

Source: IBM SPSS (2022)

Figure 3.4 shows the coding methodology for the categorical independent ‘gender’ demographic variable.

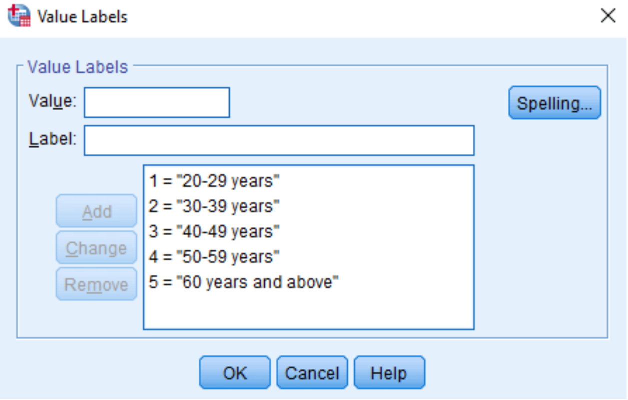


1 = "Male"
2 = "Female"

Figure 3. 4:Coding of the gender

Source: IBM SPSS (2022)

Figure 3.5 shows the coding methodology for the categorical independent 'age range' demographic variable.

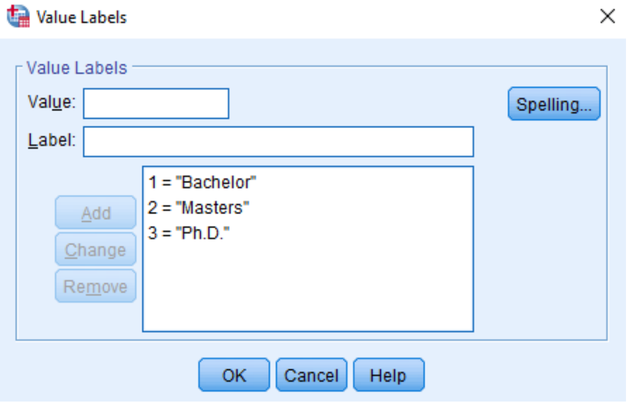


1 = "20-29 years"
2 = "30-39 years"
3 = "40-49 years"
4 = "50-59 years"
5 = "60 years and above"

Figure 3. 5: Coding of the age range

Source: IBM SPSS (2022)

Figure 3.6 shows the coding methodology for the categorical independent 'education level' demographic variable.

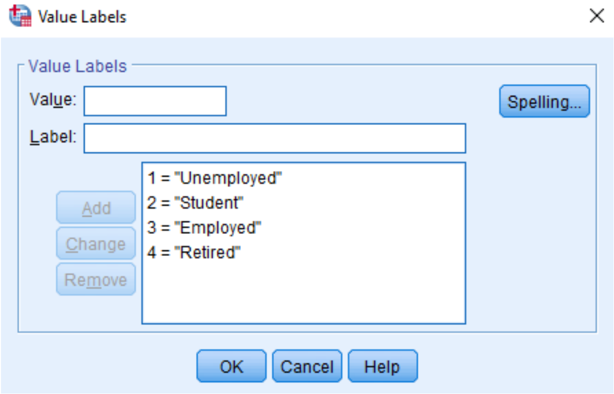


1 = "Bachelor"
2 = "Masters"
3 = "Ph.D."

Figure 3. 6: Coding of the education level

Source: IBM SPSS (2022)

Figure 3.7 shows the coding methodology for the categorical independent ‘professional status’ demographic variable.

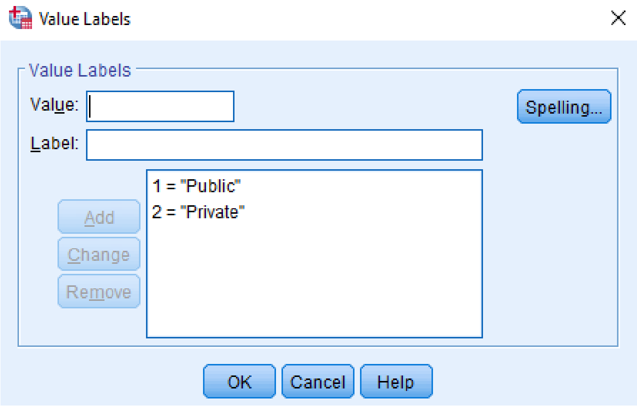


1 = "Unemployed"
2 = "Student"
3 = "Employed"
4 = "Retired"

Figure 3. 7: Coding of the professional status

Source: IBM SPSS (2022)

Figure 3.8 shows the coding methodology for the categorical independent ‘nature of institution’ demographic variable.

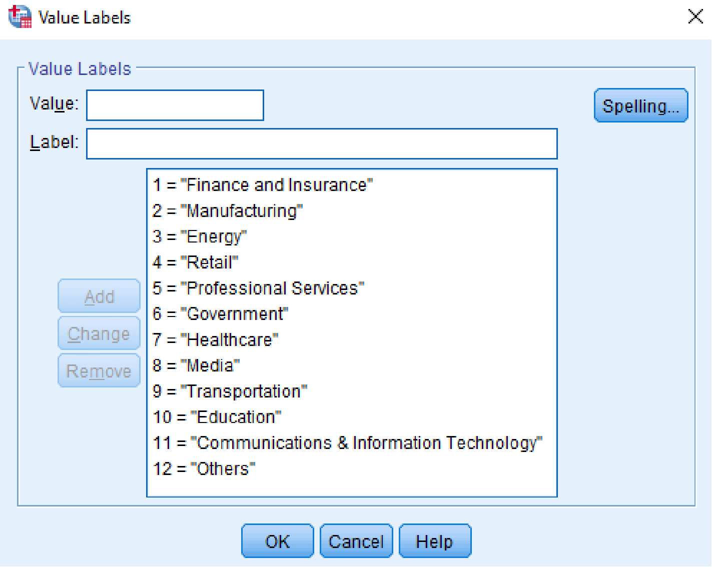


1 = "Public"
2 = "Private"

Figure 3. 8: Coding of the nature of institution

Source: IBM SPSS (2022)

Figure 3.9 shows the coding methodology for the categorical independent ‘field of work’ demographic variable.



1 = "Finance and Insurance"
2 = "Manufacturing"
3 = "Energy"
4 = "Retail"
5 = "Professional Services"
6 = "Government"
7 = "Healthcare"
8 = "Media"
9 = "Transportation"
10 = "Education"
11 = "Communications & Information Technology"
12 = "Others"

Figure 3. 9: Coding of the field of work

Source: IBM SPSS (2022)

3.9.3 Statistical tests

Orcan (2020) identifies the groups of statistical tests. i.e., parametric, and non-parametric tests. Parametric tests are tests that assume that data being tested by the researcher follows a distribution, e.g., the normal distribution. They are commonly used for testing quantitative variables. Non-parametric tests are regarded as distribution-free tests as the data tested by the researcher does not follow any distribution. These tests are generally selected when testing qualitative variables. (Orcan, 2020)

There are many various types of non-parametric tests, however, this study incorporates two important types, namely the Friedman test and the Kruskal-Wallis H Test.

Andrade (2019), Shrestha (2019), Di Leo and Sardanelli (2020), Lovell (2020), Sedgwick et al. (2022) discuss the testing of hypothesis. The null hypothesis (H_0) assumes that the variables that are being tested do not have any effect on each other or have no relationship between each other. It claims that any findings are insignificant to support the concept being studied. The alternative hypothesis (H_a) assumes that the variables being tested influence each other or a relationship exists between them. It claims that findings are significant in supporting the concept under study. The alternative is the opposite of the null hypothesis. When the null hypothesis is found to be false then the alternative hypothesis is true. A *p*-value, also known as the probability value or the asymptotic significance, is a number that ranges between 0 and 1 denoting the statistical significance level. The *p*-value describes how probable it is that the data you have collected is the way it is only because of chance and randomity. When the *p*-value is very large it is highly possible that random chance led to the data. In such a situation, the null hypothesis is true. When the *p*-value is very small it is less possible that your data is the result of random chance. It is thus strongly supported to reject the null hypothesis and accept the alternative hypothesis.

The significance level (α) and confidence levels are quite similar measurements. The significance level measures the assurance needed before the null hypothesis may be rejected. The significance level is decided by the researcher prior to performing the tests. In other words, the significance level may be regarded as the probability that you shall reject the null hypothesis, when in the real sense, it happens to be true. It is a Type I error. The confidence level expresses how confident you are that your findings are statistically significant in supporting your studied concept. The significance level is commonly chosen as $\alpha = 0.05$. This means there is a risk of 5% in concluding that the variables you are testing are related to each other, while they happen to have no relationship at all. The confidence level is evaluated by taking 1 – significance level (α). This means that you are 95% confident that you are correct when you choose to reject the null hypothesis.

A statistical significance in the results occurs when the asymptotic significance or *p*-value is less than or equal to the significance level (α). i.e., $p \leq \alpha$. In common cases, $p \leq 0.05$. This means that you shall reject the null hypothesis and accept the alternative hypothesis if you get an asymptotic significance (*p*) less than 0.05. The results are said to not be statistically significant when the asymptotic significance or *p*-value is greater than the significance level (α). i.e., $p > \alpha$. In the common case, $p > 0.05$. This means that we shall fail to reject the null hypothesis and rather reject the alternative hypothesis. We normally do not accept the null hypothesis but rather fail to reject it. (Andrade, 2019) (Shrestha, 2019) (Di Leo & Sardanelli, 2020) (Lovell, 2020) (Sedgwick et al., 2022)

3.9.3.1 Friedman test

Salerno et al. (2021) illustrate the Friedman and Wilcoxon signed rank tests. The Friedman test is used for the comparison of a group of dependent variables. The Wilcoxon signed rank test is a case of the Friedman test where two dependent variables are compared for specific differences between the groups. (Salerno et al., 2021)

The Friedman test is used in this research to find out if there is any statistically significant difference between two or more of the groups of our independent variable i.e., the social engineering techniques on the ordinal dependent variable i.e., the probability of interacting with a phishing email, measured on a 5-point scale, or the frequency of receiving a phishing email, measured on a 5-point scale.

Table 3.7 below shows the Friedman test variables. The phishing social engineering techniques are categorical independent variables. Both the probability of interacting with a phishing email and the frequency of a subject receiving a phishing email are categorical dependent ordinal variables.

Table 3. 7: Friedman Test variables

Statistical Test	**Categorical Independent variable (Social engineering techniques)**	**Categorical Dependent Variables**
Friedman test	Authority	*Dependent Ordinal variable: Probability of interacting with a phishing email* • Very unlikely (1) • Unlikely (2) • Not sure (3) • Likely (4) • Very likely (5) *Dependent Ordinal variable: Frequency of receiving a phishing email* • Less than 3 times a year (1) • 3 - 7 times a year (2) • 7 - 11 times a year (3) • 11 - 15 times a year (4) • More than 15 times a year (5)
	Commitment	
	Contrast	
	Curiosity	
	Empathy	
	Fear	
	Liking	
	Reciprocity	
	Scarcity	
	Social Proof	

Null Hypothesis Statement 1 for the Friedman Test

There is no statistically significant difference between the groups of phishing social engineering techniques in affecting the probability of a subject interacting with a phishing email.

Alternative Hypothesis Statement 1 for the Friedman Test

There is a statistically significant difference between the groups of phishing social engineering techniques in affecting the probability of a subject interacting with a phishing email.

Figure 3.10 below shows the illustration of the Friedman test for testing of the hypothesis stated above. The independent variable group is the social engineering techniques. It is tested against the probability of a subject interacting with a phishing email, i.e., an ordinal variable with ‘1’ representing a very unlikely probability and ‘5’ a very likely probability. An asymptotic significance value less than 0.05 ($p < 0.05$) will result in the rejection the null hypothesis stated above and acceptance of the alternative hypothesis. An asymptotic significance value greater than 0.05 ($p > 0.05$) will result in a failure to reject the null hypothesis stated above and consequential rejection of the alternative hypothesis.

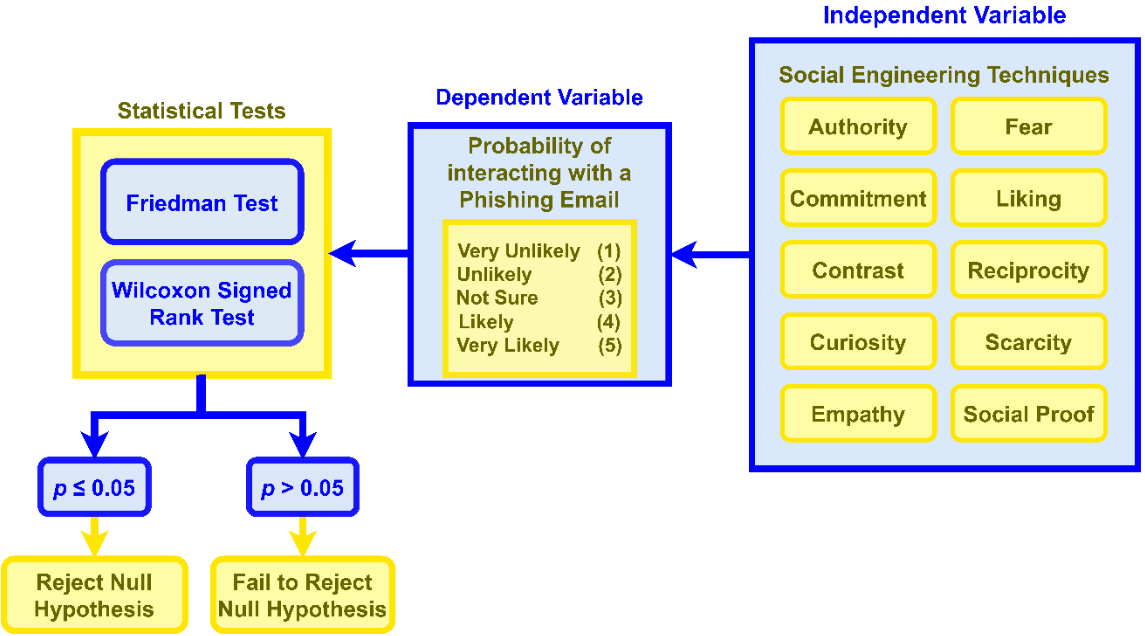


Figure 3. 10: Friedman test for the relation between social engineering techniques and the probability of interacting with a phishing email

Null Hypothesis Statement 2 for the Friedman Test

There is no statistically significant difference between the groups of the phishing social engineering techniques in affecting the frequency of a subject receiving a phishing email.

Alternative Hypothesis Statement 2 for the Friedman Test

There is a statistically significant difference between the groups of the phishing social engineering techniques in affecting the frequency of a subject receiving a phishing email.

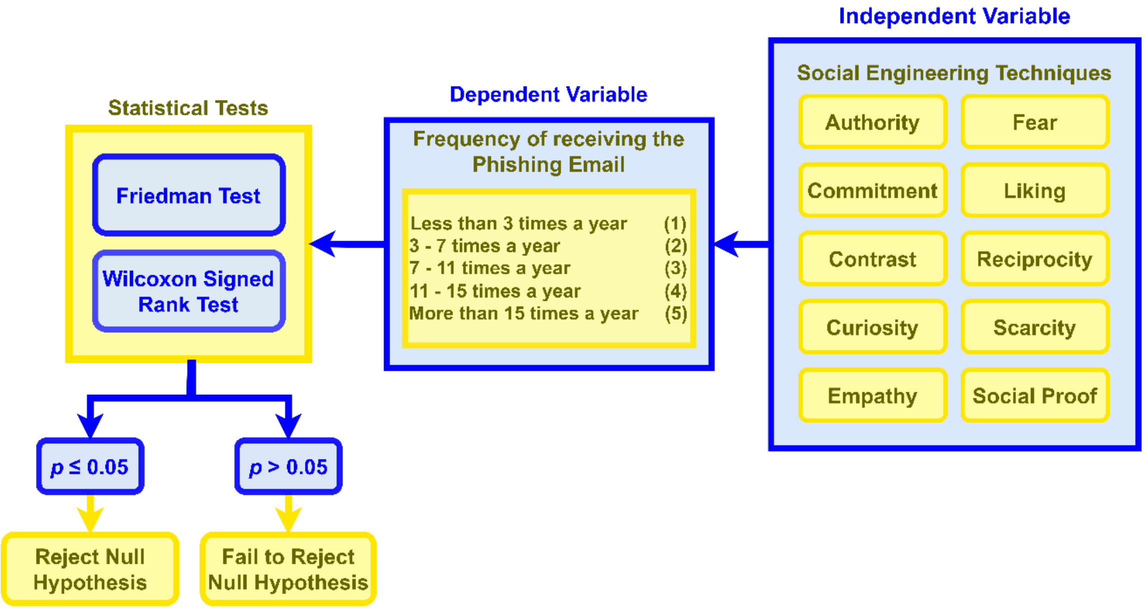


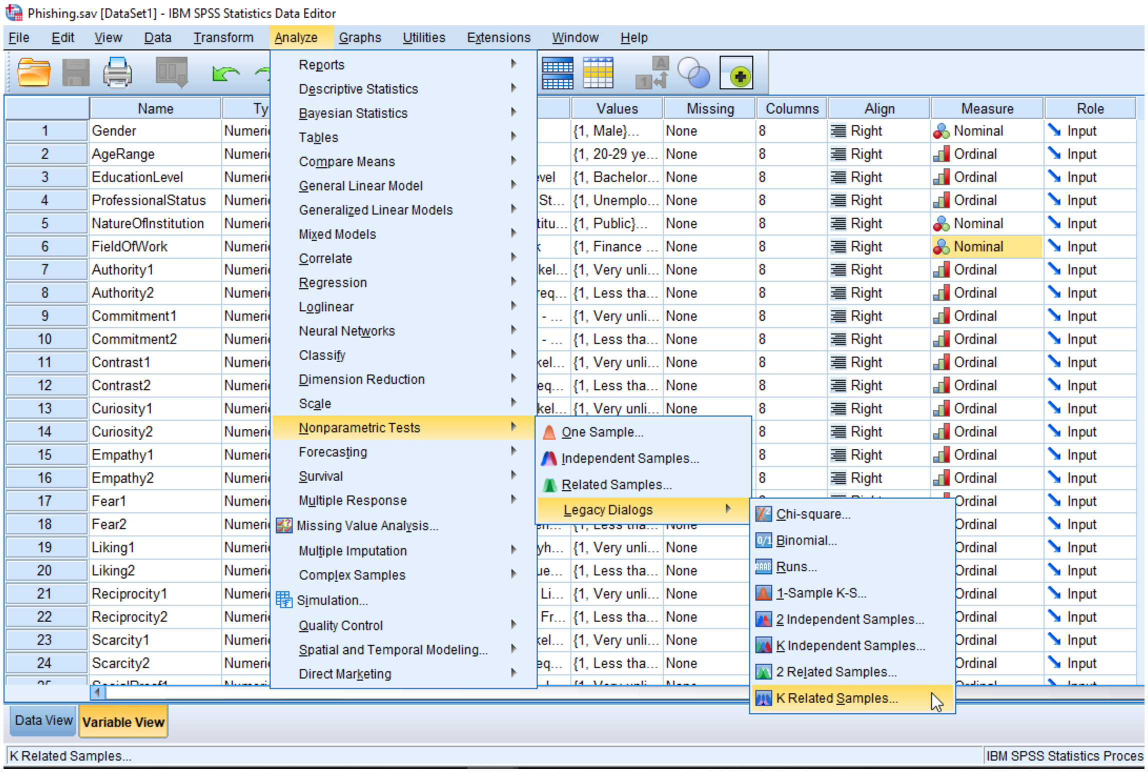
Figure 3. 11: Friedman test for the relation between social engineering techniques and the frequency of receiving a phishing email

Figure 3.11 above shows the illustration of the Friedman test for testing of the hypothesis stated above. The independent variable group is the social engineering techniques. It is tested against the frequency of a subject receiving a phishing email, i.e., an ordinal variable with ‘1’ representing a frequency of less than 5 times a year, and ‘5’ representing a frequency of more than 15 times a year. An asymptotic significance value less than 0.05 (p < 0.05) means that we should reject the null hypothesis stated above and accept the alternative hypothesis. An asymptotic significance value greater than 0.05 (p > 0.05) means that we should reject the alternative hypothesis and fail to reject the null hypothesis.

Friedman Test Setup in IBM SPSS

The Friedman Test is performed in the IBM SPSS software. Once the survey data is collected and imported into the Statistics Data Editor the Friedman test analysis is initiated as shown in figure 3.10 below.

In the menu options, the “Analyze” tab is selected. Under the options in the “Analyze” tab the “Nonparametric Tests” option is selected. In the “Nonparametric Tests” options, the “Legacy Dialogs” is selected. Under the “Legacy Dialogs” options, the “K Related Samples” is selected. In this option, the analysis of the relationships between a finite number of K related samples is evaluated. (Omar, 2021)



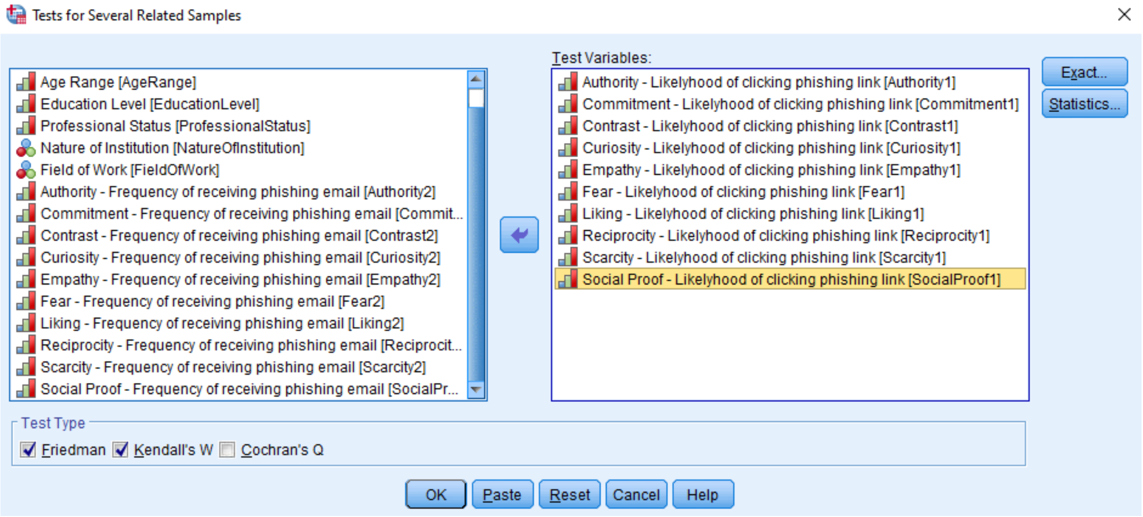
	Name	Ty		Values	Missing	Columns	Align	Measure	Role
1	Gender	Numeri		{1, Male}...	None	8	Right	Nominal	Input
2	AgeRange	Numeri		{1, 20-29 ye...	None	8	Right	Ordinal	Input
3	EducationLevel	Numeri	vel	{1, Bachelor...	None	8	Right	Ordinal	Input
4	ProfessionalStatus	Numeri	St...	{1, Unemplo...	None	8	Right	Ordinal	Input
5	NatureOfInstitution	Numeri	titu...	{1, Public}...	None	8	Right	Nominal	Input
6	FieldOfWork	Numeri	k	{1, Finance ...	None	8	Right	Nominal	Input
7	Authority1	Numeri	kel...	{1, Very unli...	None	8	Right	Ordinal	Input
8	Authority2	Numeri	eq...	{1, Less tha...	None	8	Right	Ordinal	Input
9	Commitment1	Numeri	- ...	{1, Very unli...	None	8	Right	Ordinal	Input
10	Commitment2	Numeri	- ...	{1, Less tha...	None	8	Right	Ordinal	Input
11	Contrast1	Numeri	kel...	{1, Very unli...	None	8	Right	Ordinal	Input
12	Contrast2	Numeri	eq...	{1, Less tha...	None	8	Right	Ordinal	Input
13	Curiosity1	Numeri	kel...	{1, Very unli...	None	8	Right	Ordinal	Input
14	Curiosity2	Numeri				8	Right	Ordinal	Input
15	Empathy1	Numeri				8	Right	Ordinal	Input
16	Empathy2	Numeri				8	Right	Ordinal	Input
17	Fear1	Numeri						Ordinal	Input
18	Fear2	Numeri	en...	{1, Less tha...	None			Ordinal	Input
19	Liking1	Numeri	yh...	{1, Very unli...	None			Ordinal	Input
20	Liking2	Numeri	ue...	{1, Less tha...	None			Ordinal	Input
21	Reciprocity1	Numeri	Li...	{1, Very unli...	None			Ordinal	Input
22	Reciprocity2	Numeri	Fr...	{1, Less tha...	None			Ordinal	Input
23	Scarcity1	Numeri	kel...	{1, Very unli...	None			Ordinal	Input
24	Scarcity2	Numeri	eq...	{1, Less tha...	None			Ordinal	Input

Figure 3. 12: Analysis of K Related Samples for the Friedman Test

Source: IBM SPSS (2022)

Figure 3.11 shows the setting of the test variables in IBM SPSS for testing if there is any statistically significant difference between the groups of the phishing social engineering techniques in affecting the probability of a subject interacting with a phishing email.

Figure 3.12 shows the setting of the test variables in IBM SPSS for testing if there is any statistically significant difference between the groups of the phishing social engineering techniques in affecting the frequency of a subject receiving a phishing email.



Tests for Several Related Samples

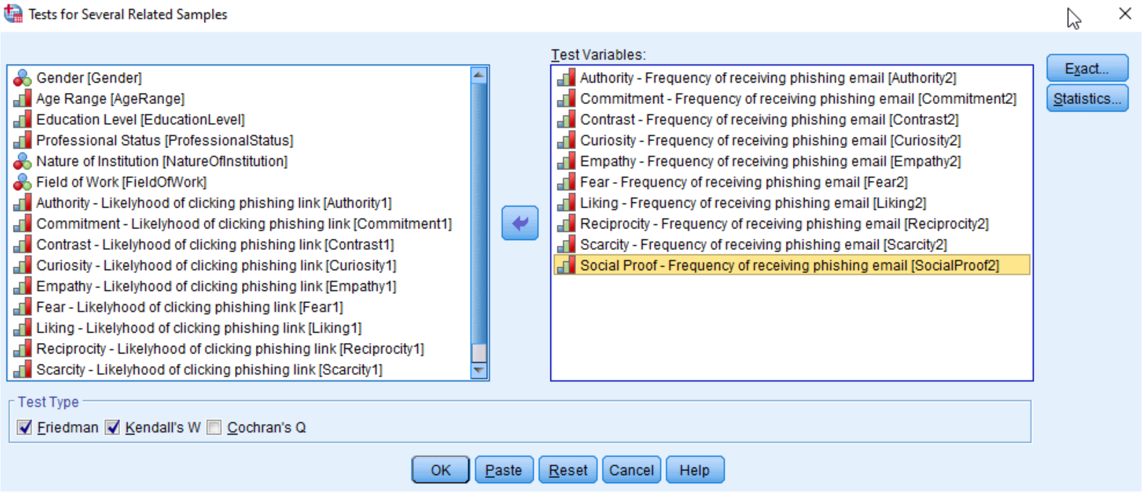
Age Range [AgeRange]
Education Level [EducationLevel]
Professional Status [ProfessionalStatus]
Nature of Institution [NatureOfInstitution]
Field of Work [FieldOfWork]
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commit...
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocit...
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialPr...

Test Variables:
Authority - Likelihood of clicking phishing link [Authority1]
Commitment - Likelihood of clicking phishing link [Commitment1]
Contrast - Likelihood of clicking phishing link [Contrast1]
Curiosity - Likelihood of clicking phishing link [Curiosity1]
Empathy - Likelihood of clicking phishing link [Empathy1]
Fear - Likelihood of clicking phishing link [Fear1]
Liking - Likelihood of clicking phishing link [Liking1]
Reciprocity - Likelihood of clicking phishing link [Reciprocity1]
Scarcity - Likelihood of clicking phishing link [Scarcity1]
Social Proof - Likelihood of clicking phishing link [SocialProof1]

Test Type
☑ Friedman ☑ Kendall's W □ Cochran's Q

Figure 3. 13: Friedman test variables for the likelihood of clicking a phishing link triggered by the social engineering techniques

Source: IBM SPSS (2022)



Tests for Several Related Samples

Gender [Gender]
Age Range [AgeRange]
Education Level [EducationLevel]
Professional Status [ProfessionalStatus]
Nature of Institution [NatureOfInstitution]
Field of Work [FieldOfWork]
Authority - Likelihood of clicking phishing link [Authority1]
Commitment - Likelihood of clicking phishing link [Commitment1]
Contrast - Likelihood of clicking phishing link [Contrast1]
Curiosity - Likelihood of clicking phishing link [Curiosity1]
Empathy - Likelihood of clicking phishing link [Empathy1]
Fear - Likelihood of clicking phishing link [Fear1]
Liking - Likelihood of clicking phishing link [Liking1]
Reciprocity - Likelihood of clicking phishing link [Reciprocity1]
Scarcity - Likelihood of clicking phishing link [Scarcity1]

Test Variables:
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commitment2]
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocity2]
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialProof2]

Test Type
☑ Friedman ☑ Kendall's W □ Cochran's Q

Figure 3. 14: Friedman test variables for the frequency of receiving a phishing email triggered by the social engineering techniques

Source: IBM SPSS (2022)

3.9.3.2 Kruskal-Wallis H test

Niedoba et al. (2023) interpret the Kruskal-Wallis H test as a one that compares groups of an independent variable on a dependent one. (Niedoba et al., 2023) Aslam and Sattam (2020) and Călin and Tuşa (2023) outline the Mann Whitney U test as an equivalent case of the Kruskal-Wallis H test where by two groups of the independent variable are compared on a dependent variable. (Aslam & Sattam, 2020) (Călin & Tuşa, 2023)

In this study, we have used the Kruskal-Wallis H test is used to find out if there is any *statistically significant difference* between *two or more of the groups* of the *independent variable* i.e., the demographics - gender (male, female), age range (20 – 29 years, 30 – 39 years, 40 – 49 years, 50 – 59 years, 60 years and above), education level (bachelor, masters, Ph.D.), professional status (unemployed, student, employed, retired), nature of institution (public, private), and field of work (finance and insurance, manufacturing, energy, retail, professional services, government, healthcare, media, transportation, education, communications & information technology, others), on the *ordinal dependent variable* i.e., the probability of interacting with a phishing email, measured on a 5-point scale – "very unlikely (1)", "unlikely (2)" ,"not sure (3)", "likely (4)", "very likely (5)", or the frequency of receiving a phishing email, likewise also measured on a 5-point scale - "less than 3 times a year (1)", "3 - 7 times a year (2)", "7 - 11 times a year (3)", "11 - 15 times a year (4)", "more than 15 times a year (5)".

Table 3. 8: Kruskal-Wallis H Test variables

Statistical Test	**Categorical Independent variables (Demographics)**	**Groups within the Categorical Independent Variables**	**Categorical Dependent Variables**
Kruskal-Wallis H test	Gender	Male	*Dependent Ordinal variable:* *Probability of interacting with a phishing email* • Very unlikely (1) • Unlikely (2) • Not sure (3) • Likely (4) • Very likely (5) *Dependent Ordinal variable:* *Frequency of receiving a phishing email* • Less than 3 times a year (1) • 3 - 7 times a year (2) • 7 - 11 times a year (3) • 11 - 15 times a year (4) • More than 15 times a year (5)
		Female	
	Age Range	20 – 29 years	
		30 – 39 years	
		40 – 49 years	
		50 – 59 years	
		60 years and above	
	Education Level	Bachelor	
		Masters	
		Ph.D.	
	Professional Status	Unemployed	
		Student	
		Employed	
		Retired	
	Nature of Institution	Public	
		Private	
	Field of work	Finance and Insurance	
		Manufacturing	
		Energy	
		Retail	
		Professional Services	
		Government	
		Healthcare	
		Media	
		Transportation	
		Education	
		Communications & Information Technology	
		Others	

Null Hypothesis Statement 1 for the Kruskal-Wallis Test

There is no statistically significant difference between the groups in the demographic variable in affecting the probability of a subject interacting with a phishing email, for a moderating categorical variable of social engineering techniques.

Alternative Hypothesis Statement 1 for the Kruskal-Wallis Test

There is a statistically significant difference between the groups in the demographic variable in affecting the probability of a subject interacting with a phishing email, for a moderating categorical variable of social engineering techniques.

Figure 3.15 below shows the illustration of the Kruskal-Wallis H test for testing of the hypothesis stated above. The independent variables are the groups of the various demographics. They are each tested against the probability of a subject interacting with a phishing email, considering the effect of the moderating variable, i.e., the social engineering techniques. The null hypothesis mentioned above is rejected for *p*-values less than 0.05, and the alternative hypothesis is consequently accepted. The alternative hypothesis is rejected for *p*-values greater than 0.05, and consequently the null hypothesis cannot be rejected.

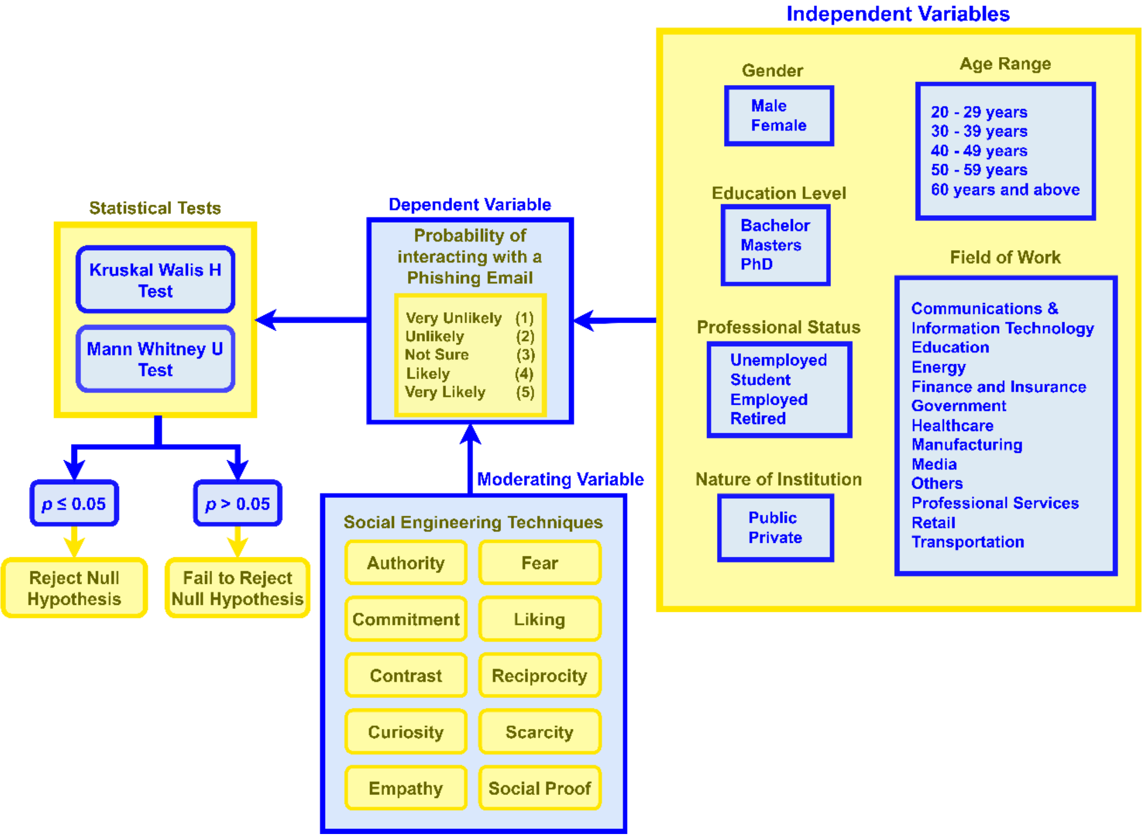


Figure 3. 15: Kruskal-Wallis H test for the relation between demographics and the probability of interacting with a phishing email

Null Hypothesis Statement 2 for the Kruskal-Wallis Test

There is no statistically significant difference between the groups in the demographic variable in affecting the frequency of a subject receiving a phishing email, for a moderating categorical variable of social engineering techniques.

Alternative Hypothesis Statement 2 for the Kruskal-Wallis Test

There is a statistically significant difference between the groups in the demographic variable in affecting the frequency of a subject receiving a phishing email, for a moderating categorical variable of social engineering techniques.

Figure 3.16 below shows the illustration of the Kruskal-Wallis H test for testing the hypothesis stated above. The independent variables are the groups of the various demographics. They are each tested against the frequency of a subject receiving a phishing email, considering the effect of the moderating variable, i.e., the social engineering techniques. *p*-values of less than 0.05, lead to the null hypothesis mentioned above being rejected, and the alternative hypothesis being accepted. Similarly, *p*-values greater than 0.05 lead to the alternative hypothesis being rejected and the null hypothesis mentioned above not being rejected.

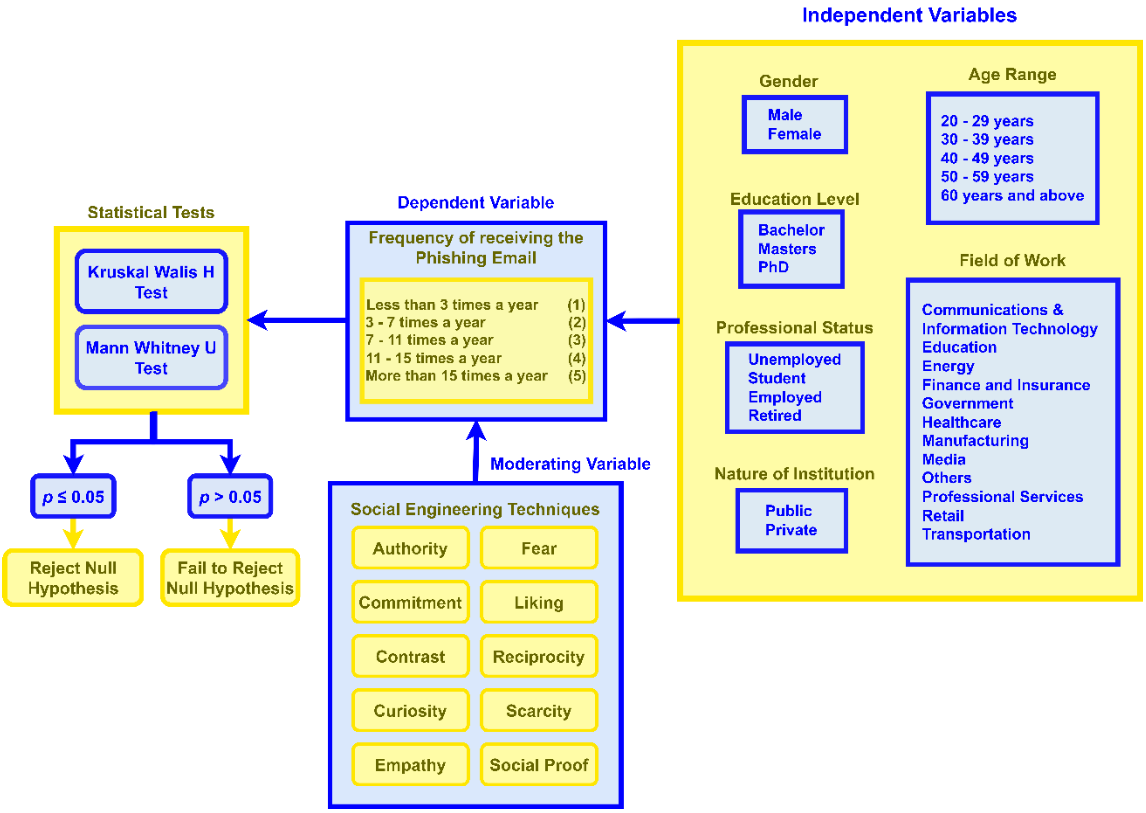
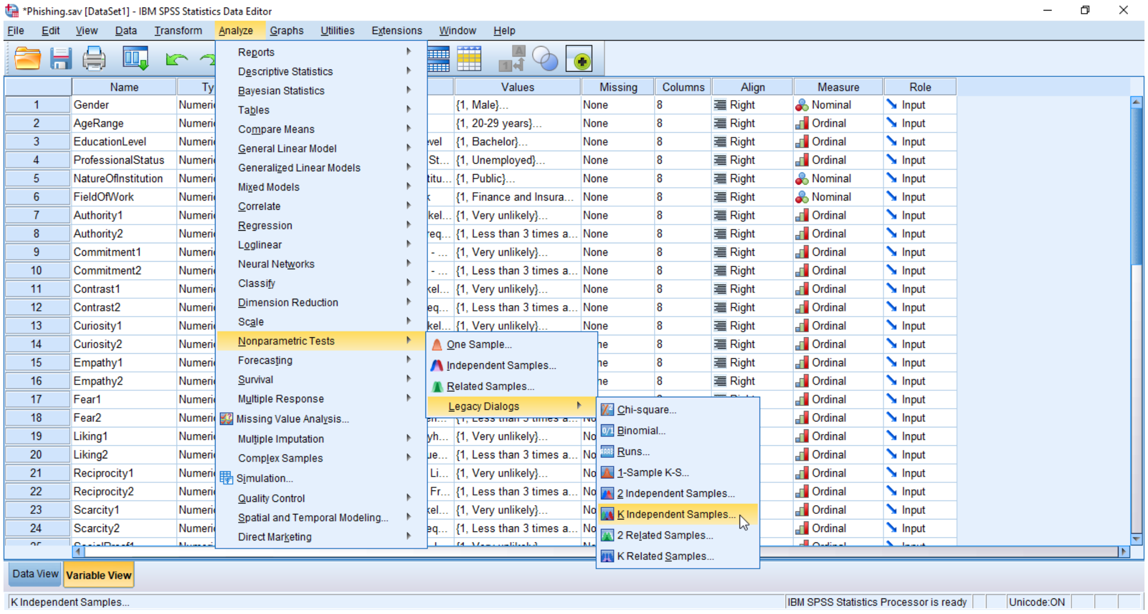


Figure 3. 16: Kruskal-Wallis H test for the relation between demographics and the frequency of receiving a phishing email

Kruskal-Wallis H Test Setup in IBM SPSS

The Kruskal-Wallis H Test is performed in the IBM SPSS software. Once the survey data is collected and imported into the Statistics Data Editor the Kruskal-Wallis H test analysis is initiated as shown in figure 3.17 below.

In the menu options, the “Analyze” tab is selected. Under the options in the “Analyze” tab the “Nonparametric Tests” option is selected. In the “Nonparametric Tests” options, the “Legacy Dialogs” is selected. Under the “Legacy Dialogs” options, the “K Independent Samples” is selected. In this option, the analysis of the relationships between a finite number of K independent samples is evaluated. (O’Loughlin, 2021)

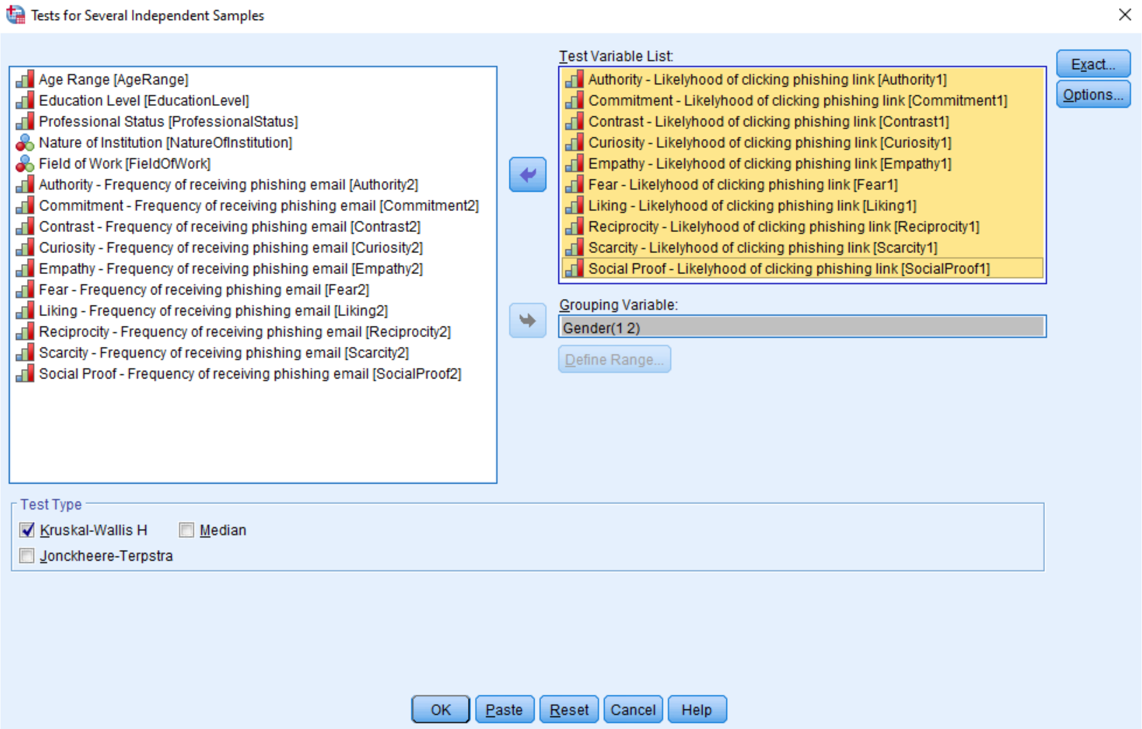


	Name	Ty		Values	Missing	Columns	Align	Measure	Role
1	Gender	Numeri		{1, Male}...	None	8	Right	Nominal	Input
2	AgeRange	Numeri		{1, 20-29 years}...	None	8	Right	Ordinal	Input
3	EducationLevel	Numeri	vel	{1, Bachelor}...	None	8	Right	Ordinal	Input
4	ProfessionalStatus	Numeri	St...	{1, Unemployed}...	None	8	Right	Ordinal	Input
5	NatureOfInstitution	Numeri	titu...	{1, Public}...	None	8	Right	Nominal	Input
6	FieldOfWork	Numeri	k	{1, Finance and Insura...	None	8	Right	Nominal	Input
7	Authority1	Numeri	kel...	{1, Very unlikely}...	None	8	Right	Ordinal	Input
8	Authority2	Numeri	req...	{1, Less than 3 times a...	None	8	Right	Ordinal	Input
9	Commitment1	Numeri	- ...	{1, Very unlikely}...	None	8	Right	Ordinal	Input
10	Commitment2	Numeri	- ...	{1, Less than 3 times a...	None	8	Right	Ordinal	Input
11	Contrast1	Numeri	kel...	{1, Very unlikely}...	None	8	Right	Ordinal	Input
12	Contrast2	Numeri	eq...	{1, Less than 3 times a...	None	8	Right	Ordinal	Input
13	Curiosity1	Numeri	kel...	{1, Very unlikely}...	None	8	Right	Ordinal	Input
14	Curiosity2	Numeri			ne	8	Right	Ordinal	Input
15	Empathy1	Numeri			ne	8	Right	Ordinal	Input
16	Empathy2	Numeri			ne	8	Right	Ordinal	Input
17	Fear1	Numeri						Ordinal	Input
18	Fear2	Numeri						Ordinal	Input
19	Liking1	Numeri	yh...	{1, Very unlikely}...	No			Ordinal	Input
20	Liking2	Numeri	ue...	{1, Less than 3 times a...	No			Ordinal	Input
21	Reciprocity1	Numeri	Li...	{1, Very unlikely}...	No			Ordinal	Input
22	Reciprocity2	Numeri	Fr...	{1, Less than 3 times a...	No			Ordinal	Input
23	Scarcity1	Numeri	kel...	{1, Very unlikely}...	No			Ordinal	Input
24	Scarcity2	Numeri	eq...	{1, Less than 3 times a...	No			Ordinal	Input

Figure 3. 17: Analysis of K Independent Samples for the Kruskal-Wallis H test

Source: IBM SPSS (2022)

Figure 3.18 below shows the setting of the Kruskal-Wallis H test for testing if the gender has any effect on the likelihood of clicking a phishing link triggered by the social engineering techniques.



Tests for Several Independent Samples

Age Range [AgeRange]
Education Level [EducationLevel]
Professional Status [ProfessionalStatus]
Nature of Institution [NatureOfInstitution]
Field of Work [FieldOfWork]
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commitment2]
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocity2]
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialProof2]

Test Variable List:
Authority - Likelyhood of clicking phishing link [Authority1]
Commitment - Likelyhood of clicking phishing link [Commitment1]
Contrast - Likelyhood of clicking phishing link [Contrast1]
Curiosity - Likelyhood of clicking phishing link [Curiosity1]
Empathy - Likelyhood of clicking phishing link [Empathy1]
Fear - Likelyhood of clicking phishing link [Fear1]
Liking - Likelyhood of clicking phishing link [Liking1]
Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
Scarcity - Likelyhood of clicking phishing link [Scarcity1]
Social Proof - Likelyhood of clicking phishing link [SocialProof1]

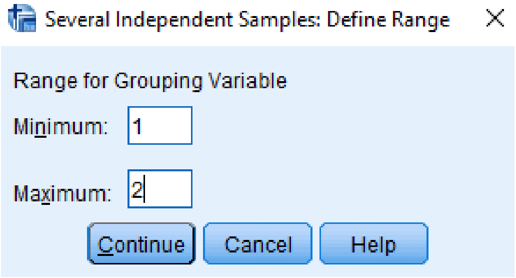
Grouping Variable:
Gender(1 2)

Test Type
☑ Kruskal-Wallis H ☐ Median
☐ Jonckheere-Terpstra

Figure 3. 18: Kruskal-Wallis H test variables for the likelihood of clicking a phishing link triggered by the social engineering techniques against the gender grouping variable

Source: IBM SPSS (2022)

The range for grouping variable should be defined by clicking on the “Define Range…” button. As shown in Figure 3.19 below, the gender variable will have a minimum range of ‘1’ that denotes the Male and a maximum range of ‘2’ that denotes the female. The values of 1 and 2 are defined by the coded value labels shown previously in Figure 3.4. The process is repeated for the age range that has a minimum value of 1 and maximum value of 5. Likewise, the education level has a minimum value of 1 and maximum value of 3. The professional status ranges from 1 to 4. The nature of the institution ranges from 1 to 2. The field of work ranges from 1 to 12.



Several Independent Samples: Define Range

Range for Grouping Variable

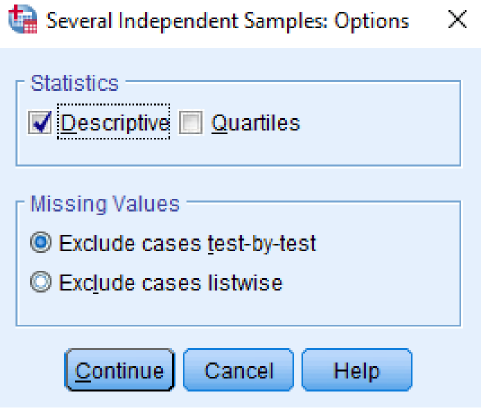
Minimum: 1

Maximum: 2

Figure 3. 19: Defining the Range for the Grouping Variable

Source: IBM SPSS (2022)

The "Descriptive Statistics" options is selected by clicking on the "Options" button and checking the "Descriptive" checkbox available in the "Statistics" menu as shown in Figure 3.20 below.



Several Independent Samples: Options

Statistics

☑ Descriptive ☐ Quartiles

Missing Values

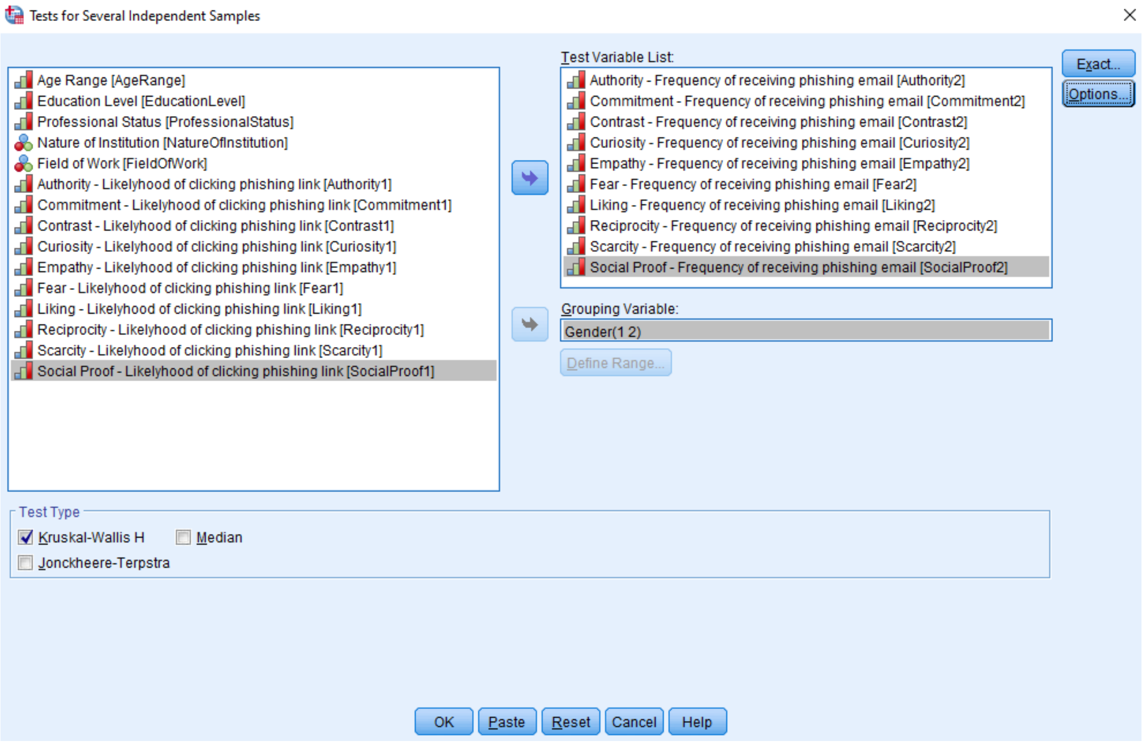
● Exclude cases test-by-test

○ Exclude cases listwise

Figure 3. 20: Selection of the Descriptive Statistics test options for the Kruskal-Wallis H test

Source: IBM SPSS (2022)

Figure 3.21 below shows the setting of the Kruskal-Wallis H test for testing if the gender has any effect on the frequency of a subject receiving a phishing email triggered by the social engineering techniques.



Tests for Several Independent Samples

- Age Range [AgeRange]
- Education Level [EducationLevel]
- Professional Status [ProfessionalStatus]
- Nature of Institution [NatureOfInstitution]
- Field of Work [FieldOfWork]
- Authority - Likelyhood of clicking phishing link [Authority1]
- Commitment - Likelyhood of clicking phishing link [Commitment1]
- Contrast - Likelyhood of clicking phishing link [Contrast1]
- Curiosity - Likelyhood of clicking phishing link [Curiosity1]
- Empathy - Likelyhood of clicking phishing link [Empathy1]
- Fear - Likelyhood of clicking phishing link [Fear1]
- Liking - Likelyhood of clicking phishing link [Liking1]
- Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
- Scarcity - Likelyhood of clicking phishing link [Scarcity1]
- Social Proof - Likelyhood of clicking phishing link [SocialProof1]

Test Variable List:

- Authority - Frequency of receiving phishing email [Authority2]
- Commitment - Frequency of receiving phishing email [Commitment2]
- Contrast - Frequency of receiving phishing email [Contrast2]
- Curiosity - Frequency of receiving phishing email [Curiosity2]
- Empathy - Frequency of receiving phishing email [Empathy2]
- Fear - Frequency of receiving phishing email [Fear2]
- Liking - Frequency of receiving phishing email [Liking2]
- Reciprocity - Frequency of receiving phishing email [Reciprocity2]
- Scarcity - Frequency of receiving phishing email [Scarcity2]
- Social Proof - Frequency of receiving phishing email [SocialProof2]

Grouping Variable: Gender(1 2)

Test Type

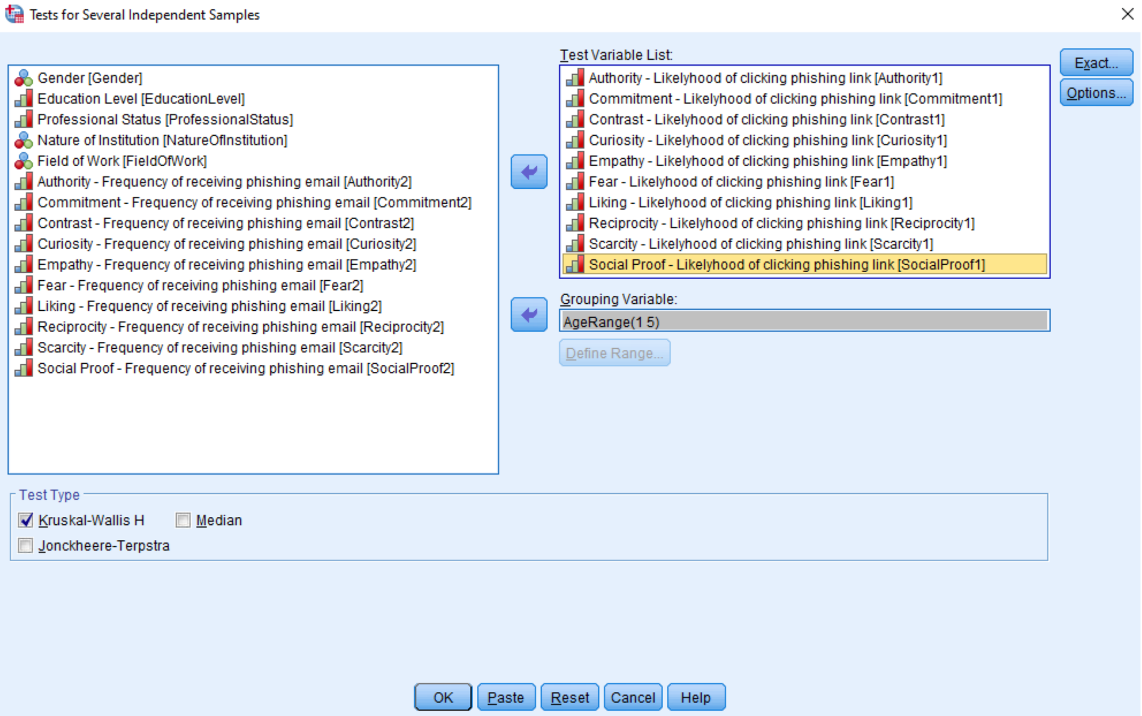
☑ Kruskal-Wallis H ☐ Median

☐ Jonckheere-Terpstra

Figure 3. 21: Kruskal-Wallis H test variables for the frequency of receiving a phishing email triggered by the social engineering techniques against the gender grouping variable

Source: IBM SPSS (2022)

Figure 3.22 below shows the setting of the Kruskal-Wallis H test for testing if the age range has any effect on the likelihood of clicking a phishing link triggered by the social engineering techniques.



Tests for Several Independent Samples

- Gender [Gender]
- Education Level [EducationLevel]
- Professional Status [ProfessionalStatus]
- Nature of Institution [NatureOfInstitution]
- Field of Work [FieldOfWork]
- Authority - Frequency of receiving phishing email [Authority2]
- Commitment - Frequency of receiving phishing email [Commitment2]
- Contrast - Frequency of receiving phishing email [Contrast2]
- Curiosity - Frequency of receiving phishing email [Curiosity2]
- Empathy - Frequency of receiving phishing email [Empathy2]
- Fear - Frequency of receiving phishing email [Fear2]
- Liking - Frequency of receiving phishing email [Liking2]
- Reciprocity - Frequency of receiving phishing email [Reciprocity2]
- Scarcity - Frequency of receiving phishing email [Scarcity2]
- Social Proof - Frequency of receiving phishing email [SocialProof2]

Test Variable List:

- Authority - Likelyhood of clicking phishing link [Authority1]
- Commitment - Likelyhood of clicking phishing link [Commitment1]
- Contrast - Likelyhood of clicking phishing link [Contrast1]
- Curiosity - Likelyhood of clicking phishing link [Curiosity1]
- Empathy - Likelyhood of clicking phishing link [Empathy1]
- Fear - Likelyhood of clicking phishing link [Fear1]
- Liking - Likelyhood of clicking phishing link [Liking1]
- Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
- Scarcity - Likelyhood of clicking phishing link [Scarcity1]
- Social Proof - Likelyhood of clicking phishing link [SocialProof1]

Grouping Variable: AgeRange(1 5)

Test Type

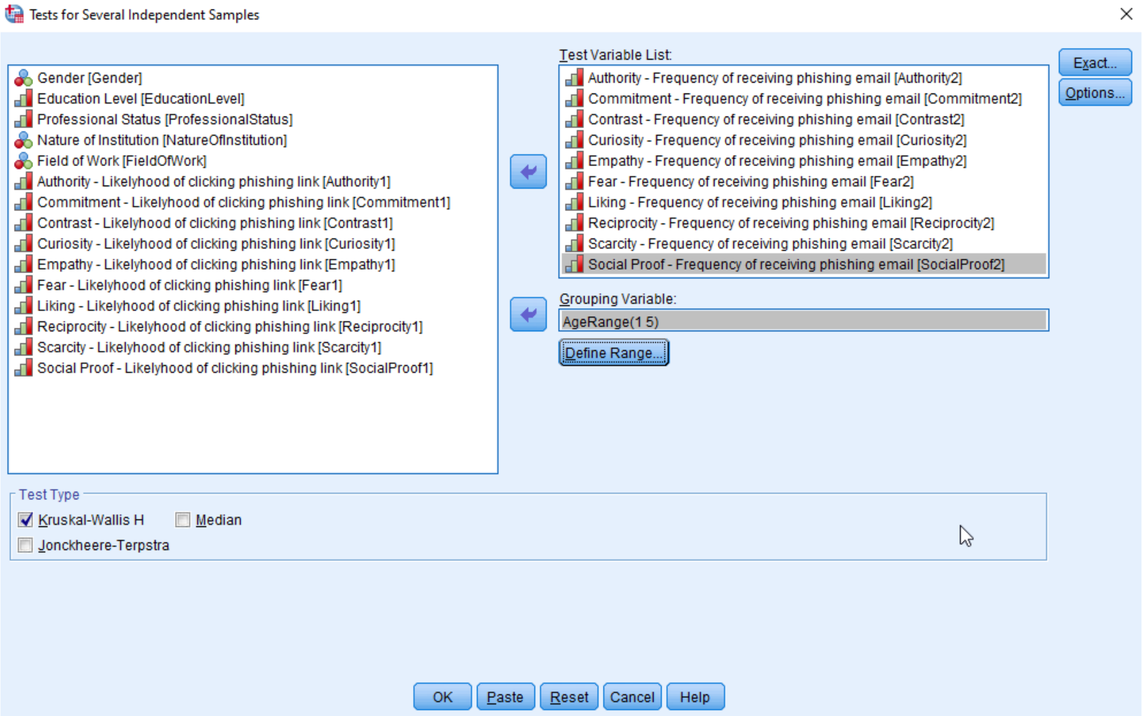
☑ Kruskal-Wallis H ☐ Median

☐ Jonckheere-Terpstra

Figure 3. 22: Kruskal-Wallis H test variables for the likelihood of clicking a phishing link triggered by the social engineering techniques against the age range grouping variable

Source: IBM SPSS (2022)

Figure 3.23 below shows the setting of the Kruskal-Wallis H test for testing if the age range has any effect on the frequency of a subject receiving a phishing email triggered by the social engineering techniques.



Tests for Several Independent Samples

Gender [Gender]
Education Level [EducationLevel]
Professional Status [ProfessionalStatus]
Nature of Institution [NatureOfInstitution]
Field of Work [FieldOfWork]
Authority - Likelyhood of clicking phishing link [Authority1]
Commitment - Likelyhood of clicking phishing link [Commitment1]
Contrast - Likelyhood of clicking phishing link [Contrast1]
Curiosity - Likelyhood of clicking phishing link [Curiosity1]
Empathy - Likelyhood of clicking phishing link [Empathy1]
Fear - Likelyhood of clicking phishing link [Fear1]
Liking - Likelyhood of clicking phishing link [Liking1]
Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
Scarcity - Likelyhood of clicking phishing link [Scarcity1]
Social Proof - Likelyhood of clicking phishing link [SocialProof1]

Test Variable List:
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commitment2]
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocity2]
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialProof2]

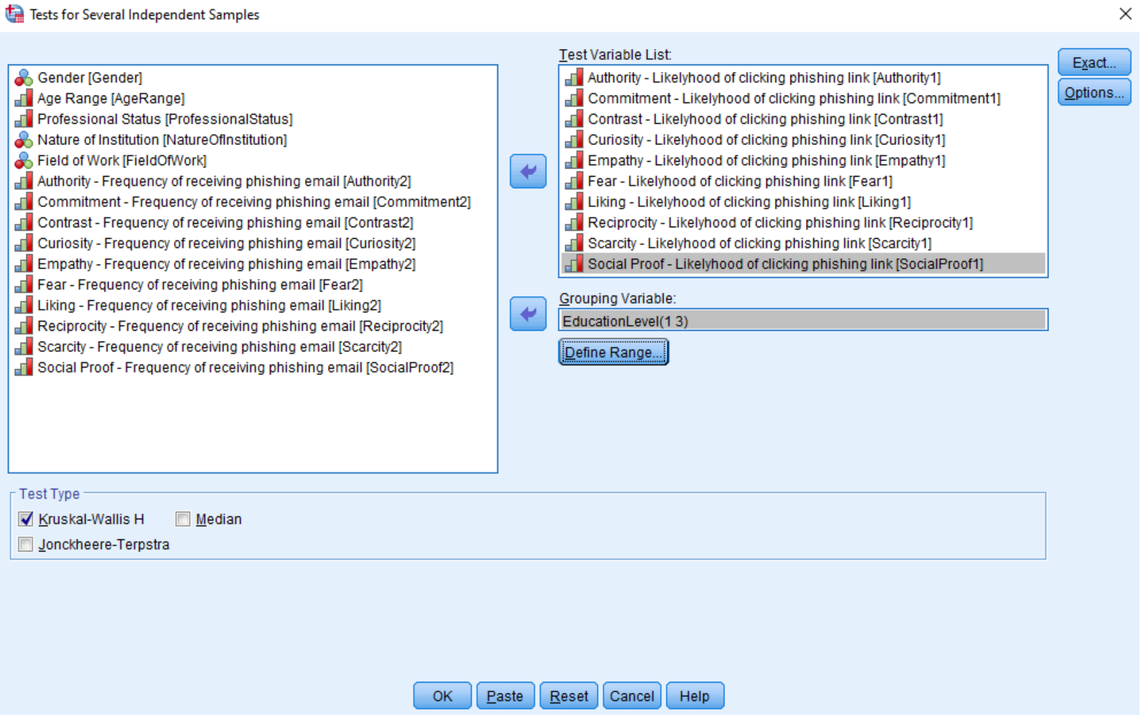
Grouping Variable:
AgeRange(1 5)

Test Type
☑ Kruskal-Wallis H □ Median
□ Jonckheere-Terpstra

Figure 3. 23: Kruskal-Wallis H test variables for the frequency of receiving a phishing email triggered by the social engineering techniques against the age range grouping variable

Source: IBM SPSS (2022)

Figure 3.24 below shows the setting of the Kruskal-Wallis H test for testing if the education level has any effect on the likelihood of clicking a phishing link triggered by the social engineering techniques.



Tests for Several Independent Samples

- Gender [Gender]
- Age Range [AgeRange]
- Professional Status [ProfessionalStatus]
- Nature of Institution [NatureOfInstitution]
- Field of Work [FieldOfWork]
- Authority - Frequency of receiving phishing email [Authority2]
- Commitment - Frequency of receiving phishing email [Commitment2]
- Contrast - Frequency of receiving phishing email [Contrast2]
- Curiosity - Frequency of receiving phishing email [Curiosity2]
- Empathy - Frequency of receiving phishing email [Empathy2]
- Fear - Frequency of receiving phishing email [Fear2]
- Liking - Frequency of receiving phishing email [Liking2]
- Reciprocity - Frequency of receiving phishing email [Reciprocity2]
- Scarcity - Frequency of receiving phishing email [Scarcity2]
- Social Proof - Frequency of receiving phishing email [SocialProof2]

Test Variable List:

- Authority - Likelyhood of clicking phishing link [Authority1]
- Commitment - Likelyhood of clicking phishing link [Commitment1]
- Contrast - Likelyhood of clicking phishing link [Contrast1]
- Curiosity - Likelyhood of clicking phishing link [Curiosity1]
- Empathy - Likelyhood of clicking phishing link [Empathy1]
- Fear - Likelyhood of clicking phishing link [Fear1]
- Liking - Likelyhood of clicking phishing link [Liking1]
- Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
- Scarcity - Likelyhood of clicking phishing link [Scarcity1]
- Social Proof - Likelyhood of clicking phishing link [SocialProof1]

Grouping Variable: EducationLevel(1 3)

Test Type

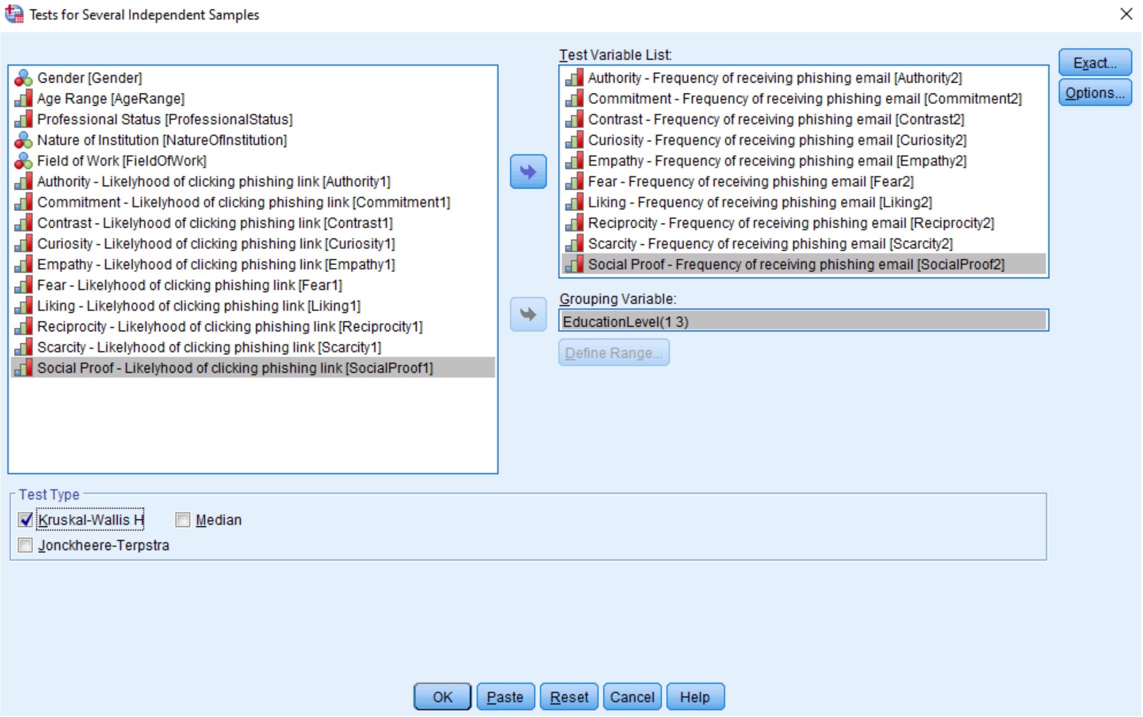
☑ Kruskal-Wallis H ☐ Median

☐ Jonckheere-Terpstra

Figure 3. 24: Kruskal-Wallis H test variables for the likelihood of clicking a phishing link triggered by the social engineering techniques against the education level grouping variable

Source: IBM SPSS (2022)

Figure 3.25 below shows the setting of the Kruskal-Wallis H test for testing if the education level has any effect on the frequency of a subject receiving a phishing email triggered by the social engineering techniques.



Tests for Several Independent Samples

Gender [Gender]
Age Range [AgeRange]
Professional Status [ProfessionalStatus]
Nature of Institution [NatureOfInstitution]
Field of Work [FieldOfWork]
Authority - Likelyhood of clicking phishing link [Authority1]
Commitment - Likelyhood of clicking phishing link [Commitment1]
Contrast - Likelyhood of clicking phishing link [Contrast1]
Curiosity - Likelyhood of clicking phishing link [Curiosity1]
Empathy - Likelyhood of clicking phishing link [Empathy1]
Fear - Likelyhood of clicking phishing link [Fear1]
Liking - Likelyhood of clicking phishing link [Liking1]
Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
Scarcity - Likelyhood of clicking phishing link [Scarcity1]
Social Proof - Likelyhood of clicking phishing link [SocialProof1]

Test Variable List:
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commitment2]
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocity2]
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialProof2]

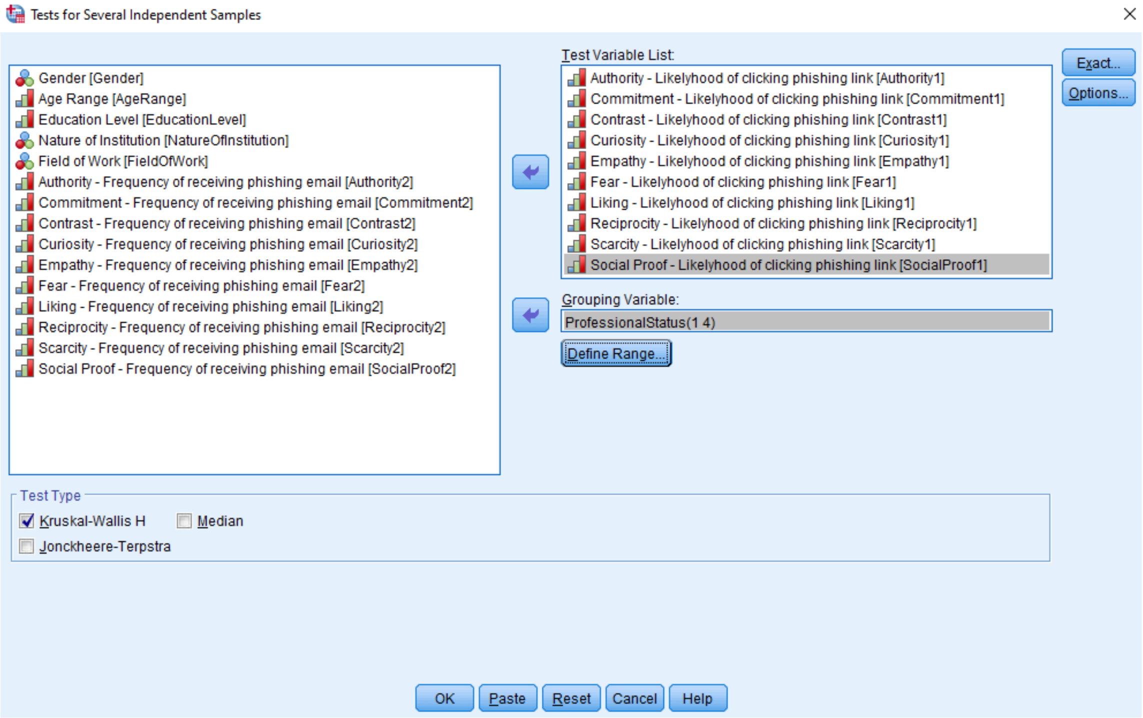
Grouping Variable:
EducationLevel(1 3)

Test Type
☑ Kruskal-Wallis H □ Median
□ Jonckheere-Terpstra

Figure 3. 25: Kruskal-Wallis H test variables for the frequency of receiving a phishing email triggered by the social engineering techniques against the education level grouping variable

Source: IBM SPSS (2022)

Figure 3.26 below shows the setting of the Kruskal-Wallis H test for testing if the professional status has any effect on the likelihood of clicking a phishing link triggered by the social engineering techniques.


Tests for Several Independent Samples

Gender [Gender]
Age Range [AgeRange]
Education Level [EducationLevel]
Nature of Institution [NatureOfInstitution]
Field of Work [FieldOfWork]
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commitment2]
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocity2]
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialProof2]

Test Variable List:
Authority - Likelihood of clicking phishing link [Authority1]
Commitment - Likelihood of clicking phishing link [Commitment1]
Contrast - Likelihood of clicking phishing link [Contrast1]
Curiosity - Likelihood of clicking phishing link [Curiosity1]
Empathy - Likelihood of clicking phishing link [Empathy1]
Fear - Likelihood of clicking phishing link [Fear1]
Liking - Likelihood of clicking phishing link [Liking1]
Reciprocity - Likelihood of clicking phishing link [Reciprocity1]
Scarcity - Likelihood of clicking phishing link [Scarcity1]
Social Proof - Likelihood of clicking phishing link [SocialProof1]

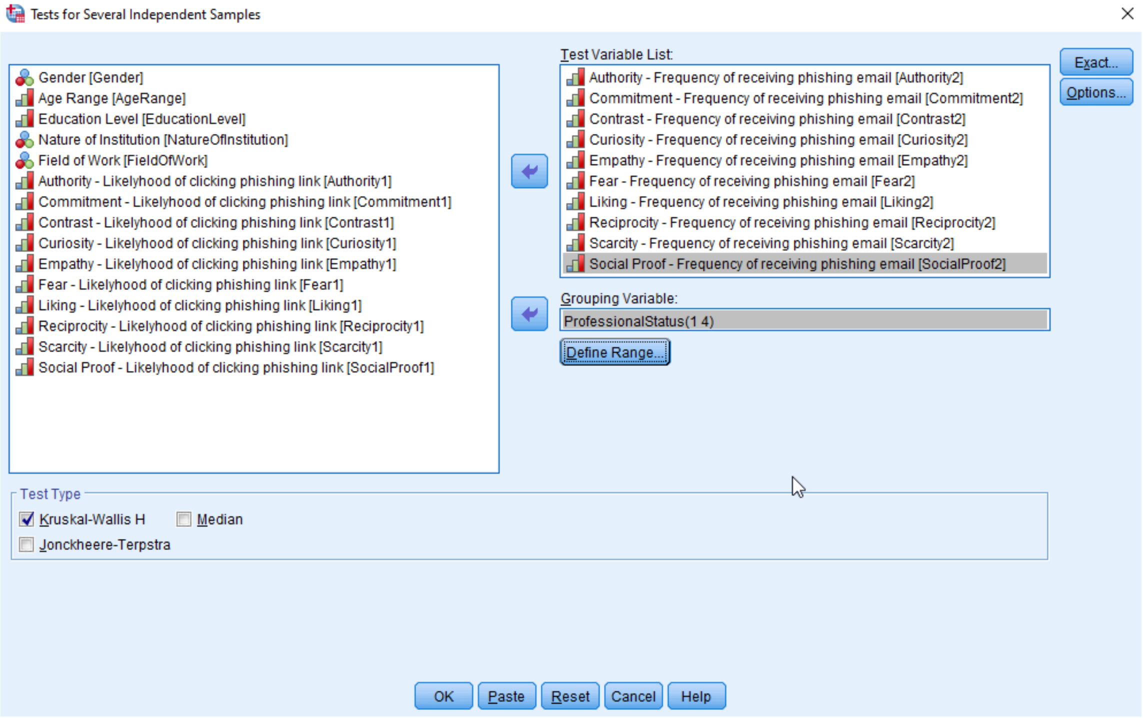
Grouping Variable:
ProfessionalStatus(1 4)

Test Type
☑ Kruskal-Wallis H ☐ Median
☐ Jonckheere-Terpstra

Figure 3. 26: Kruskal-Wallis H test variables for the likelihood of clicking a phishing link triggered by the social engineering techniques against the professional status grouping variable

Source: IBM SPSS (2022)

Figure 3.27 below shows the setting of the Kruskal-Wallis H test for testing if the professional status has any effect on the frequency of a subject receiving a phishing email triggered by the social engineering techniques.



Tests for Several Independent Samples

Gender [Gender]
Age Range [AgeRange]
Education Level [EducationLevel]
Nature of Institution [NatureOfInstitution]
Field of Work [FieldOfWork]
Authority - Likelyhood of clicking phishing link [Authority1]
Commitment - Likelyhood of clicking phishing link [Commitment1]
Contrast - Likelyhood of clicking phishing link [Contrast1]
Curiosity - Likelyhood of clicking phishing link [Curiosity1]
Empathy - Likelyhood of clicking phishing link [Empathy1]
Fear - Likelyhood of clicking phishing link [Fear1]
Liking - Likelyhood of clicking phishing link [Liking1]
Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
Scarcity - Likelyhood of clicking phishing link [Scarcity1]
Social Proof - Likelyhood of clicking phishing link [SocialProof1]

Test Variable List:
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commitment2]
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocity2]
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialProof2]

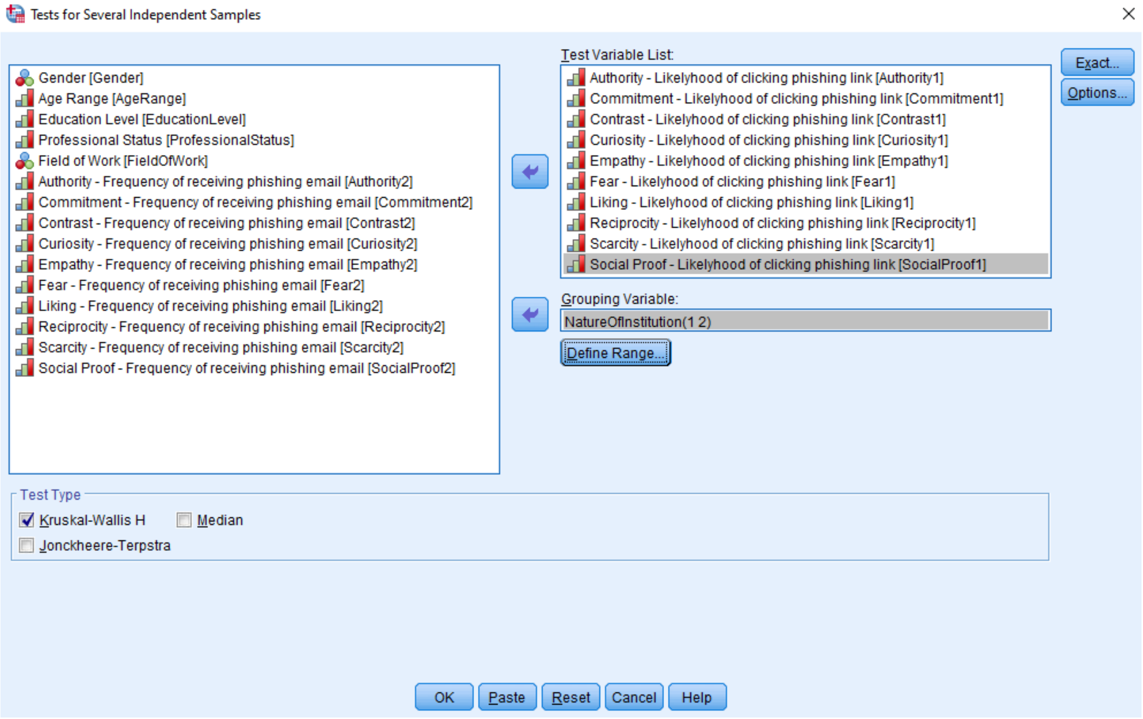
Grouping Variable:
ProfessionalStatus(1 4)

Test Type
☑ Kruskal-Wallis H □ Median
□ Jonckheere-Terpstra

Figure 3. 27: Kruskal-Wallis H test variables for the frequency of receiving a phishing email triggered by the social engineering techniques against the professional status grouping variable

Source: IBM SPSS (2022)

Figure 3.28 below shows the setting of the Kruskal-Wallis H test for testing if the nature of institution has any effect on the likelihood of clicking a phishing link triggered by the social engineering techniques.



Tests for Several Independent Samples

Gender [Gender]
Age Range [AgeRange]
Education Level [EducationLevel]
Professional Status [ProfessionalStatus]
Field of Work [FieldOfWork]
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commitment2]
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocity2]
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialProof2]

Test Variable List:
Authority - Likelyhood of clicking phishing link [Authority1]
Commitment - Likelyhood of clicking phishing link [Commitment1]
Contrast - Likelyhood of clicking phishing link [Contrast1]
Curiosity - Likelyhood of clicking phishing link [Curiosity1]
Empathy - Likelyhood of clicking phishing link [Empathy1]
Fear - Likelyhood of clicking phishing link [Fear1]
Liking - Likelyhood of clicking phishing link [Liking1]
Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
Scarcity - Likelyhood of clicking phishing link [Scarcity1]
Social Proof - Likelyhood of clicking phishing link [SocialProof1]

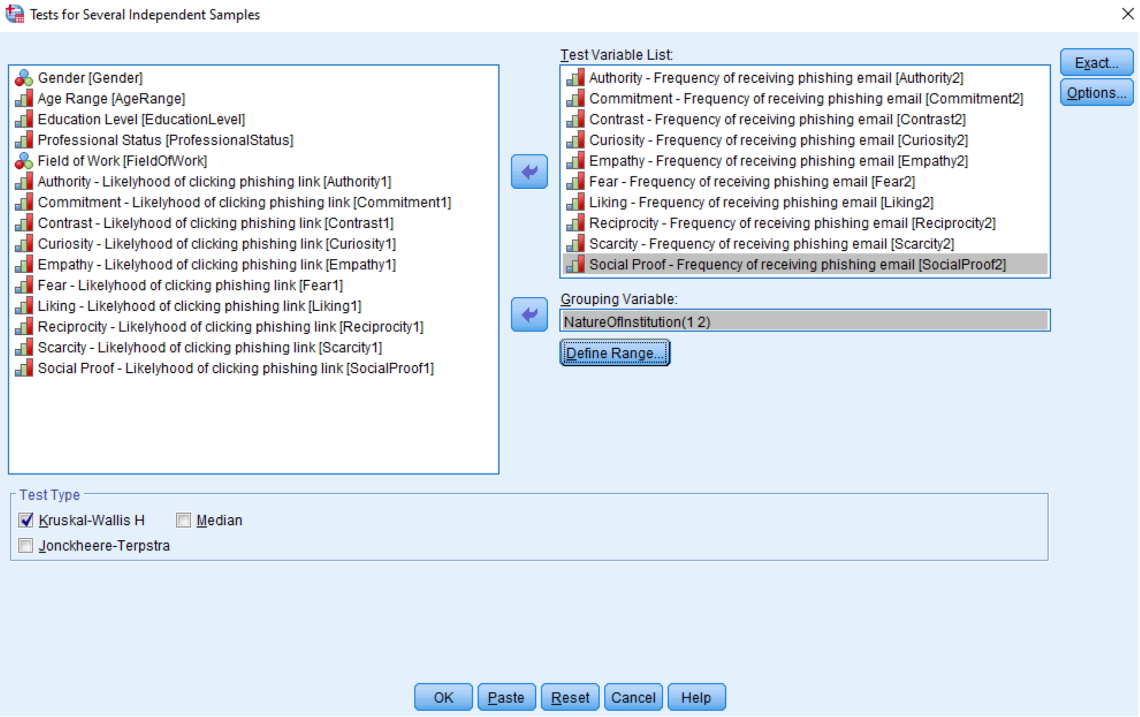
Grouping Variable: NatureOfInstitution(1 2)

Test Type
☑ Kruskal-Wallis H □ Median
□ Jonckheere-Terpstra

Figure 3. 28: Kruskal-Wallis H test variables for the likelihood of clicking a phishing link triggered by the social engineering techniques against the nature of institution grouping variable

Source: IBM SPSS (2022)

Figure 3.29 below shows the setting of the Kruskal-Wallis H test for testing if the nature of institution has any effect on the frequency of a subject receiving a phishing email triggered by the social engineering techniques.



Tests for Several Independent Samples

Gender [Gender]
Age Range [AgeRange]
Education Level [EducationLevel]
Professional Status [ProfessionalStatus]
Field of Work [FieldOfWork]
Authority - Likelyhood of clicking phishing link [Authority1]
Commitment - Likelyhood of clicking phishing link [Commitment1]
Contrast - Likelyhood of clicking phishing link [Contrast1]
Curiosity - Likelyhood of clicking phishing link [Curiosity1]
Empathy - Likelyhood of clicking phishing link [Empathy1]
Fear - Likelyhood of clicking phishing link [Fear1]
Liking - Likelyhood of clicking phishing link [Liking1]
Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
Scarcity - Likelyhood of clicking phishing link [Scarcity1]
Social Proof - Likelyhood of clicking phishing link [SocialProof1]

Test Variable List:
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commitment2]
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocity2]
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialProof2]

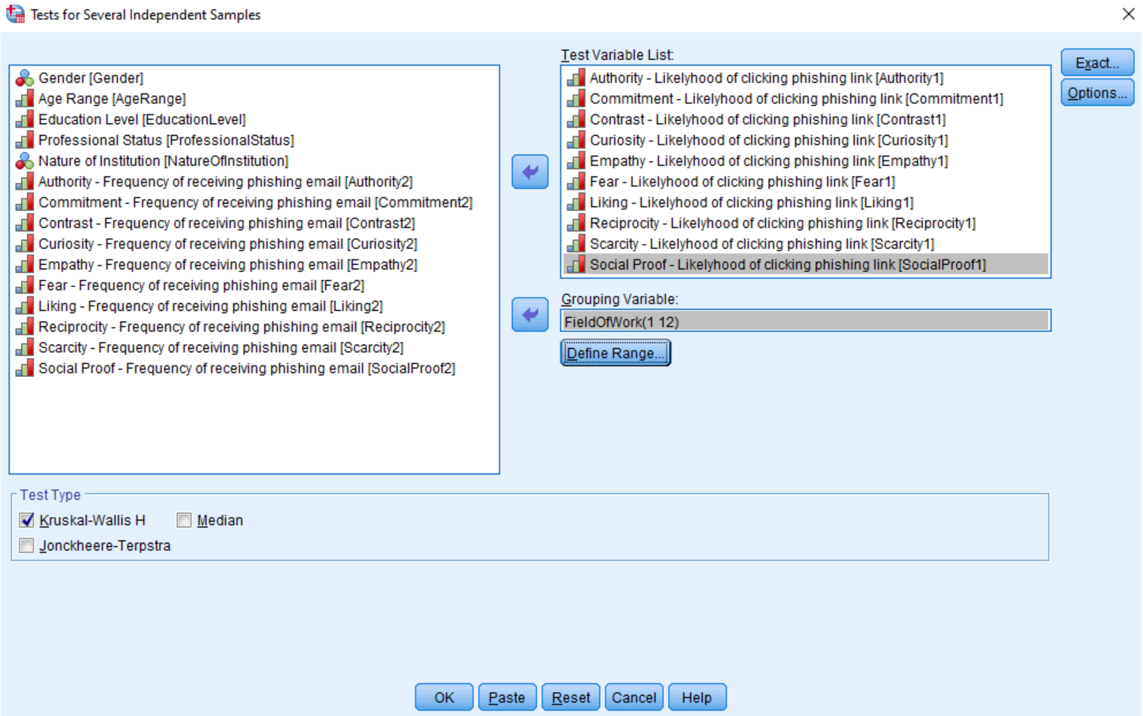
Grouping Variable:
NatureOfInstitution(1 2)

Test Type
☑ Kruskal-Wallis H □ Median
□ Jonckheere-Terpstra

Figure 3. 29: Kruskal-Wallis H test variables for the frequency of receiving a phishing email triggered by the social engineering techniques against the nature of institution grouping variable

Source: IBM SPSS (2022)

Figure 3.30 below shows the setting of the Kruskal-Wallis H test for testing if the field of work has any effect on the likelihood of clicking a phishing link triggered by the social engineering techniques.



Tests for Several Independent Samples

- Gender [Gender]
- Age Range [AgeRange]
- Education Level [EducationLevel]
- Professional Status [ProfessionalStatus]
- Nature of Institution [NatureOfInstitution]
- Authority - Frequency of receiving phishing email [Authority2]
- Commitment - Frequency of receiving phishing email [Commitment2]
- Contrast - Frequency of receiving phishing email [Contrast2]
- Curiosity - Frequency of receiving phishing email [Curiosity2]
- Empathy - Frequency of receiving phishing email [Empathy2]
- Fear - Frequency of receiving phishing email [Fear2]
- Liking - Frequency of receiving phishing email [Liking2]
- Reciprocity - Frequency of receiving phishing email [Reciprocity2]
- Scarcity - Frequency of receiving phishing email [Scarcity2]
- Social Proof - Frequency of receiving phishing email [SocialProof2]

Test Variable List:

- Authority - Likelyhood of clicking phishing link [Authority1]
- Commitment - Likelyhood of clicking phishing link [Commitment1]
- Contrast - Likelyhood of clicking phishing link [Contrast1]
- Curiosity - Likelyhood of clicking phishing link [Curiosity1]
- Empathy - Likelyhood of clicking phishing link [Empathy1]
- Fear - Likelyhood of clicking phishing link [Fear1]
- Liking - Likelyhood of clicking phishing link [Liking1]
- Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
- Scarcity - Likelyhood of clicking phishing link [Scarcity1]
- Social Proof - Likelyhood of clicking phishing link [SocialProof1]

Grouping Variable: FieldOfWork(1 12)

Test Type

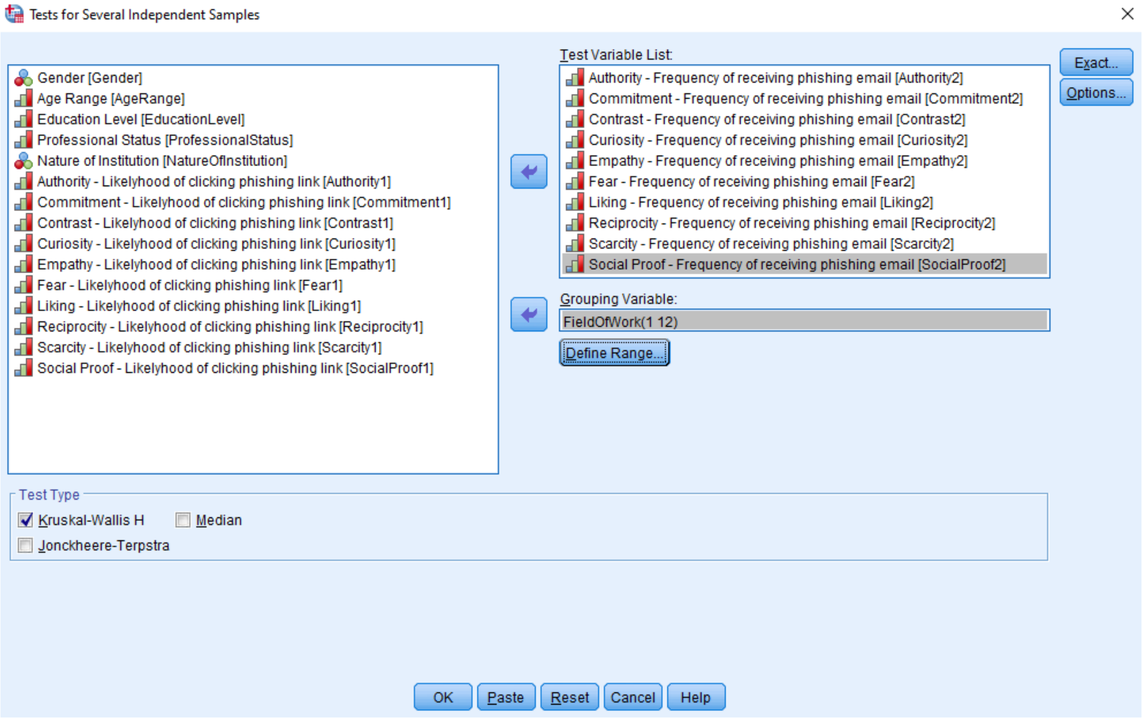
☑ Kruskal-Wallis H □ Median

□ Jonckheere-Terpstra

Figure 3. 30: Kruskal-Wallis H test variables for the likelihood of clicking a phishing link triggered by the social engineering techniques against the field of work grouping variable

Source: IBM SPSS (2022)

Figure 3.31 below shows the setting of the Kruskal-Wallis H test for testing if the field of work has any effect on the frequency of a subject receiving a phishing email triggered by the social engineering techniques.



Tests for Several Independent Samples

Gender [Gender]
Age Range [AgeRange]
Education Level [EducationLevel]
Professional Status [ProfessionalStatus]
Nature of Institution [NatureOfInstitution]
Authority - Likelyhood of clicking phishing link [Authority1]
Commitment - Likelyhood of clicking phishing link [Commitment1]
Contrast - Likelyhood of clicking phishing link [Contrast1]
Curiosity - Likelyhood of clicking phishing link [Curiosity1]
Empathy - Likelyhood of clicking phishing link [Empathy1]
Fear - Likelyhood of clicking phishing link [Fear1]
Liking - Likelyhood of clicking phishing link [Liking1]
Reciprocity - Likelyhood of clicking phishing link [Reciprocity1]
Scarcity - Likelyhood of clicking phishing link [Scarcity1]
Social Proof - Likelyhood of clicking phishing link [SocialProof1]

Test Variable List:
Authority - Frequency of receiving phishing email [Authority2]
Commitment - Frequency of receiving phishing email [Commitment2]
Contrast - Frequency of receiving phishing email [Contrast2]
Curiosity - Frequency of receiving phishing email [Curiosity2]
Empathy - Frequency of receiving phishing email [Empathy2]
Fear - Frequency of receiving phishing email [Fear2]
Liking - Frequency of receiving phishing email [Liking2]
Reciprocity - Frequency of receiving phishing email [Reciprocity2]
Scarcity - Frequency of receiving phishing email [Scarcity2]
Social Proof - Frequency of receiving phishing email [SocialProof2]

Grouping Variable:
FieldOfWork(1 12)

Test Type
☑ Kruskal-Wallis H ☐ Median
☐ Jonckheere-Terpstra

Figure 3. 31: Kruskal-Wallis H test variables for the frequency of receiving a phishing email triggered by the social engineering techniques against the field of work grouping variable

Source: IBM SPSS (2022)

As shown in table 3.9 below, 5 hypotheses were made relating to specific objectives 2 and 3. No hypothesis was made for specific objective 1 as exploratory research is used for the objective. Friedman and Kruskal-Wallis H Tests are used for specific objective 2 and a simulated phishing test for specific objective 3.

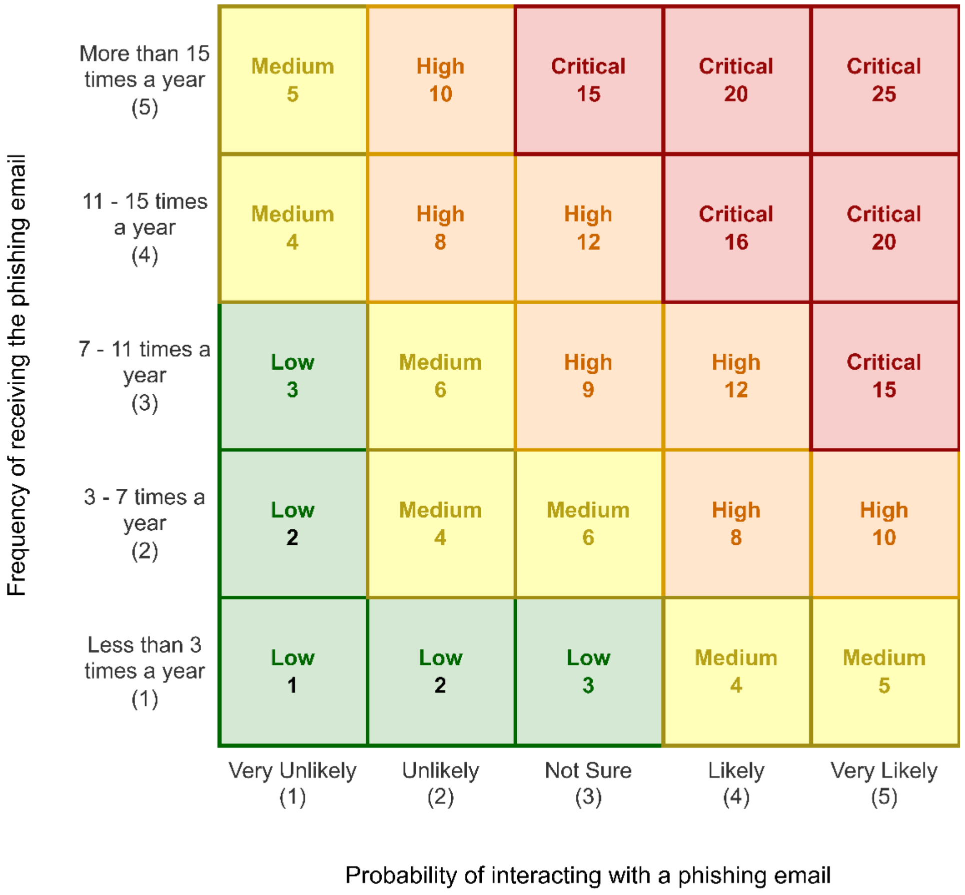
Table 3. 9: Hypothesis and Test Methods mapped to specific objectives

SN	Specific Objective	Hypothesis	Test Method	Test Tool
1	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups of the phishing social engineering techniques in affecting the probability of a subject interacting with a phishing email.	Friedman Test	IBM© Statistical Package for Social Sciences (SPSS)
2	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups of the phishing social engineering techniques in affecting the frequency of a subject receiving a phishing email.	Friedman Test	IBM© Statistical Package for Social Sciences (SPSS)
3	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups in the demographic variable in affecting the probability of a subject interacting with a phishing email, for a moderating categorical variable of social engineering techniques.	Kruskal-Wallis H Test	IBM© Statistical Package for Social Sciences (SPSS)

4	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups in the demographic variable in affecting the frequency of a subject receiving a phishing email, for a moderating categorical variable of social engineering techniques.	Kruskal-Wallis H Test	IBM© Statistical Package for Social Sciences (SPSS)
5	*Specific Objective 3:* To assess the performance level of the proposed security risk scale against results of a phishing attack performed at a bank.	There is no relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale.	Simulated Phishing Test	KnowBe4® Phishing Simulator

3.10 Security Risk Scale Design Methodology

The design of the security risk scale is a standard 5x5 risk matrix which consists of the probability of interacting with a phishing email and frequency of receiving the phishing email axes. The probability of interacting with a phishing email is categorized with nominal descriptors, and a score from 1 to 5 is assigned for each descriptor as follows: very unlikely=1, unlikely=2, not sure=3, likely=4 and very likely=5. Likewise, the frequency of receiving the phishing email axis scale is: ‘less than 3 times a year’=1, ‘3 - 7 times a year’=2, ‘7 - 11 times a year’=3, ‘11 - 15 times a year’=4, ‘more than 15 times a year’=5. Since a score is assigned to both the probability of interacting with a phishing email and frequency of receiving the phishing email, risk scores are estimated by multiplying the two scores to categorize the level of risk or risk rating (e.g., low, medium, high, and critical)



Frequency of receiving the phishing email	Very Unlikely (1)	Unlikely (2)	Not Sure (3)	Likely (4)	Very Likely (5)
More than 15 times a year (5)	Medium 5	High 10	Critical 15	Critical 20	Critical 25
11 - 15 times a year (4)	Medium 4	High 8	High 12	Critical 16	Critical 20
7 - 11 times a year (3)	Low 3	Medium 6	High 9	High 12	Critical 15
3 - 7 times a year (2)	Low 2	Medium 4	Medium 6	High 8	High 10
Less than 3 times a year (1)	Low 1	Low 2	Low 3	Medium 4	Medium 5

Probability of interacting with a phishing email

Figure 3. 32: Risk matrix

Source: (Kaya, 2018)

The security risk is derived from the risk formula of the product of the likelihood of the risk event occurring and impact or effect of the risk event. The likelihood of the risk event occurring is taken as the mean score of how frequently the respondents received a phishing email for the given social engineering technique. The impact or effect of the risk event is the mean score of how probable the respondent shall interact with a phishing email for the given social engineering technique.

The values of the risk associated with each emotional trigger in the phishing email i.e., authority, commitment, contrast, curiosity, empathy, fear, liking, reciprocity, scarcity, and social proof are evaluated by taking the mean score of the responses related to the specific trigger. Each emotion trigger is plotted onto the scale and the risk rating is noted.

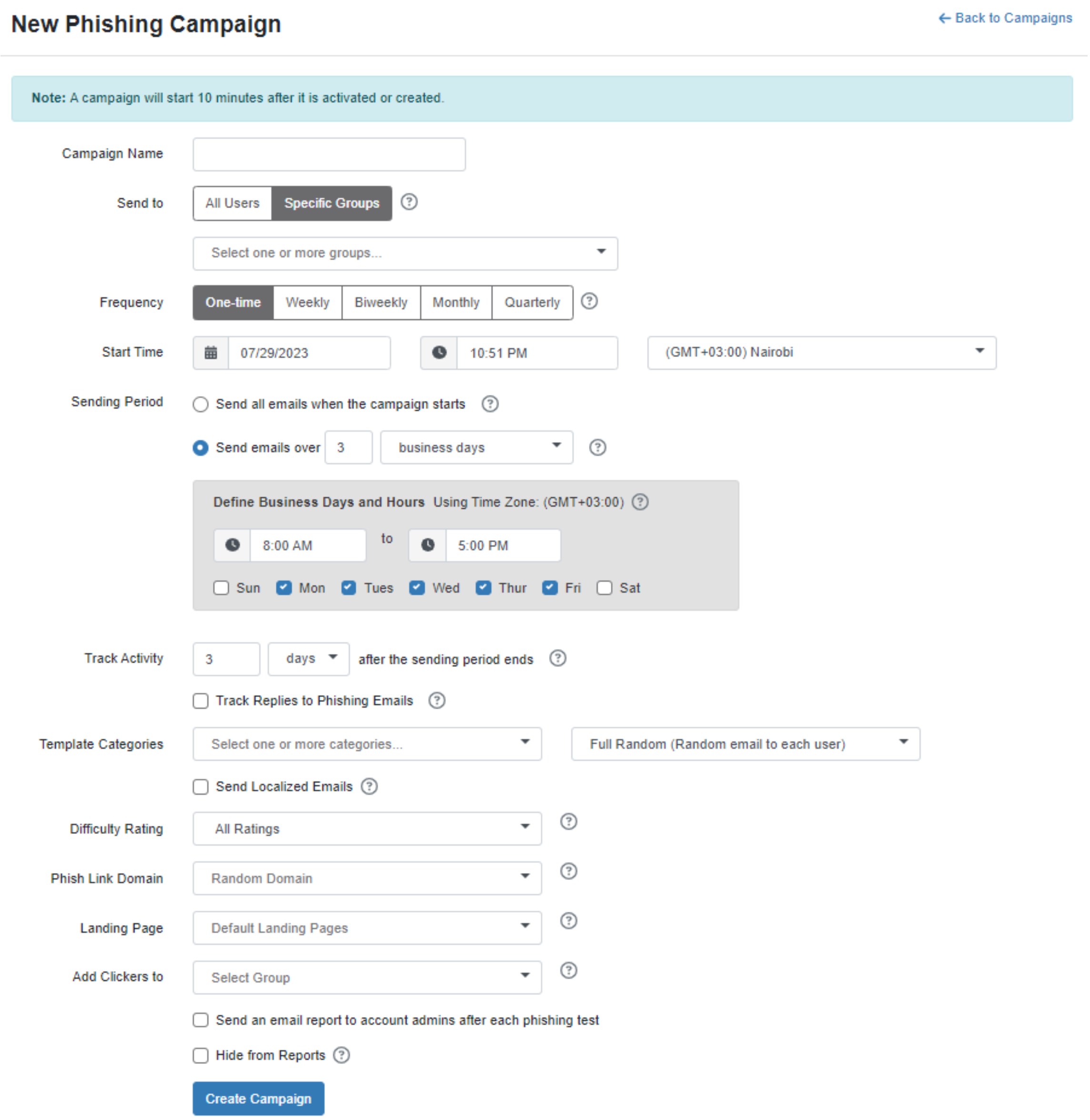
3.11 Phishing Test Methodology

The phishing test was conducted at CRDB Bank Plc using the KnowBe4 Phishing Simulator. The phishing attacks were targeted at all bank staff. Three separate phishing attacks were launched for the social engineering techniques of Authority, Commitment, and Reciprocity. The click rates were measured for a timing window of 3 days from the initiation of the phishing campaign. Each campaign was separated by a 2-week interval to give independence in the results and limit the results of one campaign directly affecting the results of the other.

3.11.1 KnowBe4 Phishing Simulation Setup

In the KnowBe4 Phishing Simulator, a new phishing campaign is initiated as shown in Figure 3.33 below. A campaign name is given for the phishing campaign setup. The campaign may either be targeted to all users in the organization or multiple specific groups of users. A frequency may be set of "One-time", "Weekly", "Biweekly", "Monthly", and "Quarterly". A start and end time is given for the campaign. Options are available to send all the emails at once, when the campaign starts, or to send the phishing emails over a selected number of business days. The business days between Sunday to Saturday and the times for running the campaign are created. The phishing interaction activity may start to be tracked within a selected number of days after the sending period ends. Tracking of the replies to the phishing email is possible. Template categories may be created and defined, which helps to classify the phishing campaigns. The emails may be sent as localized ones or not. The difficulty rating, phishing link domain, and landing page are all selectable from a list. The tested users that happen to click on a link may be added to a defined clickers group. Options for sending an email report to account admins after each phishing test may be selected. You can decide whether to keep the clickers hidden from the phishing campaign reports, or not.

Figure 3.33 below shows the “New Phishing Campaign” template. The phishing campaign is created here.



New Phishing Campaign

← Back to Campaigns

Note: A campaign will start 10 minutes after it is activated or created.

Campaign Name:

Send to: All Users | [✓ Specific Groups] ?

Select one or more groups...

Frequency: [✓ One-time] | Weekly | Biweekly | Monthly | Quarterly ?

Start Time: 07/29/2023 | 10:51 PM | (GMT+03:00) Nairobi

Sending Period: ○ Send all emails when the campaign starts ?

● Send emails over 3 business days ?

Define Business Days and Hours Using Time Zone: (GMT+03:00) ?

8:00 AM to 5:00 PM

☐ Sun ☑ Mon ☑ Tues ☑ Wed ☑ Thur ☑ Fri ☐ Sat

Track Activity: 3 days after the sending period ends ?

☐ Track Replies to Phishing Emails ?

Template Categories: Select one or more categories... | Full Random (Random email to each user)

☐ Send Localized Emails ?

Difficulty Rating: All Ratings ?

Phish Link Domain: Random Domain ?

Landing Page: Default Landing Pages ?

Add Clickers to: Select Group ?

☐ Send an email report to account admins after each phishing test

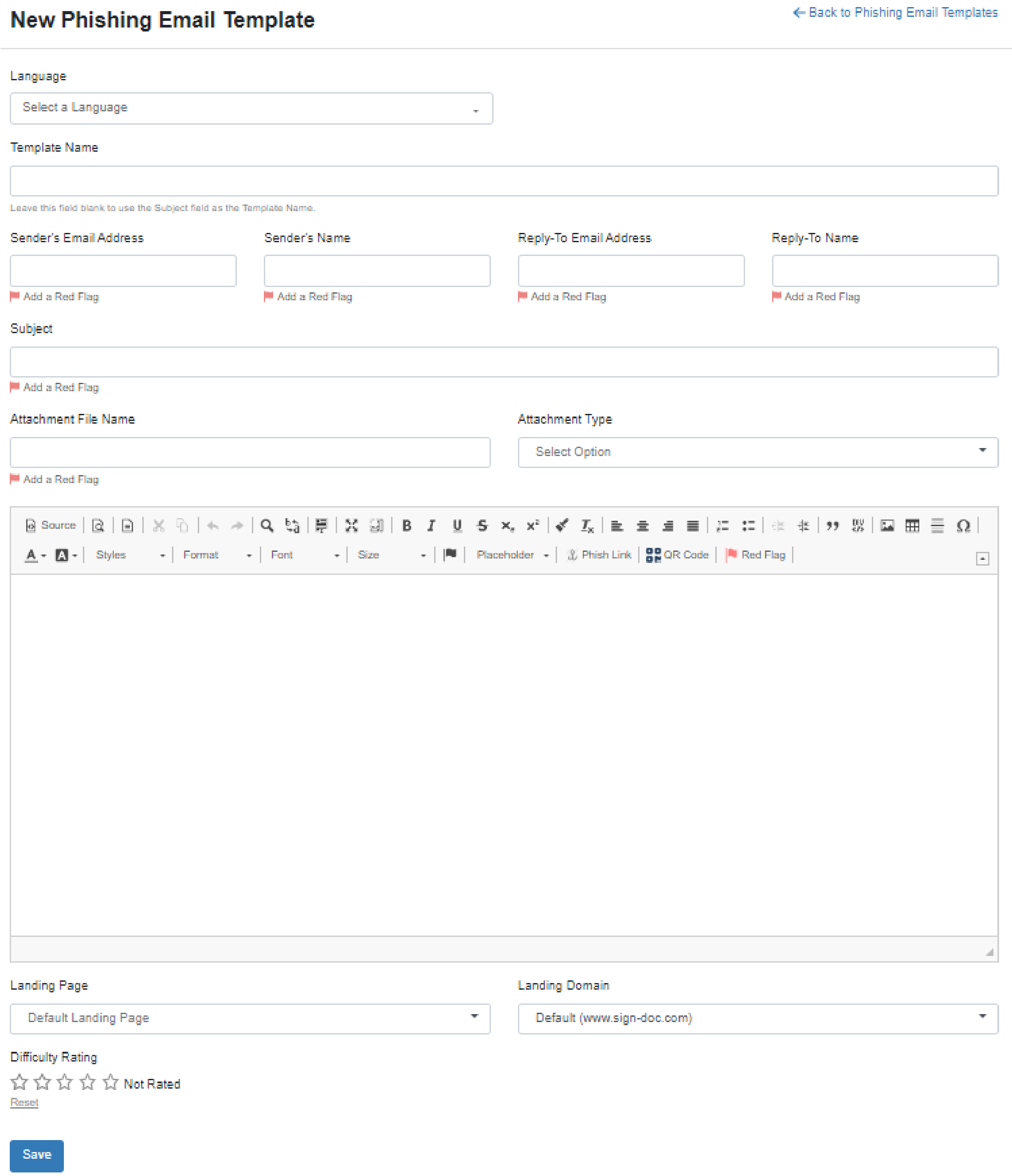
☐ Hide from Reports ?

Create Campaign

Figure 3. *33*: **New Phishing Campaign Setup in KnowBe4**

Source: KnowBe4 Phishing Simulator (2022)

Figure 3.34 below shows the “New Phishing Email Template”. The phishing email that is used in the campaign is created here.



New Phishing Email Template

← Back to Phishing Email Templates

Language

Select a Language

Template Name

Leave this field blank to use the Subject field as the Template Name.

Sender's Email Address	Sender's Name	Reply-To Email Address	Reply-To Name
Add a Red Flag	Add a Red Flag	Add a Red Flag	Add a Red Flag

Subject

Add a Red Flag

Attachment File Name

Add a Red Flag

Attachment Type

Select Option

Landing Page

Default Landing Page

Landing Domain

Default (www.sign-doc.com)

Difficulty Rating

☆ ☆ ☆ ☆ ☆ Not Rated

Reset

Save

Figure 3. ***34*****: New Phishing Email Template in KnowBe4**

Source: KnowBe4 Phishing Simulator (2022)

Figure 3.35 below shows the "New Landing Page" template. The page where the users are redirected once they click on a phishing link is created here.

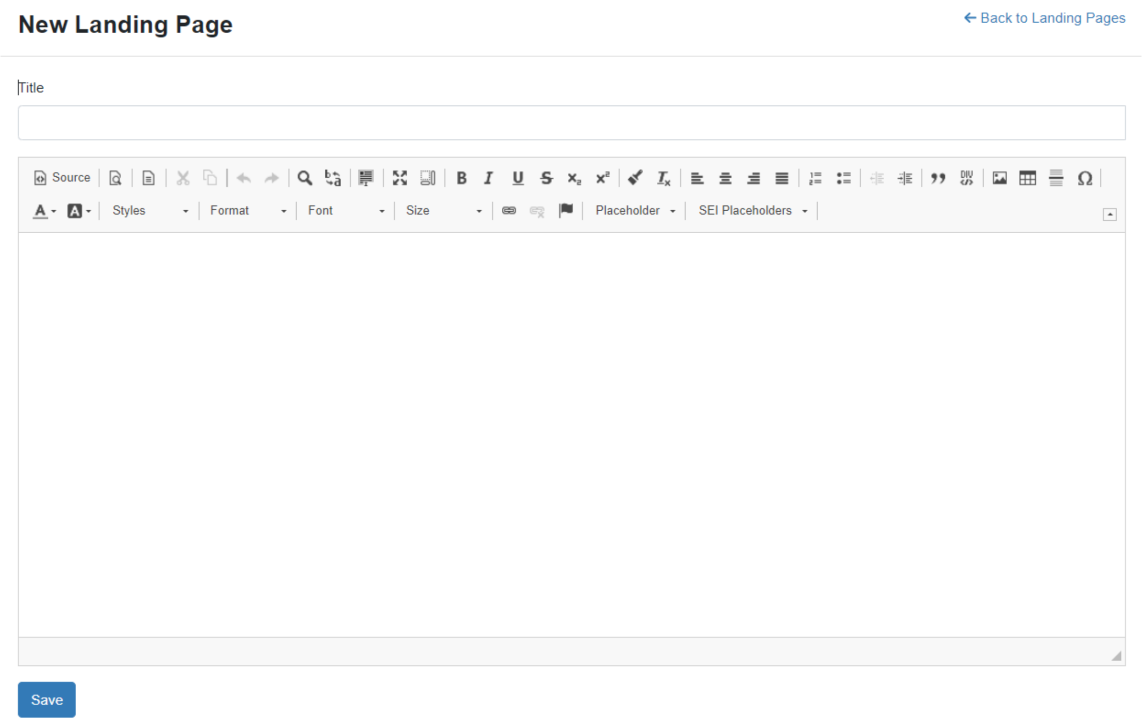
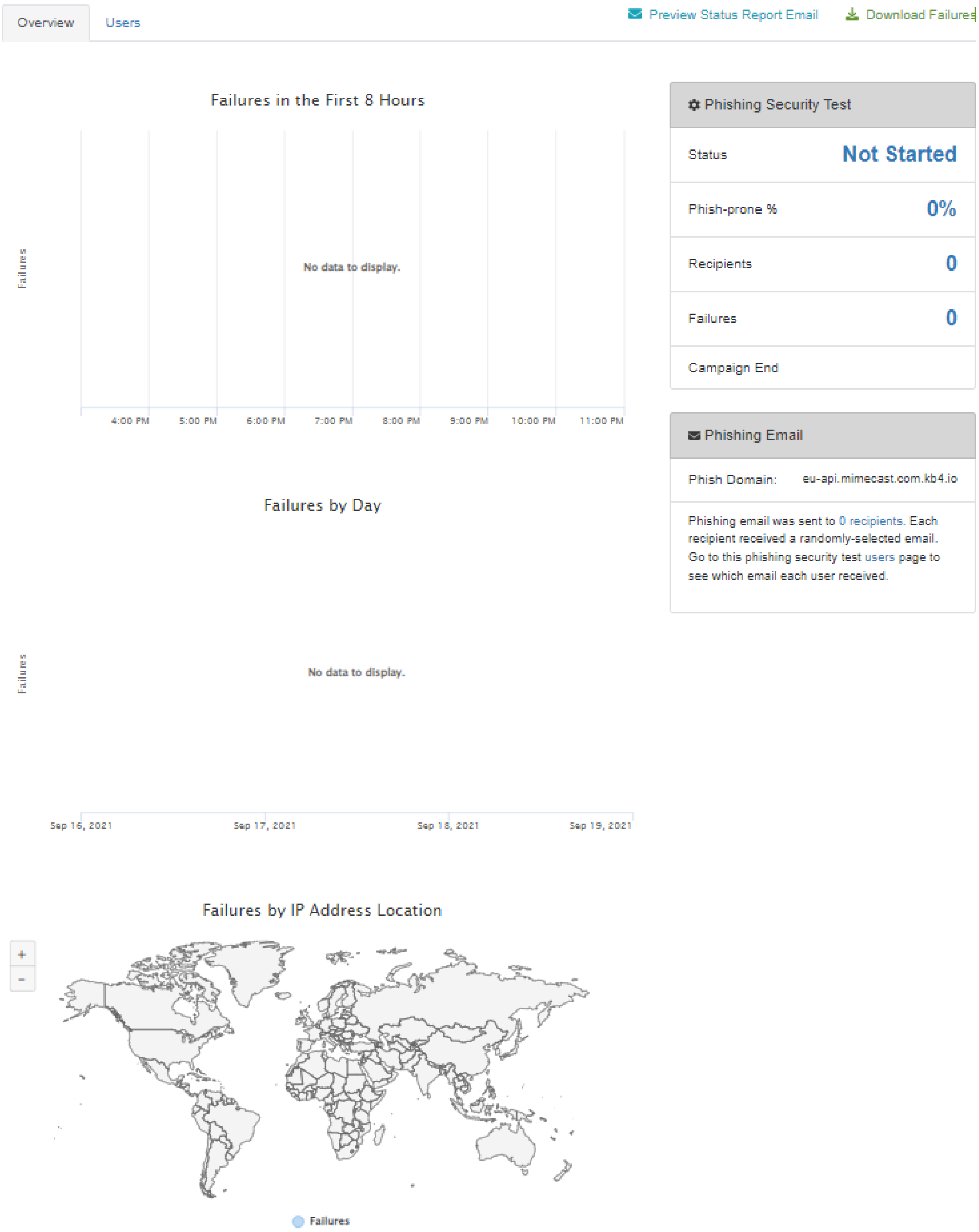


Figure 3. ***35*****: New Landing Page Template in KnowBe4**

Source: KnowBe4 Phishing Simulator (2022)

Figure 3.36 below shows the "Overview" tab of the phishing security test. Failures are considered as successful phishing attempts. This means the user interacted with the phishing email by either clicking the phishing links, downloading attachments, giving up sensitive data, etc. Analytics of failures in the first 8 hours, failures by day, and failures by IP address location are readily populated. The overall phish-prone percentage of users in the campaign is evaluated and displayed alongside the total recipients and failures of the campaign.



Phishing Security Test

Status	Not Started
Phish-prone %	0%
Recipients	0
Failures	0
Campaign End	

Phishing Email

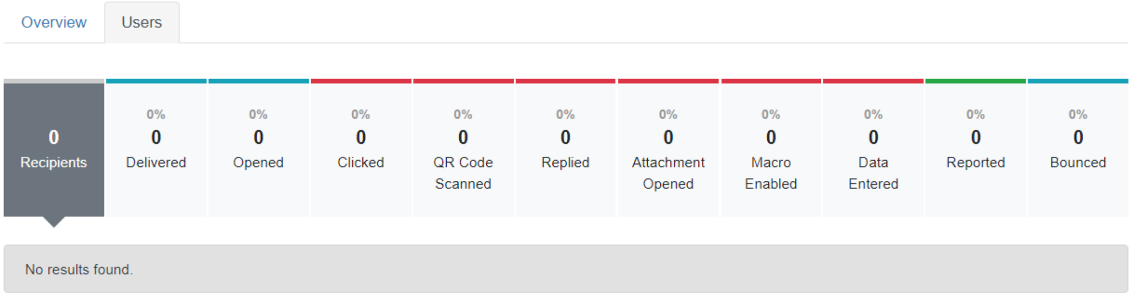
Phish Domain: eu-api.mimecast.com.kb4.io

Phishing email was sent to 0 recipients. Each recipient received a randomly-selected email. Go to this phishing security test users page to see which email each user received.

Figure 3. ***36*****: Phishing Security Test Dashboard in KnowBe4**

Source: KnowBe4 Phishing Simulator (2022)

Figure 3.37 below shows the "Users" tab. The total recipients of the phishing emails in the campaign are shown. Percentages of phishing emails that were delivered, opened, clicked, QR codes scanned, replied to, attachments opened, macros enabled, data entered, reported, and bounced are calculated and displayed for analysis.



Recipients	Delivered	Opened	Clicked	QR Code Scanned	Replied	Attachment Opened	Macro Enabled	Data Entered	Reported	Bounced
	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
0	0	0	0	0	0	0	0	0	0	0

No results found.

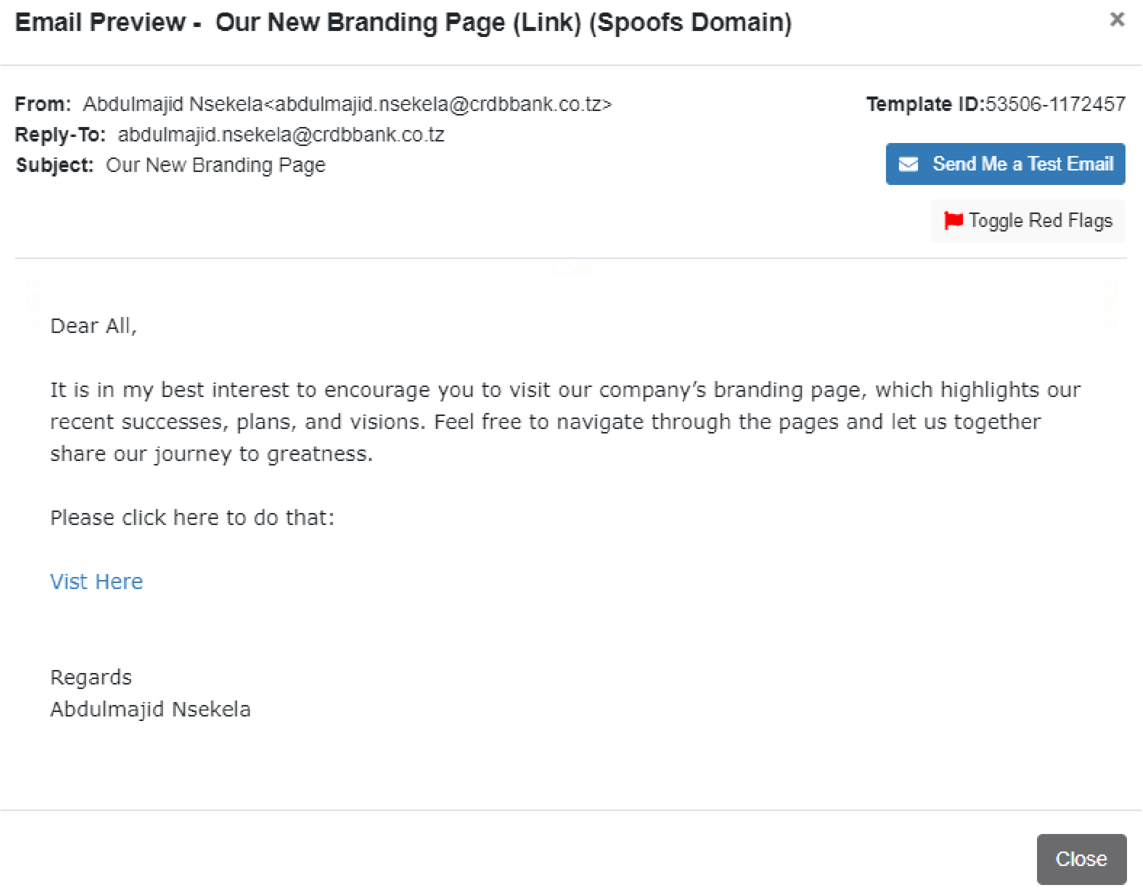
Figure 3. *37*: **Phishing Results Overview in KnowBe4**

Source: KnowBe4 Phishing Simulator (2022)

3.11.2 Authority Phishing Email

The authority social engineering technique was evaluated in a phishing email to all bank staff by pretending to be an authoritative figure i.e., the chief executive officer (CEO), and requesting the staff to navigate to the bank's brand page via a link in the email.

Figure 3.38 below shows the phishing campaign email template for the authority social engineering technique.



Email Preview - Our New Branding Page (Link) (Spoofs Domain)

From: Abdulmajid Nsekela<abdulmajid.nsekela@crdbbank.co.tz>
Reply-To: abdulmajid.nsekela@crdbbank.co.tz
Subject: Our New Branding Page

Template ID:53506-1172457

Dear All,

It is in my best interest to encourage you to visit our company's branding page, which highlights our recent successes, plans, and visions. Feel free to navigate through the pages and let us together share our journey to greatness.

Please click here to do that:

Vist Here

Regards
Abdulmajid Nsekela

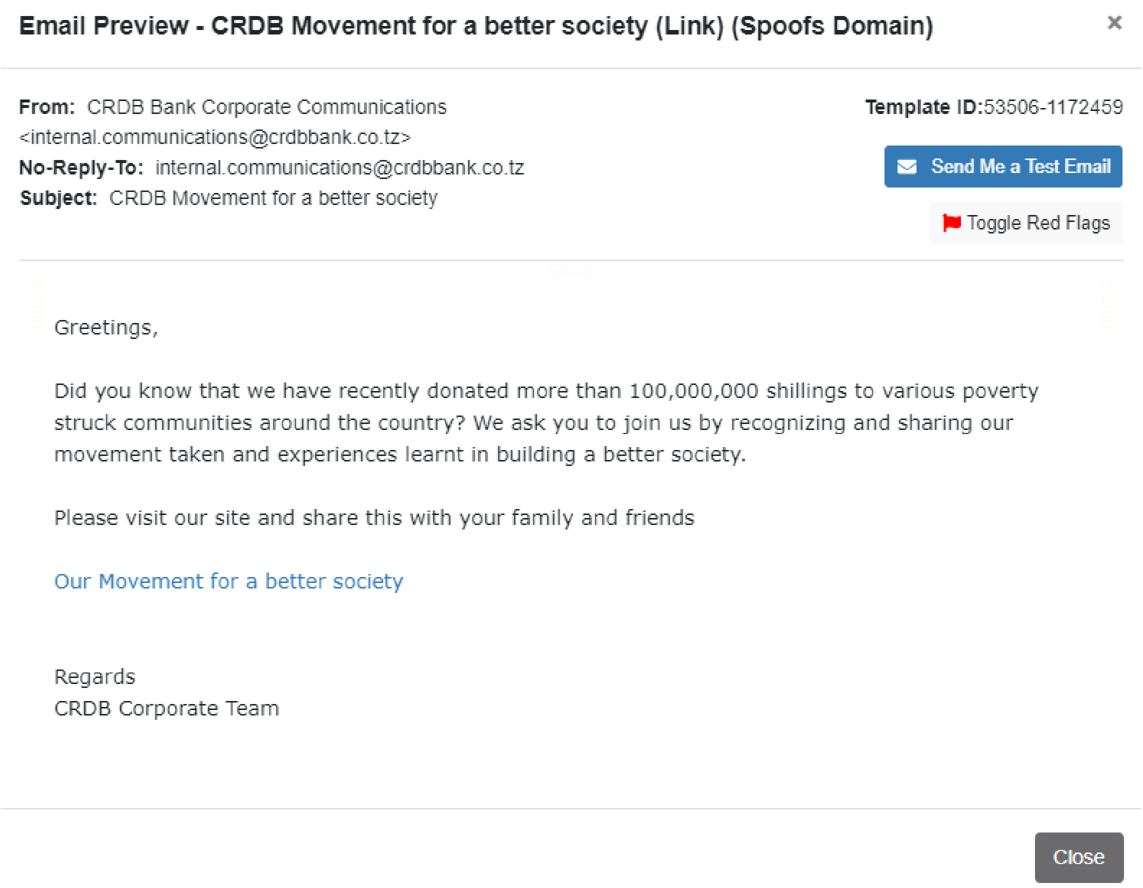
Figure 3. 38: Phishing test template for the authority technique

Source: KnowBe4 Phishing Simulator (2022)

3.11.3 Reciprocity Phishing Email

The reciprocity social engineering technique was tested in a phishing email to all bank staff by pretending to be the bank's corporate communications channel to convince the staff to navigate to a social movement page. The reciprocity technique was applied by illustrating the decent work the bank has done for the staff's community, so they in turn deserve a reciprocating hand of support for the started initiative.

Figure 3.39 below shows the phishing campaign email template for the reciprocity social engineering technique.



Email Preview - CRDB Movement for a better society (Link) (Spoofs Domain)

From: CRDB Bank Corporate Communications <internal.communications@crdbbank.co.tz>
No-Reply-To: internal.communications@crdbbank.co.tz
Subject: CRDB Movement for a better society

Template ID:53506-1172459

Greetings,

Did you know that we have recently donated more than 100,000,000 shillings to various poverty struck communities around the country? We ask you to join us by recognizing and sharing our movement taken and experiences learnt in building a better society.

Please visit our site and share this with your family and friends

Our Movement for a better society

Regards
CRDB Corporate Team

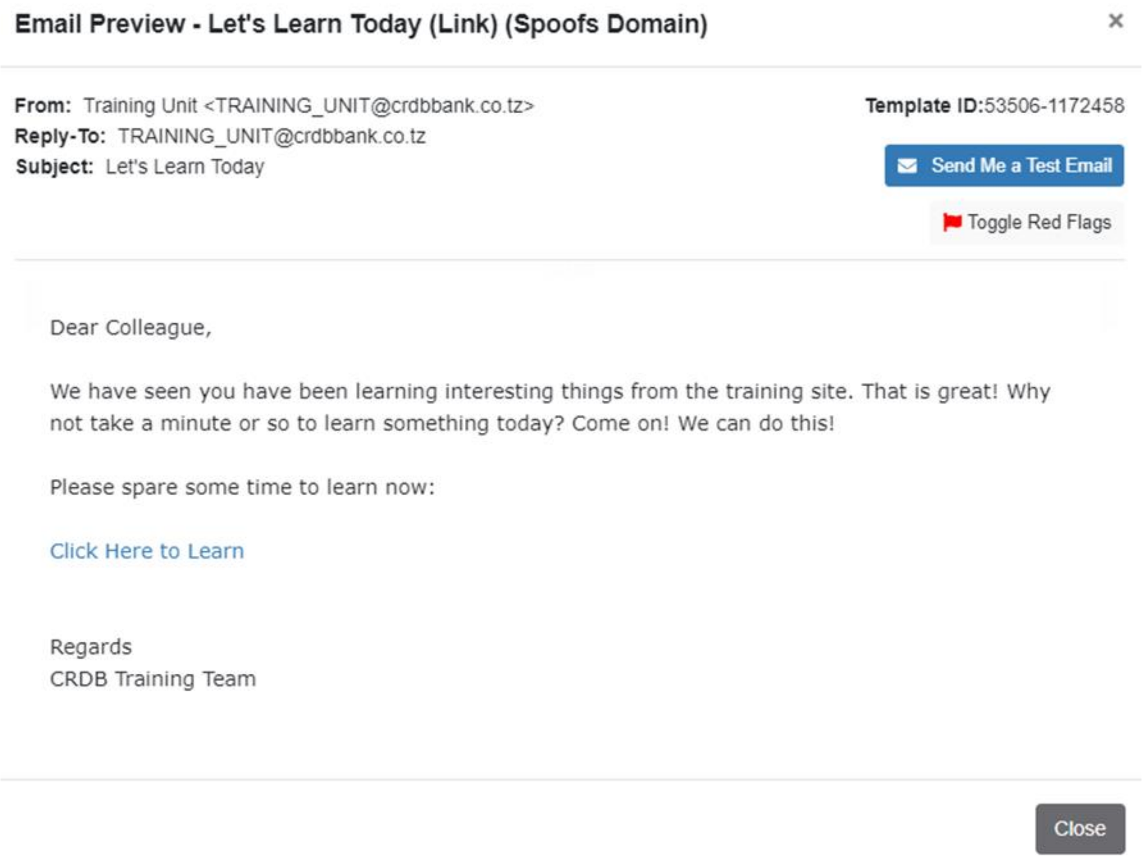
Figure 3. 39: Phishing test template for the reciprocity technique

Source: KnowBe4 Phishing Simulator (2022)

3.11.4 Commitment Phishing Email

The commitment social engineering technique was tested in a phishing email to all bank staff by pretending to be the human resources training unit and motivating the employees to take a learning course.

Figure 3.40 below shows the phishing campaign email template for the commitment social engineering technique.



Email Preview - Let's Learn Today (Link) (Spoofs Domain)

From: Training Unit <TRAINING_UNIT@crdbbank.co.tz>
Reply-To: TRAINING_UNIT@crdbbank.co.tz
Subject: Let's Learn Today

Template ID:53506-1172458

Dear Colleague,

We have seen you have been learning interesting things from the training site. That is great! Why not take a minute or so to learn something today? Come on! We can do this!

Please spare some time to learn now:

Click Here to Learn

Regards
CRDB Training Team

Figure 3. 40: Phishing test template for the commitment technique

Source: KnowBe4 Phishing Simulator (2022)

3.12 Performance Evaluation Methodology

We aim to find out the performance level of the proposed security risk scale against the results of a phishing attack performed at a bank, in our third specific objective. We therefore assess if a relationship exists between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale.

Null Hypothesis for the Performance Evaluation

There is no relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale.

Alternative Hypothesis for the Performance Evaluation

There is a relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale.

If the risk ratings of the sampled phishing social engineering techniques, (authority, reciprocity, and commitment) in our simulated phishing attack follow a similar distribution as the risk ratings of the designed security risk scale, we may therefore reject the null hypothesis and accept the alternative hypothesis. It signifies that the relationships between the risk ratings derived on the designed security risk scale are not by random chance but have significant meaning.

The security risk scale presented is derived qualitatively from the respondents' opinions on how they shall behave when subjected to a phishing email and how much they have experienced the phishing email. A measure of the accuracy of the responses collected from the questionnaire that derives the security risk scale is evaluated with respect to the results of the simulated phishing attack. In our evaluation we disregard the frequency of receiving phishing emails, as we are in full control of this variable. This is because we pose as hackers when conducting the phishing test. Any value of the phishing attack frequency is primarily based on our preference and cannot be considered for evaluation. However, since the 'probability of a user interacting with the phishing email' variable is dependent on the choice and behavior of the user, we use the percentage of users that interacted with or clicked the phishing email of a specific social engineering technique, from the simulated phishing attack, as the element to quantify the risk for the respective phishing social engineering technique.

To get the error rate, we first find the absolute value of the actual percentage of users that interacted with the phishing email (clicked) for the specific social engineering technique used during the phishing tests minus the percentage probability (taken from our security risk scale) of a subject interacting with a phishing email for the same social engineering technique. We then take the percentage of the value obtained by dividing the absolute value evaluated with the percentage probability of the subject interacting with a phishing email for the specified social engineering technique. The accuracy is obtained by subtracting the error rate from 100%.

$$\text{Accuracy} = 100\% - \text{Error Rate} \tag{1}$$

$$\text{Error Rate} = \frac{|\text{Phishing Simulation Test Value - Security Risk Scale Value}|}{\text{Security Risk Scale Value}} \times 100\% \tag{2}$$

(Cuemath, 2023)

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Identification of the factors affecting the effectiveness of phishing attempts through mail messages

For our first specific objective of identifying the factors that affect the effectiveness of phishing attempts through mail servers, an exploratory research methodology unveiled these factors, which may also be termed as the phishing social engineering techniques: -

Authority Humans shall typically conform when an eminent authority has confronted them.

Commitment The desire to work hard with effort can allow hackers to convince a victim into following their instructions.

Contrast The email has two choices that contradict. If the target disagrees with one option, they may select the other.

Curiosity Someone is more likely to follow the hacker's request if they are very interested in finding out more about it.

Empathy Sympathy makes a victim more vulnerable to accepting the demands in the phishing email.

Fear When people are frightened, they tend to do things they do not necessarily want, so the attacker scares them in the email.

Liking The hacker may act like they are someone the victim cares about to get them to perform their demands.

Reciprocity One pretends to have done a good deed, knowing people shall be inclined to return the favor.

Scarcity When there is very little time or few opportunities offered, a victim may quickly agree to the phishing request.

Social Proof Usually, people feel better doing something if everyone is doing it. (Karamagi, 2021)

Figure 4. 1: Phishing social engineering techniques or factors that affect the effectiveness of phishing

4.2 Design of a security risk scale based on the relationships between phishing variables and the security risk

4.2.1 Demographic Analysis of Collected Data

For our second specific objective of designing a security risk scale based on the relationships between phishing variables and the security risk, the survey questionnaire respondents were distributed as in Figure 4.2 below.

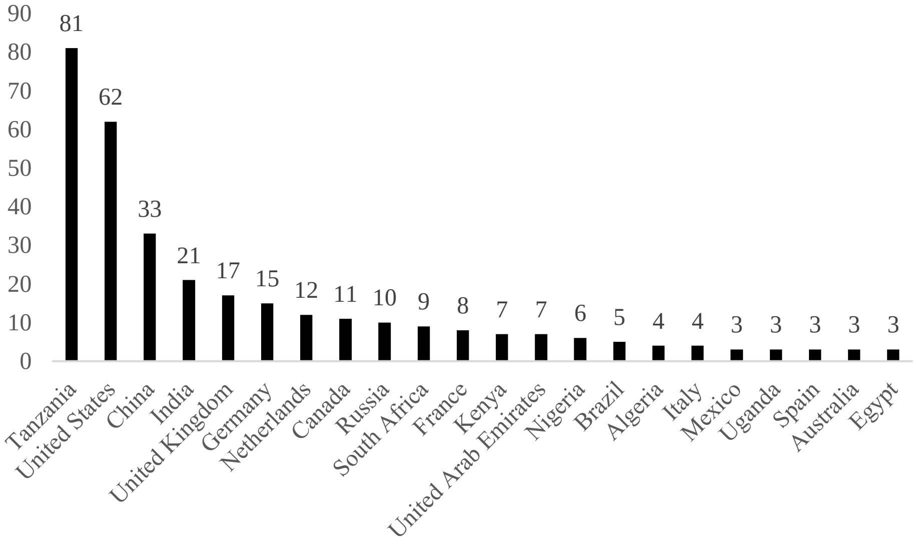


Figure 4. 2: Geographic location of survey respondents

Source: Field data (2022)

Note. The actual geographic location of the respondent may be different from the recorded location if the respondent answered the online survey while connected to a virtual private network (VPN) of a server situated at a location different from their current location.

A total of 327 responses were collected. The responses consisted of 177 (54.1%) Female and 150 (45.9%) Male respondents (*N*=327) as shown in Figure 4.3.

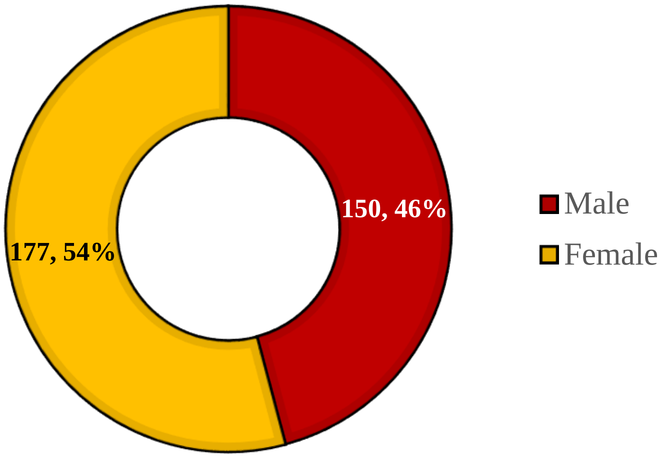


Figure 4. 3: Gender of total respondents

Source: Field data (2022)

The age range of the survey respondents was 91 (27.8%) 40-49 years, 88 (26.9%) 30-39 years, 74 (22.6%) 20-29 years, 37 (11.3%) 50-59 years, and 37 (11.3%) 60 years and above (*N*=327) as shown in Figure 4.4.

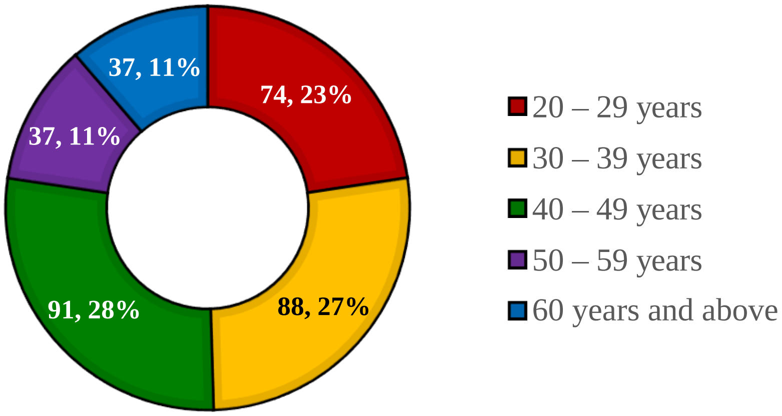


Figure 4. 4: Age Range of total respondents

Source: Field data (2022)

The education level of the survey respondents was 173 (52.9%) Bachelors, 107 (32.7%) Masters, and 47 (14.4%) Ph.D. (*N*=327) as shown in Figure 4.5.

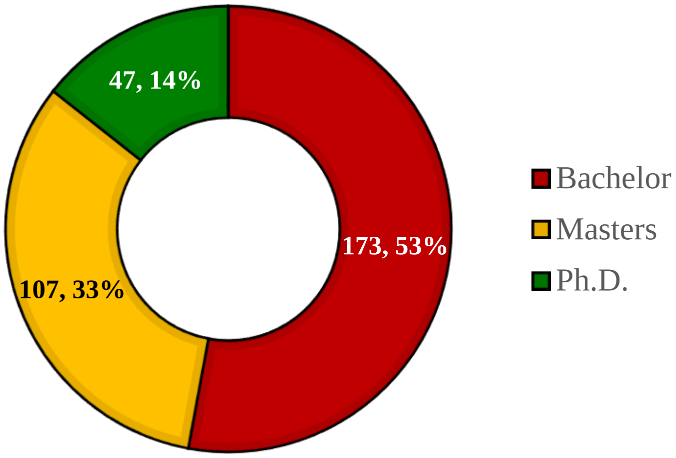


Figure 4. 5: Education Level of total respondents

Source: Field data (2022)

The professional status of the respondents was 157 (48%) Employed, 97 (29.7%) Student, 37 (11.3%) Retired, and 36 (11%) Unemployed (*N*=327) as shown in Figure 4.6.

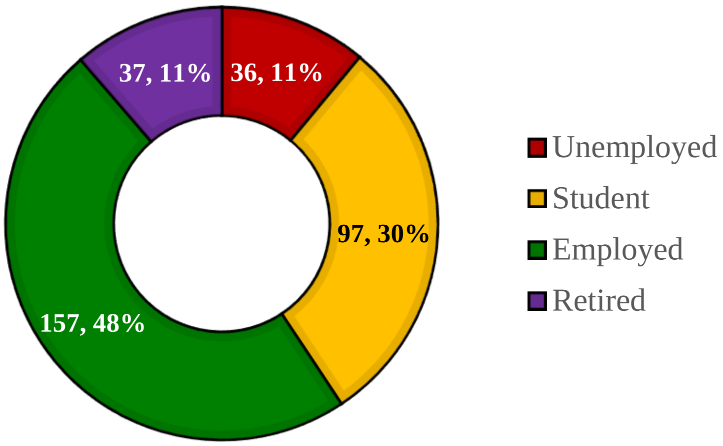


Figure 4. 6: Professional Status of total respondents

Source: Field data (2022)

The nature of institution of the respondents was 186 (56.9%) Private and 141 (43.1%) Public (*N*=327) as shown in Figure 4.7.

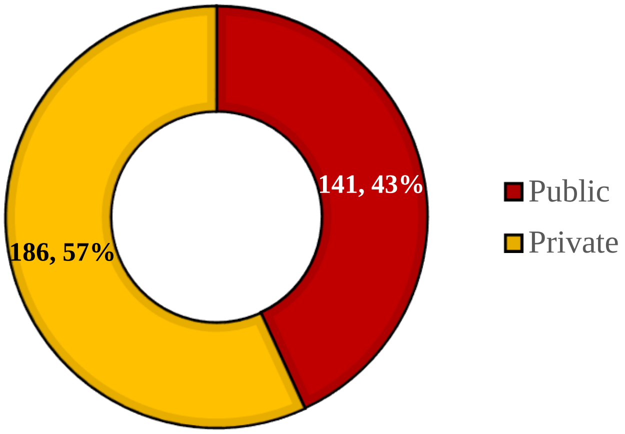


Figure 4. 7: Nature of Institution of total respondents

Source: Field data (2022)

The field of work of the respondents was: 30 (9.2%) Communications & Information Technology; 29 (8.9%) Education; 27 (8.3%) Energy; 64 (19.6%) Finance and Insurance; 16 (4.9%) Government; 27 (8.3%) Healthcare; 23 (7%) Manufacturing; 22 (6.7%) Media; 25 (7.6%) Others; 20 (6.1%) Professional Services; 23 (7%) Retail; and 21 (6.4%) Transportation (*N*=327) as shown in Figure 4.8.

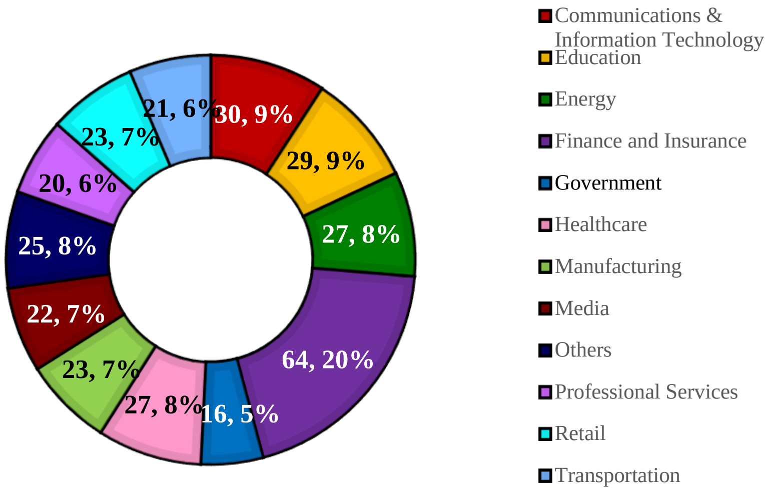


Figure 4. 8: Field of work of total respondents

Source: Field data (2022)

4.2.2 Sampling of Collected Data

Out of the total 327 responses, 100 total responses were statistically analyzed. The responses consisted of 50 male and 50 female respondents from the population as in Table 4.1.

Table 4. 1: Selection of respondents for analysis based on gender

SN	Gender	Male	Female	Total
1	Respondents	50	50	100
	Total	**50**	**50**	**100**

Source: Field data (2022)

For both the 50 male and 50 female respondents, 10 responses from each age range were selected for analysis as shown in Table 4.2.

Table 4. 2: Selection of respondents for analysis based on age range

SN	Age Range	Male	Female	Total
1	20 – 29 years	10	10	20
2	30 – 39 years	10	10	20
3	40 – 49 years	10	10	20
4	50 – 59 years	10	10	20
5	60 years and above	10	10	20
	Total	**50**	**50**	**100**

Source: Field data (2022)

The 50 male responses consisted of 18 bachelor, 17 masters and 15 Ph.D. respondents. The 50 female responses consisted of 17 bachelor, 18 masters and 15 Ph.D. respondents as shown in Table 4.3.

Table 4. 3: Selection of respondents for analysis based on education level

SN	Education Level	Male	Female	Total
1	Bachelor	18	17	35
2	Masters	17	18	35
3	Ph.D.	15	15	30
	Total	**50**	**50**	**100**

Source: Field data (2022)

Responses from 10 unemployed, 15 students, 15 employed and 10 retired were similarly selected from both the 50 male and 50 female respondents, as shown in Table 4.4.

Table 4. 4: Selection of respondents for analysis based on professional status

SN	Professional Status	Male	Female	Total
1	Unemployed	10	10	20
2	Student	15	15	30
3	Employed	15	15	30
4	Retired	10	10	20
	Total	**50**	**50**	**100**

Source: Field data (2022)

For both the 50 male and 50 female respondents, 25 responses from each type of institution i.e., public, and private, was selected, as shown in Table 4.5.

Table 4. 5: Selection of respondents for analysis based on nature of institution

SN	Nature of Institution	Male	Female	Total
1	Public	25	25	50
2	Private	25	25	50
	Total	**50**	**50**	**100**

Source: Field data (2022)

Out of the 50 male respondents, 4 responses each, were selected from the fields of finance and insurance, manufacturing, energy, retail, professional services, government, media, transportation, education, and others. 5 responses were selected from the healthcare and communications & information technology groups each.

Similarly, from the 50 female respondents, 4 responses each, were selected from the fields of manufacturing, energy, retail, professional services, government, healthcare, media, transportation, education, communications & information technology, and others. 5 responses were selected from the finance and insurance and education groups each. The selection is shown in Table 4.6.

Table 4. 6: Selection of respondents for analysis based on field of work

SN	Field of Work	Male	Female	Total
1	Communications & Information Technology	5	4	9
2	Education	4	5	9
3	Energy	4	4	8
4	Finance and Insurance	4	5	9
5	Government	4	4	8
6	Healthcare	5	4	9
7	Manufacturing	4	4	8
8	Media	4	4	8
9	Others	4	4	8
10	Professional Services	4	4	8
11	Retail	4	4	8
12	Transportation	4	4	8
	Total	**50**	**50**	**100**

Source: Field data (2022)

4.2.2 Selected Respondents Questionnaire Results

Figure 4.9 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the authority emotion trigger.

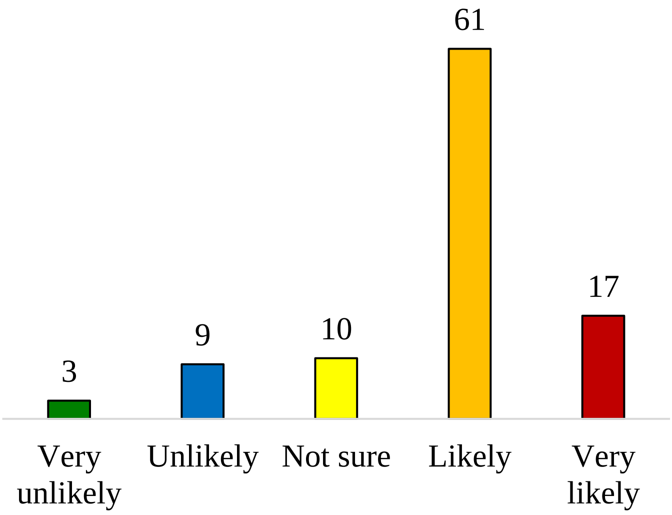


Figure 4. 9: Respondents' likelihood of clicking a phishing link (Authority Case)

Source**:** Field Data (2022)

Figure 4.10 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the authority emotion trigger.

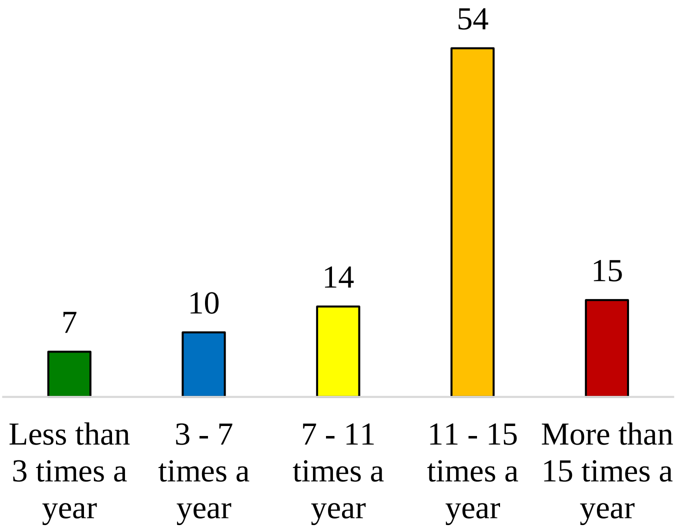


Figure 4. 10: Respondents' frequency of receiving a phishing email (Authority Case)

Source: Field Data (2022)

Figure 4.11 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the commitment emotion trigger.

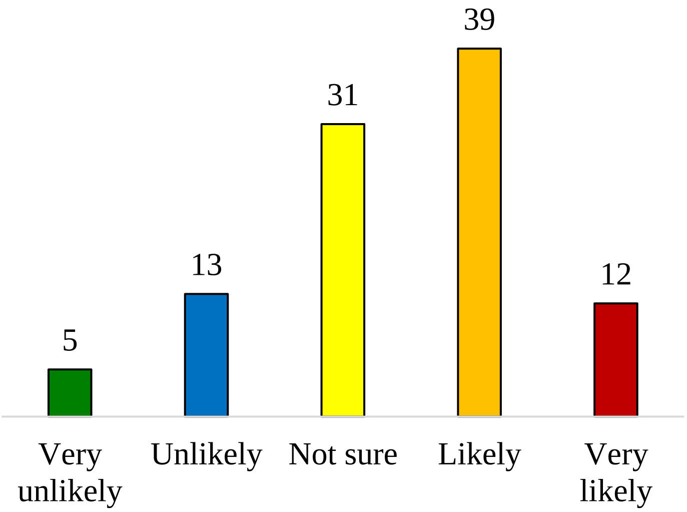


Figure 4. 11: Respondents' likelihood of clicking a phishing link (Commitment Case)

Source: Field Data (2022)

Figure 4.12 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the commitment emotion trigger.

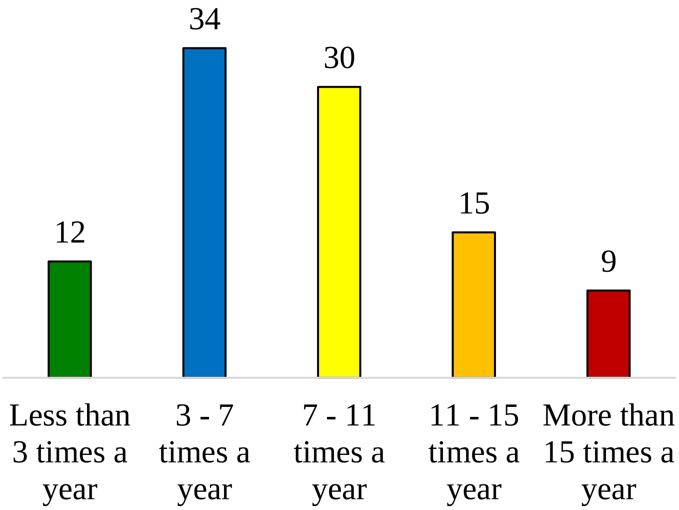


Figure 4. 12: Respondents' frequency of receiving a phishing email (Commitment Case)

Source: Field Data (2022)

Figure 4.13 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the contrast emotion trigger.

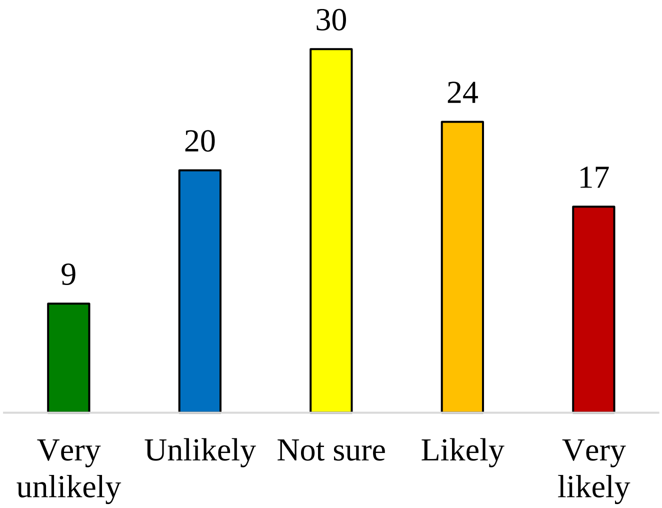


Figure 4. 13: Respondents' likelihood of clicking a phishing link (Contrast Case)

Source: Field Data (2022)

Figure 4.14 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the contrast emotion trigger.

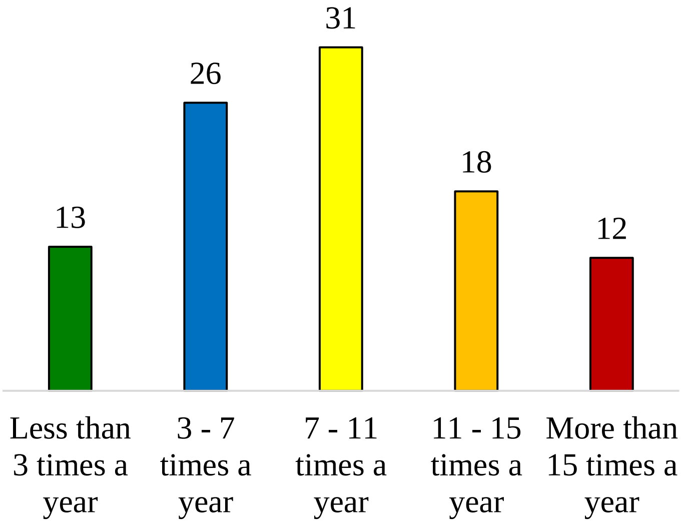


Figure 4. 14: Respondents' frequency of receiving a phishing email (Contrast Case)

Source: Field Data (2022)

Figure 4.15 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the curiosity emotion trigger.

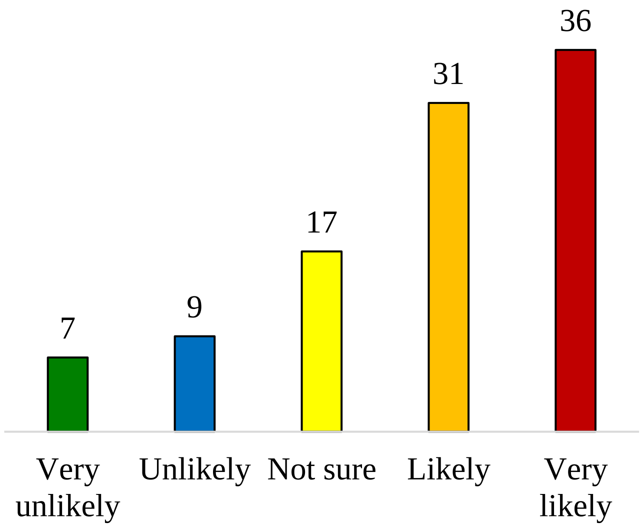


Figure 4. 15: Respondents' likelihood of clicking a phishing link (Curiosity Case)

Source: Field Data (2022)

Figure 4.16 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the curiosity emotion trigger.

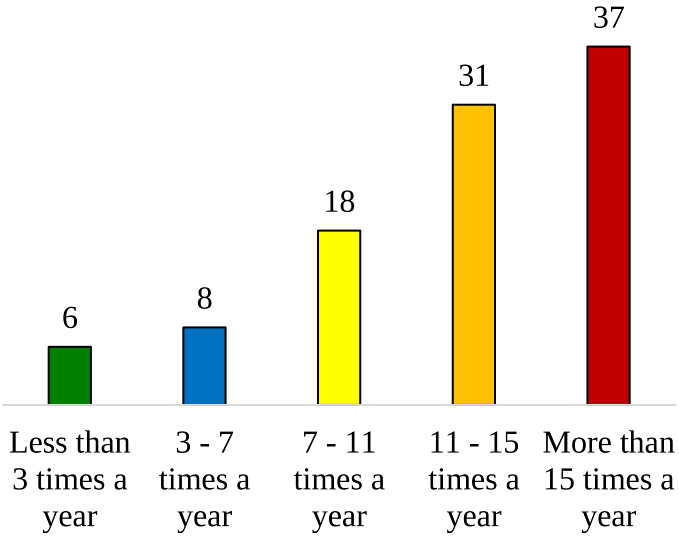


Figure 4. 16: Respondents' frequency of receiving a phishing email (Curiosity Case)

Source: Field Data (2022)

Figure 4.17 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the empathy emotion trigger.

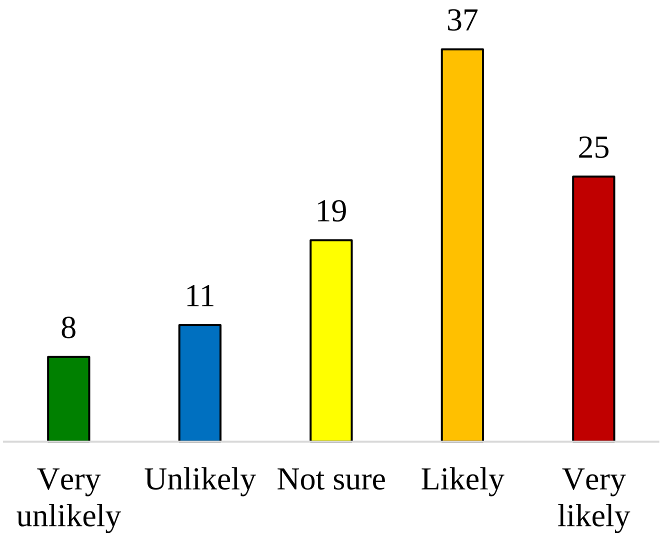


Figure 4. 17: Respondents' likelihood of clicking a phishing link (Empathy Case)

Source: Field Data (2022)

Figure 4.18 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the empathy emotion trigger.

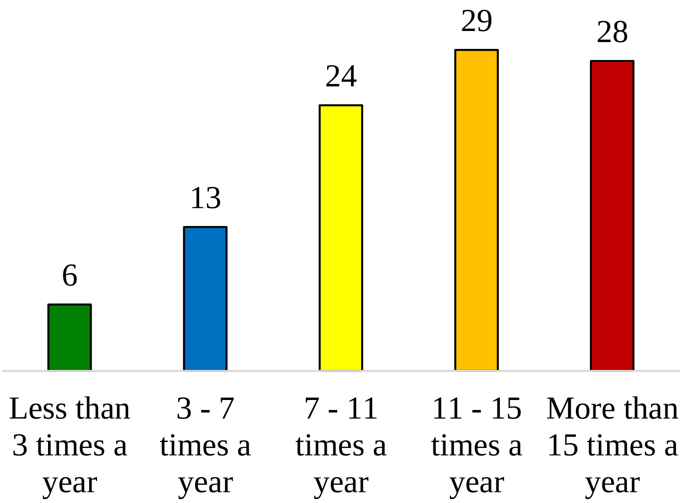


Figure 4. 18: Respondents' frequency of receiving a phishing email (Empathy Case)

Source: Field Data (2022)

Figure 4.19 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the fear emotion trigger.

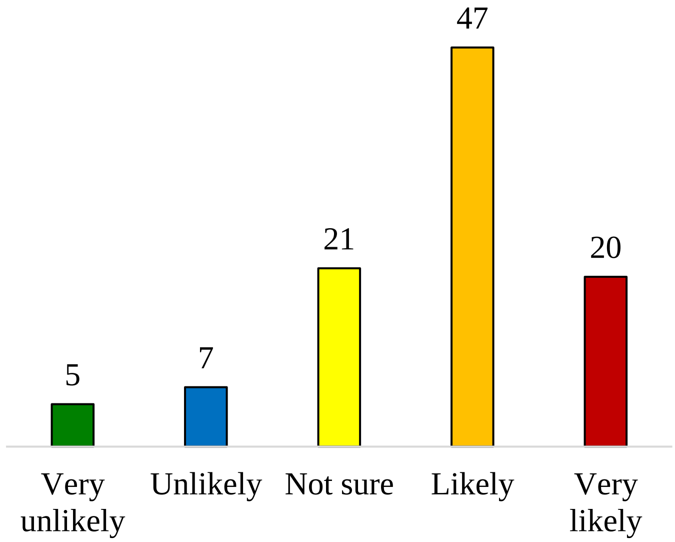


Figure 4. 19: Respondents' likelihood of clicking a phishing link (Fear Case)

Source: Field Data (2022)

Figure 4.20 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the fear emotion trigger.

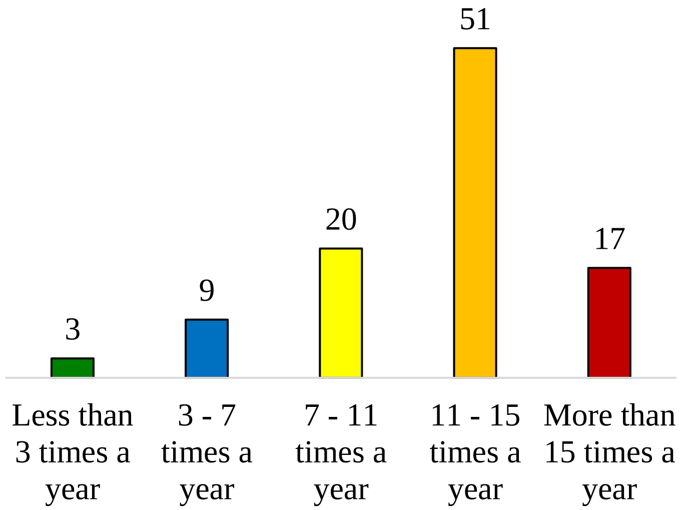


Figure 4. 20: Respondents’ frequency of receiving a phishing email (Fear Case)

Source: Field Data (2022)

Figure 4.21 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the liking emotion trigger.

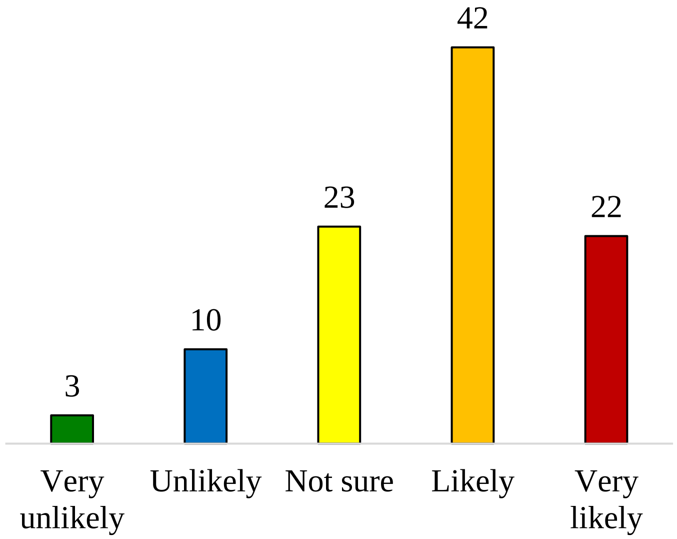


Figure 4. 21: Respondents' likelihood of clicking a phishing link (Liking Case)

Source: Field Data (2022)

Figure 4.22 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the liking emotion trigger.

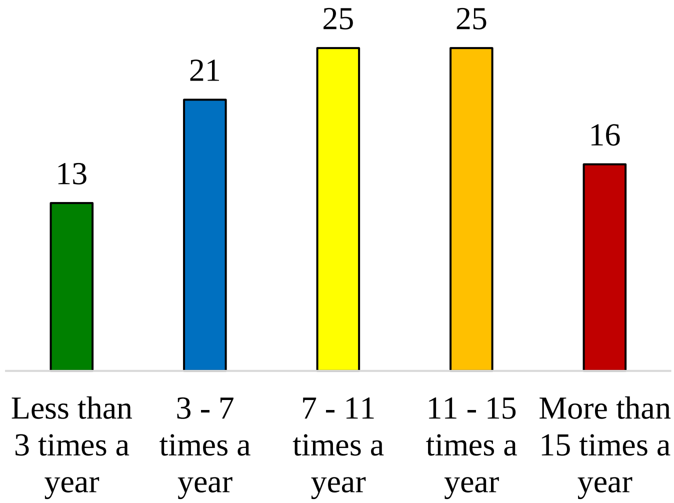


Figure 4. 22: Respondents' frequency of receiving a phishing email (Liking Case)

Source: Field Data (2022)

Figure 4.23 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the reciprocity emotion trigger.

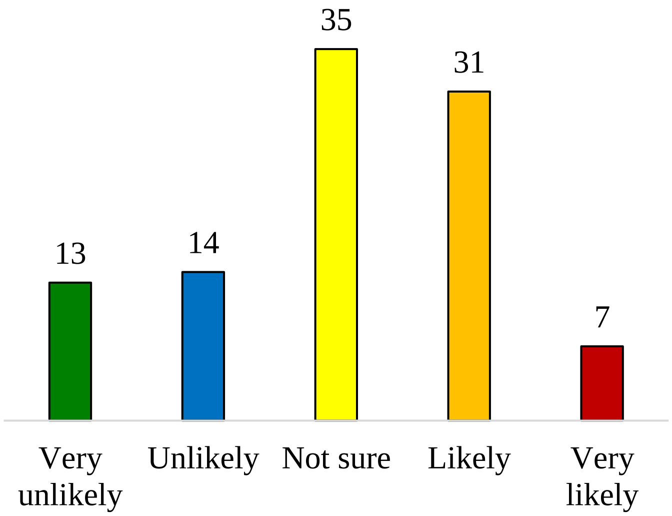


Figure 4. 23: Respondents' likelihood of clicking a phishing link (Reciprocity Case)

Source: Field Data (2022)

Figure 4.24 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the reciprocity emotion trigger.

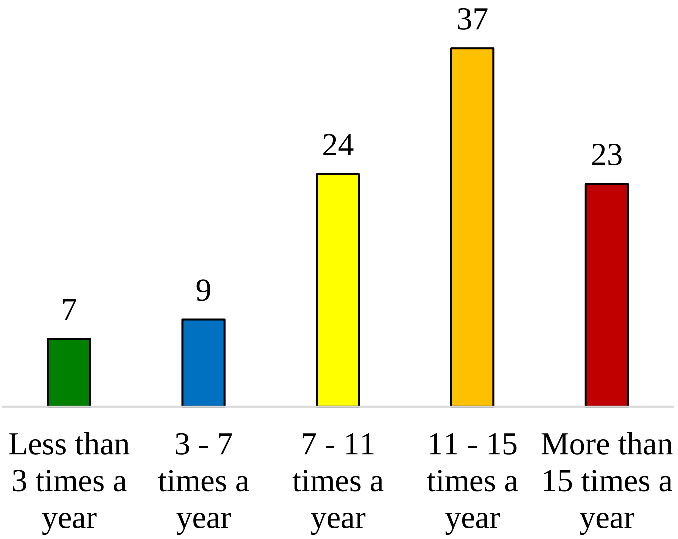


Figure 4. 24: Respondents' frequency of receiving a phishing email (Reciprocity Case)

Source: Field Data (2022)

Figure 4.25 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the scarcity emotion trigger.

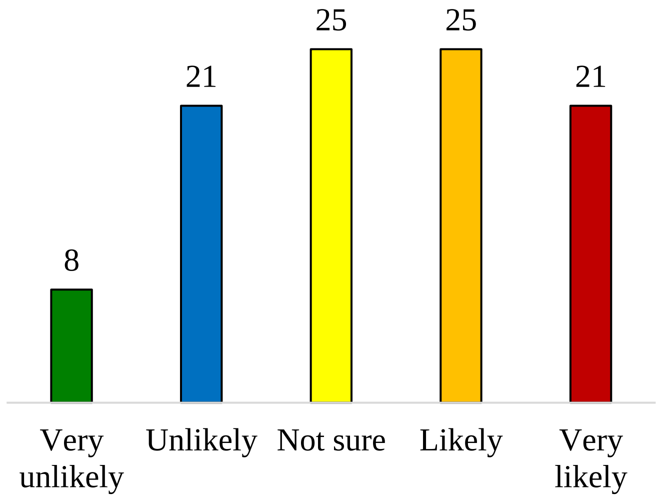


Figure 4. 25: Respondents' likelihood of clicking a phishing link (Scarcity Case)

Source: Field Data (2022)

Figure 4.26 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the scarcity emotion trigger.

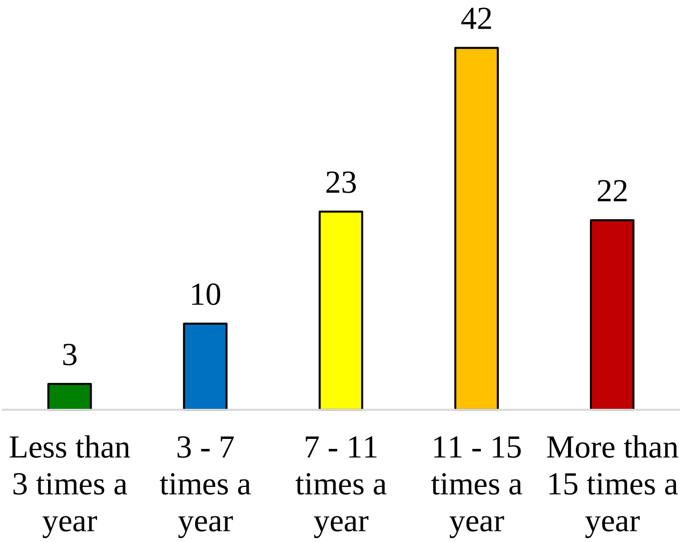


Figure 4. 26: Respondents’ frequency of receiving a phishing email (Scarcity Case)

Source: Field Data (2022)

Figure 4.27 below shows the number and percentage of respondents with respect to their responses for the likelihood of clicking on a malicious phishing link in the email that uses the social proof emotion trigger.

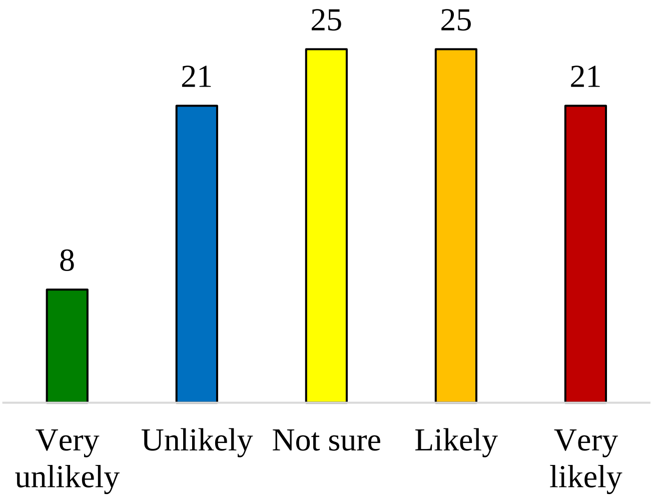


Figure 4. 27: Respondents' likelihood of clicking a phishing link (Social Proof Case)

Source: Field Data (2022)

Figure 4.28 below shows the number and percentage of respondents with respect to their responses for the frequency of receiving a malicious phishing email that uses the social proof emotion trigger.

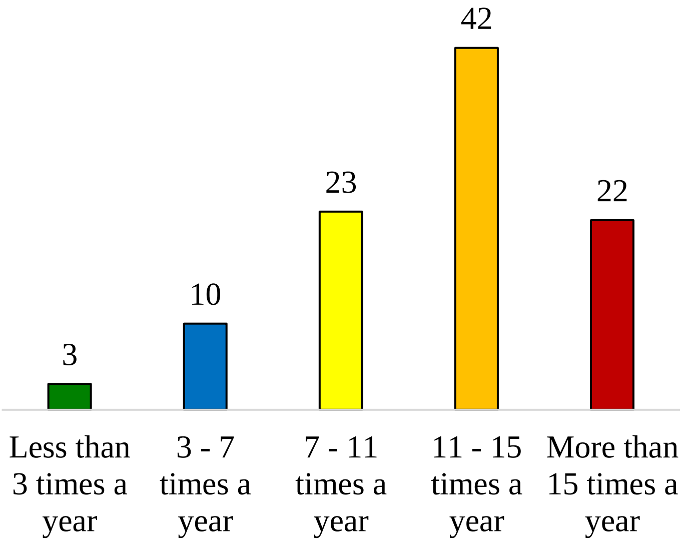


Figure 4. 28: Respondents' frequency of receiving a phishing email (Social Proof Case)

Source: Field Data (2022)

4.2.3 Hypothesis Test Results

The Friedman test that was conducted to check if there is any effect of the social engineering techniques on the probability of a subject interacting with a phishing email returned an asymptotic significance of less than 0.05 which means the probability of a subject interacting with a phishing email is affected by the social engineering techniques. Table 4.7 below displays the total number of samples N=100 with 9 degrees of freedom, chi-square coefficient χ^2=52.31, asymptotic significance *p*-value=3.957E-08, and Kendall's coefficient of concordance W=0.058.

A summary of the results in the American Psychological Association (APA) format is depicted below: -

χ^2 *(9, N=100) = 52.306, p < .001, W = .058.*

Table 4. 7: Friedman test results for the effect of phishing variables on the probability of clicking a phishing link

N	100
Chi-Square	52.305824
Degrees of Freedom	9
Asymptotic Significance	3.957E-08
Kendall's W	0.058

Source: IBM SPSS Output (2022)

The Friedman test that was conducted to check if there is any effect of the social engineering techniques on the frequency of a subject receiving a phishing email also returned an asymptotic significance of less than 0.05 which means the frequency of a subject receiving a phishing email is also affected by the social engineering techniques. Table 4.8 below displays the total number of samples N=100 with 9 degrees of freedom, chi-square coefficient χ^2=89.57, asymptotic significance *p*-value=1.983E-15, and Kendall’s coefficient of concordance W=0.100.

A summary of the results in APA format is depicted below: -

χ^2 (9, N=100) = 89.573, p < .001, W = .100

Table 4. 8: Friedman test results for the effect of phishing variables on the frequency of receiving phishing emails triggering the phishing variables

N	100
Chi-Square	89.573008
Degrees of Freedom	9
Asymptotic Significance	1.983E-15
Kendall’s W	0.100

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the gender of a subject has any effect on the probability of them clicking on a phishing link themed with the social engineering techniques returned no asymptotic significance value of less than 0.05 for all social engineering techniques as shown in Table 4.9 below. In other words, the gender did not have any effect on the probability of a subject clicking on a phishing link that was themed with any of the phishing variables.

Table 4. 9: Kruskal-Wallis H test results for the effect of gender on the probability of clicking a phishing link triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	2.695636876	1	0.100623275
Commitment	0.158515284	1	0.690527153
Contrast	0.212337156	1	0.6449417
Curiosity	0.074783427	1	0.784495342
Empathy	0.442837146	1	0.505756255
Fear	2.204385156	1	0.137618754
Liking	0.620148459	1	0.430992123
Reciprocity	0.394838563	1	0.529766949
Scarcity	0.891754293	1	0.345002354
Social Proof	0.194739592	1	0.659000827

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the gender of a subject has any effect on the frequency of them receiving a phishing email themed with the social engineering techniques returned an asymptotic significance value of less than 0.05 for the social proof technique. This means that the gender of the subject has an effect on the frequency of them receiving a phishing email that triggers the social proof phishing variable. Table 4.10 below shows the social proof phishing variable for a total number of samples N=100 with 1 degree of freedom, Kruskal-Wallis H value χ^2=4.00716079, and asymptotic significance *p*-value=0.045307387.

A summary of the results in APA format is depicted below: -

χ^2 (1, N=100) = 4.007, p = .045

Table 4. 10: Kruskal-Wallis H test results for the effect of gender on the frequency of receiving phishing emails triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	0.274866036	1	0.600086115
Commitment	0.157753162	1	0.691233607
Contrast	0.0500084	1	0.823048658
Curiosity	0.337286779	1	0.561399547
Empathy	1.519641901	1	0.217673692
Fear	0.631365055	1	0.426855045
Liking	1.324553271	1	0.249776513
Reciprocity	0.100087621	1	0.75172451
Scarcity	0.258126309	1	0.611410337
Social Proof	4.00716079	1	0.045307387

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the age range of a subject has any effect on the probability of them clicking on a phishing link themed with the social engineering techniques returned an asymptotic significance value of less than 0.05 for the authority technique. This means that the age range of a subject has an effect on the probability of them clicking on a phishing link that triggers the authority phishing variable. Table 4.11 below shows the authority phishing variable for a total number of samples N=100 with 4 degrees of freedom, Kruskal-Wallis H value χ^2=14.17248268, and asymptotic significance *p*-value=0.00676443.

A summary of the results in APA format is depicted below: -

χ^2 (4, N=100) = 14.172, p = .007

Similarly, the Kruskal-Wallis H test that was performed to check if the age range of a subject has any effect on the probability of them clicking on a phishing link themed with the social engineering techniques returned an asymptotic significance value of less than 0.05 for the commitment technique. This means that the age range of a subject has an effect on the probability of them clicking on a phishing link that triggers the commitment phishing variable. Table 4.11 below shows the commitment phishing variable for a total number of samples N=100 with 4 degrees of freedom, Kruskal-Wallis H value χ^2=10.37754367, and asymptotic significance *p*-value=0.034526257.

A summary of the results in APA format is depicted below: -

χ^2 (4, N=100) = 10.378, p = .035

Table 4. 11: Kruskal-Wallis H test results for the effect of age range on the probability of clicking a phishing link triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	14.17248268	4	0.00676443
Commitment	10.37754367	4	0.034526257
Contrast	3.679872009	4	0.451060191
Curiosity	5.395386064	4	0.249079312
Empathy	0.612076335	4	0.961712324
Fear	2.035351771	4	0.729256623
Liking	0.441613289	4	0.978930314
Reciprocity	1.518808769	4	0.823304589
Scarcity	1.069957545	4	0.899009012
Social Proof	3.462594577	4	0.483588667

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the age range of a subject has any effect on the frequency of them receiving a phishing email themed with the social engineering techniques returned an asymptotic significance value of less than 0.05 for the fear technique. This means that the age range of a subject has an effect on the frequency of a subject receiving a phishing email that triggers the fear phishing variable. Table 4.12 below shows the fear phishing variable for a total number of samples N=100 with 4 degrees of freedom, Kruskal-Wallis H value χ^2=10.371412, and asymptotic significance *p*-value=0.034615115.

A summary of the results in APA format is depicted below: -

χ^2 (4, N=100) = 10.371, p = .035

Table 4. 12: Kruskal-Wallis H test results for the effect of age range on the frequency of receiving phishing emails triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	1.056621689	4	0.901092158
Commitment	2.426666408	4	0.657813654
Contrast	4.337904242	4	0.362202747
Curiosity	6.712229407	4	0.151899803
Empathy	1.144118276	4	0.887210662
Fear	10.371412	4	0.034615115
Liking	5.437503305	4	0.245277853
Reciprocity	4.299212275	4	0.367023747
Scarcity	2.140637534	4	0.709910639
Social Proof	0.615243067	4	0.961354867

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the education level of a subject has any effect on the probability of them clicking on a phishing link themed with the social engineering techniques returned an asymptotic significance value of less than 0.05 for the commitment technique. This means that the education level of a subject has an effect on the probability of them clicking on a phishing link themed with the commitment phishing variable. Table 4.13 below shows the commitment phishing variable for a total number of samples N=100 with 2 degrees of freedom, Kruskal-Wallis H value χ^2=6.166208671, and asymptotic significance *p*-value=0.045816805.

A summary of the results in APA format is depicted below: -

χ^2 (2, N=100) = 6.166, p = .046

Table 4. 13: Kruskal-Wallis H test results for the effect of education level on the probability of clicking a phishing link triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	1.884363392	2	0.389776533
Commitment	6.166208671	2	0.045816805
Contrast	0.929999646	2	0.628135216
Curiosity	1.792259663	2	0.408146202
Empathy	1.997735046	2	0.368296292
Fear	4.360813687	2	0.11299555
Liking	0.250658771	2	0.882206269
Reciprocity	0.111213835	2	0.945910884
Scarcity	0.613782511	2	0.735730603
Social Proof	0.272788253	2	0.87249869

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the education level of a subject has any effect on the frequency of them receiving a phishing email themed with the social engineering techniques returned no asymptotic significance value of less than 0.05 for all social engineering techniques as shown in Table 4.14 below. In other words, the education level did not have any effect on the frequency of a subject receiving a phishing email that was themed with any of the phishing variables.

Table 4. 14: Kruskal-Wallis H test results for the effect of education level on the frequency of receiving phishing emails triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	0.291117194	2	0.864539229
Commitment	0.014871992	2	0.992591583
Contrast	5.084557809	2	0.078686875
Curiosity	3.172222676	2	0.204720153
Empathy	5.356539649	2	0.068681883
Fear	0.551261296	2	0.759093252
Liking	2.307657487	2	0.315426766
Reciprocity	5.486997553	2	0.064344824
Scarcity	3.912741124	2	0.141370587
Social Proof	0.3595071	2	0.835476089

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the professional status of a subject has any effect on the probability of them clicking on a phishing link themed with the social engineering techniques returned an asymptotic significance value of less than 0.05 for the authority technique. This means that the professional status of a subject has an effect on the probability of them clicking on a phishing link themed with the authority phishing variable. In simpler words, as an example, someone who is unemployed or retired would react differently to clicking a phishing link with an authority theme than someone who is employed. Table 4.15 below shows the authority phishing variable for a total number of samples N=100 with 3 degrees of freedom, Kruskal-Wallis H value χ^2=12.97897299, and asymptotic significance *p*-value=0.004682299.

A summary of the results in APA format is depicted below: -

χ^2 (3, N=100) = 12.979, p = .005

Table 4. 15: Kruskal-Wallis H test results for the effect of professional status on the probability of clicking a phishing link triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	12.97897299	3	0.004682299
Commitment	5.992620087	3	0.111969826
Contrast	1.099043715	3	0.77730494
Curiosity	6.313077723	3	0.097333036
Empathy	1.65125071	3	0.647825692
Fear	1.483283666	3	0.686133791
Liking	1.449008281	3	0.694088184
Reciprocity	2.901098901	3	0.407126477
Scarcity	1.554895095	3	0.669659732
Social Proof	1.234311464	3	0.74478731

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the professional status of a subject has any effect on the frequency of them receiving a phishing email themed with the social engineering techniques returned no asymptotic significance value of less than 0.05 for all social engineering techniques as shown in Table 4.16 below. In other words, the professional status did not have any effect on the frequency of a subject receiving a phishing email that was themed with any of the phishing variables.

Table 4. 16: Kruskal-Wallis H test results for the effect of professional status on the frequency of receiving phishing emails triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	2.718310952	3	0.437124503
Commitment	1.256059886	3	0.739592573
Contrast	1.85251995	3	0.603573233
Curiosity	0.303529041	3	0.959363402
Empathy	4.243519885	3	0.236340678
Fear	2.341137546	3	0.504685885
Liking	5.726486473	3	0.125702589
Reciprocity	3.567222092	3	0.312147725
Scarcity	2.026253118	3	0.566975691
Social Proof	1.862382555	3	0.601454775

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the nature of institution of a subject has any effect on the probability of them clicking on a phishing link themed with the social engineering techniques returned no asymptotic significance value of less than 0.05 for all social engineering techniques as shown in Table 4.17 below. In other words, the nature of institution did not have any effect on the probability of a subject clicking on a phishing link that was themed with any of the phishing variables.

Table 4. 17: Kruskal-Wallis H test results for the effect of nature of institution on the probability of clicking a phishing link triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	0.367646741	1	0.544289798
Commitment	0.017934498	1	0.893466038
Contrast	0.063336781	1	0.801297695
Curiosity	2.240602637	1	0.134428579
Empathy	0.30150586	1	0.582939918
Fear	0.768523334	1	0.380674259
Liking	0.625877282	1	0.428871599
Reciprocity	0.21385635	1	0.643761482
Scarcity	0.07036314	1	0.790808781
Social Proof	0.026372414	1	0.870994133

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was done to check if the nature of institution of a subject has any effect on the frequency of them receiving a phishing email themed with the social engineering techniques returned no asymptotic significance value of less than 0.05 for all social engineering techniques as shown in Table 4.18 below. In other words, the nature of institution did not have any effect on the frequency of a subject receiving a phishing email that was themed with any of the social engineering techniques.

Table 4. 18: Kruskal-Wallis H test results for the effect of nature of institution on the frequency of receiving phishing emails triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	0.233083439	1	0.62924687
Commitment	1.631806084	1	0.201453424
Contrast	0.660743385	1	0.416297623
Curiosity	0.367253657	1	0.544505079
Empathy	0.859849067	1	0.353780933
Fear	0.268875316	1	0.604087219
Liking	0.223791623	1	0.636165955
Reciprocity	0.001071092	1	0.973891857
Scarcity	0.011075726	1	0.91618436
Social Proof	2.18279014	1	0.139561249

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was done to check if the field of work of a subject has any effect on the probability of them clicking on a phishing link themed with the social engineering techniques returned no asymptotic significance value of less than 0.05 for all social engineering techniques as shown in Table 4.19 below. In other words, the field of work did not have any effect on the probability of a subject clicking on a phishing link that was themed with any of the phishing variables.

Table 4. 19: Kruskal-Wallis H test results for the effect of field of work on the probability of clicking a phishing link triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	8.776219417	11	0.642539614
Commitment	5.201282751	11	0.921027812
Contrast	9.453824109	11	0.580078053
Curiosity	13.72825938	11	0.248396356
Empathy	5.184659565	11	0.921894623
Fear	10.92377486	11	0.44967115
Liking	9.075123466	11	0.614958115
Reciprocity	5.780818087	11	0.887580969
Scarcity	9.432808729	11	0.582007733
Social Proof	8.885002534	11	0.632506333

Source: IBM SPSS Output (2022)

The Kruskal-Wallis H test that was performed to check if the field of work of a subject has any effect on the frequency of them receiving a phishing email themed with the social engineering techniques returned no asymptotic significance value of less than 0.05 for all social engineering techniques as shown in Table 4.20 below. In other words, the field of work did not have any effect on the frequency of a subject receiving a phishing email that was themed with any of the phishing variables.

Table 4. 20: Kruskal-Wallis H test results for the effect of field of work on the frequency of receiving phishing emails triggering the phishing variables

Phishing Variable	Kruskal-Wallis H	Degrees of Freedom	Asymptotic Significance
Authority	8.757586902	11	0.644256923
Commitment	15.65645612	11	0.154371574
Contrast	15.25797984	11	0.170988501
Curiosity	10.6475346	11	0.473246352
Empathy	10.35351538	11	0.498896368
Fear	9.62535757	11	0.564367581
Liking	10.30197108	11	0.503446674
Reciprocity	16.45315349	11	0.125123915
Scarcity	5.066529066	11	0.927901843
Social Proof	13.45507944	11	0.264624423

Source: IBM SPSS Output (2022)

Table 4.21 below shows a summary of the hypothesis test results for the specific objective of designing a security risk scale based on the relationships between phishing variables and the security risk.

Table 4. 21: Hypothesis Test Results for Specific Objective 2

SN	Specific Objective	Hypothesis	Result
1	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups of the phishing social engineering techniques in affecting the probability of a subject interacting with a phishing email.	A Friedman test revealed a significant effect of the social engineering techniques on the probability of a subject interacting with a phishing email, χ^2 (9, N=100) = 52.306, p < .001, W = .058.
2	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups of the phishing social engineering techniques in affecting the frequency of a subject receiving a phishing email.	The Friedman test revealed a significant effect of the social engineering techniques on the frequency of a subject receiving a phishing email, χ^2 (9, N=100) = 89.573, p < .001, W = .100.
3	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups in the demographic variable in affecting the probability of a subject interacting with a phishing email, for a moderating	Kruskal–Wallis' H test revealed a statistically significant difference in the probability of a subject interacting with a phishing email provoking authority on the age range, χ^2 (4, N=100) = 14.172, p = .007, and authority on the professional status, χ^2 (3, N=100) = 12.979, p =

		categorical variable of social engineering techniques.	.005. Similarly, a significant difference in the probability of a subject interacting with a phishing email provoking commitment on the age range χ^2 (4, N=100) = 10.378, p = .035, and commitment on the education level, χ^2 (2, N=100) = 6.166, p = .046, was found.
4	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups in the demographic variable in affecting the frequency of a subject receiving a phishing email, for a moderating categorical variable of social engineering techniques.	The Kruskal–Wallis H test revealed that a statistical significance exists between the frequency of a subject receiving a phishing email provoking social proof and the gender, χ^2 (1, N=100) = 4.007, p = .045. A significance was also found for the frequency of a subject receiving a phishing email provoking fear influencing the age range, χ^2 (4, N=100) = 10.371, p = .035.

Source: IBM SPSS (2022)

4.2.4 Security Risk Scale Results

The mean of the categorical results from the survey responses for the probability of a subject interacting with a phishing email and the frequency of a subject receiving a phishing email for each emotional trigger are shown in Table 4.22 below.

Figure 4.29 displays the security risk scale result, which is a plot of the mean scores for each emotion trigger depicted in Table 4.22 onto the risk matrix in Figure 3.5

Table 4. 22: Phishing security risk evaluation

Social Engineering Technique	Probability of a subject interacting with a phishing email	Frequency of a subject receiving a phishing email	Phishing Security Risk Score
Curiosity	3.8	3.85	14.63
Fear	3.7	3.7	13.69
Authority	3.8	3.6	13.68
Empathy	3.6	3.6	12.96
Scarcity	3.3	3.7	12.21
Liking	3.7	3.1	11.47
Reciprocity	3.05	3.6	10.98
Social Proof	3.1	3.25	10.075
Commitment	3.4	2.75	9.35
Contrast	3.2	2.9	9.28

Source: Field data (2022)

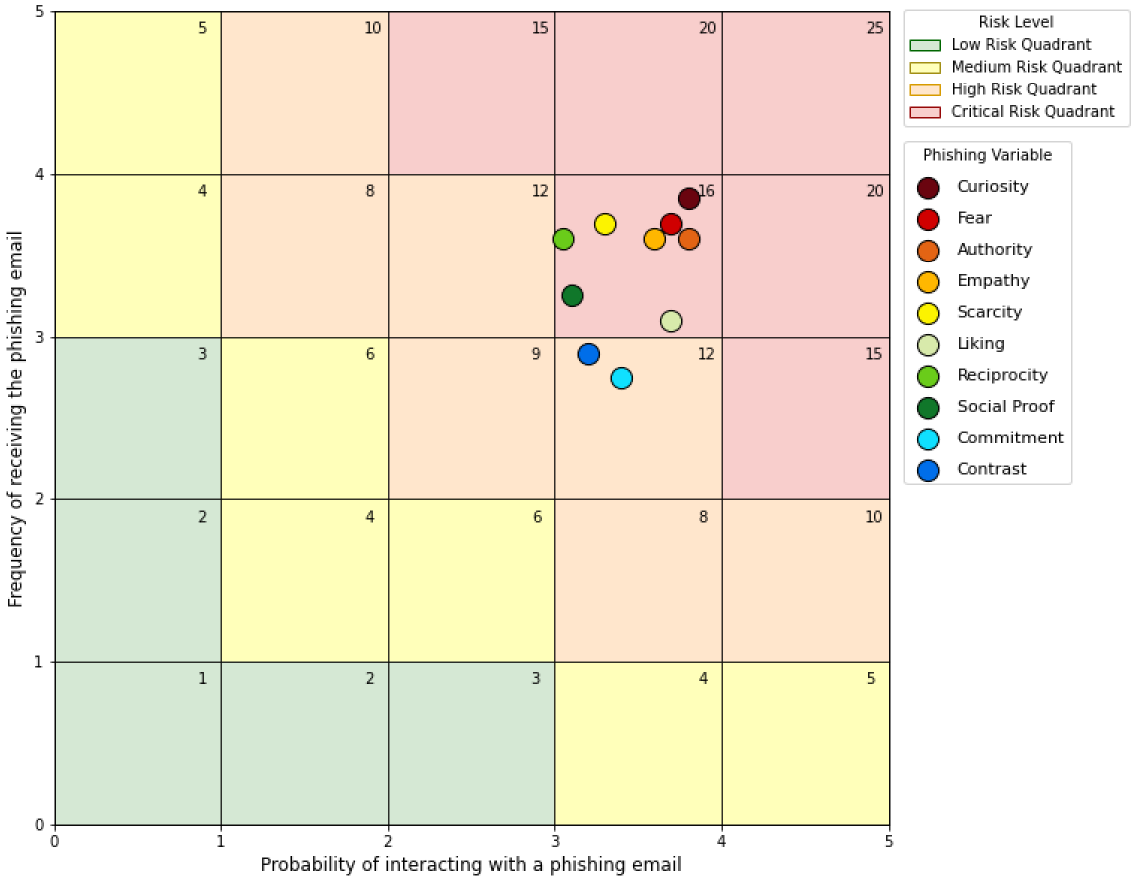


Figure 4. 29: Security Risk Scale

Source: Field data (2022)

4.2.5 Experimental Phishing Test Results

The phishing email for the authority social engineering technique was sent to 4236 recipients and delivered successfully to 4227 users. 3213 users opened the phishing mail and 2561 clicked on the link in it. 16 users reported the email as suspicious to the security operating center. The phishing email for the reciprocity social engineering technique was sent to 4229 recipients and delivered successfully to 4102 users. 1908 users opened the phishing mail and 567 clicked on the link in it. 45 users reported the email as suspicious to the security operating center. The phishing email for the commitment social engineering technique was sent to 4233 recipients and delivered successfully to 4094 users. 1527 users opened the phishing mail and 195 clicked on the link in it. 87 users reported the email as suspicious to the security operating center. Table 4.23 summarizes the phishing test results for the 3 phishing campaigns for the emotional triggers of authority, reciprocity, and commitment. The number of recipients, and the number phishing emails delivered, opened, clicked, and reported for each phishing social engineering technique is tabulated.

Table 4. 23: Phishing tests results for the sampled phishing social engineering techniques

Phishing Technique	Recipients	Delivered	Opened	Clicked	Reported
Authority	4236	4227	3213	2561	16
Reciprocity	4229	4102	1908	567	45
Commitment	4233	4094	1527	195	87

Source: Phishing test results (2022)

Figure 4.30 below illustrates the phishing test results for the authority, reciprocity, and commitment phishing social engineering techniques.

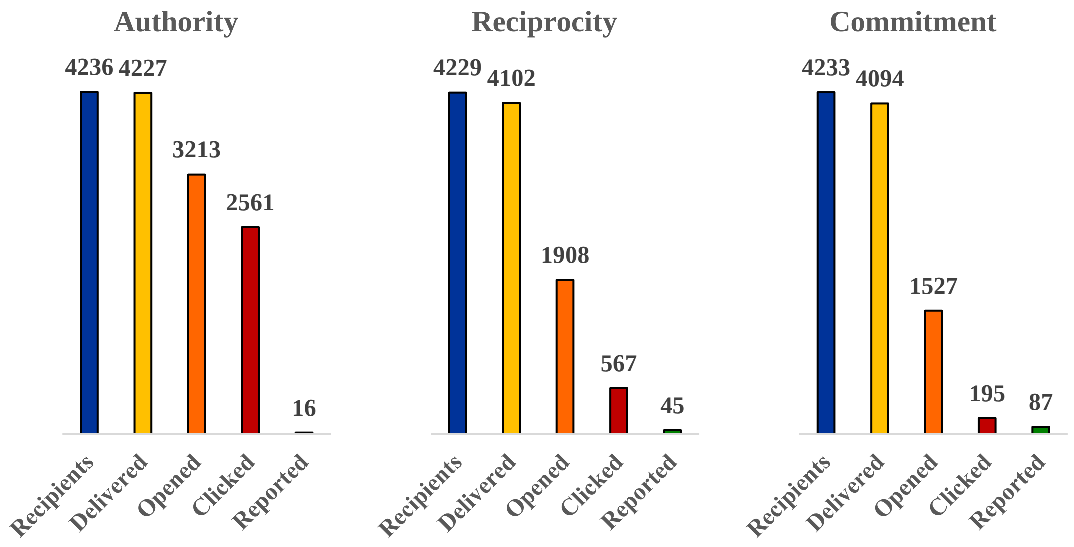


Figure 4. 30: Phishing tests results for the sampled phishing social engineering techniques

Source: Phishing test results (2022)

4.3 Assessment of the performance level of the proposed security risk scale against results of a phishing attack performed at a bank

The risk ratings distribution of the sampled phishing social engineering techniques, (authority, reciprocity, and commitment) in our simulated phishing attack are compared to that of the designed security risk scale.

Figure 4.31 below shows a condensed security risk scale that focuses on the authority, reciprocity, and commitment social engineering techniques only. It is the same risk scale in Figure 4.29 without the other phishing social engineering techniques.

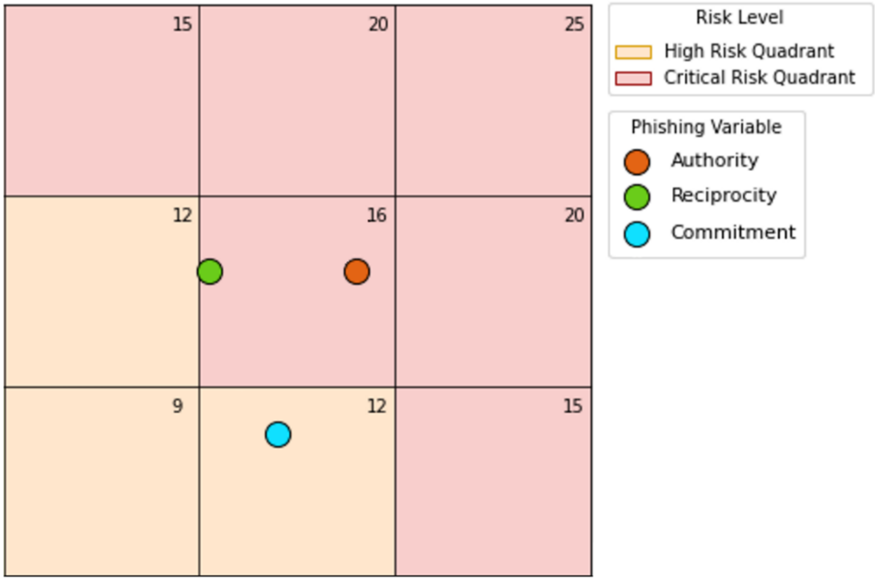


Figure 4. 31: Condensed Security Risk Scale with Authority, Reciprocity and Commitment Social Engineering Techniques

Source: Field data (2022)

Table 4.24 below shows the implied risk ratings of the authority, reciprocity, and commitment social engineering techniques by taking the probability of a subject interacting with a phishing email as per the designed security risk scale. It is referenced from Table 4.22 that tabulates the phishing security risk evaluation.

Table 4.25 below tabulates the implied risk ratings from for Authority, Reciprocity and Commitment Social Engineering Techniques by taking the percentage of users that interacted with the phishing email corresponding to the associated phishing technique, in the simulated phishing test. It is referenced from Table 4. 23 that tabulates the phishing tests results for the sampled phishing social engineering techniques.

Table 4. 24: Implied risk ratings for Authority, Reciprocity and Commitment Social Engineering Techniques as per the designed security risk scale

Social Engineering Technique	Probability of a subject interacting with a phishing email as per the designed security risk scale (%)
Authority	$\frac{3.8}{5} = 0.76$
Reciprocity	$\frac{3.05}{5} = 0.61$
Commitment	$\frac{3.4}{5} = 0.68$

Source: Field data (2022)

Table 4. 25: Implied risk ratings for Authority, Reciprocity and Commitment Social Engineering Techniques as per the phishing simulation tests results

Phishing Technique used in the simulated phishing test	Number of users that opened the phishing email received	Number of users that clicked on a link in the phishing email received	Percentage of users that interacted with the phishing email in the simulated phishing test (%)
Authority	3213	2561	80
Reciprocity	1908	567	30
Commitment	1527	195	13

Source: Phishing test results (2022)

Figure 4.32 below shows the distribution of risk ratings from the designed security risk scale and the distribution of risk ratings from the simulated phishing test, for the authority, reciprocity, and commitment social engineering techniques.

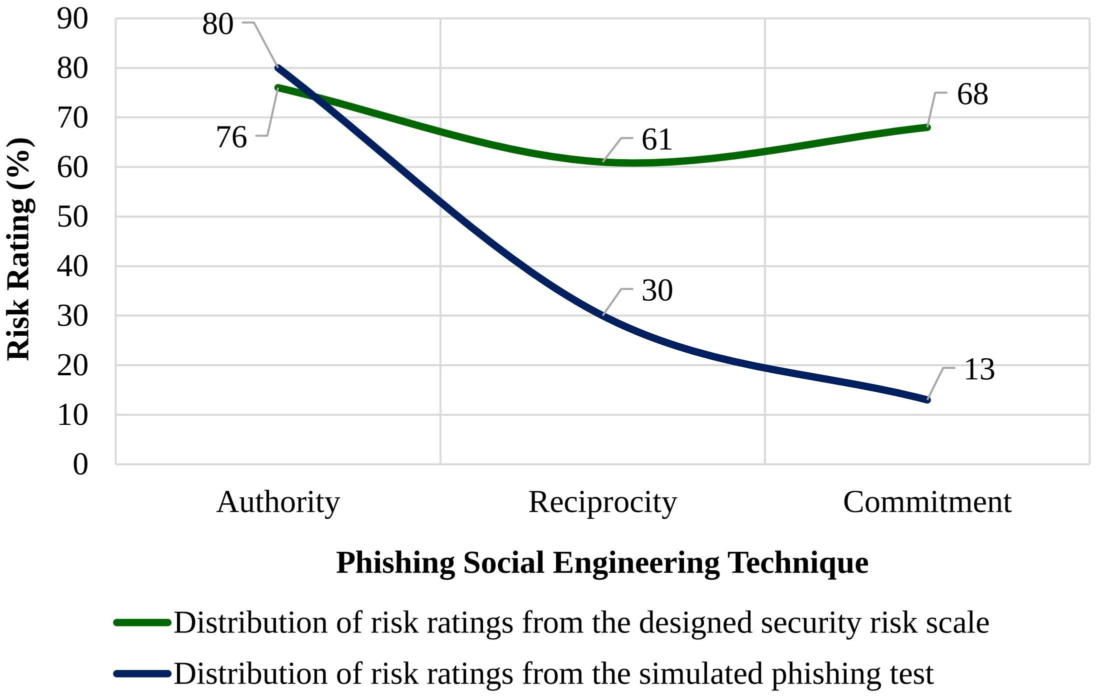


Figure 4. 32: Comparison of the distributions of risk ratings with respect to the sampled social engineering techniques.

Source: Field data and Phishing test results

From the plot in Figure 4.32 above it can be seen that the two distributions are similar. We may therefore reject the null hypothesis and accept the alternative hypothesis. This means that there is a relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale.

Table 4.26 below shows a summary of the hypothesis test results for the specific objective of assessing the performance level of the proposed security risk scale against results of a phishing attack performed at a bank.

Table 4. 26: Hypothesis Test Results of Specific Objective 3

Specific Objective	**Null Hypothesis**	**Result**
Specific Objective 3: To assess the performance level of the proposed security risk scale against results of a phishing attack performed at a bank.	There is no relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale.	The nature of the distribution of risk ratings from the designed security risk scale and the nature of the distribution of risk ratings from the simulated phishing test, for the authority, reciprocity, and commitment social engineering techniques are similar. We may therefore reject the null hypothesis and accept the alternative hypothesis. This means that there is a relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale.

Source: Field data and Phishing test results (2022)

The phishing test using the authority technique was the first test to be conducted in the series of phishing tests and had the least error (5.263%). The error was found to increase significantly in the second test, i.e., the reciprocity technique (50.820%). The test with the largest error was the final test, i.e., the commitment technique (80.882%). The increase in error through subsequent phishing tests can be justified by users gaining awareness and suspicion of the possibility of phishing attempts following the significant success of the first phishing test.

Table 4.27 below shows a comparison of the risk ratings derived from the security risk scale and that from the phishing test. The error and accuracy are tabulated as well. The calculations for obtaining the error and accuracy are shown below.

The Error and Accuracy percentage are evaluated using equations 1 and 2 from chapter 3.12 - Performance Evaluation Methodology.

$$\text{Accuracy} = 100\% - \text{Error Rate}$$

$$\text{Error Rate} = \frac{|\text{Phishing Simulation Test Value - Security Risk Scale Value}|}{\text{Security Risk Scale Value}} \times 100\%$$

$$\text{Authority Technique Error Rate} = \frac{|80 - 76|}{76} \times 100\% = 5.263\%$$

$$\text{Authority Technique Accuracy} = 100\% - 5.263\% = 94.737\%$$

Reciprocity Technique Error Rate = $\frac{|30 - 61|}{61}$ ×100% = 50.820%

Reciprocity Technique Accuracy = 100% - 50.820% = 49.180%

Commitment Technique Error Rate = $\frac{|13 - 68|}{68}$ ×100% = 80.882%

Commitment Technique Accuracy = 100% - 80.882% = 19.118%

Table 4. 27: Performance measurement of the security risk scale

Phishing Technique	Probability of a subject interacting with a phishing email as per the designed security risk scale (%)	Percentage of users that interacted with the phishing email in the simulated phishing test (%)	Error (%)	Accuracy (%)
Authority	76	80	5.263	94.737
Reciprocity	61	30	31	69
Commitment	68	13	80.882	19.118

Source: Field data and phishing test results (2022)

4.5 Discussion

Risk measurement of emails is essential to prevent or reduce the magnitude of successful phishing attacks. Our findings have added on to the user-behavior-based risk rating technique which measures the likelihood a user is not vigilant enough to avoid the phishing attack. Techniques such as the Tessian (2021) Human Layer Rik Hub, KnowBe4 (2022) Virtual Risk Officer, Yang et al.'s (2022) multidimensional phishing susceptibility prediction model, Affinity IT Security Services' (2019) Phishing Risk scale formulate their risk scale by rating the behavioral actions the user performs when subjected to a phishing email. However, the consideration of the risk posed by the email content that the user is subjected to is addressed by our study. Furthermore, since phishing mainly depends on exploiting the human emotional factor our scale is applicable when finding out the risk of manipulating a specific emotion that the user has.

In a changing world, some techniques are used more than others that change the impact of the method used to attack the user, and so as the risk. Our study has evaluated which emotions of an individual, out of the various emotions attacked by phishers, poses the greatest risk of successful exploitation. A security risk scale has been developed to enhance phishing detection in mail systems. The factors affecting the effectiveness of phishing attempts through mail messages have been identified, a security risk scale based on the relationships between phishing variables and the security risk has been designed, and performance level of the proposed security risk scale against results of a phishing attack performed at a bank has been assessed. This study has facilitated the measurement of the risk associated with a phishing email based on the actual content that is written in the email.

Human beings are considered as the weakest link to security, and social engineering targets the human factor, i.e., the capability to exhibit emotions. This risk scale complements studies by Salahdine and Kaabouch (2019) who found that awareness and security policies are an efficient defense against social engineering. (Salahdine & Kaabouch, 2019) by providing phishing security risk information to normal email users, organizations, security solution vendors, and anyone interested. Moreover, as Lyimo and Kamugisha (2022) found that the employees do not have sufficient knowledge on the approaches to keep themselves secure from internet threats.

By rating the different emotions exploited by phishers using social engineering techniques, an individual may gain caution when facing a phishing email. Awareness on the trending phishing risks may reduce possible exploitation and loss of sensitive data. As Oreku (2020) pointed out a key challenge in Tanzania being the construction of a nation that realizes the significance of information security, organizations may in turn allocate adequate resources and budget to counter the phishing email content risk, with a consideration of criticality.

Our findings align with Semlambo, Mfoi et al. (2022) who found that the prime factors influencing information system security were human factors, security policies, work conditions, and demographics. The demographic factors included the education level, work experience, and age. Our survey found a statistically significant difference between the groups in our demographic variable in affecting the risk factors. Work environment factors involved management support and organizational culture.

With regards to the observation of Lubua and Pretorius (2019) on the deficiency of viable security policies facing organizations in Tanzania, proper security governance and policies can be set in relation to the risk ratings derived from the security risk scale. Phishing risk mitigation strategies may take the evaluated severity measures into account to provide substantial controls.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The emotion that will result in significant user interaction when manipulated in a phishing email was determined by an experimental test. Data illustrating the rate users receive phishing emails and the probability of them interacting with them, was collected from 327 users, based on the Likert scale. Out of 10 social engineering techniques where emotions are triggered, a major cause of successful phishing attacks was found to be manipulation of curiosity, fear, authority, and empathy emotions. A security risk scale to enhance phishing detection has been developed consisting of critical, high, medium, and low severity levels of risk. Table 5.1 below tabulates a summary of conclusions drawn from the results of the tests performed on the hypotheses.

Table 5. 1: Summary of conclusions made for hypotheses

SN	Specific Objective	Null Hypothesis	Conclusion
1	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups of the phishing social engineering techniques in affecting the probability of a subject interacting with a phishing email.	We reject the null hypothesis and accept the alternative hypothesis. Therefore, there is a statistically significant difference between the groups of the phishing social engineering techniques in affecting the probability of a subject interacting with a phishing email.
2	*Specific Objective 2:* To design a security risk scale	There is no statistically significant difference between the	We reject the null hypothesis and accept the alternative hypothesis. Therefore, there

	based on the relationships between phishing variables and the security risk.	groups of the phishing social engineering techniques in affecting the frequency of a subject receiving a phishing email.	is a statistically significant difference between the groups of the phishing social engineering techniques in affecting the frequency of a subject receiving a phishing email.
3	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups in the demographic variable in affecting the probability of a subject interacting with a phishing email, for a moderating categorical variable of social engineering techniques.	We reject the null hypothesis and accept the alternative hypothesis. Therefore, a there is a statistically significant difference between the groups in the demographic variable in affecting the probability of a subject interacting with a phishing email, for a moderating categorical variable of social engineering techniques.
4	*Specific Objective 2:* To design a security risk scale based on the relationships between phishing variables and the security risk.	There is no statistically significant difference between the groups in the demographic variable in affecting the frequency of a subject receiving a phishing email, for a moderating categorical variable of social engineering techniques.	We reject the null hypothesis and accept the alternative hypothesis. Therefore, there is a statistically significant difference between the groups in the demographic variable in affecting the frequency of a subject receiving a phishing email, for a moderating categorical variable of social engineering techniques.
5	*Specific Objective 3:* To assess the performance level of the proposed security risk scale against results of a phishing attack performed at a bank.	There is no relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale.	We reject the null hypothesis and accept the alternative hypothesis. Therefore, there is a relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale.

5.2 Recommendations

There is a need of reinforcing organizational controls, systems, processes and skills on a country level. (Oreku, 2020) With regards to the extensive scope of information security, stronger efforts are needed in Tanzania to facilitate cybersecurity awareness programs on both the individual and national level. (Ndibwile et al., 2018) The national ICT policy needs to cater for securing online transactions. (Mlelwa, 2019) The government of Tanzania needs to reinforce cybersecurity and forensics to mitigate the challenges faced by digital transactions. (Kidunda & Pastory, 2022) Prosecutive measures are to be instilled by legislation to charge cyberterrorists for arranging and carrying out cyberterrorism. (Magalla & Mnyigumba, 2021) Commercial banks in Tanzania need to liaise with the government to perform substantial cybersecurity investments in information systems. Robust cybersecurity regulations and policies need to be enacted by the government to enable protection of banks and the money entrusted by customers. (James & Mbogoro, 2020) Small businesses in Tanzania require their organizational environment to be assessed, organizational data and customer information backed up, strategies for detection and prevention to be well defined, organizational data and customer information to be protected, employees trained, and networks and electronic devices be secured. (Kayumbe & Michael, 2021) Key improvements are needed for the development of proper information systems security policies, procedures, and frameworks, along with the endorsement of security awareness and training programs. (Semlambo, Stanslaus, et al., 2022) Efforts have been made by the government to keep track of the usage of information technology but more action and intervention is required while still observing users freedom of use. (Malale & Christopher, 2022) Users or organizations with mail servers are recommended to train their staff on the use of this developed security risk scale and all its features in relation to phishing attacks triggered by emotions. This will assist in resolving the ever-growing security problem of susceptibility to phishing attacks by manipulation of emotions and social engineering attacks.

5.3 Suggestion for the Future Studies

An automated email phishing detection framework that is contextually aware of the risk posed by the content forged in the phishing email may be constructed to complement this study. A phisher or external threat actor targets the organization with email phishing attacks that are received by the organization's mail server as shown in step 1. The inbound emails from the mail server are directed to the artificial intelligence (AI) layer as shown in step 2. Text mining is performed using natural language processing models, after an initial pre-processing of the content in the emails, to create a vectorized form of the words. Preprocessing involves sentence segmentation, tokenization, stemming, lemmatization, removal of noise, i.e., stop words ('a', 'the', 'and', etc.), special characters, and punctuation marks, dependency parsing, and part of speech (PoS) tagging. The corpus contains datasets to be used in the model's training algorithms. Step 3 feeds datasets into the text mining block. The corpus is connected to available public, paid, or premium cloud services to receive larger quality, and new datasets. Machine learning algorithms are used to classify the vectorized words and detect if the content in the email is a phishing or not, with the output at step 4. Detected phishing emails are taken in for sentiment and emotion analysis in step 5. Once the emotion is detected from the contextual data it increments its respective emotion counter in the frequency count matrix in step 6. The information regarding the emotion used by the attacker and its count are stored in the repository in step 7. At this point, the frequency of a user receiving a phishing email targeting a specific emotion is obtained from the live environment or real-world. The detected emotion is fed to the phishing attack layer in step 8. In step 9, a phishing email campaign is orchestrated in the context of the emotion detected in step 7. A simulated phishing attack is devised and staged for launch in step 9. The organization users receive test phishing emails in step 10 to determine the probability of a user interacting with a phishing email triggering the emotion detected in step 6. The interaction of the organization users with the orchestrated phishing email that triggers the detected emotion in step 6 is recorded into results in step 11. The results portraying the impact of the phishing email, or its probability of exploitation are stored into the repository in step 12. In step 13, the security risk scale is derived from the repository data of multiple emotions. The mean frequency of a user receiving a phishing email targeting a specific emotion is plotted against the mean probability of a user interacting with a phishing email triggering the emotion detected, on a risk matrix. The email phishing detection framework is shown in Figure 5.1.

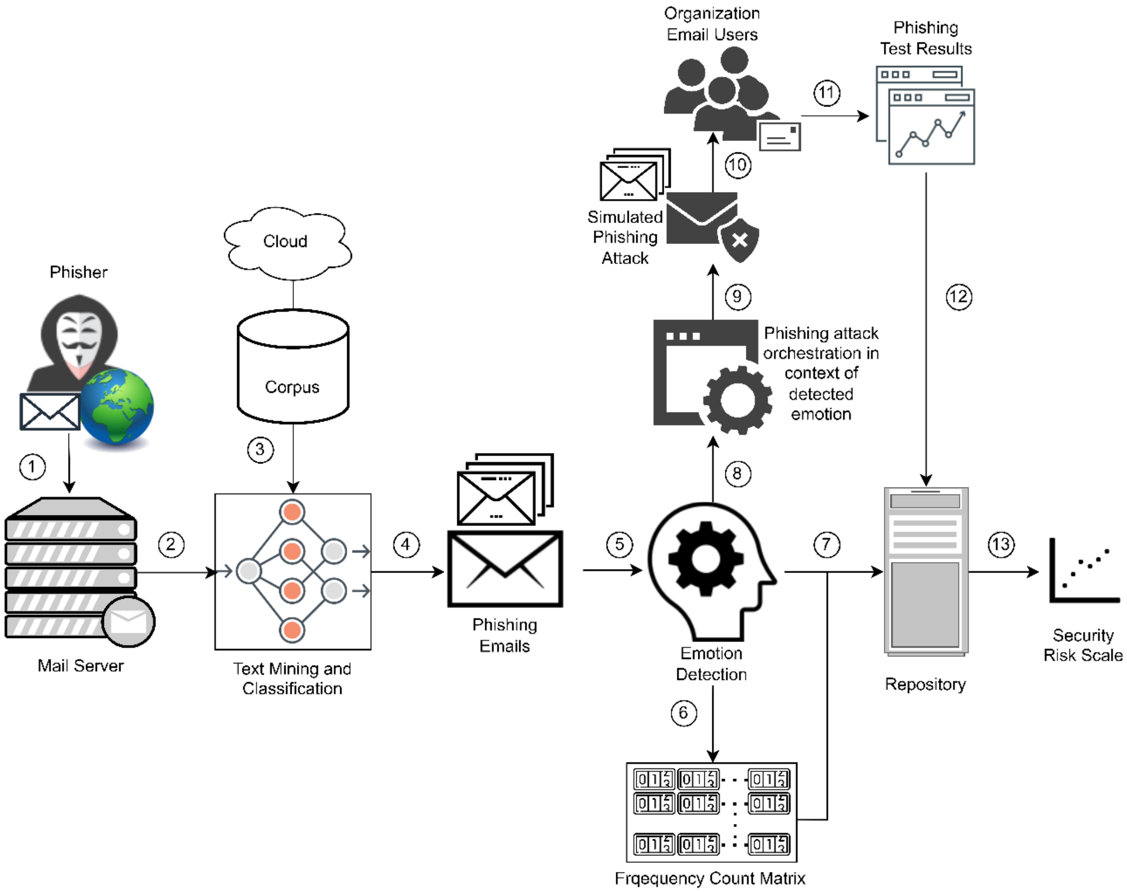


Figure 5. 1: Email Phishing Detection Framework

REFERENCES

Aaron, G., Chapin, L., Piscitello, D., & Strutt, C. (2022). Phishing Landscape 2022 An Annual Study of the Scope and Distribution of Phishing. In *Interisle Consulting Group, LLC* (Issue July). https://interisle.net/PhishingLandscape2022.pdf

Abass, I. A. M. (2018). Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security*, *09*(04), 257–264. https://doi.org/10.4236/jis.2018.94018

Abdelaziz, O., Deb, S., Hodhod, R., & Ray, L. (2021). *A Novel Phishing Email Detection Algorithm based on Multinomial Naive Bayes Classifier and Natural Language Processing*. 69–73. https://doi.org/10.5220/0010412600690073

Abnormal Security. (2022a). *H2 2022 Email Threat Report: Threat Actors Impersonate 265 Different Brands in Credential Phishing Attacks*. https://cdn2.assets-servd.host/gifted-zorilla/production/files/H2-2022-Email-Threat-Report.pdf

Abnormal Security. (2022b). *H2 2022 Email Threat Report: Threat Actors Impersonate 265 Different Brands in Credential Phishing Attacks*.

Affinity IT Security Services. (2019). *Measuring Phishing Risk*. https://affinity-it-security.com/measuring-phishing-risk/

Ahmed, D. S., Allah, H. A. A. A., & Abbas, I. (2021). Effective Phishing Emails Detection Method. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(14), 4898–4904. https://turcomat.org/index.php/turkbilmat/article/view/11456

Akinyetun, T. S. (2021). Poverty, Cybercrime and National Security in Nigeria. *Journal* *of Contemporary Sociological Issues*, *1*(2), 1–23. https://doi.org/10.19184/csi.v1i2.24188

Al-Ababneh, M. M. (2020). Linking Ontology, Epistemology and Research Methodology. *Science & Philosophy*, *8*(1), 75–91. https://doi.org/10.23756/sp.v8i1.500

Andrade, C. (2019). The P Value and Statistical Significance: Misunderstandings, Explanations, Challenges, and Alternatives. *Indian Journal of Psychological Medicine*, *41*(3), 210–215. https://doi.org/10.4103/IJPSYM.IJPSYM

Anti-Phishing Working Group. (2022). *Phishing Activity Trends Report, 2nd Quarter 2022* (Issue June). https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf?_ga=2.58552874.145886931.1665636510-990710295.1665486458&_gl=1*1d6jwtf*_ga*OTkwNzEwMjk1LjE2NjU0ODY0NTg.*_ga_55RF0RHXSR*MTY2NTYzNjUxMC4yLjAuMTY2NTYzNjUxMC4wLjAuMA..

APWG. (2022). Phishing Activity Trends Report, 4th Quarter 2022. *Anti-Phishing Working Group, December*.

Aslam, M., & Sattam, M. (2020). Analyzing alloy melting points data using a new Mann-Whitney test under indeterminacy. *Journal of King Saud University - Science*, *32*(6), 2831–2834. https://doi.org/10.1016/j.jksus.2020.07.005

Bagui, S., Nandi, D., Bagui, S., & White, R. J. (2021). Machine Learning and Deep Learning for Phishing Email Classification using One-Hot Encoding. *Journal of Computer Science*, *17*(7), 610–623. https://doi.org/10.3844/jcssp.2021.610.623

Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). Cyber Security in Financial Sector Development: Challenges and potential solutions for financial inclusion. *Consultative Group to Assist the Poor (CGAP), November*, 1–14.

Benard, M. C., Charles, M., Charo, J. S., & Mvurya, M. (2021). Cyber-Crimes Issues on Social Media Usage Among Higher Learning Institutions Students in Dar ES Salaam Region , Tanzania. *International Journal of Scientific Research in Science, Engineering and Technology*, *8*(4), 138–148.

Bishel, E. (2022). *Africa , China , and the Development of Digital Infrastructure Governance : A Case Study of Ghana and Tanzania*.

Bolster. (2022). *2022 State of Phishing and Online Fraud Report*. https://boost.bolster.ai/rs/540-RFH-299/images/2022_PhishingandFraudReport.pdf

Bountakas, P., Koutroumpouchos, K., & Xenakis, C. (2021). A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3465481.3469205

Bountakas, P., & Xenakis, C. (2023). HELPHED: Hybrid Ensemble Learning PHishing Email Detection. *Journal of Network and Computer Applications*, *210*. https://doi.org/10.1016/j.jnca.2022.103545

Bukht, T. F. N., Raza, M. A., Awan, J. H., & Ahmad, R. (2020). Analyzing cyber-attacks targeted on the Banks of Pakistan and their Solutions. *International Journal of Computer Science and Network Security*, *20*(February), 31–38.

Bullee, J., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information & Computer Security*, *25*(5). https://doi.org/10.1108/ICS-03-2017-0009

Călin, M. F., & Tuşa, E. (2023). Using t-Student and U-Mann-Whitney tests to identify differences in the study of the impact of the Covid 19 pandemic in online education in schools. *Analele Stiintifice Ale Universitatii Ovidius Constanta, Seria Matematica*, *31*(2), 39–59. https://doi.org/10.2478/auom-2023-0018

Castillo, E., Dhaduvai, S., Liu, P., Thakur, K.-S., Dalton, A., & Strzalkowski, T. (2020). Email Threat Detection Using Distinct Neural Network Approaches. *Proceedings for the First International Workshop on Social Threats in Online Conversations: Understanding and Management*, *May*, 48–55. https://www.aclweb.org/anthology/2020.stoc-1.8

Chanda, J. (2020). *Assessment of Electronic Banking Services Adoption Towards Customer Use in Tanzania: A Case of Some Selected Commercial Banks*.

Chowdhury, T., Sivaraman, R., Mittal, A., Engels, D. W., & Kommanapalli, H. (2022). Phishing Detection Using Natural Language Processing and Machine Learning. *SMU Data Science Review, 6*(2). https://doi.org/10.1109/ICICT55905.2022.00038

Cofense. (2022). *2022 Annual State of Phishing Report: It's Always a Phish*. https://cofense.com/wp-content/uploads/2022/03/2022-AnnualReport-Final-Web.pdf?utm_source=email&utm_medium=marketing&utm_campaign=annual-report-ty&mkt_tok=NDA0LUpIVS02MTIAAAGHZo9GYERDsmpmKyR4w62cvdakGOatjvYJQo-PoNnZZahjD4lkmsJBltfFkXcmDlL22cJzX-BmfDM8aB17

Cross, C. (2021). Dissent as cybercrime: social media, security and development in Tanzania. *Journal of Eastern African Studies*, *15*(3), 442–463. https://doi.org/10.1080/17531055.2021.1952797

Cuemath. (2023). *Accuracy Formula*.

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-Methods Research: A Discussion on its Types, Challenges, and Criticisms. *Journal of Practical Studies in Education*, *2*(2), 25–36. https://doi.org/10.46809/jpse.v2i2.20

Denny, E., & Weckesser, A. (2022). How to do qualitative research?: Qualitative research methods. *BJOG: An International Journal of Obstetrics and Gynaecology*, *129*(7), 1166–1167. https://doi.org/10.1111/1471-0528.17150

Di Leo, G., & Sardanelli, F. (2020). Statistical significance: p value, 0.05 threshold, and applications to radiomics—reasons for a conservative approach. *European Radiology Experimental*, *4*(1). https://doi.org/10.1186/s41747-020-0145-y

EasyDMARC. (2022a). *Phishing Statistics: EasyDMARC Report - From January to June 2022* (Issue June). https://assets.easydmarc.com/static/phishing-statistics-2022-07-06.pdf

EasyDMARC. (2022b). *Phishing Statistics: EasyDMARC Report - From January to June 2022* (Issue June).

Euphemia, C., Njoku, O., Okolie, A., Nnenna, J., & Onyekachi, A. (2019). Level of Awareness of Cybersecurity for Business Protection in Nigeria. *International Journal of Innovative Science and Research Technology*, *4*(12). www.ijisrt.com761

Fang, Y., Zhang, C., Huang, C., Liu, L., & Yang, Y. (2019). Phishing Email Detection

Using Improved RCNN Model With Multilevel Vectors and Attention Mechanism. *IEEE Access*, *7*, 56329–56340. https://doi.org/10.1109/ACCESS.2019.2913705

Fick, N., Miscik, J., & Segal, A. (2022). *Confronting Reality in Cyberspace Foreign Policy for a Fragmented Internet*. *80*.

FireEye. (2018). Spear-Phishing Attacks: Why they are successful and how to stop them. *White Paper*.

Franchina, L., Ferracci, S., & Palmaro, F. (2021). Detecting phishing e-mails using text mining and features analysis. *CEUR Workshop Proceedings*, *2940*, 106–119.

Ghelerter, D. A., Wilson, J. E., Welch, N. L., & Rusk, J.-D. (2022). Cybercrime in the Developing World. *KSU Conference on Cybersecurity Education, Research and Practice*.

Gupta, B. B., Nalin, A. G. A., & Psannis, K. (2018). Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. *Telecommunication Systems*. https://doi.org/10.22363/2313-2272-2018-18-1-117-130

Halgaš, L., Agrafiotis, I., & Nurse, J. R. C. (2020). *Catching the Phish: Detecting Phishing Attacks Using Recurrent Neural Networks (RNNs)* (pp. 219–233). https://doi.org/10.1007/978-3-030-39303-8_17

IBM Security. (2022). IBM: X-Force Threat Intelligence Index. In *Computer Fraud & Security* (Vol. 2022, Issue 3). https://doi.org/10.12968/s1361-3723(22)70561-1

Interpol. (2021). African Cyberthreat Assessment Report: Interpol’s Key Insight into Cybercrime in Africa. In *Interpol* (Issue October). https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessme nt_ENGLISH.pdf

ITU. (2020). Global Cybersecurity Index (2020). *ITU Publications*, 78.

Jajoo, A. (2017). *Term Paper on Morris Worm*. *December*, 1–18.

James, J., & Mbogoro, F. (2020). *Adoption of cash deposits through Automated Teller Machines (ATMs) by banks in Tanzania : A case of selected commercial banks in Dar es Salaam*. *24*(1), 17.

K. Mbura, O., & Sekela, M. (2020). Promotion Strategies and Performance of Commercial Banks: Evidence from CRDB Bank Plc in Tanzania. *Tanzanian Economic Review*, *10*(1), 163–182. https://doi.org/10.56279/ter.v10i1.61

Kaliyadan, F., & Kulkarni, V. (2019). Types of Variables, Descriptive Statistics, and Sample Size. *Indian Dermatology Online Journal*, *10*(1), 82–86. https://doi.org/10.4103/idoj.IDOJ

Kandel, B. (2020). Qualitative versus Quantitative Research. *Marsyangdi Journal*, *1*(September), 1–5.

Karamagi, R. (2021). A Review of Factors Affecting the Effectiveness of Phishing. *Computer and Information Science*, *15*(1), 20. https://doi.org/10.5539/cis.v15n1p20

Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K., & Alazab, M. (2019). A Comprehensive Survey for Intelligent Spam Email Detection. *IEEE Access*, *7*(December), 168261–168295. https://doi.org/10.1109/ACCESS.2019.2954791

Kavishe, A. M. (2021). *Exploring the Experience of Cyberstalking among Female Students in Tanzanian Universities : A Case Study of the University of Dar es Salaam by A thesis submitted in fulfilment of the requirements of the award of the degree of*

Doctor of Philosophy (PhD) (Issue September). https://ukzn-dspace.ukzn.ac.za/handle/10413/20010

Kaya, G. K. (2018). Good Risk Assessment Practice in Hospitals. *Cambridge University*, *January*.

Kayumbe, E., & Michael, L. (2021). Cyber threats: Can Small Businesses in Tanzania outsmart Cybercriminals. *International Research Journal of Advanced Engineering and Science*, *6*(1), 141–144.

Kidunda, E., & Pastory, D. (2022). Examination of Factors Influencing the Intention To Adopt Cryptocurrencies in Tanzania. *Business Education Journal*, *11*(1), 1–11. https://doi.org/10.54156/cbe.bej.11.1.324

Kim, K. S. (2022). Methodology of Non-probability Sampling in Survey Research. *American Journal of Biomedical Science & Research*, *15*(6), 616–618. https://doi.org/10.34297/ajbsr.2022.15.002166

KnowBe4®. (2022a). *Phishing by Industry Benchmarking Report*. https://www.knowbe4.com/hubfs/2022-Phishing-by-Industry-Benchmarking-Report.pdf?hsCtaTracking=5545cbd3-4d37-4ec2-a812-0b2830feefbb%7C753ae012-a008-46ca-ade5-5035e74f6667

KnowBe4®. (2022b). *Virtual Risk Officer (VRO) and Risk Score Guide*. https://support.knowbe4.com/hc/en-us/articles/360001358728-Virtual-Risk-Officer-VRO-and-Risk-Score-Guide

Korkmaz, M., Kocyigit, E., Sahingoz, O. K., & Diri, B. (2022). A Hybrid Phishing Detection System Using Deep Learning-based URL and Content Analysis.

Elektronika Ir Elektrotechnika, *28*(5), 80–89. https://doi.org/10.5755/j02.eie.31197

Kshetri, N. (2019a). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Kshetri, N. (2019b). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Kumar, R., & Dey, S. (2019). STUDY OF COMPUTER VIRUS TRANSMISSION. *International Journal of Research and Analytical Reviews*, *6*(1), 542–549.

Kundy, E. D., & Lyimo, B. J. (2019). Cyber Security Threats in Higher Learning Institutions in Tanzania, A Case of University of Arusha and Tumaini University Makumira. *Olva Academy-School of Researchers*, *2*(3).

Lee, Y., Saxe, J., & Harang, R. (2020). *CATBERT: Context-Aware Tiny BERT for Detecting Social Engineering Emails*. http://arxiv.org/abs/2010.03484

LexisNexis® Emailage®. (2022). *Emailage Email Risk Score Identity and Fraud Protection | LexisNexis Risk Solutions*. https://risk.lexisnexis.com/global/en/products/lexisnexis-emailage

Lissah, J., Kirobo, A., & Govella, M. M. (2022). Adoption of Cashless Economy in the World: A Review. *IOSR Journal of Economics and Finance*, *13*(2), 37–48. https://doi.org/10.9790/5933-1302083748

Loi, H., & Olmsted, A. (2017). Low-cost Detection of Backdoor Malware. *12th International Conference for Internet Technology and Secured Transactions*

(ICITST), December.

Lovell, D. P. (2020). Null hypothesis significance testing and effect sizes: can we 'effect' everything … or … anything? *Current Opinion in Pharmacology*, *51*, 68–77. https://doi.org/https://doi.org/10.1016/j.coph.2019.12.001

Lu, L. (2019). Detect Reverse Shell Attack. *TriagingX*.

Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security policy framework and procedural compliance in public organisations. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, *July*, 1847–1856.

Lyimo, B. J. (2022). Information Security Vulnerabilities and Tanzania Ministry of Education. *Olva Academy – School of Researchers*, *4*(1), 96–104.

Lyimo, B. J., & Kamugisha, A. (2022). The Analysis of Internet Security Awareness of Employees in Tanzania. *Olva Academy-School of Researchers*, *4*(1), 96–102. https://www.researchgate.net/publication/359203939

Magalla, A., & Mnyigumba, I. V. (2021). Legislations on Cyber Terrorism in Tanzania: A Reality Or Fairytalr? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3833598

Magufuli, J. J. (2019). *Efficacy of communications regulation in the prevention of content cybercrimes in Tanzania: A case of Dar-es-salaam city*. 90–93. http://repository.udom.ac.tz

Malale, E., & Christopher, T. (2022). The Ethical Relevance of Technology and Its Impact and Development, Particularly in Tanzania. *International Journal of Innovative Research and Development*, *11*(6), 10–15.

https://doi.org/10.24940/ijird/2022/v11/i6/jun22027

Malekela, M.-S. A. (2022). The Efficacy of Legal Framework on Data Protection in Tanzania Mainland. In *Research Report*.

Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J. C. (2019). Understanding Man-in-the-middle-attack through Survey of Literature. *Indonesian Journal of Computing, Engineering and Design (IJoCED)*, *1*(1), 44. https://doi.org/10.35806/ijoced.v1i1.36

Mambile, C., & Mbogoro, P. E. (2020). Cybercrimes awareness, cyber laws and its practice in public sector Tanzania. *International Journal of Advanced Technology and Engineering Exploration*, *7*(68), 119–126. https://doi.org/10.19101/IJATEE.2020.762051

Mambina, I. S., Ndibwile, J. D., & Michael, K. F. (2022). Classifying Swahili Smishing Attacks for Mobile Money Users: A Machine-Learning Approach. *IEEE Access*, *10*(June), 83061–83074. https://doi.org/10.1109/ACCESS.2022.3196464

Mansour, Y. M., & A. Alenizi, M. (2020). Enhanced Classification Method for Phishing Emails Detection. *Journal of Information Security and Cybercrimes Research*, *3*(1), 58–63. https://doi.org/10.26735/ygmy6142

Maseno, E. M. (2017). VISHING ATTACK DETECTION MODEL FOR MOBILE USERS. *KCA University*.

Mlelwa, K. L. (2019). A Novel Framework for Secure E-Commerce Transactions. *International Journal of Cyber-Security and Digital Forensics*, *6*(2), 92–100. https://doi.org/10.17781/p002273

Mlyatu, M. M., & Sanga, C. (2023). Secure Web Application Technologies

Implementation through Hardening Security Headers Using Automated Threat Modelling Techniques. *Journal of Information Security*, *14*, 1–15. https://doi.org/10.4236/jis.2023.141001

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business & Social Science*, *11*(4), 384–396.

Mpofu, F. Y., & Mhlanga, D. (2022). Digital Financial Inclusion, Digital Financial Services Tax and Financial Inclusion in the Fourth Industrial Revolution Era in Africa. *Economies, 10*(8). https://doi.org/10.3390/economies10080184

Msaki, L. (2019). *Assessment of the Challenges on E-Commerce Engagement: The Case of Selected Traditional Retailers*.

Mshangi, M. (2020). *Enhancing Security of Information Systems in Tanzania: The Case of Education Sector*. The Open University of Tanzania.

Mswahili, A. (2022). Factors for Acceptance and Use of Mobile Money Interoperability Services. *The Journal of Informatics, 2*(1), 1–21. https://journals.iaa.ac.tz/index.php/tji/article/view/45

Mtakati, B., & Sengati, F. (2021a). Cybersecurity Posture of Higher Learning Institutions in Tanzania. *The Journal of Informatics: 2714-1993, 1*(1), 1–12. https://journals.iaa.ac.tz/index.php/tji/article/view/1%0Ahttps://journals.iaa.ac.tz/index.php/tji/article/download/1/16

Mtakati, B., & Sengati, F. (2021b). Cybersecurity Posture of Higher Learning Institutions in Tanzania. *The Journal of Informatics: 2714-1993*, *1*(1), 1–12.

Mulisa, F. (2022). Sampling techniques involving human subjects: Applications, pitfalls, and suggestions for further studies. *International Journal of Academic Research in Education*, *8*(1), 74–83. https://doi.org/10.17985/ijare.1225214

Muralidharan, T., & Nissim, N. (2023). Improving malicious email detection through novel designated deep-learning architectures utilizing entire email. *Neural Networks*, *157*, 257–279. https://doi.org/10.1016/j.neunet.2022.09.002

Mwabukojo, E. (2020). Technology Transfer Strategy : A Neglected Approach in Tanzania. *Munich Personal RePEc Archive*, *100619*, 59. https://mpra.ub.uni-muenchen.de/100619/

Mwita, K. M. (2022). *Research in Business & Social Science Factors to consider when choosing data collection methods*. *11*(5), 532–538. https://www.ssbfnet.com/ojs/index.php/ijrbs%0AFactors

Nadim, M., Antonio, S., Lee, W., City, N. Y., Akopian, D., & Antonio, S. (2021). *Characteristic Features of the Kernel - level Rootkit for Learning - based Detection Model Training*. 1–7.

Ndibwile, J. D. (2020). *Validation Agents and Persuasive Designs for Phishing Detection and Update Compliance on Smartphones* (Issue January). https://doi.org/10.13140/RG.2.2.26035.37929

Ndibwile, J. D., Luhanga, E. T., Fall, D., & Kadobayashi, Y. (2019). A demographic perspective of smartphone security and its redesigned notifications. *Journal of Information Processing*, *27*, 773–786. https://doi.org/10.2197/ipsjjip.27.773

Ndibwile, J. D., Luhanga, E. T., Fall, D., Miyamoto, D., & Kadobayashi, Y. (2018). A comparative study of smartphone-user security perception and preference towards redesigned security notifications. *ACM International Conference Proceeding Series*, *December*, 150–155. https://doi.org/10.1145/3283458.3283486

Niedoba, T., Surowiak, A., Hassanzadeh, A., & Khoshdast, H. (2023). Evaluation of the Effects of Coal Jigging by Means of Kruskal–Wallis and Friedman Tests. *Energies*, *16*(4), 1–17. https://doi.org/10.3390/en16041600

Noah, N., Tayachew, A., Ryan, S., & Das, S. (2022). PhisherCop: Developing an NLP-Based Automated Tool for Phishing Detection. *SAGE Journals*. https://doi.org/10.2139/ssrn.4140375

Ntigwigwa, A. N. (2019). *Factors that contribute to Cybercrime in Mobile Money Services in Tanzania: A Case of Kibaha Town*.

Nuru, A. S. (2020). *Factors Influencing the Adoptation of Mobile Banking among the Bank Customers in Tanzania: A Case Study of KCB Bank*. 1–71.

O’Loughlin, E. (2021). *How To... Perform a Kruskal-Wallis Test in SPSS*. https://www.youtube.com/watch?v=W6110_EGTyY

Okoli, C. (2021). Inductive, Abductive and Deductive Theorizing. *SSRN Electronic Journal*, *July*. https://doi.org/10.2139/ssrn.3774317

Olayemi, O. (2019). Text Analysis and Machine Learning Approach to Phished Email Detection. *International Journal of Computer Applications*, *182*(36), 11–16. https://doi.org/10.5120/ijca2019918354

Olivia, O. E. (2022). Examining the Effect of the Elevated Rate of Cybercrime on the

Growth and Sustainable development of Nigeria's Economy. *Nau.Jcpl*, *9*(1), 2022.

Omar, M. (2021). *How to do Friedman's ANOVA test in SPSS*. https://www.youtube.com/watch?v=vorDRJjkgo8

Oreku, G. S. (2020). A Rule-based Approach for Resolving Cybercrime in Financial Institutions : The Tanzania case. *Huria Journal*, *27*(March), 93–114.

Pallangyo, H. J. (2022). Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services. *Tanzania Journal of Engineering and Technology*, *41*(2), 189–204.

Panga, R. C. T., Marwa, J., & Ndibwile, J. D. (2022). A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania. *Journal of Cybersecurity and Privacy*, *2*(3), 466–489. https://doi.org/10.3390/jcp2030024

Pantserev, K. A. (2022). Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity. *Vestnik RUDN. International Relations*, *22*(2), 288–302. https://doi.org/10.22363/2313-0660-2022-22-2-288-302

Parekh, D. H., Adhvaryu, N., & Dahiya, V. (2020). *Keystroke Logging : Integrating Natural Language Processing Technique to Analyze Log Data*. *3*, 2028–2033. https://doi.org/10.35940/ijitee.C8817.019320

PhishLabs. (2022). *Quarterly Threat Trends & Intelligence Report* (Issue May). https://info.phishlabs.com/hubfs/Agari PhishLabs_QTTI Report - May 2022.pdf

Ponemon Institute, & IBM Security. (2022a). *Cost of a Data Breach Report 2022*.

https://www.ibm.com/downloads/cas/3R8N1DZJ

Ponemon Institute, & IBM Security. (2022b). *Cost of a Data Breach Report 2022*.

Proofpoint. (2022). *2022 State of the Phish: An In-Depth Exploration of User Awareness, Vulnerability and Resilience*. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-uk-tr-state-of-the-phish-2022.pdf

Rosenthal, M. (2021). Must-Know Phishing Statistics: Updated 2021. *Tessian*. https://www.tessian.com/blog/phishing-statistics-2020/

Salahdine, F., El Mrabet, Z., & Kaabouch, N. (2021). Phishing Attacks Detection: A Machine Learning-Based Approach. *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 0250–0255. https://doi.org/10.1109/UEMCON53757.2021.9666627

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4). https://doi.org/10.3390/FI11040089

Salerno, J. P., Doan, L., Sayer, L. C., Drotning, K. J., Rinderknecht, R. G., & Fish, J. N. (2021). Changes in Mental Health and Well-Being Are Associated With Living Arrangements With Parents During COVID-19 Among Sexual Minority Young Persons in the U.S. *Psychology of Sexual Orientation and Gender Diversity*, *10*(1), 150–156. https://doi.org/10.1037/sgd0000520

Salim, A. M. (2022). Assessment of Mobile Money Transaction Frauds and Consequences Confronting Zanzibar Telecom Service Providers. *Asian Journal of Economics, Business and Accounting*, *20*(July), 16–31. https://doi.org/10.9734/ajeba/2022/v22i2030671

Saxena, S., Shrivastava, A., & Birchha, V. (2019). A Data Mining approach to Deal with Phishing URL Classification Problem. *International Journal of Computer Applications*, *178*(41), 44–49. https://doi.org/10.5120/ijca2019919319

Sedgwick, P. M., Hammer, A., Kesmodel, U. S., & Pedersen, L. H. (2022). Current controversies: Null hypothesis significance testing. *Acta Obstetricia et Gynecologica Scandinavica*, *101*(6), 624–627. https://doi.org/10.1111/aogs.14366

Semlambo, A. A., Mfoi, D. M., & Sangula, Y. (2022). Information Systems Security Threats and Vulnerabilities : A Case of the Institute of Accountancy Arusha (IAA). *Journal of Computer and Communications*, *10*(November), 29–43. https://doi.org/10.4236/jcc.2022.1011003

Semlambo, A. A., Stanslaus, N., & Munguyatosha, G. (2022). Factors Affecting the Security of Information Systems in Public Higher Learning Institutions in Tanzania. *The Information Technologist: An International Journal of Information and Communication Technology (ICT)*, *19*(2), 43–65.

Shaaban, S. Y., & Athumani, H. I. (2020). *Assessing Strategies to Create Cyber Security Awareness among Employees in National Microfinance Bank in Tanzania*. *VIII*(12), 250–259.

Shrestha, J. (2019). P-Value: a true test of significance in agricultural research. *Nepal Agricultural Research Council*, *1*(1), 1–5. https://doi.org/10.5281/zenodo.4030711

Somesha, M., & Pais, A. R. (2022). Classification of Phishing Email Using Word Embedding and Machine Learning Techniques. *Journal of Cyber Security and Mobility*, *11*(3), 279–320. https://doi.org/10.13052/jcsm2245-1439.1131

Soutis, E. (2020). *The Role of Government Laws and Regulations in the Adaption of E-Banking in Commercial Banks in Tanzania : A Case of CRDB Bank*.

Staller, K. M. (2021). Big enough? Sampling in qualitative inquiry. *Qualitative Social Work*, *20*(4), 897–904. https://doi.org/10.1177/14733250211024516

Steves, M., Greene, K., & Theofanos, M. (2020). Categorizing human phishing difficulty: a Phish Scale. *Journal of Cybersecurity*, *6*(1), 1–16. https://doi.org/10.1093/cybsec/tyaa009

Stratton, S. J. (2021). Population Research: Convenience Sampling Strategies. *Prehospital and Disaster Medicine*, *36*(4), 373–374. https://doi.org/10.1017/S1049023X21000649

TCRA. (2022). *Communication Statistics Quarter 3 - 2021/2022 March 2022* (Issue March 2022). https://www.tcra.go.tz/uploads/newsdocs/sw-1653821474-QUARTERLY COMMUNICATIONS STATISTICS - March 2022 Report.pdf

Tessian®. (2021). *Tessian Human Layer Risk Hub*. https://www.tessian.com/human-layer-risk-hub/?utm_medium=content&utm_source=pdf&utm_campaign=datasheet-risk-hub

TZ-CERT. (2022). *Tanzania Computer Emergency Response Team (TZ-CERT) Weekly Honeypot Reports*. https://www.tzcert.go.tz/resources-2/reports/

Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. E. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change*, *167*, 120743. https://doi.org/https://doi.org/10.1016/j.techfore.2021.120743

Valeros, V., & Garcia, S. (2020). Growth and Commoditization of Remote Access Trojans. *Proceedings - 5th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2020*, *September*, 454–462. https://doi.org/10.1109/EuroSPW51379.2020.00067

Van Vuuren, J. J., Leenen, L., & Pieterse, P. (2019). Framework for the development and implementation of a cybercrime strategy in Africa. *14th International Conference on Cyber Warfare and Security, ICCWS 2019*, *February*, 156–167.

Verizon. (2022). *2022 Data Breach Investigations Report*. https://doi.org/10.1142/9789811218712_0009

Verma, P., Goyal, A., & Gigras, Y. (2020). Email phishing: text classification using natural language processing. *Computer Science and Information Technologies*, *1*(1), 1–12. https://doi.org/10.11591/csit.v1i1.p1-12

Wambalaba, F., Musuva, P., Ouma, J., Makatiani, W., Kaimba, B., & Nicos, K. (2021). *Cyber Security Risk Minimization Best Practices - African Experiences*. *November*, 1–45.

Wikipedia. (2022). *Sutton's law*. https://en.wikipedia.org/wiki/Sutton%27s_law

Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International Management Review*, *15*(1), 45–55.

Yang, R., Zheng, K., Wu, B., Li, D., Wang, Z., & Wang, X. (2022). Predicting User Susceptibility to Phishing Based on Multidimensional Features. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/7058972

Yang, Z., Qiao, C., Kan, W., & Qiu, J. (2019). Phishing Email Detection Based on Hybrid

Features. *IOP Conference Series: Earth and Environmental Science*, *252*(4). https://doi.org/10.1088/1755-1315/252/4/042051

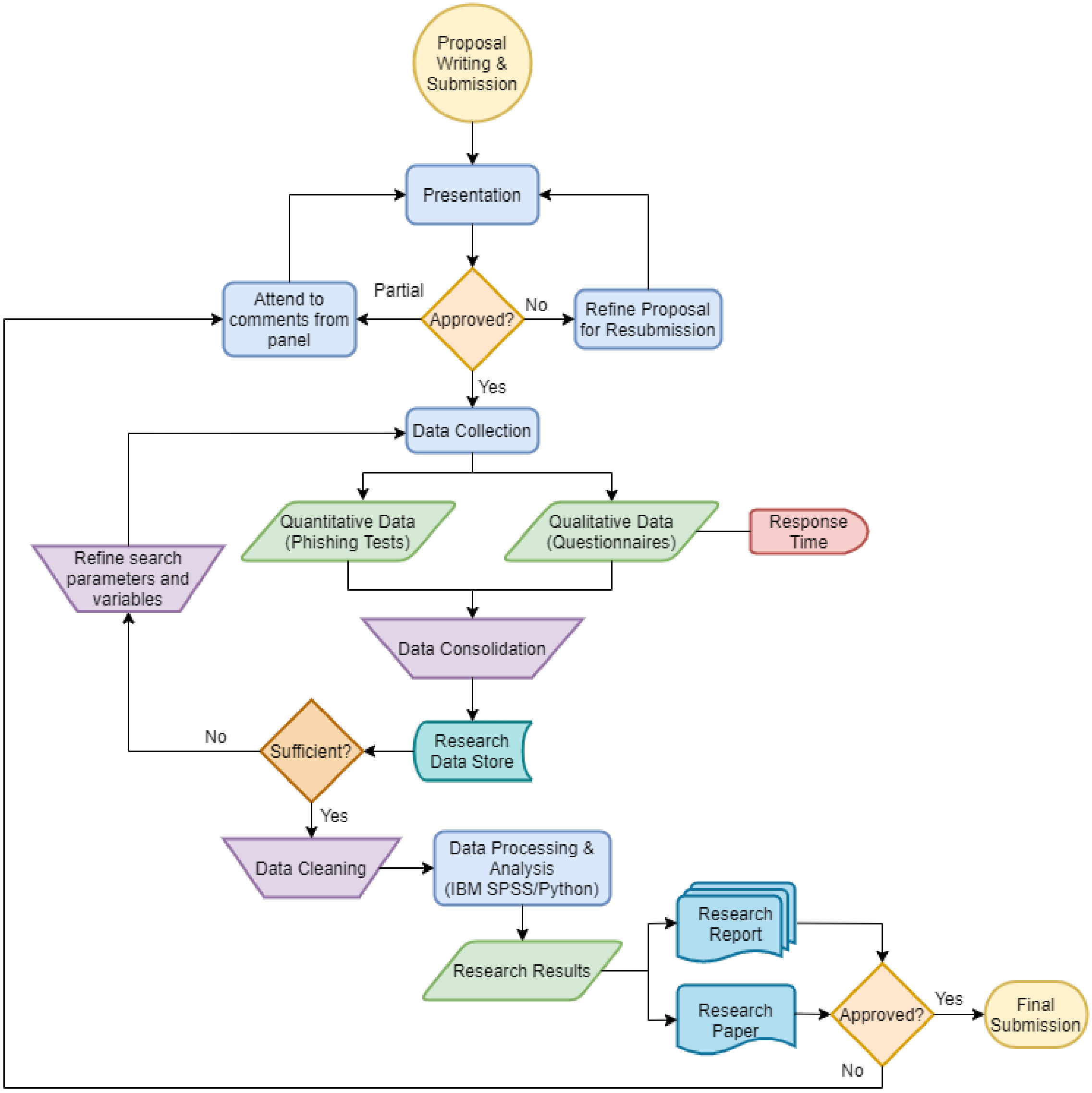
Zscaler. (2022). *2022 ThreatLabz Phishing Report*. https://www.zscaler.com/resources/industry-reports/2022-threatlabz-phishing-report.pdf

APPENDICES

Appendix I: Budget

SN	Particular	Qty.	Unit Price (TZS)	Total Price (TZS)
1.	Research Consultants – Data Collection support	1	800,000	800,000
2.	Hard Cover	4	25,000	100,000
	Total in TZS			900,000

Appendix II: Workplan


Proposal Writing & Submission
Presentation
Attend to comments from panel
Partial
Approved?
No
Refine Proposal for Resubmission
Yes
Data Collection
Quantitative Data (Phishing Tests)
Qualitative Data (Questionnaires)
Response Time
Refine search parameters and variables
Data Consolidation
Research Data Store
No
Sufficient?
Yes
Data Cleaning
Data Processing & Analysis (IBM SPSS/Python)
Research Report
Research Results
Research Paper
Approved?
Yes
Final Submission
No

Appendix III: Research Questionnaire

Demographic Information

What is your gender?

● Male

○ Female

What is your age range?

○ Below 20 years

○ 20 – 29 years

● 30 – 39 years

○ 40 – 49 years

○ 50 – 59 years

○ 60 years and above

What is your education level?

● Bachelor

○ Masters

○ Ph.D.

○ Not Applicable

What is your professional status?

○ Unemployed

○ Student

◉ Employed

○ Retired

If employed, what is the nature of your institution?

◉ Public/Government sector

○ Private sector

○ Not Applicable

If employed, what is your field of work in your institution?

○ Finance and Insurance

○ Manufacturing

○ Energy

○ Retail

○ Professional Services

◉ Government

○ Healthcare

○ Media

○ Transportation

○ Education

○ Communications & Information Technology

○ Others

Research Questions

Authority Social Engineering Technique

1. Consider you have received an email from your Chief Executive Officer directed to you specifically, as in the figure below.

From: <CEO’s Full Name> **your_ceo@your_company.com**

To: <Your Full Name> **your_email@your_company.com**

Dear (Your Name),

It is in my best interest to encourage you to visit our company’s branding page, which highlights our recent successes, plans, and visions. Feel free to navigate through the pages and let us together share our journey to greatness.

Visit Here

Best Regards,

CEO’s Full Name

How likely is it that you shall click on the link in the email?

● Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

2. Refer to Question 1. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

● Less than 3 times a year

○ 3 - 7 times a year

○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Commitment Social Engineering Technique

3. Consider you have received an email from your company's training and learning team directed to you specifically, as in the figure below.

From: <Your Training Team> your_training_team@your_company.com

To: <Your Full Name> your_email@your_company.com

Dear (Your Name),

We have seen you have been learning interesting things from the training site. That is great! Why not take a minute or so to learn something today? Come on! We can do this!

Click Here to Learn

Best Regards,

Training Team

How likely is it that you shall click on the link in the email?

● Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

4. Refer to Question 3. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

● Less than 3 times a year

○ 3 - 7 times a year

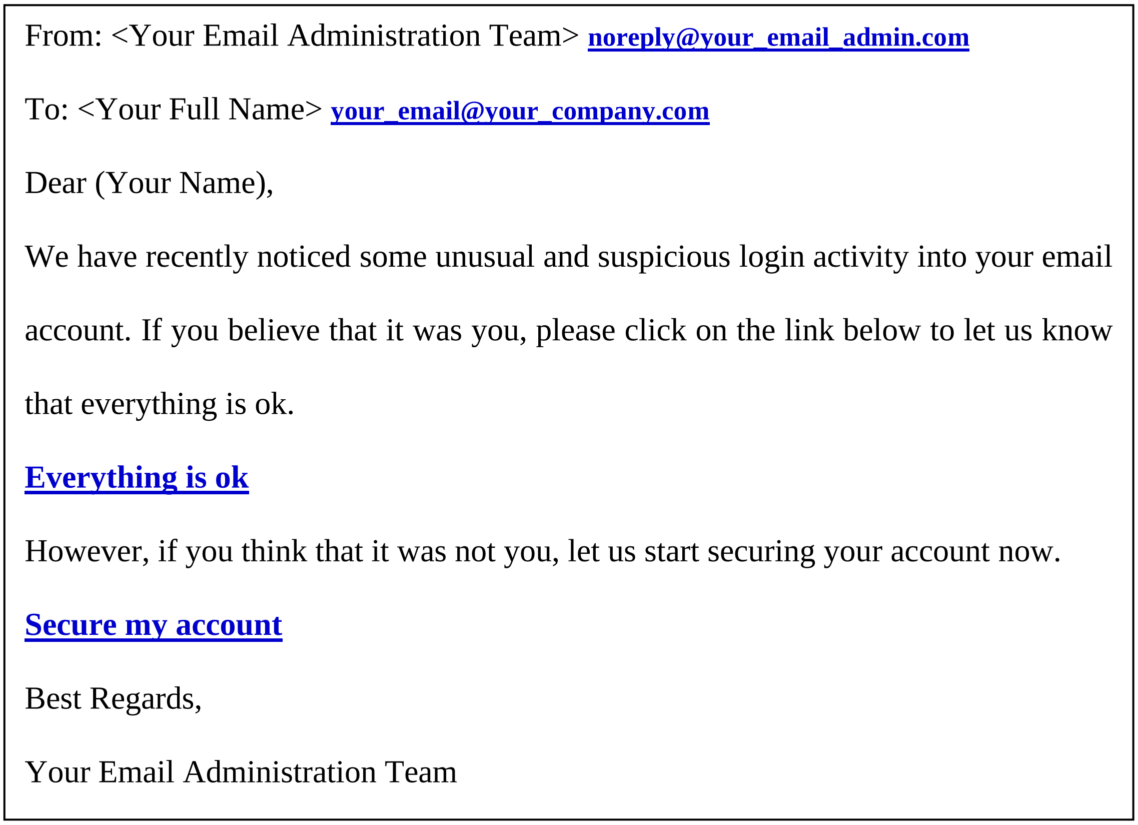
○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Contrast Social Engineering Technique

5. Suppose you have received an email from your email administration group intended for you specifically, as in the figure below.



From: <Your Email Administration Team> **noreply@your_email_admin.com**

To: <Your Full Name> **your_email@your_company.com**

Dear (Your Name),

We have recently noticed some unusual and suspicious login activity into your email account. If you believe that it was you, please click on the link below to let us know that everything is ok.

Everything is ok

However, if you think that it was not you, let us start securing your account now.

Secure my account

Best Regards,

Your Email Administration Team

How likely is it that you shall click on any of the given links in the email?

◉ Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

6. Refer to Question 5. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

◉ Less than 3 times a year

○ 3 - 7 times a year

○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Curiosity Social Engineering Technique

7. Suppose you have received an email from your company's marketing team intended for you specifically, as in the figure below.

From: <Your Marketing Team> **your_marketing_team@your_company.com**

To: <Your Full Name> **your_email@your_company.com**

Dear (Your Name),

A number of employees having been making a lot of money following a very simple mechanism, and even better, they spend so little time working for it. Do you want to know how they manage to do this?

Start making money now

Best Regards,

Marketing Team

How likely is it that you shall click on the link in the email?

● Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

8. Refer to Question 7. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

● Less than 3 times a year

○ 3 - 7 times a year

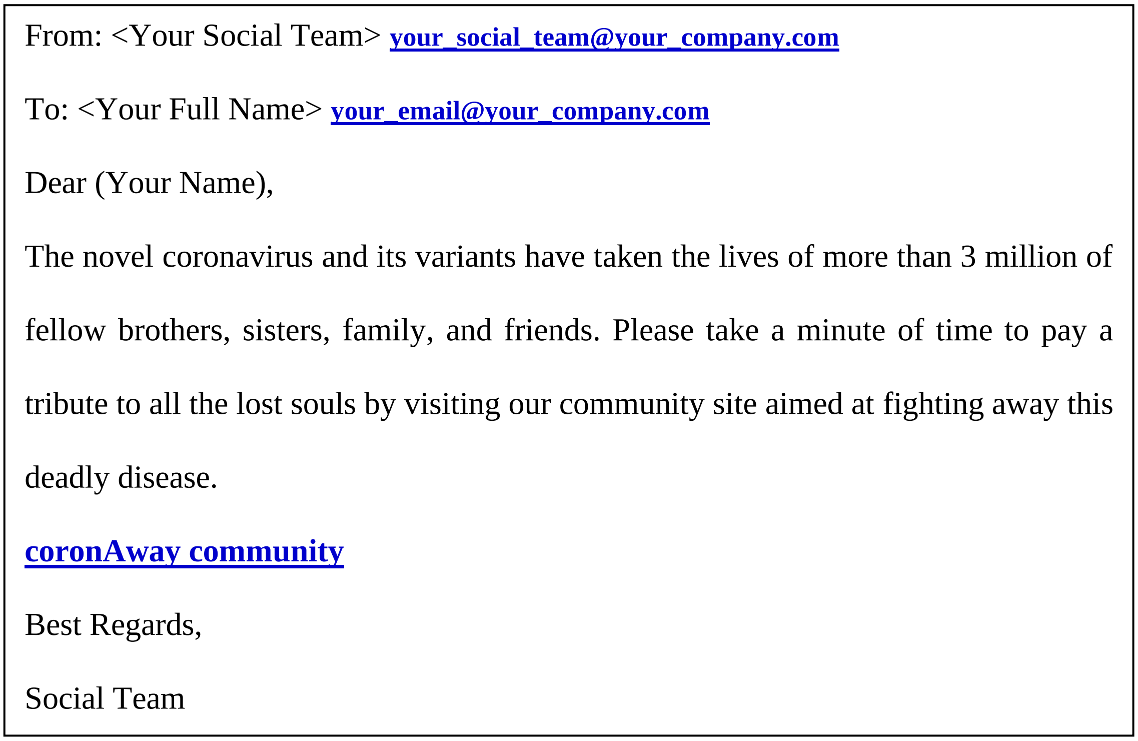
○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Empathy Social Engineering Technique

9. Take it that you have received an email from your company’s social communications team directed to you specifically, as in the figure below.



From: <Your Social Team> **your_social_team@your_company.com**

To: <Your Full Name> **your_email@your_company.com**

Dear (Your Name),

The novel coronavirus and its variants have taken the lives of more than 3 million of fellow brothers, sisters, family, and friends. Please take a minute of time to pay a tribute to all the lost souls by visiting our community site aimed at fighting away this deadly disease.

coronAway community

Best Regards,

Social Team

How likely is it that you shall click on the link in the email?

● Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

10. Refer to Question 9. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

● Less than 3 times a year

○ 3 - 7 times a year

○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Fear Social Engineering Technique

11. Take it that you have received an email from the National Identification Authority (NIDA) directed to you specifically, as in the figure below.

From: <NIDA> **noreply@nida.gov.org**

To: <Your Full Name> **your_email@your_company.com**

Dear (Your Name),

We have noticed that important details from the registration of your national identification are missing. A failure to provide all your correct details may lead to fines, penalties and possible jail time. To find out your missing details and the necessary steps to take, follow the link below.

Submit details to NIDA

Best Regards,

National Identification Authority

How likely is it that you shall click on the link in the email?

● Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

12. Refer to Question 11. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

● Less than 3 times a year

○ 3 - 7 times a year

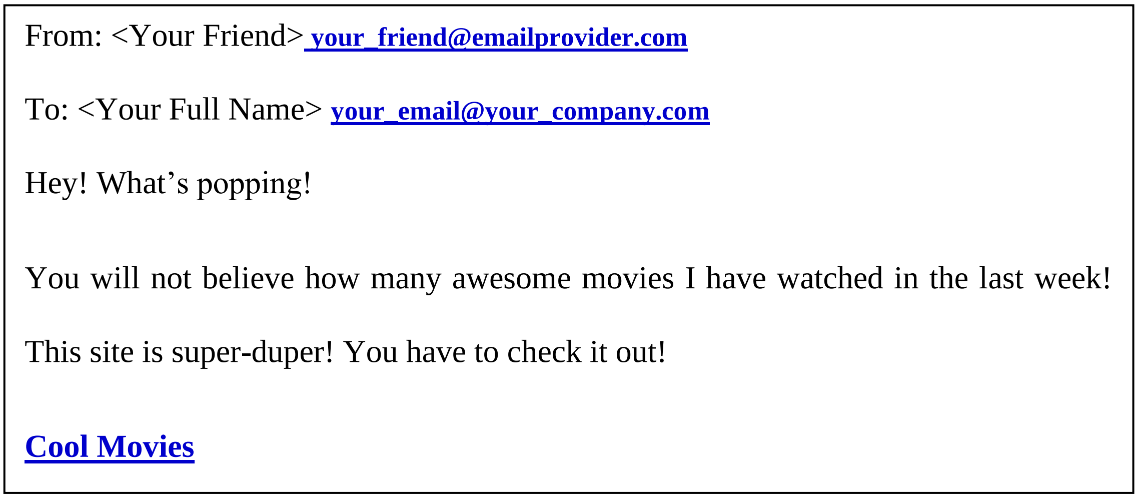
○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Liking Social Engineering Technique

13. Consider you have received an email from a good friend of yours, intended for you, as in the figure below.



From: <Your Friend> **your_friend@emailprovider.com**

To: <Your Full Name> **your_email@your_company.com**

Hey! What's popping!

You will not believe how many awesome movies I have watched in the last week! This site is super-duper! You have to check it out!

Cool Movies

How likely is it that you shall click on the link in the email?

● Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

14. Refer to Question 13. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

● Less than 3 times a year

○ 3 - 7 times a year

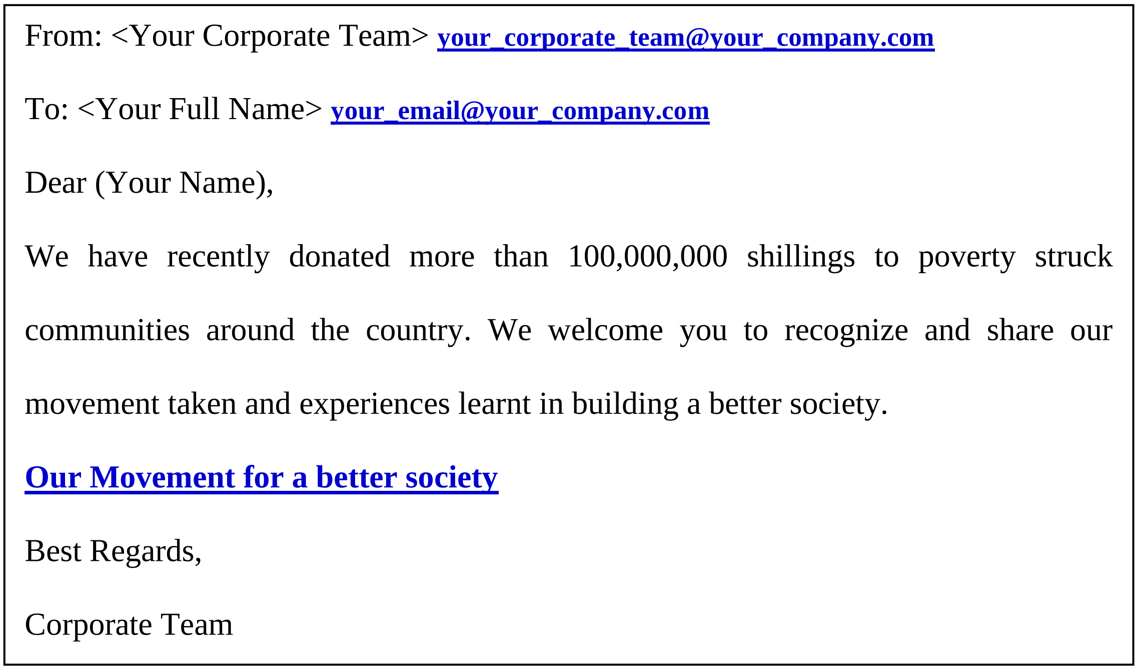
○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Reciprocity Social Engineering Technique

15. Consider you have received an email from your company's corporate communications team, intended for you specifically, as in the figure below.



From: <Your Corporate Team> **your_corporate_team@your_company.com**

To: <Your Full Name> **your_email@your_company.com**

Dear (Your Name),

We have recently donated more than 100,000,000 shillings to poverty struck communities around the country. We welcome you to recognize and share our movement taken and experiences learnt in building a better society.

Our Movement for a better society

Best Regards,

Corporate Team

How likely is it that you shall click on the link in the email?

● Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

16. Refer to Question 15. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

● Less than 3 times a year

○ 3 - 7 times a year

○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Scarcity Social Engineering Technique

17. Suppose you have received an email from your mobile phone company directed to you specifically, with your cellphone number in it, as in the figure below.

From: <Your Mobile Phone Company> **noreply@your_mobilephone_company.com**

To: <Your Full Name> **your_email@your_company.com**

Dear (Your Name),

Congratulations! Your number +255<<your number>> has won our lucky draw and you are the winner of our 10,000,000 shillings prize. Visit our site below within 24 hours to claim your reward.

Claim your Prize!

Best Regards,

Your Mobile Phone Company

How likely is it that you shall click on the link in the email?

● Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

18. Refer to Question 17. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

● Less than 3 times a year

○ 3 - 7 times a year

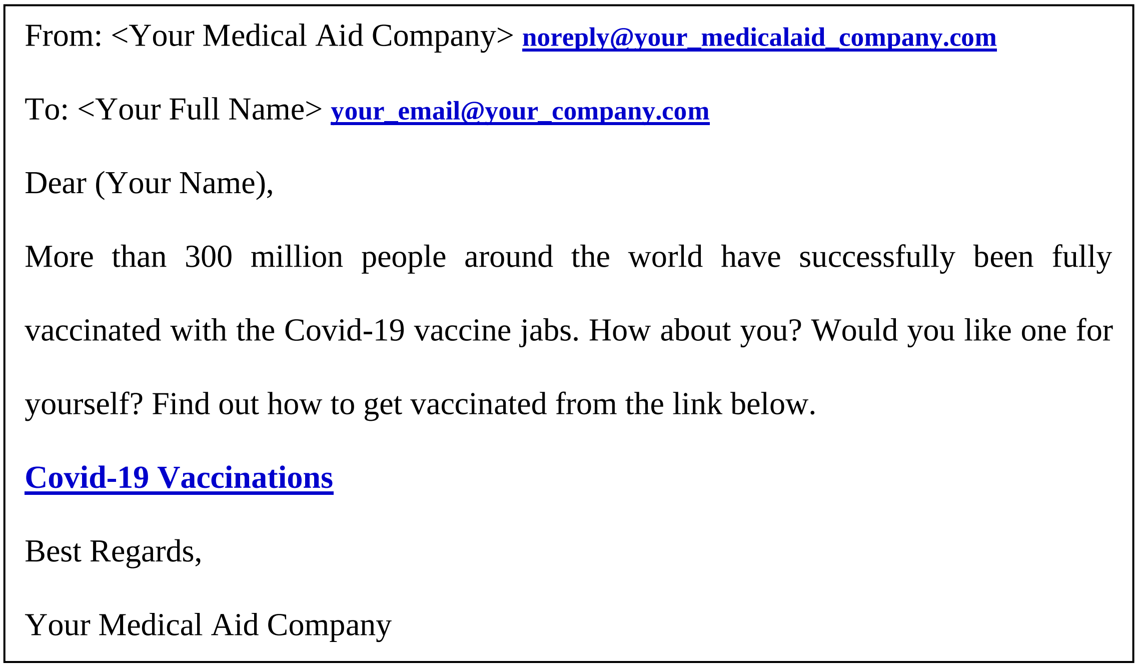
○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Social Proof Social Engineering Technique

19. Suppose you have received an email from your medical aid company directed to you specifically, as in the figure below.



From: <Your Medical Aid Company> **noreply@your_medicalaid_company.com**

To: <Your Full Name> **your_email@your_company.com**

Dear (Your Name),

More than 300 million people around the world have successfully been fully vaccinated with the Covid-19 vaccine jabs. How about you? Would you like one for yourself? Find out how to get vaccinated from the link below.

Covid-19 Vaccinations

Best Regards,

Your Medical Aid Company

How likely is it that you shall click on the link in the email?

◉ Very unlikely

○ Unlikely

○ Not sure

○ Likely

○ Very likely

20. Refer to Question 19. How frequently have you encountered a possibly similar suspicious email as in the scenario above?

◉ Less than 3 times a year

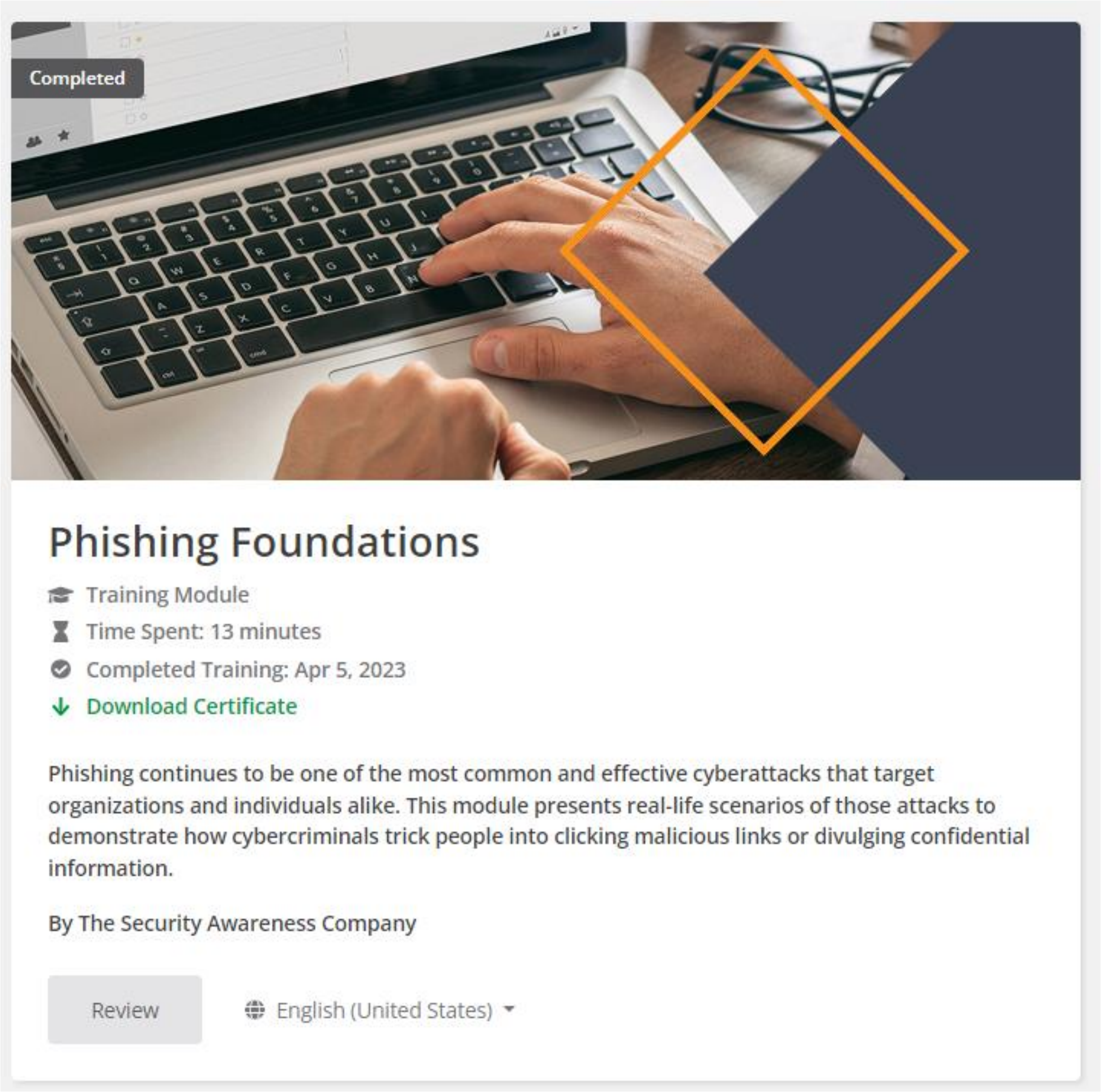
○ 3 - 7 times a year

○ 7 - 11 times a year

○ 11 - 15 times a year

○ More than 15 times a year

Appendix IV: Security Awareness Training



Phishing Foundations

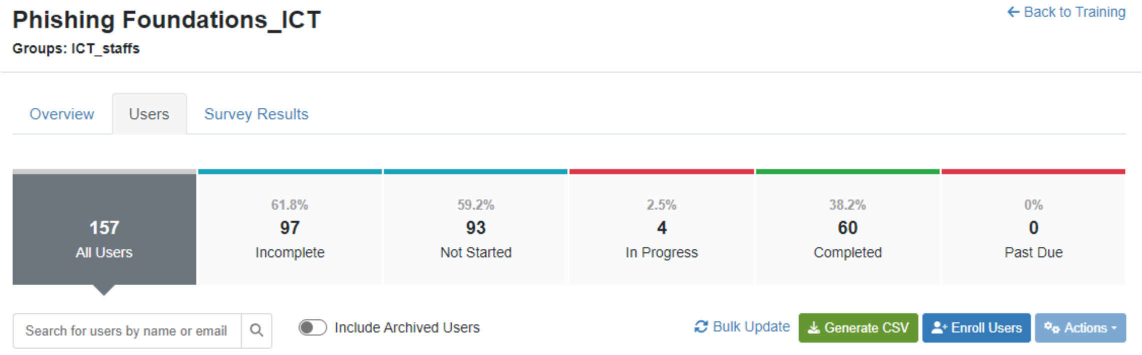
Training Module

Time Spent: 13 minutes

Completed Training: Apr 5, 2023

Phishing continues to be one of the most common and effective cyberattacks that target organizations and individuals alike. This module presents real-life scenarios of those attacks to demonstrate how cybercriminals trick people into clicking malicious links or divulging confidential information.

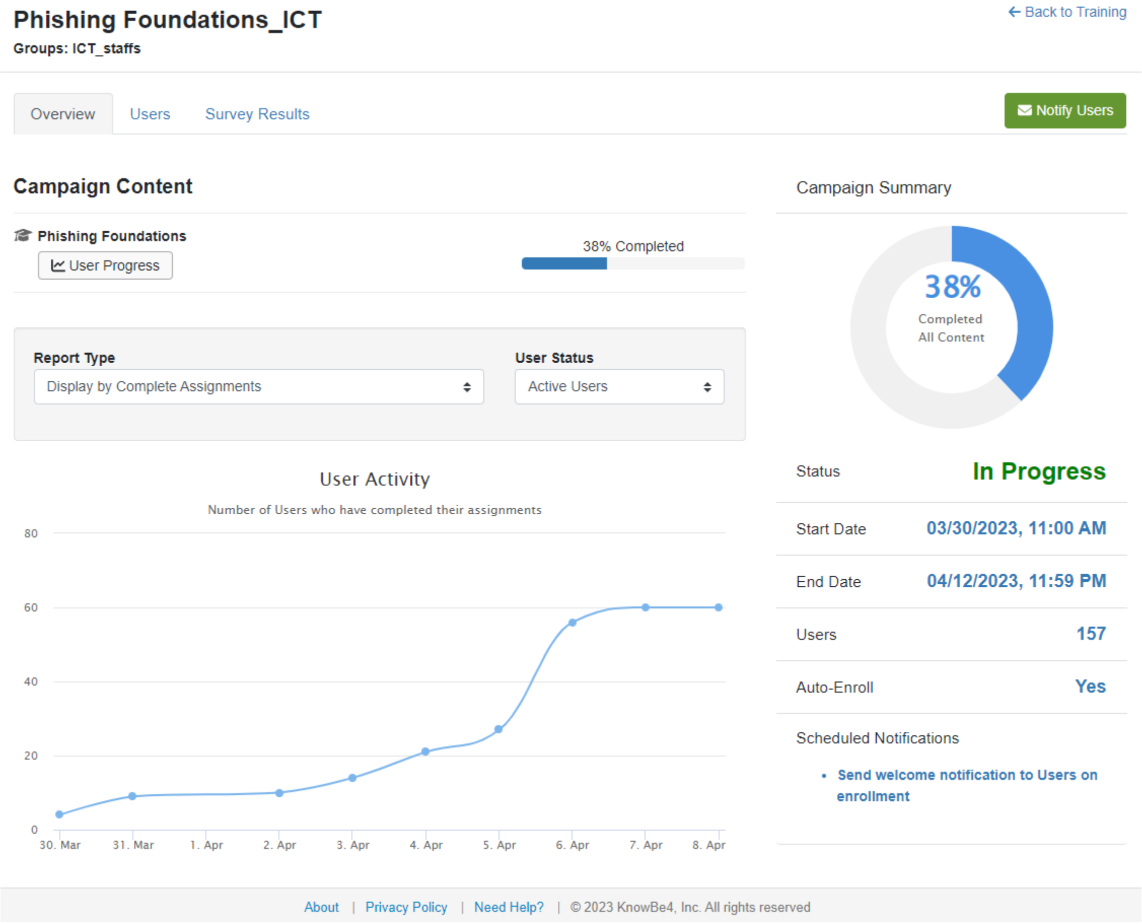
By The Security Awareness Company



Phishing Foundations_ICT

Groups: ICT_staffs

	61.8%	59.2%	2.5%	38.2%	0%
157	97	93	4	60	0
All Users	Incomplete	Not Started	In Progress	Completed	Past Due



Phishing Foundations_ICT

Groups: ICT_staffs

Campaign Content

Phishing Foundations

38% Completed

Report Type: Display by Complete Assignments

User Status: Active Users

User Activity

Number of Users who have completed their assignments

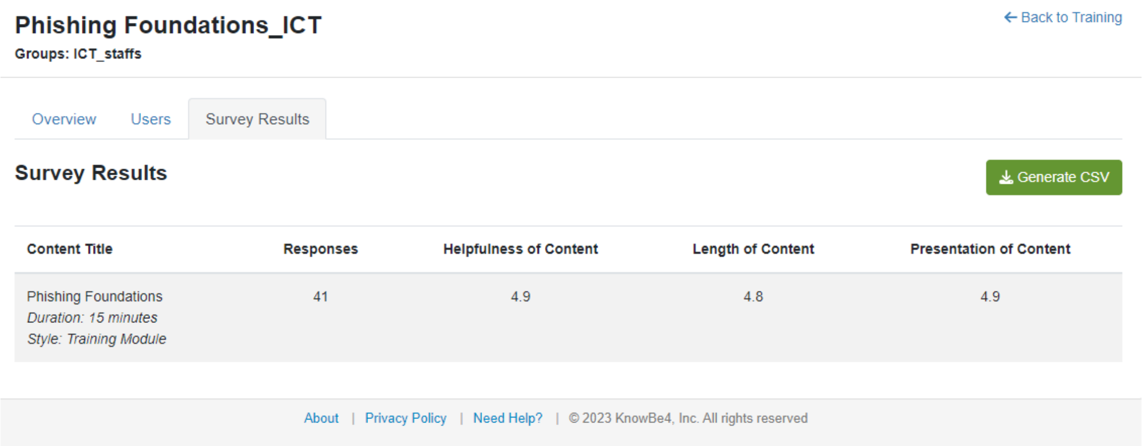
Campaign Summary

Status	In Progress
Start Date	03/30/2023, 11:00 AM
End Date	04/12/2023, 11:59 PM
Users	157
Auto-Enroll	Yes

Scheduled Notifications

- Send welcome notification to Users on enrollment

About | Privacy Policy | Need Help? | © 2023 KnowBe4, Inc. All rights reserved



← Back to Training
Overview
Users
Survey Results
Generate CSV
About | Privacy Policy | Need Help? | © 2023 KnowBe4, Inc. All rights reserved

Phishing Foundations_ICT

Groups: ICT_staffs

Survey Results

Content Title	Responses	Helpfulness of Content	Length of Content	Presentation of Content
Phishing Foundations *Duration: 15 minutes* *Style: Training Module*	41	4.9	4.8	4.9

Appendix V: Action Plan Matrix

S. No.	Comments from Discussant (Dr. Lilian Mutalemwa)	Response from Student	Pages where comments are attended
1.	What do you mean by the case study of Tanzania? It is better to be specific. You can also be specific on the type of security risk scale, maybe based on the technique you use?	An in-depth literature review of different cases related to phishing in Tanzania has been performed. The security risk scale has been proposed specifically as an email content-based type. The security risk scale rates the risk based on the email content attacking the users' emotions	2-5,10-23
2.	The statement of problem is not well explained. Can you explain the importance of figure 1.1?	Figure 1.1 has been removed. The problem statement has been revised to be clear. The research problem has been identified as the need for an email-content based risk scale that will consider the human emotion attacked by the phisher. Most of the current phishing security risk scales are either user behavior-based and work on characterizing the user phishing susceptibility risk or email domain based to plot the risk posed by a specific email address.	4-5, 38-40
3.	You stated that "The solution devised by LexisNexis can be improved to include the risk score based on the actual content in the emails". Are you improving the LexisNexis solution? Has anyone else done this? What were their observations?	The risk scale from LexisNexis Emailage is based on the email identity data, such as the email domain, the IP address etc. Most of the other risk scales are based on user behavior and interaction to phishing emails. As an improvement to the techniques by LexisNexis et. al., a security risk scale based on email content has been proposed.	39-40
4.	How did you decide to use the different statistical tests?	The choice of the statistical tests used were based on proving or disproving the null hypotheses	66-68

		constructed to find existence of statistical significance between independent variables and dependent variables for various use cases.	
5.	In section 3.3 you are presenting data for (Nov 2021, December 2021, and January 2022) and you mention that it is for the past 3 months. It is better to state the period, rather than past 3 months.	The definition of the secondary data collected has been revised to include a larger scope and mention the specific period of January 2019 to March 2022.	2

S. No.	Comments from Discussant (Dr. Juliana Kamaghe)	Response from Student	Pages where comments are attended
1.	The title is ok.	The title has not been changed: A Security Risk Scale to Enhance Phishing Detection	-
2.	Background: Regarding the concept behind risk of phishing, you should talk of the risk involved in the perspective of Tanzania.	Various literatures in the context of phishing in Tanzania have been introduced in the background. E.g., Oreku (2020), Msaki (2019), Mswahili (2022), Lissah et al. (2022), Salim (2022), Kavishe (2021), Ndibwile et al. (2018), Panga et al. (2022), and Mwabukojo (2020)	1-4
3.	The Statement is not clear as to what is the problem so far. Try to explain the problem based on the literature you have read. Remove pictures and try to show what is prevailing at least.	The statement of the problem has been revised in Section 1.2 – Statement of Problem, with regards to improving existing literatures mentioned in Chapter 2: Literature Review. Section 2.2 – Related Works	4-5
4.	Objective 1&2 should be objective 1, and objective 3 should be objective 2. Add one objective on testing your solutions.	The objectives have been revised to combine what was previously objective 1 and 2 into a single specific objective i.e., Specific Objective 1. What was previously objective 3 has now been mentioned as Specific Objective 2. A new objective i.e., Specific Objective 3 has been added to test the security risk scale.	5
5.	The research gap should come from literature review. Try to capture it as “from this and this”, then “from those”, so we can see the research gaps “from there”. Why did you take a gap from only	The research gap has been revised to find gaps from the literatures mentioned in the literature review section and propose a security risk scale aimed at closing the gaps. Five more literatures on different types of security risk scales have been searched for and the gaps have been identified.	40-41

	one research? i.e., LexisNexis. I need to see at least five.		
6.	The title is “social engineering techniques”, but you have explained about “factors affecting effectiveness of phishing”. Why did you rephrase?	The phishing social engineering techniques may also be considered as the factors affecting the susceptibility of victims to phishing because these social engineering techniques are emotional manipulation techniques that have a direct impact on the user. This will affect whether the user shall be easily susceptible to a phishing attack or not.	111-112
7.	How did you come up with your sample size? What are the criteria for your study size? Where did you get your data of attacks? Are you going to use it as a sample?	Purposive and convenient sampling methodologies are used to sample the data. A target population size of not less than 300 respondents has been chosen based on criteria such as time, resources, and participants available for the research study. 100 respondents (around 30% of the population) are randomly selected as per the demographic clusters listed in Chapter 3: Table 3.3 – Demographic Information. The sample size of the groups within the clusters is selected based on optimum availability of respondents. Data of the attacks has been collected from the honeypots reports of the Tanzania Computer Emergency Response Team (TZ-CERT) from the period of January 2019 to March 2022. Primary data from respondents shall be taken for sampling. The secondary data from TZ-CERT is used to analyze the phishing risk from a Tanzanian perspective.	2, 52-56, 118-121
8.	General comments: 1. Follow the OUT-research guidelines for	The proposal has been revised and edited to meet the Open University of Tanzania research guidelines.	4-5

	writing your proposal i.e., spacing, number of pages etc. 2. Work on the research problem.	The research problem has been revised as per the recommendations in comment 3.	
9.	How have you tested the risk scale?	The risk scale is tested by performing real phishing tests at a bank for three sample emotions, i.e., authority, reciprocity, and commitment. An assumption is made to reject the null hypothesis that claims there is no relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale The assumption is proved to be correct for the samples chosen, giving a true positive outcome in rejecting the null hypothesis. Error and accuracy calculations are performed to evaluate the difference in the phishing outcome between the security risk scale and the actual phishing tests.	108-110, 162-168
10.	What conclusions can you draw out from your scale? What does the scale tell us about the risk?	Based on qualitative data gathered from respondents from the social communities, it was found that the emotions manipulated by the hackers in their phishing emails do not result in low or medium risk to the user. Most of the social engineering techniques as per our findings, are of critical risk. The top risk social engineering technique evaluated was curiosity, followed by fear, authority, and empathy. Commitment and contrast fell in the high-risk region. The conclusions for the null hypothesis made are shown in Table 5.1: Summary of conclusions made for hypotheses.	171-172

11.	You have used an email content risk scale in your research gap, why?	The email content-based risk scale is like the risk scale in this research as far as analyzing the content in the email. However, the risk scale devised by Steves et al. does not consider the emotion used by the hacker in their social engineering scheme. They rather investigate cues and premise alignment. Risk decreases if there are many cues and less premise alignment, and vice versa.	40-41
12.	How are phishing variables related to the security risk?	The conceptual framework has been revised to clearly indicate the independent, dependent, and moderating variables. The phishing variables are the social engineering techniques. They have been used in one case as an independent variable, and in another case as a moderating variable. In both cases they are related to components of risk i.e., the probability of interacting with a phishing email and the frequency of receiving the phishing email. The components that make up the risk are dependent variables. In the case where the phishing variable is the moderating variable, demographics are the independent variable. Chapter 3.9.3: Statistical tests – shows how the relationships between the phishing variables and security risk are evaluated statistically. Chapter 4.2.3: Hypothesis Test Results – shows the results of the statistical tests to determine the relations between the phishing variables and the security risk. Table 4.22: Phishing security risk evaluation - shows the phishing	41-43, 66-96, 142-160

		variables/social engineering techniques and the respective rated risk. Figure 4.29 shows the designed security risk scale that graphically plots the phishing variables into risk quadrants.	
13.	What do you mean by the commitment phishing variable?	Commitment as a social engineering technique is when the hacker plots a scenario in the phishing email to trigger the character of hard work and dedication that the victim may have and trick them into following their instructions because of the quality of the victim of commitment to excellence. Chapter 3.11.4 shows the use of the commitment phishing variable as a sample for the phishing test.	107, 111
14.	May you name at least five phishing variables?	The phishing variables, the factors affecting the effectiveness of phishing, and the phishing social engineering techniques all constitute to the same meaning in our study. An explorative research methodology was used to determine the phishing variables, namely authority, commitment, contrast, curiosity, empathy, fear, liking, reciprocity, scarcity, and social proof.	61, 111
15.	What is the innovative part of your research?	Costs of securing systems may be optimized by focusing on higher risk phishing emails. The research paves the way for future studies on dynamic risk scales that may be derived using machine learning and simulated phishing attacks, that are based on real-life phishing experiences that occur daily. Human beings are considered as the weakest link to security, and social	6-7, 173-176

		engineering targets the human factor, i.e., the capability to exhibit emotions. Studies have found that awareness is an efficient defense against social engineering. This research provides a unique form of awareness on the emotions manipulated by hackers and their risk when applied to phishing. There are relatively small differences in risk values, between the various emotions used in the hacker's technique, as from our security risk scale. However, small deviations may be very significant when considering motivated hackers versus untrained users. Additionally, when searching through the top and reputable search engines over several top results and significant pages, for any research on email content-based phishing risk scales, that consider emotion manipulation in emails to rate the risk of the phishing attack, no significant journal, article, paper, or research was found. Based on this point, we may claim the risk scale designed in this research is a novel one.	
16.	What is the authority and empathy principle?	The authority principle is used by an attacker when they pose as a leader or someone in charge to trick victims who may be indulged to follow orders given. The empathy principle is used by an attacker to manipulate victims into feeling sorry for the made-up situation and give in to the demands.	111

S. No.	Comments from Discussant (Dr. Edephonce Nfuka)	Response from Student	Pages where comments are attended
1.	A conceptual framework should be devised. There are only independent and dependent variables in the Kruskal Wallis H test concept, but phishing variables are considered. Why?	The conceptual framework has been revised to include the phishing variables. The phishing variables when applied to the Kruskal Wallis H test are a categorical moderating variable. It affects the relationship between the independent and dependent variables. Non-parametric tests were performed to relate the independent and dependent variables, but with a consideration of the effect of the moderating variable i.e., social engineering techniques or the phishing variables.	41-43
2.	Steves et al. developed an email content-based risk scale. How does this differ from yours?	The email content-based risk scale developed by Steves et al. focuses on cues and premise alignment in the phishing email. Cues are indicators in the email that would give away the identity of the hacker. E.g., a suspicious looking attachment. The premise alignment is a spear-phishing factor that shows how the email content relates to the target's premises. The less the number cues and the greater the premise alignment imply that it is harder for phishing to be detected. The risk scale in this study accounts to the emotional technique that the hacker is using within the theme of the phishing email. The risk increases when either the probability of a user interacting with the phishing email or the frequency of receiving the phishing email for the specific emotion increase.	40-41

		Risk severity in the design of Steves et al. is based on the capability of a hacker hiding the fact to the user that their email is a phishing one, whereas the risk severity in this research is based on the capability of an emotion triggered by the hacker in making the phishing attempt successful.	
3.	What are the benefits of your risk scale?	The risk scale provides phishing security risk information to normal email users, organizations, security solution vendors, and anyone interested. Awareness on the trending phishing risks may reduce possible exploitation. Organizations may allocate adequate resources and budget to counter the phishing email content risk, with a consideration of criticality. Proper security governance and controls can be set in relation to the risk ratings derived from the security risk scale. Risk mitigation strategies may take the severity measures into account to provide feasible solutions. Organizational costs for security may be tuned to focus on high-risk phishing emails. A dynamic risk scale can be designed with reference to the proposed risk scale that leverages on natural language processing and phishing simulations to populate the risk from live phishing attacks.	6-7. 173-176

S. No.	Comments from Discussant (Dr. Khamis Kalegele)	Response from Student	Pages where comments are attended
1.	Considering the risk scale designed, what is the use of the arc-like sectors for the risk levels? If you take a situation where the frequency of receiving the phishing email is very large, but the probability of interacting with the phishing email is negligible, then the risk would be zero. It is therefore better to illustrate your risk levels in the form of quadrants instead of arcs.	A risk matrix has been designed with risk quadrants for critical, high, medium, and low risk to replace the arc-like design for risk levels.	96-98, 158-160
2.	From your scale, how have you considered type I (false-positive) and type II (false-negative) errors?	Our risk scale is derived qualitatively from responses of respondents via a questionnaire. Their subjective option is the basis of determining the risk factors that make up the scale. As an investigator, we have not placed judgement to the null hypothesis. We are observing and scaling the views from the society. In specific objective iii, we have added an assumption to reject the null hypothesis that claims there is no relationship between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale. We found that our assumption of rejecting the null hypothesis resulted in a true positive for the samples chosen for the phishing tests performed at the bank.	108-110, 162-168

		A measure of the error rate of the risk scale derived from the responses collected from the questionnaire has been evaluated with respect to the results of the simulated phishing attack.	
3.	You have talked about using natural language processing to extract emotions from phishing emails. How do you consider processing power for training, the high costs, and the errors in the machine learning?	The concept of applying artificial intelligence was a suggestion for project expansions and future ideas. It is not in the scope of the current research but can be taken into consideration when aiming to develop or enhance this research.	174-176

S. No.	Comments from Discussant (Dr. Catherine Mkude)	Response from Student	Pages where comments are attended
1.	How does your risk scale address the gap?	The security risk scale in this study closes the gap left from the risk scales by Yang et al. (2022), Affinity IT Security Services (2019), KnowBe4 (2022), Tessian (2021), LexisNexis (2017), and Steves et al. (2020) by rating the risk posed by the social engineering triggers used by the hacker in the phishing email content.	40, 41

S. No.	Comments from Discussant (Dr. Rogers Bhalalusesa)	Response from Student	Pages where comments are attended
1.	The reference should be shown for the Friedman test. Is it chi-square or ANOVA?	Studies by Salerno et al. (2021) have discussed the Friedman test with Omar (2021) demonstrating the practical evaluation. The Friedman test is based on the chi-square distribution, but it may be considered as the non-parametric version of the parametric one-way analysis of variances (ANOVA) with repeated measures.	68, 72-74
2.	Have you used the nominal or the ordinal scale?	Both the nominal and ordinal scale have been used depending on the variable nature. Nominal for variables that have no rank or order, and ordinal for the ranked or categorical variables.	58-60
3.	Best to remain with a single chart.	The pie-chart has been omitted and the histogram selected for the illustration of the questionnaire results.	122-141
4.	Area of research – it is a bit confusing where the study area is.	The area for the questionnaire survey extends globally with respect to the online coverage of the survey. The area of the phishing experiment was conveniently sampled to take place at CRDB Bank Plc in Dar es salaam, Tanzania.	52-57
5.	What is the difference between a scale and a framework?	A risk scale is a tool to manage risk while a risk management framework is a collection of tools, processes, policies, and governance of the risk items as denoted by Ullah et al. (2021)	7
6.	What is the difference between phishing and man in the middle?	Phishing is a social engineering technique as explained by Rosenthal (2021), that aims to trick a victim to perform an unintended action via following malicious instructions in an email or message. Mallik et al.	1

		(2019) describe the man in the middle attack as an active attack achieved by intercepting the communication path between two devices and posing as the other device to each device.	

S. No.	Comments from External Examiner	Response from Student	Pages where comments are attended
1.	**CHAPTER 1: INTRODUCTION** Problem statement is too long. Normally it is supposed to be 1-2 paragraphs. It is recommended that this subsection is summarized to 1-2 pages only.	The problem statement has been revised as recommended as well as its subsection content.	4-5
2.	**CHAPTER 1: INTRODUCTION** The context is missing. It would be interesting if you can include some examples of phishing or security holes as a result of phishing or any social engineering techniques in the context of Tanzania. As of now, it looks like you are trying to address the problem that is not affecting us.	Various literatures in the context of phishing in Tanzania have been viewed in the introduction section. They include Oreku (2020), Msaki (2019), Mswahili (2022), Lissah et al. (2022), Salim (2022), Kavishe (2021), Ndibwile et al. (2018), Panga et al. (2022), and Mwabukojo (2020)	1-4
3.	**CHAPTER 2: LITERATURE REVIEW** Include some Tanzania context on phishing or security holes that have affected several sectors. How those phishing or security holes affected the specific sector?	A number of literatures in the context of phishing in Tanzania have been added to the review of literature. Some include Mshangi (2020), Mtakai and Sengati (2021), Msaki (2019), Semlambo, Mfoi, et al. (2022), Mlyatu and Sanga (2023), Lyimo (2022), etc.	10-23
4.	**CHAPTER 2: LITERATURE REVIEW** Include a subsection in this chapter to explain related works. Summarize at least 5 related works.	The subsection has been included to investigate the related works in the domain of email phishing detection based on content analysis as well as initiatives to develop scales that measure risk related to phishing.	29-40
5.	**CHAPTER 2: LITERATURE REVIEW**	The research gap has been improved with regards to the section of related works,	40-41

	Improve your research gap sub section. Having discussed related work, what is new in your work? What are you adding in the domain knowledge that others have not covered?	illustrating improvements to existing phishing detection models and phishing risk scales.	
6.	**CHAPTER 3: RESEARCH METHODOLOGY** The candidate is advised to focus on explaining what research methods (Philosophy, methods etc.) you have used for your study.	The research philosophy, approach, design, methods, and strategy used in the study have been identified and explained.	44-50
7.	**CHAPTER 3: RESEARCH METHODOLOGY** In the abstract you have indicated that you have conducted an experimental test. But, in this chapter there is no information regarding the experimental test you have conducted. Please include and explain in detail the experimental test.	The experimental test methodology that was performed at CRDB Bank Plc has been explained. The setup, implementation technique, and motives have been discussed.	98-107
8.	**CHAPTER 3: RESEARCH METHODOLOGY** This chapter is one of the weakest chapters in this work. It looks like the majority of data and information which is supposed to be in this chapter has been moved into chapter 4.	The research methodology chapter has been rearranged to concentrate on methodology issues only. Likewise, the results and discussion chapter has been revised to pin the results of the item topics in the methodology chapter.	44-110
9.	**CHAPTER 3: RESEARCH METHODOLOGY** It is a mixed research method. Did the candidate start with qualitative followed by quantitative? or vice versa? And why?	The study is mixed research. The aim of applying a specific research methodology is based on achieving the specific objectives mentioned in the objectives section.	44-50

10.	**CHAPTER 3: RESEARCH METHODOLOGY** The experimental test …including the expected hypothesis are missing in this chapter.	The experimental tests and hypotheses have been included in a sub-section of this chapter to illustrate the hypotheses with regards to the specific objectives and the test methods performed to reach conclusions.	98-110
11.	**CHAPTER 3: RESEARCH METHODOLOGY** Demographic data which takes nearly 70% of this chapter can be moved into Chapter 4. In addition, some findings which have been included in this chapter can be moved into Chapter 4.	The demographic data results from the respondents of the survey have been moved to chapter 4 to highlight the distribution of demographic information of the respondents. Any findings or results information has been moved from the methodology chapter to its respective chapter of results and discussion.	113-118
12.	**CHAPTER 3: RESEARCH METHODOLOGY** There is a lot of reorganization required in this chapter. In subsection 3.4, the subtitle is Data Collection Techniques.	The chapter has been reorganized to only include methodological aspects of the research. Section 3.4, is now Section 3.6, and has been revised to explain the Data Collection Techniques.	50-52
13.	**CHAPTER 4: RESULTS AND DISCUSSION** This chapter is very long with the majority of the content need to be moved into chapter 3. The candidate can summarize the findings to reduce the number of pages.	The content which was in this chapter that relates to the research methodology process has been moved to chapter 3. The demographic results from the survey have been summarized.	111-170
14.	**CHAPTER 4: RESULTS AND DISCUSSION** The discussion sub-section needs to be rewritten. It is expected that the candidate will discuss the findings in relation to the related works discussed in the Literature review. I have suggested an	The discussion sub-section has been rewritten to discuss the findings in relation to the related works discussed in the literature review.	168-170

	inclusion of this subsection in the Literature review.		
15.	**CHAPTER 5: CONCLUSION AND RECOMMENDATIONS** The suggestion for the future studies section is missing. I strongly recommended this subsection to be added into the thesis.	The suggestion for future studies section has been added to the thesis.	174-176
16.	**CHAPTER 5: CONCLUSION AND RECOMMENDATIONS** The recommendation sub-section needs to be added as a submission	The recommendation sub-section has been added as a submission.	173-174
17.	**OTHER COMMENTS** Citations: Throughout the document …intext citation needs to be rewritten as the candidate uses & sign instead of and.	All intext citations have been rewritten to include the ‘and’ word instead of the ‘&’ symbol for cases where two authors are cited in the reference.	Throughout the thesis
18.	**OTHER COMMENTS** The reference section misses a lot of articles which were cited in the thesis. The candidate needs to cross check all the citations and references and ensure that they are included.	The reference section has been redeveloped using Mendeley software to ensure that all articles cited in the thesis are included programmatically as a bibliography.	References section

S. No.	Comments from Second External Examiner	Response from Student	Pages where comments are attended
1.	**CHAPTER 1: INTRODUCTION** The section has been improved.	Noted.	-
2.	**CHAPTER 2: LITERATURE REVIEW** The section has been improved.	Noted.	-
3.	**CHAPTER 3: RESEARCH METHODOLOGY** The research methods (philosophy, methods etc.) still missing.	The research philosophy, approach, design, methods, and strategy used in the research has been added.	44=50
4.	**CHAPTER 3: RESEARCH METHODOLOGY** The detailed information about the experiment and how it was conducted is missing including hypothesis. The link between the experiment text and the findings need to be shown clearly.	The phishing test methodology has been explained. The KnowBe4 Phishing Simulation Setup is illustrated with the details on creating a phishing campaign, email template, and landing page. The linkage between the experiment text and findings has been explained. Three phishing social engineering techniques (authority, reciprocity, and commitment) are taken as a sample, to observe the link between the nature of the distribution of risk ratings in the simulated phishing attack with that of the designed security risk scale.	98-110
5.	**CHAPTER 3: RESEARCH METHODOLOGY** Population….why you chose this population for the study? sampling strategy is	The population was selected based on purposive and convenience sampling methodologies. Literatures from Oreku (2020), Mpofu and Mhlanga (2022),	52=57

	missing. Demographic information is missing.	Ntigwigwa (2019), Nuru (2020), Chanda (2020), and APWG (2022) describe financial institutions as a major target area for phishing, making them a significant location for performing the experiment. The demographic information has been added.	
6.	**CHAPTER 4: RESULTS AND DISCUSSION** The candidate needs to opt for either pie chart or histogram. As of now, the two have been used and thus make it an unnecessary duplicate.	The duplicate pie-chart has been removed. A histogram has been chosen for illustrating the questionnaire results for the categorical variables.	122=141
7.	**CHAPTER 4: RESULTS AND DISCUSSION** Table 4. 7: Hypothesis Test Results of Specific Objective 2 need to be improved. The hypotheses need to be stated in the methodology and how they are going to be evaluated. As of now, they have just been dropped from nowhere. The justification of using each of the statistical approaches used need to be clearly stated in the methodology.	The hypothesis for each of the objectives subject to a test have been mentioned in the methodology. The setup for performing the Friedman (Omar, 2021) and Kruskal-Wallis H (O'Loughlin, 2021) tests in IBM SPSS have been shown. The setup of the phishing campaign in KnowBe4 has also been shown. Literatures from Andrade (2019), Shrestha (2019), Di Leo & Sardanelli (2020), Lovell (2020) and Sedgwick et al. (2022) highlight the aspects of the statistical testing methodology. Salerno et al. (2021) describe the Friedman test and Niedoba et al. (2023), Aslam & Sattam Aldosari (2020), and Călin & Tuşa (2023) interpret the Kruskal-Wallis H test.	58=110

8.	**CHAPTER 5: CONCLUSION AND RECOMMENDATIONS** The section has been improved.	Noted.	-
9.	**OTHER COMMENTS** The work has improved significantly. However, the language check is required as there are a lot of grammatical and spelling mistakes in the document.	Grammar and spelling checked has been performed on the entire scope of the dissertation	Throughout the thesis

OUT/DPGS/S2

THE OPEN UNIVERSITY OF TANZANIA
DIRECTORATE OF POSTGRADUATE STUDIES

Kawawa Road, Kinondoni Municipality,
P.O. Box 23409
Dar es Salaam, Tanzania
http://www.out.ac.tz

Tel: 255-22-2666752/2668445 ext. 100
Fax: 255-22-2668759,
E-mail: dpgs@out.ac.tz

REQUISITION FORM FOR RESEARCH CLEARANCE LETTER

Date: 01/04/2022

1. Name of Student: ROBERT METHOD KARAMAGI
2. Gender: MALE
3. Reg. Number: PG 201902753 Year of Entry 2020
4. Faculty FACULTY OF SCIENCE, TECHNOLOGY AND ENVIRONMENTAL STUDIES
5. Programme MASTER OF SCIENCE: COMPUTER SCIENCE (MSc CS)
6. Title of Research:
   A SECURITY RISK SCALE TO ENHANCE PHISHING DETECTION
7. Tentative dates for data collection:
   From 01/04/2022 to 31/06/2022
8. Student Email robertokaramagi@gmail.com
9. Student Phone Number 0762 087 332
10. Research Location/site:

S/N	Region	District Council/ Municipality	Name of Organization	Postal Address	Place
1	DAR ES SALAAM	KINONDONI	CRDB BANK PLC	P.O.BOX 268	ALI HASSAN MWINYI ROAD
2					
3					
4					
5					
6					

11. Date of submission 30/05/2022 Signature Robert Karamagi

12. Comments by Supervisor:

Received. Good Progress

Name of Supervisor DR OSAS ALY Signature Date 30/05/2022

THE OPEN UNIVERSITY OF TANZANIA
DIRECTORATE OF POSTGRADUATE STUDIES

P.O. Box 23409,
Dar es Salaam, Tanzania
http://www.out.ac.tz

Tel: 255-22-2666 752/
2668992/2668445
E-mail: drpc@out.ac.tz

POSTGRADUATE STUDENTS ACADEMIC PROGRESS REPORT FORM

(To be filled and submitted, every six months by all registered postgraduate students)

PERIOD COVERED: FROM ...01/03/2022.........TO .....01/09/2022........DATE

A CANDIDATE PARTICULARS

1. Name of Candidates:....ROBERT METHOD KARAMAGI.............................
2. Registration No.......PG201902753...
3. Address: ...15 MATITU STREET..........Mobile No .....0762 087 332..................

   Email: ...roberto karamagi@gmail.com...
4. Degree Proposed: ..MASTER OF SCIENCE IN COMPUTER SCIENCE.......

   ....(MScCS)..
5. Nature of Programme: By Thesis OR Coursework and Dissertation

   BY COURSEWORK..
6. Research Topic: ..A SECURITY RISK SCALE TO ENHANCE PHISHING DETECTION
7. Department, Institute and Faculty ..DEPARTMENT OF INFORMATION & COMMUNICATION TECHNOLOGY (ICT)

   FACULTY OF SCIENCE, TECHNOLOGY AND ENVIRONMENT STUDIES (FSTES)

B SECTION TO BE COMPLETED BY A CANDIDATE

I have done the following for my [✓ dissertation]/ ~~Thesis~~

	Nothing	About a Third	Half way	Nearly completed	Completed
Literature Review					✓
Designing of Methodology					✓
Getting Supplies for Study					✓
Data Analysis					✓
Writing of Dissertation					✓
Presentation of the Seminar(s)					
Submission of required articles					
Submission					

Candidate's Comments: ....

Candidate's Name...ROBERT METHOD KARAMAGI.........Signature ....

Date ....13/09/2022..

C SECTION TO BE COMPLETED BY SUPERVISOR

1	(a) (b) (c)	When did you last meet with the candidates? ....10/09/2022.......... .... How often have you met the candidates during past 6 months? ....20 times.......... If you have not met, comments on the reasons ....NL.......... ....
2		When did you begin supervising the candidate? Date ....05/09/2020....Month ....Year....2020....
3		If you have just been appointed the candidates' supervisor, did the previous supervisor hand you any report on the candidates Explain ....NL..........
4	(a) (b) (c) (d)	What progress has the candidate made? ....Good.......... Literature review ....✓.......... Field work / data collection ....✓.......... Preparation of thesis / dissertation draft ..✓.......... Others ....
5	(a) (b) (c) (d)	Is the candidate making satisfactory progress? ....YES.......... Will he / she be able to complete the study on time? ....YES.......... Will he / she need time extension? ....NO.......... If the answer above is yes how long? ....NL.......... ....
6		Any other remarks..........Good Progress.......... Name and signature of supervisor ....Dr. BALO Ally.......... Date ....14/09/2022..........

D SECTION TO BE COMPLETED BY THE HEAD OF DEPARTMENT

Comments on the report by the Supervisor (s)..........

....

....

OUT/DPGS/S3

THE OPEN UNIVERSITY OF TANZANIA
DIRECTORATE OF POSTGRADUATE STUDIES

P.O. Box 23409,
Dar es Salaam, Tanzania
http://www.out.ac.tz

Tel: 255-22-2666 752/
2668992/2668445
E-mail: drpc@out.ac.tz

POSTGRADUATE STUDENTS ACADEMIC PROGRESS REPORT FORM

(To be filled and submitted, every six months by all registered postgraduate students)

PERIOD COVERED: FROM JANUARY 2023 TO APRIL 2023 DATE

A CANDIDATE PARTICULARS

1. Name of Candidates: ROBERT METHOD KARAMAGI
2. Registration No. PG201902753
3. Address: 15 HADHINA STREET Mobile No 0762 087 332
   Email: robertokaramagi@gmail.com
4. Degree Proposed: MASTER OF SCIENCE COMPUTER SCIENCE (MSc. CS)
5. Nature of Programme: By Thesis OR Coursework and Dissertation
   COURSEWORK AND DISSERTATION
6. Research Topic: A SECURITY RISK SCALE TO ENHANCE PHISHING DETECTION
7. Department, Institute and Faculty DEPARTMENT OF ICT AND MATHEMATICS

B SECTION TO BE COMPLETED BY A CANDIDATE

I have done the following for my dissertation / Thesis

	Nothing	About a Third	Half way	Nearly completed	Completed
Literature Review					✓
Designing of Methodology					✓
Getting Supplies for Study					✓
Data Analysis					✓
Writing of Dissertation					✓
Presentation of the Seminar(s)					✓
Submission of required articles					✓
Submission					✓

Candidate's Comments:

Candidate's Name: ROBERT METHOD KARAMAGI Signature

Date 27/04/2023

C SECTION TO BE COMPLETED BY SUPERVISOR

1	(a) (b) (c)	When did you last meet with the candidates? JAN 2023 How often have you met the candidates during past 6 months? 2 times If you have not met, comments on the reasons NIL
2		When did you begin supervising the candidate? Date 07 Month July Year 2020
3		If you have just been appointed the candidates' supervisor, did the previous supervisor hand you any report on the candidates Explain NIL
4	(a) (b) (c) (d)	What progress has the candidate made? Literature review DONE Field work / data collection DONE Preparation of thesis / dissertation draft DONE Others
5	(a) (b) (c) (d)	Is the candidate making satisfactory progress? Yes Will he / she be able to complete the study on time? ~~At~~ Examination Stage Will he / she need time extension? No. If the answer above is yes how long? Examination Stage
6		Any other remarks Good Progress Name and signature of supervisor Dr. SAID ALLY Date 02/05/2023

D SECTION TO BE COMPLETED BY THE HEAD OF DEPARTMENT

Comments on the report by the Supervisor (s)……………………………………

……………………………………………………………………

……………………………………………………………………

E SECTION TO BE CONMPLETED BY FACULTY / INSTITUTE, DEAN / DIRECTOR

1. Comment briefly on the supervisor's / Head of Department's report

   ....

2. Has the candidate requested up-grading status of his / her thesis?

   ....

   ....

   ....

3. Any other remarks? ....

   ....

   ....

4. Name and signature of the Faculty / Institute Dean / Director

   Name...

   Signature: ....

   Date..

F. INFORMATION FROM BURSAR'S OFFICE (Section to be completed by the Director of Finance)

1. The candidate has paid all /part /not paid his / her fees ....

2. Other remarks: ....

   Name:...Signature: ....

   Date: ....

NB: Delete whichever is not applicable

F. SECTION TO BE COMPLETED BY THE DIRECTOR OF POSTGRADUATE STUDIES

1. Remarks from Director of Postgraduate Studies:...

   ....

   Name:...Signature: ....

   Date..

NB: Delete whichever is not applicable

Received: Date Month Year | Revised: Date Month Year | Accepted: Date Month Year | Published: Date Month Year
Volume XX(XX) Pages XXX-XXX DOI: https://doi.org/XXXX/XXXX

JICTS
Journal of ICT Systems

Security Risk Scale: *Case of Email Phishing Detection using Text Mining*

Robert Karamagi [a, 1] **Said Ally** [a, 2]

[a]*Mathematics and ICT Department, The Open University of Tanzania, Dar Es Salaam, Tanzania*
[a]*Mathematics and ICT Department, The Open University of Tanzania, Dar Es Salaam, Tanzania*

[1]Corresponding author
Email: robertokaramagi@gmail.com

Keywords

Phishing, Risk Scale,
Social Engineering,
Kruskal-Wallis H Test,
Friedman Test
Text Mining

Abstract

The rise of cyber security defense has led to attackers needing to deploy more resources to break into systems. However, the human factor remains the weakest link for system penetration through social engineering techniques especially when phishing is used. While cybersecurity and risk management go hand in hand, a measure of the risk posed by the threats in our environment is crucial control factor. In this study, an experimental test was conducted from 327 simulated phishing tests with probable responses of mail users to determine the emotion that triggers interaction when false email is used to trick victims into unintentionally submitting data and provide unauthorized access to mail server.

Four major causes of successful phishing attacks where emotions are triggered were found to be the manipulation of curiosity, fear, authority, and empathy emotions. For enhancing phishing detection, a framework that dynamically scales the security risks resulting from the social engineering attack through content of the phishing email received in real time is proposed. Although the technical controls have proven to be far more effective in securing systems, the framework provides administrative techniques with risk scales that organizations with mail servers can use to train their staff and resolve the ever-growing security problem of social engineering attacks through phishing emails.

1. Introduction

Phishing is a social engineering technique where a malicious individual sends a fake message to a mail user. It is a deliberate action requesting the victim to perform some action that will help the malicious attacker achieve an unethical mission, such as stealing login information or bank credit card details. [1] Phishing action has financial and legal impacts on users [2], and it is reported as one of the potential cyber security threats in Tanzania.

As one of the malicious acts, phishing has constricted e-commerce growth and led to losses of up to $85 million, according to the Tanzania Cybercrime Study Report of 2016 [3], with $30 million a year as the estimated cost of malicious insider threats [4]. Although phishing attacks can happen even in a Short Message Service (SMS) [5], they are considered a major threat for most of first-time mail users as they are unaware of the dangers and prevailing threats [6], especially in rural areas. [7]

It is evident that web attacks are doubling every year [8], with 70.54% related to phishing [3]. This is massively influenced by the rise of the cashless economy [9], the usage of mobile money services [10], and the lack of sufficient and sophisticated protection techniques [11].

Various efforts have been made to sophisticate the detection of phishing emails using artificial intelligence (AI) techniques. A vast number of models have been proposed that leverage on different machine learning (ML) algorithms to understand the content written in the email using text mining and natural language processing (NLP). Through AI application, it has been possible to detect whether an email is a phishing one or not, with motivating accuracy. The following are the most common phishing detection techniques:

- Support Vector Machines (SVM) with accuracy of 95%. The model is useful for classifying between phishing and non-phishing emails through analysis of the email-header structure, email-URL information, email-script function and email psychological features used for preparations of a classification dataset [12].
- An improved recurrent convolutional neural network (RCNN) model with multilevel vectors, word Embedding and [13] phishing classifier in comparison to Long Short-Term Memory (LSTM) layers [14]. The model has accuracy of 99.8%.
- Naive Bayes, K-Nearest Neighbor algorithms and Decision Tree (J48) classification which classify the word embedding and for removal of noise and non-words [15]. The model has accuracy of 99%.
- Back propagation with accuracy of 95.7%. The model works through a classical feed forward network with multiple hidden layers to detect phishing email [16].
- Bidirectional Encoder Representations from Transformers (BERT) model which uses email content and context features to detect phishing [17]. The model has accuracy of 87%.
- Natural language processing (NLP) for lexical and semantic analysis of email content using random forest, decision tree and logistic regression with accuracy of 98.95%. [18]
- Text mining and text analytics with accuracy of 99.2%. The model uses text categorization, information extraction, clustering, and text summarization. Email metadata and content - including the body and subject are analyzed to detect phishing [19].
- Artificial Neural Network (ANN) with two hidden layers to extract content features present in the email body and header with accuracy of 94.5% [20].

- Multi-layer perceptron (MLP) neural network and Random Forest classifiers with feature selection to extract header and hyperlinks in the email [21] with accuracy of 99.5%.
- Built upon Stochastic Gradient Descent classifier (SGD) with accuracy of 96% to predict a phishing email by analyzing the content such as subject line, email address and body [22].

With regards to measuring the phishing risk, various authors have made appreciable contributions, but their methods are limited when it comes to providing risk measurements based on the psychological manipulation or social engineering technique observed within the content of the phishing email. Most of the risk scales append a risk score based on the user that is tricked by the phishing email. Such risk scales include Affinity IT Security Services (2019), Yang et al. (2022), KnowBe4® (2017), and Tessian® (2021).

Affinity IT Security Services (2019) developed a 10-point single dimensional phishing risk scale to attach a respective risk score to an individual based on the actions they perform when they are subjected to a phishing attack. They proposed the factors responsible for either an increase or decrease in the phishing score in which the risk of all individuals is initially taken as neutral with a score of 5. In this scale, no change in the risk score of a user who simply reads a phishing email. However, the risk score shall increase when a user clicks a link in the phishing email and increase more if the user gives away classified information in the process. On the other hand, the risk score decreases when a phishing email is left untouched and decreases more if the phishing email is reported to the responsible authority. [23]

Yang et. al (2022) devised a technique to predict the risk of a user being susceptible to phishing by what they called the multidimensional phishing susceptibility prediction model (MPSPM). The model is based on multiple supervised machine learning experiment using both legitimate and phishing emails with decision factors being demographic, personality, knowledge experience, security behavior, and cognitive factors to determine/classify if the email is susceptible or easily tricked (high-risk) and non-susceptible (low risk). [24]

KnowBe4® (2017) designed the Virtual Risk Officer (VRO) to aid organizations in determining the vulnerability extent of their staff to phishing attacks. Using this approach, the risk score of a user is dynamically allocated using a deep learning neural network algorithm based on AI factors such as Phish-prone Percentage, Security Awareness Training Status, Breach Data, Job Function, User Risk Booster, and Group Risk Booster [25].

Tessian® (2022) developed the Risk Hub to provide a granular insight into the email users' levels of risk and risk enhancers where the risk score increases when bad security actions are performed by the user [26]. The platform focuses on the behavior of users to convey an extensive spectrum of risk assessments over incoming and outgoing email threats, phishing attacks, and data breaches. A contextually rich risk profile of a user is provided by a unique data modelling technique called the Behavior Intelligence Model. Table 1 compares risk scales showing their types and measured objects.

Table 1. Comparison of Risk Scales

Author	Name of Risk Scale	Type of Risk Scale	Measured object
Affinity IT Security Services (2019)	'Phishing Risk' scale	User Interaction	User
Yang et al. (2022)	Multidimensional Phishing Susceptibility Prediction Model (MPSPM)	User Personality	User
KnowBe4® (2017)	Virtual Risk Officer (VRO)	User Personality and Interaction	User
Tessian® (2021)	Tessian Human Layer Rik Hub	User Personality and Interaction	User
LexisNexis® Risk Solutions (2017)	Emailage	Email Identity	Email
Steves et al. (2020)	NIST Phish Scale	Email Content	Email

Despite all these risk scales, with evolving technology, cybercriminals are getting more sophisticated in their attacking mechanisms, and as a result, the cost of cyber defenses is skyrocketing. As of 2023, enterprise email phishing detection and prevention solutions have charged at least $3 per user per month, the cost which increases based on the number of incidents.

Thus, this study tries to address the social engineering techniques used by hackers in phishing emails to emotionally manipulate their victims and to find out if they have any effect on the probability of a user interacting with that phishing email. Furthermore, the study determines the impact of the demographic factors on the probability of a user interacting with a phishing email for a given social engineering technique and its frequency. Lastly, the study assesses the accuracy level of the security risk scale of the proposed phishing detection framework.

2. Method

The study is both exploratory and experimental in nature, proposing a phishing security risk framework that applies text mining and phishing simulation attacks to generate a security risk scale. The framework provides an assessment of the risk posed by the content forged in the phishing email as shown in Figure 1.

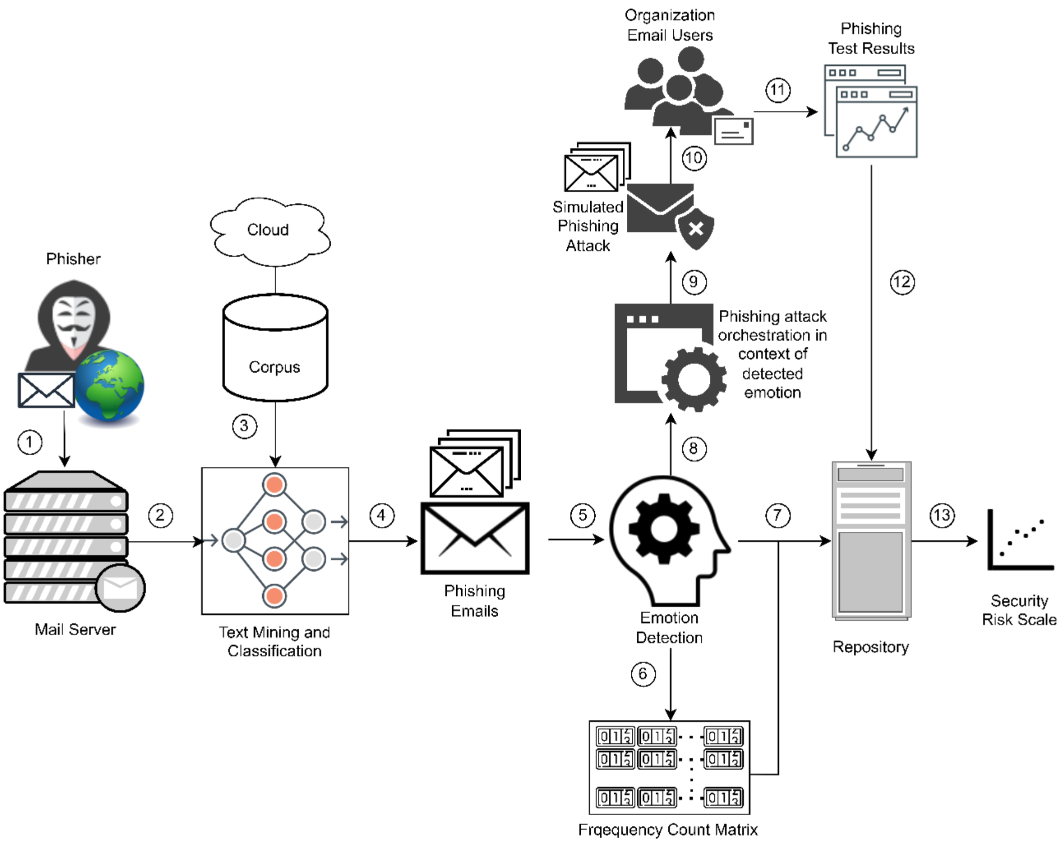


Figure 1: Email Phishing Security Risk Scale Architecture

The entire process is based on the following steps:

- Step 1: A phisher or external threat actor targets the organization with email phishing attacks that are received by the organization's mail server.
- Step 2: The inbound emails from the mail server are directed to the AI layer. Text mining is performed using natural language processing models, after an initial pre-processing of the content in the emails, to create a vectorized form of the words. Pre-processing involves sentence segmentation, tokenization, stemming, lemmatization, removal of noise, i.e., stop words ('a', 'the', 'and', etc.), special characters, and punctuation marks, dependency parsing, and part of speech (PoS) tagging. The corpus contains datasets to be used in the model's training algorithms.
- Step 3: Datasets are fed into the text mining block. The corpus is connected to available cloud services to receive new datasets.
- Step 4: ML algorithms are used to classify the vectorized words and detect if the content in the email is a phishing or not.
- Step 5: Detected phishing emails are taken in for sentiment and emotion analysis.
- Step 6: Once the emotion is detected from the contextual data, it increments its respective emotion counter in the frequency count matrix.
- Step 7: The information regarding the emotion used by the attacker and its count are stored in the repository. At this point, the frequency of a user receiving a phishing email targeting a specific emotion is

obtained from the live environment or real-world.

- Step 8: The detected emotion is fed to the phishing simulation layer.
- step 9: A phishing email campaign is orchestrated in the context of the emotion detected. A simulated phishing attack is devised and staged for launch.
- Step 10: The organization users receive test phishing emails to determine the probability of a user interacting with a phishing email triggering the emotion detected.
- Step 11: The interaction of the organization users with the orchestrated phishing email that triggers the detected emotion is recorded into results.
- Step 12: The results portraying the impact of the phishing email, or its probability of exploitation are stored into the repository.
- Step 13: The phishing security risk scale is derived from the repository data of multiple emotions.

The mean frequency of a user receiving a phishing email targeting a specific emotion is plotted against the mean probability of a user interacting with a phishing email triggering the emotion detected, on the proposed security risk matrix.

An experimental test was conducted in a bank where three separate phishing attacks were launched for social engineering. The SE techniques applied include Authority, Commitment, and Reciprocity. The click rates were measured for a timing window of three days for a single phishing campaign. The interval for each campaign was two weeks to give independence in the results.

- Campaign 1 (Authority Test): A p*hishing email pretends to be sent by the bank CEO, requesting the staff navigate to the bank's brand page via a link in the email.*
- Campaign 2 (Commitment Test): A *phishing email pretends to be from the human resources training unit and motivates the employees to take a learning course.*
- Campaign 3 (Reciprocity Test): A p*hishing email convinces bank staff to navigate to a social movement page illustrating the decent work the bank has done for the staff community, so they in turn deserve a reciprocating hand of support for the started initiative.*

The phishing test involved mail users with at least bachelor's-level education working in the banking sector. The test was carried out using the KnowBe4 phishing simulator. The probability of a mail user interacting with a phishing email was determined using a Friedman statistical test on 5-point scale nominal descriptors: *very unlikely (1), unlikely (2), not sure (3), likely (4),* and *very likely (5),* as clearly indicated in Figure 2.

The Friedman test was also used to determine if the social engineering technique used by the hacker in the phishing email has any effect on the frequency that the user will receive that phishing email. The technique was used to find out the frequency of receiving a phishing email using various forms of social engineering techniques as pointed out by:

- *Authority: humans will typically conform when an eminent authority confronts them.*
- *Commitment: the desire to work hard with effort—can allow hackers to convince a victim to follow their instructions.*
- *Contrast: email has two choices that contradict each other. If the target disagrees with one option, they may select the other.*
- *Curiosity: Someone is more likely to follow the hacker's request if they are very interested in finding out more about it.*
- *Empathy makes a victim more vulnerable to accepting the demands in the phishing email.*

- *Fear: when people are frightened, they tend to do things they do not necessarily want, so the attacker scares them in the email.*
- *A likeable hacker may act like they are someone the victim cares about to get them to perform their demands.*
- *Reciprocity: one pretends to have done a good deed, knowing people will be inclined to return the favor.*
- *Scarcity: when there is very little time or few opportunities offered, a victim may quickly agree to the phishing request.*
- *Social proof: usually, people feel better doing something if everyone else is doing it.*

Similarly, a Kruskal-Wallis H Test was used to determine if demographic factors affect the probability of a user interacting with a phishing email, for a given social engineering technique used by the hacker. To measure accuracy, measurements were evaluated using the following formula:

$$\text{Accuracy}=100\%\text{-Error Rate}$$

$$\text{Error Rate}=\frac{\text{PST Value-SRS Value}}{\text{SRS Value}}\text{x}100\%$$

where PST=Phishing Simulation Test and SRS=Security Risk Scale

3. Results

Based on the analysis of the phishing emails which emotionally manipulate victims, all ten studied techniques including Authority, Commitment, Contrast, Curiosity, Empathy, Fear, Liking, Reciprocity, Scarcity, and Social Proof were found to be the key social engineering techniques used by hackers.

The Friedman test used to determine the relationship between phishing variables and security risk, revealed a significant effect of social engineering techniques on the probability of a subject interacting with a phishing email (9, n = 100) = 52.306, p < .001, W =.058 and a significant influence on the frequency of a subject receiving a phishing email (9, N = 100) = 89.573, p < .001, W =.100. The Friedman test returned an asymptotic significance of less than 0.05 which means the probability of a subject interacting with a phishing email is affected by the social engineering techniques. The chance of a subject interacting with a phishing email provoking authority on the age range was statistically significant with (4, N = 100) = 14.172, p =.007; on the professional status, (3, N = 100) = 12.979, p =.005.

The Kruskal-Wallis H test that was performed to check if the education level of a subject and age have any effect on the probability of them clicking on a phishing link themed with the social engineering techniques returned an asymptotic significance value of less than 0.05 for the commitment technique. This means that the education level of a subject influences the probability of them clicking on a phishing link themed with the commitment phishing variable. Using a Kruskal-Wallis' H test, the probability of a subject interacting with a phishing email provoking commitment on the age range and education level was found to be (4, N = 100) = 10.378, p =.035 and (2, N = 100) = 6.166, p =.046, respectively.

Regarding the professional status of a subject, the results show that the subject influences the probability of clicking on a phishing link themed with the authority phishing variable. In simpler words, someone who is unemployed or retired would react differently to clicking a phishing link with an authority theme than someone who is employed. A Kruskal-Wallis H test was also used to check if the gender of a subject has any effect on the frequency of receiving a phishing email. The results show that the gender of the subject influences the frequency of receiving a phishing email that triggers the social proof phishing variable. Table 2 summarizes the calculation of the phishing security risk by taking the product of the frequency and probability of the subject receiving a phishing email.

Table 2. Security Risk Calculations

Social Engineering Technique	Probability of a subject interacting with a phishing email	Frequency of a subject receiving a phishing email	Phishing Security Risk Score
Curiosity	3.8	3.85	14.63
Fear	3.7	3.7	13.69
Authority	3.8	3.6	13.68
Empathy	3.6	3.6	12.96
Scarcity	3.3	3.7	12.21
Liking	3.7	3.1	11.47
Reciprocity	3.05	3.6	10.98
Social Proof	3.1	3.25	10.075
Commitment	3.4	2.75	9.35
Contrast	3.2	2.9	9.28

Figure 2 shows the derived phishing security risk scale that plots the mean values found from the phishing questionnaire survey for each social engineering technique.

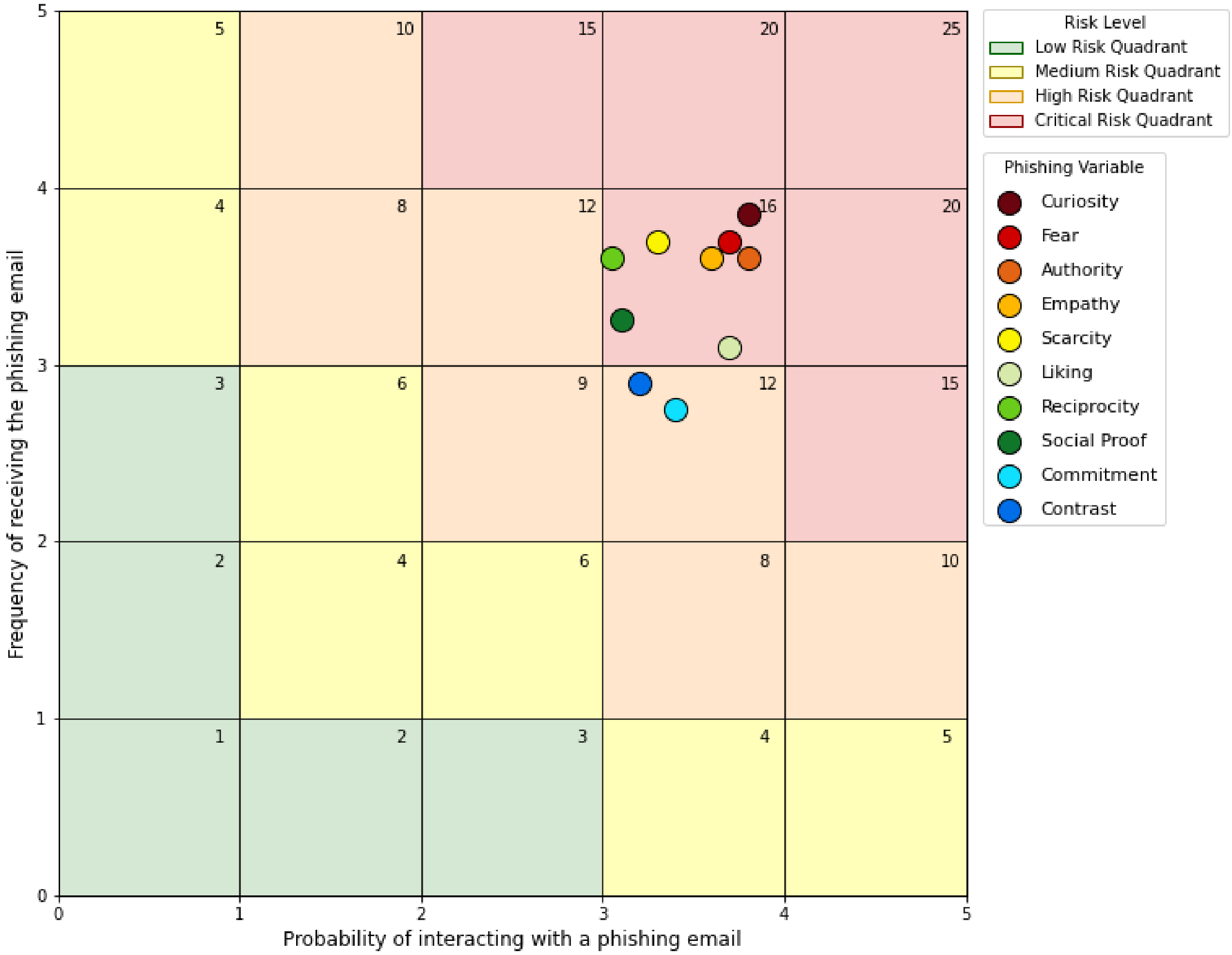


Figure 2: Phishing Security Risk Scale

Table 3 summarizes the phishing test results for the 3 phishing campaigns for the emotional triggers of authority, reciprocity, and commitment. The number of recipients, and the number phishing emails delivered, opened, clicked, and reported for each phishing social engineering technique is tabulated. The risk ratings distribution of the sampled phishing social engineering techniques, (authority, reciprocity, and commitment) in our simulated phishing attack are compared to that of the designed security risk scale.

Table 3. Phishing tests results for the sampled phishing social engineering techniques

Phishing Technique	Recipients	Delivered	Opened	Clicked	Reported
Authority	4236	4227	3213	2561	16
Reciprocity	4229	4102	1908	567	45
Commitment	4233	4094	1527	195	87

Table 4 below shows the derived risk ratings of the authority, reciprocity, and commitment social engineering techniques by taking the probability of a subject interacting with a phishing email as per the designed security risk scale. It refers to the values from Table 2 that tabulates the phishing security risk evaluation.

Table 4. Risk ratings for Authority, Reciprocity and Commitment Social Engineering Techniques as per the designed security risk scale

Social Engineering Technique	Probability of a subject interacting with a phishing email as per the designed security risk scale (%)
Authority	$\frac{3.8}{5} = 0.76$
Reciprocity	$\frac{3.05}{5} = 0.61$
Commitment	$\frac{3.4}{5} = 0.68$

Table 5 below tabulates the derived risk ratings from for Authority, Reciprocity and Commitment Social Engineering Techniques by taking the percentage of users that interacted with the phishing email corresponding to the associated phishing technique, in the simulated phishing test. It refers to the values from Table 3 that tabulates the phishing tests results for the sampled phishing social engineering techniques.

Table 5. Risk ratings for Authority, Reciprocity and Commitment Social Engineering Techniques as per the phishing simulation tests results.

Phishing Technique used in the simulated phishing test	Number of users that opened the phishing email received	Number of users that clicked on a link in the phishing email received	Percentage of users that interacted with the phishing email in the simulated phishing test (%)
Authority	3213	2561	80
Reciprocity	1908	567	30
Commitment	1527	195	13

Figure 3 below shows the distribution of risk ratings from the designed security risk scale and the distribution of risk ratings from the simulated phishing test, for the authority, reciprocity, and commitment social engineering techniques. The plot shows that the distributions are similar in nature. This implies that a relationship exists between the risk ratings of the phishing social engineering techniques derived from the designed security risk scale and the risk ratings from the simulated phishing test.

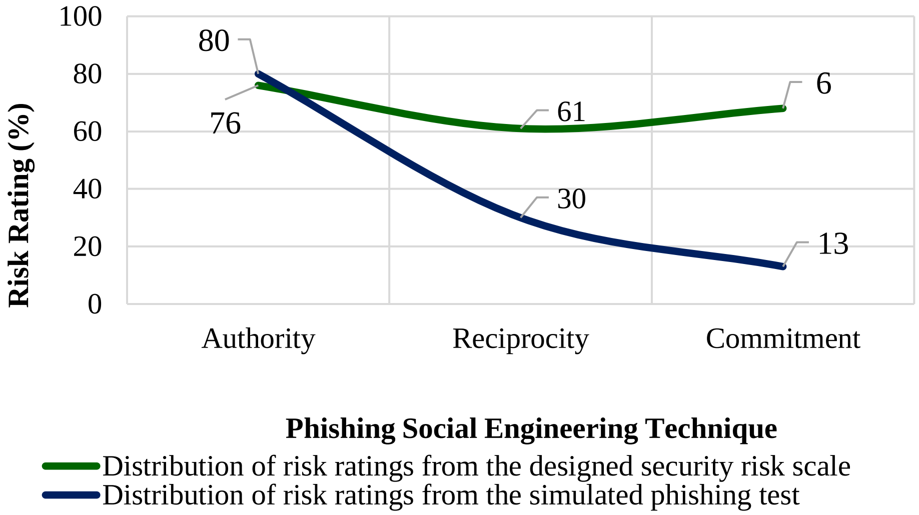


Figure 3: Comparison of the distributions of risk ratings with respect to the sampled social engineering techniques

The phishing test using the authority technique was the first test to be conducted in the series of phishing tests and had the least error (5.263%). The error was found to increase significantly in the second test, i.e., the reciprocity technique (50.820%). The test with the largest error was the final test, i.e., the commitment technique (80.882%). The increase in error through subsequent phishing tests can be justified by users gaining awareness and suspicion of the possibility of phishing attempts following the significant success of the first phishing test.

Accuracy = 100% - Error Rate

$$\text{Error Rate} = \frac{|\text{PST Value - SRS Value}|}{\text{SRS Value}} \times 100\%$$

$$\text{Error Rate (Authority)} = \frac{|80 - 76|}{76} \times 100\% = 5.263\%$$

$$\text{Error Rate (Reciprocity)} = \frac{|30 - 61|}{61} \times 100\% = 50.820\%$$

$$\text{Error Rate (Commitment)} = \frac{|13 - 68|}{68} \times 100\% = 80.882\%$$

Table 6 below shows a comparison of the risk ratings derived from the security risk scale and that from the phishing test. The error and accuracy are tabulated as well. The calculations for obtaining the error and accuracy are shown below.

Table 6: Performance measurement of the security risk scale

Phishing Technique	Probability of a subject interacting with a phishing email as per the designed security risk scale (%)	Percentage of users that interacted with the phishing email in the simulated phishing test (%)	Error (%)	Accuracy (%)
Authority	76	80	5.263	94.737
Reciprocity	61	30	51	49
Commitment	68	13	80.882	19.118

4. Discussion

If we were to ask ourselves, what follows once we can tell with satisfactory accuracy, that the email is a phishing one? Conventional measures involve blocking the email from the users' mailboxes, and the domain which the phishing email came from. Our research suggests that the phishing emails do not exhibit the same content composition. Hackers concoct the phishing emails in different ways to help them achieve their objective. Their main goal is to psychologically manipulate the mind of their victim into performing a poor security decision. We define phishing social engineering techniques as methods hackers use when trying to trick victims into surrendering to their demands. This form of social engineering is observed in the content of the phishing email. It is the context of the phishing email or more over like the voice of the hacker, or the theme, or tone of the phishing email. These techniques are emotional manipulation techniques that are variable depending on the choice of the hacker. From one angle we have observed the detection of phishing emails by reading the content using artificial intelligence and shed light on the need to distinguish the manipulative style in its content. But from another perspective, what should we do once we have identified a phishing email, and are able to classify the social engineering technique used in it? An obvious and logical answer is to prevent these phishing emails from causing damage. But how do we prevent them? We need cybersecurity controls which go hand in hand with risk management. Before we may be able to implement a control to enable security within our cyber-environment, we must have a measure of the risk posed by the threats. Our study proposes a framework that scales the security risk that results from the social engineering technique that the hacker uses in the content of the phishing email. Imagine a hacker trying to trick you by telling you that you have won 1 million dollars or the same hacker telling you that you will be taken to trial and face a lawsuit against you. Which made up situation is more likely to get you to give in and submit to the demands of the hacker? Could you say the themes made up are just the same?

Our study emphasizes that efforts should be made to evaluate risk based on the phishing email that is used by the hacker. Technical controls have proven to be far more effective in securing systems, in comparison to administrative controls. Technical controls can be implemented on a phishing email to mitigate the risk of phishing. However, to reduce the risk that evolves from the user receiving the phishing email, administrative controls would have to be put in play. Risk scales of LexisNexis® Risk Solutions (2017) and Steves et al. (2020) follow a similar technique proposed by our study, where the risk is measured based on the characteristics of the phishing email. LexisNexis® Risk Solutions (2017) designed Emailage® assesses the risk by using the email, IP address, and other available information to recognize and rate the identity. A plethora of historical and conduct details are available from the email address making the risk associated with it visible. The frequency of use and composition of emails used by hackers categorizes them into related patterns. Email addresses exhibit a similar name structure, i.e., friendly name, "@" symbol, and domain name. The name of the email may be looked up through a list of flagged, or risky emails to match against any high risk known names. The domain information may give important data such as the name of the registrar and registrant, registration age, physical address such as the street/town, or city etc. The risk profile of an email is constructed by leveraging on network intelligence supported by the mining of all good and bad characteristics of the email. The email trends may be tracked in real-time giving greater assurance in the decisions made regarding the risk rating. It is simpler for a user to discover that the email is a phishing one if there are many cues available in the email. This concur with the study by [27] which revealed that a phishing email with more premise alignment such as to match the target's work surroundings is harder to realize.

Our study proposes that the phishing detection techniques using text mining and natural language processing observed from the research of Fang et al. (2019), Olayemi (2019), Yang et al. (2019), Castillo et al. (2020), Halgaš et al. (2020), Lee et al. (2020), Mansour & A. Alenizi (2020), Verma et al. (2020), Abdelaziz et al. (2021), Ahmed et al. (2021), Bagui et al. (2021), Bountakas et al. (2021), Franchina et al. (2021), Salahdine et al. (2021), Chowdhury et al. (2022), Korkmaz et al. (2022), Noah et al. (2022), Somesha & Pais (2022), Bountakas & Xenakis (2023), and Muralidharan & Nissim (2023) detect specific classes of emotions such as Authority, Commitment, Contrast, Curiosity, Empathy, Fear, Liking, Reciprocity, Scarcity, and Social Proof. When used within our proposed phishing Email Phishing Security Risk Scale Architecture, the human emotion that the hacker is working on manipulating can be identified.

5. Conclusion and Future Work

Our research has proposed an email phishing security risk framework capable of plotting a security risk scale dynamically. The scale is based on the detection of the emotion manipulated by the hacker within the content of the phishing emails received in real time and a behavior analysis of the probable responses of users from simulated phishing tests. The social engineering techniques used by hackers in phishing emails to emotionally manipulate their victims have been investigated. A relationship exists between the social engineering technique used by the hacker in the phishing email and the probability of a user interacting with that phishing email. Likewise, there is a relationship between the social engineering technique used by the hacker in the phishing email and the frequency that the user will receive that phishing email. We found that demographic factors affect both the probability of a user interacting with a phishing email, as well as the frequency that a user will receive a phishing email. for a given social engineering technique used by the hacker. The security risk scale of our proposed phishing detection framework, had the best performance of 94.737% accuracy in measuring the risk of a social engineering technique used by a hacker in a phishing email, successfully exploiting a user. Improvements in the experimental process can be made in the future as users are social beings and once tested upon social gatherings and conversations leak out the plot of the test making them appear possibly more secure than they would rather be. As the hacker will always hit by surprise, future work can involve scenarios where measurements are only by surprise and not repeated for the same population unless excessive time has passed for them to forget.

ACKNOWLEDGEMENT

We thank the referred bank for giving access to test mail servers for real time experimental test.

CONTRIBUTIONS OF CO-AUTHORS

First Author	[ORCID: 0000-0002-1036-1745]	Conceived the idea and wrote the paper
Second Author	[ORCID: 0000-0002-4419-6004]	Conceived the idea and wrote the paper

REFERENCES

[1] M. Rosenthal, *Must-Know Phishing Statistics:* Updated 2021, Tessian, 2021

[2] A. M. Salim, *Assessment of Mobile Money Transaction Frauds and Consequences Confronting Zanzibar Telecom Service Providers*, Asian J. Econ. Bus. Account., p. 16–31, 2022

[3] L. Msaki, *Assessment of the Challenges on E-Commerce Engagement: The Case of Selected Traditional Retailers*, 2019

[4] G. S. Oreku, *A Rule-based Approach for Resolving Cybercrime in Financial Institutions : The Tanzania case*, Huria J., p. 93–114, 2020

[5] I. S. Mambina, J. D. Ndibwile, and K. F. Michael, *Classifying Swahili Smishing Attacks for Mobile Money Users: A Machine-Learning Approach*, IEEE Access, p. 83061–83074, 2022

[6] E. Bishel, *Africa , China , and the Development of Digital Infrastructure Governance : A Case Study of Ghana and Tanzania*, Vienna, 2022

[7] R. C. T. Panga, J. Marwa, and J. D. Ndibwile, *A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania*, J. Cybersecurity Priv., p. 466–489, 2022

[8] TZ-CERT, *Tanzania Computer Emergency Response Team (TZ-CERT) Weekly Honeypot Reports*, 2022

[9] J. Lissah, A. Kirobo, and M. M. Govella, *Adoption of Cashless Economy in the World: A Review*, IOSR J. Econ. Financ., p. 37–48, 2022

[10] A. N. Ntigwigwa, *Factors that contribute to Cybercrime in Mobile Money Services in Tanzania: A Case of Kibaha Town*, 2019

[11] E. Mwabukojo, *Technology Transfer Strategy : A Neglected Approach in Tanzania*, Munich Pers. RePEc Arch., p. 59, 2020

[12] Z. Yang, C. Qiao, W. Kan, and J. Qiu, *Phishing Email Detection Based on Hybrid Features, in IOP Conference Series: Earth and Environmental Science*, 2019

[13] Y. Fang, C. Zhang, C. Huang, L. Liu, and Y. Yang, *Phishing Email Detection Using Improved RCNN Model With Multilevel Vectors and Attention Mechanism*, IEEE Access, p. 56329–56340, 2019

[14] L. Halgaš, I. Agrafiotis, and J. R. C. Nurse, *Catching the Phish: Detecting Phishing Attacks Using Recurrent Neural Networks (RNNs)*, p. 219–233, 2020

[15] O. Olayemi, *Text Analysis and Machine Learning Approach to Phished Email Detection*, Int. J. Comput. Appl., p. 11–16, 2019

[16] E. Castillo, S. Dhaduvai, P. Liu, K.-S. Thakur, A. Dalton, and T. Strzalkowski, *Email Threat Detection Using Distinct Neural Network Approaches*, Proc. First Int. Work. Soc. Threat. Online Conversations Underst. Manag., p. 48–55, 2020

[17] Y. Lee, J. Saxe, and R. Harang, *CATBERT: Context-Aware Tiny BERT for Detecting Social Engineering Emails*, 2020

[18] P. Bountakas, K. Koutroumpouchos, and C. Xenakis, *A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection*, ACM Int. Conf. Proceeding Ser., 2021

[19] L. Franchina, S. Ferracci, and F. Palmaro, *Detecting phishing e-mails using text mining and features analysis*, CEUR Workshop Proc., p. 106–119, 2021

[20] F. Salahdine, Z. El Mrabet, and N. Kaabouch, *Phishing Attacks Detection: A Machine Learning-Based Approach*, in 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), p. 0250–0255, 2021

[21] D. S. Ahmed, H. A. A. A. Allah, and I. Abbas, *Effective Phishing Emails Detection Method*, Turkish J. Comput. Math. Educ., p. 4898–4904, 2021

[22] N. Noah, A. Tayachew, S. Ryan, and S. Das, *PhisherCop: Developing an NLP-Based Automated Tool for Phishing Detection*, SAGE Journals, 2022

[23] Affinity IT Security Services, *Measuring Phishing Risk*, 2019

[24] R. Yang, K. Zheng, B. Wu, D. Li, Z. Wang, and X. Wang, *Predicting User Susceptibility to Phishing Based on Multidimensional Features*, Comput. Intell. Neurosci., 2022

[25] KnowBe4®, *Virtual Risk Officer (VRO) and Risk Score Guide*, 2022

[26] Tessian®, *Tessian Human Layer Risk Hub*, 2021

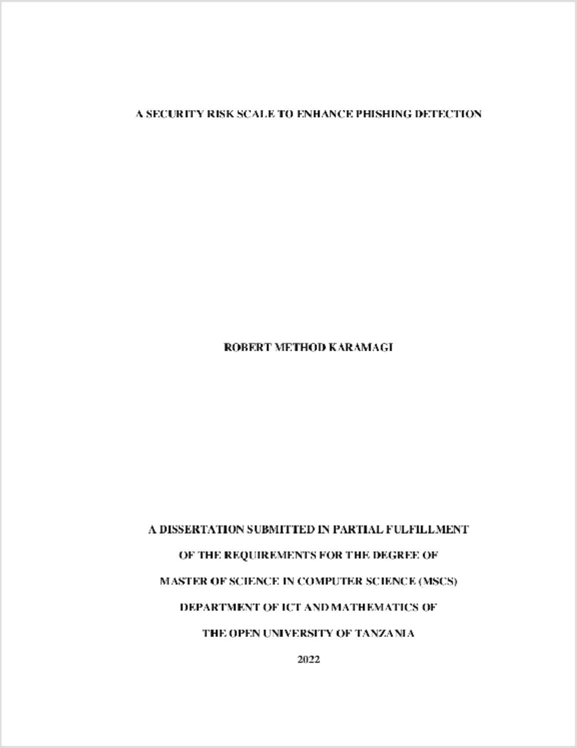
[27] M. Steves, K. Greene, and M. Theofanos, *Categorizing human phishing difficulty: a Phish Scale*, J. Cybersecurity, p. 1–16, 2020

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Robert Karamagi
Assignment title:	Master of Science in Computer Science (MSc CS)
Submission title:	A Security Risk Scale to Enhance Phishing Detection
File name:	8_-_Dissertation_-_Final_Paper_-_Robert_Karamagi_PG201902...
File size:	6.51M
Page count:	285
Word count:	46,570
Character count:	265,015
Submission date:	09-Aug-2023 05:06AM (UTC+1000)
Submission ID:	2143192655



A SECURITY RISK SCALE TO ENHANCE PHISHING DETECTION

ROBERT METHOD KARAMAGI

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN COMPUTER SCIENCE (MSCS)
DEPARTMENT OF ICT AND MATHEMATICS OF
THE OPEN UNIVERSITY OF TANZANIA
2022

A Security Risk Scale to Enhance Phishing Detection

ORIGINALITY REPORT

14%	11%	6%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repository.out.ac.tz Internet Source	2%
2	Robert Karamagi. "A Review of Factors Affecting the Effectiveness of Phishing", Computer and Information Science, 2021 Publication	1%
3	www.researchgate.net Internet Source	1%
4	acikbilim.yok.gov.tr Internet Source	1%
5	Submitted to Universiti Putra Malaysia Student Paper	<1%
6	yapireland.ie Internet Source	<1%
7	Submitted to Aspen University Student Paper	<1%
8	www.mdpi.com Internet Source	<1%
	www.surveymonkey.com	

9	Internet Source	<1 %
10	ebin.pub Internet Source	<1 %
11	Submitted to Ryerson University Student Paper	<1 %
12	cgi.di.uoa.gr Internet Source	<1 %
13	www.abacademies.org Internet Source	<1 %
14	Submitted to Napier University Student Paper	<1 %
15	www.smjournal.rs Internet Source	<1 %
16	scholar.mzumbe.ac.tz Internet Source	<1 %
17	Zhang, Xiaorui, Lizhu Liu, Jinfeng Li, Ling Weng, and Weiwei Cui. "Preparation of low contact angle TiO2–polyester “core-shell” emulsions employing ultrasonic irradiation", Materials Letters, 2014. Publication	<1 %
18	Submitted to University of Sunderland Student Paper	<1 %
	www.eriesjournal.com	

19	Internet Source	<1 %
20	journals.nauss.edu.sa Internet Source	<1 %
21	pdfs.semanticscholar.org Internet Source	<1 %
22	vital.seals.ac.za:8080 Internet Source	<1 %
23	Panagiotis Bountakas, Christos Xenakis. "HELPHED: Hybrid Ensemble Learning PHishing Email Detection", Journal of Network and Computer Applications, 2022 Publication	<1 %
24	Forestiere, Carolyn. "Beginning Research in Political Science", Oxford University Press Publication	<1 %
25	link.springer.com Internet Source	<1 %
26	Trivikram Muralidharan, Nir Nissim. "Improving malicious email detection through novel designated deep-learning architectures utilizing entire email", Neural Networks, 2022 Publication	<1 %
27	docplayer.net Internet Source	<1 %

28	pureadmin.uhi.ac.uk Internet Source	<1 %
29	Submitted to Federal University of Technology Student Paper	<1 %
30	repositorium.sdum.uminho.pt Internet Source	<1 %
31	s3-ap-southeast-1.amazonaws.com Internet Source	<1 %
32	Submitted to Regenesys Business School Student Paper	<1 %
33	answers.yahoo.com Internet Source	<1 %
34	assets.researchsquare.com Internet Source	<1 %
35	researchspace.ukzn.ac.za Internet Source	<1 %
36	www.repository.cam.ac.uk Internet Source	<1 %
37	iopscience.iop.org Internet Source	<1 %
38	www.hindawi.com Internet Source	<1 %
39	www.tnsroindia.org.in Internet Source	<1 %

40	repository.nwu.ac.za Internet Source	<1%
41	Submitted to University of Hertfordshire Student Paper	<1%
42	scholar.smu.edu Internet Source	<1%
43	stax.strath.ac.uk Internet Source	<1%
44	Submitted to Pennsylvania College of Technology Student Paper	<1%
45	Submitted to University of Johannsburg Student Paper	<1%
46	Submitted to Webster University Student Paper	<1%
47	academic.oup.com Internet Source	<1%
48	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1%
49	boost.bolster.ai Internet Source	<1%
50	www.icuadelaide.com.au Internet Source	<1%

51	www.policygroup.org Internet Source	<1 %
52	aranne5.bgu.ac.il Internet Source	<1 %
53	hdl.handle.net Internet Source	<1 %
54	www.asjp.cerist.dz Internet Source	<1 %
55	"Communication and Intelligent Systems", Springer Science and Business Media LLC, 2023 Publication	<1 %
56	Ali Selamat, Nguyet Quang Do, Ondrej Krejcar. "chapter 11 Detecting Phishing URLs With Word Embedding and Deep Learning", IGI Global, 2023 Publication	<1 %
57	Fatima Salahdine, Zakaria El Mrabet, Naima Kaabouch. "Phishing Attacks Detection A Machine Learning-Based Approach", 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2021 Publication	<1 %
58	thescipub.com Internet Source	<1 %

59	www.ajol.info Internet Source	<1 %
60	www.scitepress.org Internet Source	<1 %
61	Submitted to Middlesex University Student Paper	<1 %
62	Submitted to Technological University Dublin Student Paper	<1 %
63	Submitted to The French - Vietnamese Center for Management Education Student Paper	<1 %
64	Submitted to Universiti Kebangsaan Malaysia Student Paper	<1 %
65	projekter.aau.dk Internet Source	<1 %
66	spada.uns.ac.id Internet Source	<1 %
67	Diksha Goel, Ankit Kumar Jain. "Mobile phishing attacks and defence mechanisms: State of art and open research challenges", Computers & Security, 2018 Publication	<1 %
68	Submitted to Nottingham Trent University Student Paper	<1 %
	dokumen.pub	

69	Internet Source	<1 %
70	ir.nust.na Internet Source	<1 %
71	papers.academic-conferences.org Internet Source	<1 %
72	tojqih.net Internet Source	<1 %
73	usir.salford.ac.uk Internet Source	<1 %
74	scirp.org Internet Source	<1 %
75	waikato.researchgateway.ac.nz Internet Source	<1 %
76	www.computerscijournal.org Internet Source	<1 %
77	www.cureus.com Internet Source	<1 %
78	www.dtic.mil Internet Source	<1 %
79	www.truvantis.com Internet Source	<1 %
80	Submitted to Glasgow Caledonian University Student Paper	<1 %

81	Submitted to IAIN Padangsidimpuan Student Paper	<1 %
82	avesis.yildiz.edu.tr Internet Source	<1 %
83	doctorpenguin.com Internet Source	<1 %
84	ir.mu.ac.ke:8080 Internet Source	<1 %
85	islamicmarkets.com Internet Source	<1 %
86	methods-sagepub-com-spjimrlibrary.knimbus.com Internet Source	<1 %
87	scg.sdsu.edu Internet Source	<1 %
88	Submitted to Gazi University Student Paper	<1 %
89	Submitted to Ghana Technology University College Student Paper	<1 %
90	Submitted to Higher Education Commission Pakistan Student Paper	<1 %
91	Submitted to Swinburne University of Technology	<1 %

	Student Paper	
92	dergipark.org.tr Internet Source	<1 %
93	fhtm.uitm.edu.my Internet Source	<1 %
94	www.researchsquare.com Internet Source	<1 %
95	Submitted to Multimedia University Student Paper	<1 %
96	Submitted to University of Greenwich Student Paper	<1 %
97	Xinya Fan, Xilian Ouyang, Zheping Zhou, Ziling Zhang, Xu Zhu, Yibo Liao, Zimin Wei, Beidou Xi, Lin Tang. "A highly selective self-powered sensor based on the upconversion nanoparticles/CdS nanospheres for chlorpyrifos detection", Biosensors and Bioelectronics, 2023 Publication	<1 %
98	Yan Ge, Li Lu, Xinyue Cui, Zhe Chen, Weina Qu. "How personal characteristics impact phishing susceptibility: The mediating role of mail processing", Applied Ergonomics, 2021 Publication	<1 %
99	business.starkvilledailynews.com Internet Source	<1 %

100	um.dk Internet Source	<1 %
101	Submitted to University of Hull Student Paper	<1 %
102	rules.dnv.com Internet Source	<1 %
103	venturessahara.medium.com Internet Source	<1 %
104	www.oer.unn.edu.ng Internet Source	<1 %
105	www.pure.ed.ac.uk Internet Source	<1 %
106	Submitted to Callaghan Campus Student Paper	<1 %
107	Submitted to De Montfort University Student Paper	<1 %
108	EVANS, MARTIN G.. "ON THE ASYMMETRY OF g", Psychological Reports, 1999. Publication	<1 %
109	Somesha M., Alwyn R. Pais. "Classification of Phishing Email Using Word Embedding and Machine Learning Techniques", Journal of Cyber Security and Mobility, 2022 Publication	<1 %
	apps.dtic.mil	

110	Internet Source	<1 %
111	publications.polymtl.ca Internet Source	<1 %
112	spectrum.library.concordia.ca Internet Source	<1 %
113	A V Nikonorov, R V Skidanov, V V Evdokimova, M V Petrov, A P Alekseyev, S A Bibikov, N L Kazanskiy. "Deep learning-based image reconstruction for multi-aperture diffractive lens", Journal of Physics: Conference Series, 2019 Publication	<1 %
114	Peter G. W. Smulders, Frans J. N. Nijhuis. "The Job Demands-Job Control Model and absence behaviour: Results of a 3-year longitudinal study", Work & Stress, 1999 Publication	<1 %
115	Submitted to University of Bristol Student Paper	<1 %
116	carnegieendowment.org Internet Source	<1 %
117	deepai.org Internet Source	<1 %
118	docs.google.com Internet Source	<1 %

119	jurnal.ugm.ac.id Internet Source	<1 %
120	ntnuopen.ntnu.no Internet Source	<1 %
121	passwordmanagers.co Internet Source	<1 %
122	ppsfip.ppj.unp.ac.id Internet Source	<1 %
123	www.omicsdi.org Internet Source	<1 %
124	www.semanticscholar.org Internet Source	<1 %
125	International Journal of Event and Festival Management, Volume 4, Issue 2 (2013-06-08) Publication	<1 %
126	Norman T. Sheehan, Han - Up Park, Richard C. Powers, Sarah Keyes. "Overseeing the dynamic materiality of ESG risks: The board's role", Journal of Applied Corporate Finance, 2023 Publication	<1 %
127	Submitted to Noroff University College Student Paper	<1 %
128	Submitted to The Hong Kong Polytechnic University Student Paper	<1 %

129	academic-accelerator.com Internet Source	<1 %
130	bolster.ai Internet Source	<1 %
131	certnexus.com Internet Source	<1 %
132	essay.utwente.nl Internet Source	<1 %
133	irjaes.com Internet Source	<1 %
134	journal.unnes.ac.id Internet Source	<1 %
135	journals.iium.edu.my Internet Source	<1 %
136	journals.udsm.ac.tz Internet Source	<1 %
137	peerj.com Internet Source	<1 %
138	sersc.org Internet Source	<1 %
139	www.commonwealthofnations.org Internet Source	<1 %
140	www.diva-portal.org Internet Source	<1 %

141	www.science.gov Internet Source	<1 %
142	www.theinterscholar.org Internet Source	<1 %
143	Submitted to Brunel University Student Paper	<1 %
144	Patricio Hidalga García-Bermejo. "Development and validation of a multi-scale and multi-physics methodology for the safety analysis of fast transients in Light Water Reactors", Universitat Politecnica de Valencia, 2020 Publication	<1 %
145	Qinglin Qi, Zhan Wang, Yijia Xu, Yong Fang, Changhui Wang. "Enhancing Phishing Email Detection through Ensemble Learning and Undersampling", Applied Sciences, 2023 Publication	<1 %
146	Sugeng Santoso, Winda Widyanty, R. Nurhidajat, Muhammad Ramadhani Marfatah et al. "System dynamics modeling for developing an agrotourism-creative economy in the framework of the village innovation system", Frontiers in Environmental Science, 2022 Publication	<1 %

147	Submitted to University of California, Los Angeles Student Paper	<1 %
148	doc-developpement-durable.org Internet Source	<1 %
149	dspace.bracu.ac.bd Internet Source	<1 %
150	git.076.ne.jp Internet Source	<1 %
151	hal.univ-lorraine.fr Internet Source	<1 %
152	ijsrset.com Internet Source	<1 %
153	repositorium.uminho.pt Internet Source	<1 %
154	repository.wit.ie Internet Source	<1 %
155	researchspace.csir.co.za Internet Source	<1 %
156	scholarworks.waldenu.edu Internet Source	<1 %
157	slideplayer.com Internet Source	<1 %
158	www.corpuspublishers.com	

	Internet Source	<1%
159	www.scilit.net Internet Source	<1%
160	www.springerprofessional.de Internet Source	<1%
161	"Towards new e-Infrastructure and e-Services for Developing Countries", Springer Science and Business Media LLC, 2023 Publication	<1%
162	Johan B. Nilsson, Anders Eriksson,. "Clinical Outcome after Successful Coronary Angioplasty: Impact of Intracoronary Stent Implantation", Scandinavian Cardiovascular Journal, 2009 Publication	<1%
163	K. Greyson, M. Kissaka, D. Haule, V. Ndume. "Asynch-NET: Footstep for Always-On e-Services in the Rural Areas of Developing Countries: Case Study-Tanzania", Fourth IEEE International Workshop on Technology for Education in Developing Countries (TEDC'06), 2006 Publication	<1%
164	Submitted to La Porte High School Student Paper	<1%

165	Oluwole Nurudeen Omonijo, Zhang Yunsheng. "The role of Chinese products demand and supply in reducing market cost and improving technological performance: Empirical evidence from South Africa, Nigeria, and Egypt", Cogent Business & Management, 2023 Publication	<1 %
166	Submitted to Southeast Community College Student Paper	<1 %
167	aoemj.org Internet Source	<1 %
168	commons.erau.edu Internet Source	<1 %
169	commons.wmu.se Internet Source	<1 %
170	dokument.pub Internet Source	<1 %
171	moam.info Internet Source	<1 %
172	ouci.dntb.gov.ua Internet Source	<1 %
173	pure.tue.nl Internet Source	<1 %
174	repository.uel.ac.uk Internet Source	<1 %

175	ro.ecu.edu.au Internet Source	<1 %
176	scholar.archive.org Internet Source	<1 %
177	site.iugaza.edu.ps Internet Source	<1 %
178	vdoc.pub Internet Source	<1 %
179	www.atlantis-press.com Internet Source	<1 %
180	www.jatit.org Internet Source	<1 %
181	www.suaire.sua.ac.tz Internet Source	<1 %
182	www.tandfonline.com Internet Source	<1 %
183	www.thinkmind.org Internet Source	<1 %
184	www.unicef-irc.org Internet Source	<1 %
185	"Emerging Trends in Intelligent Computing and Informatics", Springer Science and Business Media LLC, 2020 Publication	<1 %

186	"Information and Communications Security", Springer Science and Business Media LLC, 2020 Publication	<1 %
187	Assumpta Ezugwu, Elochukwu Ukwandu, Celestine Ugwu, Modesta Ezema, Comfort Olebara, Juliana Ndunagu, Lizzy Ofusori, Uchenna Ome. "Password-Based Authentication and The Experiences of End Users", Scientific African, 2023 Publication	<1 %
188	aquila.usm.edu Internet Source	<1 %
189	Hayes, Nicky. "Doing Psychological Research, 2e", Doing Psychological Research, 2e, 2021 Publication	<1 %
190	Naheem Noah, Abebe Tayachew, Stuart Ryan, Sanchari Das. " : Developing an NLP-Based Automated Tool for Phishing Detection ", Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2022 Publication	<1 %
191	Said Salloum, Tarek Gaber, Sunil Vadera, Khaled Sharan. "A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques", IEEE Access, 2022 Publication	<1 %

192	arxiv.org Internet Source	<1 %
193	Submitted to University of Winchester Student Paper	<1 %
194	postgradproblems.com Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

OUT/DPGS/E3

THE OPEN UNIVERSITY OF TANZANIA
DIRECTORATE OF POSTGRADUATE STUDIES

P.O. Box 23409 Fax: 255-22-2668759
Dar es Salaam, Tanzania,
http://www.out.ac.tz

Tel: 255-22-2666752/2668445 ext.100
Fax: 255-22-2668759,
E-mail: drpc@out.ac.tz

PLAGIARISM REPORT FORM FOR POSTGRADUATE STUDENTS

(To Be Filled By Student Pursuing Masters By Coursework, By Thesis and PhD Students)

A: STUDENT INFORMATION

First Name.......ROBERT.......... Middle Name.......METHOD.........Last....KARAMAGI..........

Faculty.......FSTES.............Department........ICT.................Reg. No.........................

Degree:.......MSc CS.................. Model of Learning (ODL, [✓ Evening] or Executive, Thesis)

Correspondence Address:......15 MATITU STREET..

Telephone No.........0762087332.........Mobile No...

E-mail.......robertokaramagi@gmail.com..

B: DETAILS OF DISSERTATION/THESIS

Title of the Dissertation/Thesis.......A SECURITY RISK SCALE TO ENHANCE PHISHING DETECTION.

Name of the Supervisor(s)

(i) ....DR. SAID ALLY..

(ii) ....

C: PLAGIARISM ASSESSMENT
(To be completed by the supervisor)

PLAGIARISM TEST

Passed (i.e. 30% or below) ☑

Not accepted (i.e. above 30%) ☐

This is to certify that the Dissertation/Thesis submitted by ....Robert Karamagi....with the following details has been processed using plagiarism software and it is acceptable/No~~t Acceptable~~ for submission as a thesis / Dissertation.

Name of supervisor: ....DR. SAID ALLY...

Signature..........................Date.......19/09/2022.............................

C: PLAGIARISM ASSESSMENT
(To be completed by HoD or the Faculty postgraduate coordinator)

I hereby declare that I have checked this document for plagiarism with Turnitin software, and it has returned ....% of plagiarism in the document

Name.. Signature.......................................

Date..

Note: This form need to be inserted in the last page of Thesis and Dissertation

: Supervisor has to attach plagiarism results sheet generated from Turntin software