

**A HUMAN FIREWALL SIMULATOR FOR ENHANCING SECURITY
AWARENESS AGAINST BUSINESS EMAIL COMPROMISE**

BY

OKUMU DANIEL ONYANGO

**THIS THESIS IS SUBMITTED TO THE BOARD OF POST GRADUATE STUDIES IN PARTIAL
FULFILLMENT OF THE MASTER OF SCIENCE DEGREE IN INFORMATION TECHNOLOGY
SECURITY AND AUDIT OF JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND
TECHNOLOGY.**

Copyright

All rights are reserved. No part of this thesis or information herein may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the permission of the author or Jaramogi Oginga Odinga University of Science and Technology.

©2023

Declaration

I declare that the ideas described herein are my original work and have never been submitted to any institution for an award of a Master's Degree in Information Technology Security.

Daniel Onyango Okumu

REG_NO: I152/4262/2016

Signature.....

Date:

This research thesis has been submitted with approval from the following supervisors:

1. Dr. Richard Omollo

Department of Computer Science and Software Engineering

School of Informatics and Innovative Systems

Date.....

Signature.....

2. Prof. George Raburu

Department of Computer Science and Software Engineering

School of Informatics and Innovative Systems

Date.....

Signature.....

Dedication

I dedicate this research work to my family, wife, and children, and to the entire MSc. Information Technology Security & Audit Class of 2016.

Acknowledgment

I would like to acknowledge Jaramogi Oginga Odinga University of Science and Technology through the School of Informatics and Innovative Systems (SIIS) for the varied knowledge and skills availed, which were very instrumental for this research.

Lots of credit goes to my supervisors, Dr. Richard Omollo and Prof. George Raburu, for the guidance they offered in this research. Their inputs are greatly appreciated, especially the insight and the different views that led to the success. I will not forget to mention Dr. Amos Omamo, whose input gave direction to this research.

Many thanks to God and to my friends and well-wishers who provided indirect input to this thesis.

Abstract

Cybercriminals exploit the weakest link in an organization's security, targeting CEOs or CFOs through business email compromise, or CEO fraud. These attacks primarily involve social engineering, tricking employees into committing security-compromising acts. Cybercriminals often pose as senior executives or vendors, transferring money, publishing private data, or installing malware. The impact of these attacks is significant, causing businesses financial setbacks, reputational damage, and legal repercussions. The attacks can lead to CEO fraud, email account compromise, and other security-compromising acts. Despite the importance of technology defenses, human involvement remains crucial in the success or failure of attacks like Business Email Compromise (BEC), which exploits human weaknesses and poses a significant threat to enterprises. The research introduces the Human Firewall Simulator, an interactive training tool designed to enhance security awareness by allowing staff to detect and respond to (BEC) threats. This dynamic platform allows employees to interact with real-world scenarios and engage in active learning beyond traditional classrooms. The simulator is the methodological approach that offers immediate feedback and guidance for correct decision-making, promoting an iterative learning process and extending beyond conventional awareness training by addressing the need for contextualized, customized, and adaptable approaches. Participants are tested on identifying fraudulent emails and suspicious behaviors through scenarios resembling real-world BEC tactics. The simulator uses data collection and analysis to study participant behaviors, identifying susceptibility patterns and progress over time. This data-driven insight improves training modules and targeted interventions, enhancing security awareness programs' effectiveness. A simulated assessment of email security attacks revealed a low success level in pre-assessment due to lack of awareness and training for employees. However, post-assessment showed a high success level, as employees turned into human firewalls took proper actions, such as flagging and not clicking malicious links. This suggests that training and awareness programs can significantly improve email security in organizations. The organization should update its policies to accommodate and reinforce rules for employees to ensure that the tool is used regularly and actions taken by users are not deemed a threat to organizational email security. In the end, the Human Firewall Simulator fosters a vigilant culture within enterprises. Participants leave with a better understanding of threats, stronger reaction skills, and a sense of empowerment regarding BEC attack defense. In order to reduce the growing threats posed by BEC in the digital era, this research pioneers a unique paradigm in cybersecurity education that embraces experiential learning, personalization, and adaptive training approaches.

Table of Contents

Copyright	i
Declaration	ii
Dedication	iii
Acknowledgment	iv
Abstract	v
List of Figures	x
List of Tables	xi
List of abbreviations.....	xii
Definitions of terms	xiii
CHAPTER ONE: INTRODUCTION.....	1
1.0 Introduction.....	1
1.1 Background of the study	1
1.2 Statement of the Problem.....	3
1.3 Research Gap	4
1.4 Main objective.....	4
1.5 Specific objectives	4
1.6 Research questions.....	4
1.7 Significance of the study.....	4
1.8 Scope of the Study	5
1.9 Limitation.....	5
1.10 Contribution to the theory and practice.....	5
1.11. Summary of the Background of the Study.....	6
CHAPTER TWO: LITERATURE REVIEW	8
2.0 Introduction.....	8
2.1 Business Email Compromise	8
2.1.1 Steps for mitigating Business Email Compromise (BEC)	8
2.2 Social Engineering Challenges	9
2.2.1 Common social engineering techniques include	10
2.3 Techniques in Phishing	10
2.3.1 Insights from a targeted phishing	11
2.3.2 What is the prevalence of social engineering as a cyberattack?.....	11
2.4 How Hackers Steal Email address and Passwords.....	11
2.4.1 Phishing Attacks.....	11

2.4.2 Mass Theft.....	12
2.4.3 Wi-Fi Traffic Monitoring Attacks.....	12
2.4.4 Brute Force Attacks.....	12
2.4.5 Network sniffing attacks	12
2.5 Examples of Email attacks mitigated through BEC scams.....	12
2.5.1 A thread discussing a real CEO fraud attack.....	15
2.6 Actions to effectively defend against social engineering attacks	17
2.6.1 Social engineering awareness training for employees:	17
2.6.2 Simulations of social engineering attacks:	17
2.6.3 Conduct an Open-Source Intelligence analysis on the organization:.....	18
2.7 Human Firewall.....	18
2.7.1 Defensive First Line	19
2.7.2 Employees Motivation and Ability	19
2.7.4. Link the Desired Behaviors to Necessary Knowledge.....	19
2.8 Theory Supporting Human Firewall Creation	19
2.8.1 Social Cognitive Theory (SCT).....	19
2.9 Human Security Layer	20
2.9.1 Need for Human Security Layer	20
2.9.2 People always break the rules	20
2.9.3 People can be tricked.....	21
2.10 Existing email security solutions Available.....	21
2.10.1 Spam Filters:.....	21
2.10.2 Anti-Phishing Solutions:	21
2.10.3 Email Authentication Protocols (SPF, DKIM, DMARC):.....	21
2.10.4 Employee Training and Awareness Programs:	21
2.10.5 AI-Driven Threat Intelligence:	22
2.10.6 Behavioral Analysis and Anomaly Detection:	22
2.10.7 Encryption and Data Loss Prevention (DLP):.....	22
2.10.8 Continuous Monitoring and Incident Response:	22
2.11 Design of the current security model	23
2.12 How Human firewall works.....	24

2.12.1 What makes a human firewall?	24
2.12.1 Human Firewall components.....	25
2.13 Summary of Literature Review	26
CHAPTER THREE: RESEARCH METHODOLOGY	27
3.0 Introduction.....	27
3.1 Methodology	27
3.2 Simulation	27
3.2.1How users are selected to participate in the simulated Training.....	28
3.2.1The simulation human firewall has two basic steps:	29
3.3 Instruments.....	30
3.4 Ethical considerations	31
3.5 Summary of Research methodology	31
CHAPTER FOUR: DEVELOPMENT OF HUMAN FIREWALL SIMULATOR.....	32
4.0. Introduction.....	32
4.1 Model for Human Firewall Simulator.....	32
4.2. Variables that plays a role in the effectiveness of the simulator.....	33
4.2.1 Independent Variables:.....	33
4.2.2 Dependent Variables:	34
4.3 Human Firewall Simulator Development	34
4.3.1 Sequence diagram.....	34
4.3.2 Admin sequence diagram	35
4.3.3 Client sequence diagram	35
4.3.4 Use-case Diagram.....	36
4.3.5 Activity Diagram.....	37
4.4 Testing and Validation (Results) and Analysis.....	38
4.4.1 Admin Module	39
4.4.2 Client Module.....	40
4.4.3 Test Set up (Administrator Module)	42
4.4.4 Invite (Admin Module)	46
4.4.5 Administrator Module (Analysis)	47
4.5 Summary of Chapter Four.....	49
CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS	50

5.0 Introduction.....	50
5.1 Summary	50
5.1.1 Summary of the objectives	53
5.2 Conclusions.....	53
5.2.1 key assertions that drive this research to its effectiveness in improving an organization's cybersecurity posture.....	54
5.3 Recommendations.....	55
5.3.1 Model integrating Human Firewall with existing email security.....	56
5.4 Future Research Work	58
5.5 Summary of Chapter Five	58
REFERENCES	60
APPENDICES	64
APPENDIX 1: Communication from XYZ University webmaster.....	64
APPENDIX 2: Coding for the program.....	65
APPENDIX 3: DOCUMENTATION AND MANUAL	72
APPENDIX 4: Letter from Dean SIIS.....	73
APPENDIX 5: Ethical Review Letter.....	74
APPENDIX 6: Board of Post Graduate Letters	75

List of Figures

<i>Figure 2.1: BEC scam example 1 (Sabi, 2019)</i>	13
<i>Figure 2.2: BEC scam example 2 (Abbasi, 2018)</i>	13
<i>Figure 2.3: BEC scam example 3 (Cloudmark, 2016)</i>	14
<i>Figure 2.5: Email Message Flow Courtesy of (Cisco, Email Security Deployment Guide, 2010)</i> ..	24
<i>Figure 2.6: Human Firewall components (Gatner, 2017)</i>	25
<i>Figure 4.1: Model for Human Firewall simulated (Researcher, 2023)</i>	32
<i>Figure 4.2: Admin sequence diagram (Researcher, 2023)</i>	35
<i>Figure 4.3: Client sequence diagram (Researcher, 2023)</i>	36
<i>Figure 4.4: Use-case Diagram (Researcher, 2023)</i>	36
<i>Figure 4.5: Activity Diagram (Researcher, 2023)</i>	37
<i>Figure 4.6: Admin-Module (Researcher, 2023)</i>	39
<i>Figure 4.7: Login Interface (Researcher, 2023)</i>	39
<i>Figure 4.8: client side Interface (Researcher, 2023)</i>	40
<i>Figure 4.9: Tutorial (Client-side Module) (Researcher, 2023)</i>	41
<i>Figure 4.10: Assessment (Client-side Module) (Researcher, 2023)</i>	42
<i>Figure 4.11: Setting up test (Admin Module) (Researcher, 2023)</i>	43
<i>Figure 4.12: Create a similar web site displayed under your domain (Researcher, 2023)</i>	44
<i>Figure 4.13: Preview the appearance of the phishing web page that we created to look like the original one</i>	45
<i>Figure 4.14: Admin can upload CSV file and invite the members to take test. (Researcher, 2023)</i> ..	46
<i>Figure 4.15: Enter SMTP server and administrator's email credentials to invite members. (Researcher, 2023)</i>	46
<i>Figure 4.16: Analysis/ Results (Researcher, 2023)</i>	48
<i>Figure 5.1: Secure email flow integrated with human firewall (Researcher, 2023)</i>	56

List of Tables

Table 2.1: comparing the strengths and weaknesses of existing email security solutions in solving social engineering attacks:.....22

List of abbreviations

AIG	American International Group, Inc. (AIG)
API	Application Programming Interface
BEC	Business Email Compromise
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFO	Chief Finance Officer
CSV	Comma Separated Values
FBI	Federal Bureau of Investigations
HR/PR	Human Resource/Public Relations
IBAN	International Bank Account Number
ICT	Information and Communications Technology
IRIS	International Recruitment Integrity System
IT	Information Technology
LMS	Learning Management System
SMTP	Simple Mail Transfer Protocol
URL	Universal Resource Locator
NACOSTI	National Commission for Science, Technology and Innovation
SCT	Social Cognitive Theory

Definitions of terms

Artificial intelligence is the computerized simulation of human processes, for example, the acquisition of information and rules for using information, the reasoning using rules to reach rough conclusions or final conclusions, and self-correction.

Business email compromise is among the most financially destructive online crimes. It takes advantage of the fact that so many of us use email for both personal and professional transactions.

Corporate Email: Corporate emails are those email addresses that usually include the business name or brand of a company or business. This is obtained thanks to the fact that the company previously obtained the necessary internet domain to generate the different email addresses it requires.

Cybersecurity is the protection of connected systems, including hardware, software, and data, from cyberattacks. In a computer, security includes cybersecurity and physical security, both of which are used by companies to protect against unauthorized access to data centers and other computerized systems.

Firewall is a network security device that regulates network traffic according to established security rules. A firewall is a device that separates a trusted internal network from an untrustworthy external network, such as the Internet.

Fraud is a willing deception to secure an unfair or unlawful gain or to deprive a victim of a legal right. Hackers refer to this attempt to corrupt digital devices such as computers, cell phones, tablets, and even entire networks.

Hacker: A person with highly developed technical abilities and an in-depth understanding of computer networks, systems, and software is referred to as a hacker.

Human firewall: refers to the users, staff, or members of an organization who follow good practices in order to prevent attacks or data breaches by reporting any suspicious activities, i.e., by flagging or deleting suspicious mail or ignoring them.

Machine learning is an artificial intelligence application that provides systems without explicit programming with the ability to learn and grow naturally through experience.

Malware is any program harmful to a computer and the user. Malicious software includes computer viruses, worms, Trojans, and spyware.

Penetration testing, also known as penetration testing or ethical hacking, consists of testing a computer system or a web application to find vulnerabilities that an attacker could exploit.

Phishing is the fraudulent attempt to obtain information such as usernames, passwords, and credit card details by pretending to be a trustworthy entity in a communication.

Simulator is a program or device that, like a flight simulator, generates a virtual representation of a real-life environment for the purpose of training or experimentation.

Social engineering refers to the psychological manipulation of people so that they perform actions or disclose confidential information. This differs from social engineering within the sciences, which does not contain the disclosure of confidential information.

Spammers: the use of messaging systems for unsolicited messages, in particular advertising, and then sending messages to multiple people on the site.

Spoofing is a situation where one person impersonates another in order to gain an illegitimate advantage.

Webinar is a seminar or other presentation that takes place over the Internet, allowing participants from different places to see and hear the presenter, ask questions, and sometimes answer surveys.

CHAPTER ONE: INTRODUCTION

1.0 Introduction

This chapter introduces knowledge in this research area, giving a basic idea about this study area to enable the reader to understand the need for the study.

1.1 Background of the study

The bad guys are quite inventive; they pose as organization leaders, demand documents, or ask payroll staff to deliver money to bank accounts. Due to the penetration of business email, often known as CEO fraud, the FBI estimates that their efforts were worth approximately \$12 billion. Only layered controls and non-technical security can effectively defend against these kinds of phishing assaults. (FBI, 2016). A significant factor in the rise in cyberattacks is the Internet's immense development, commercial connectedness, and network, as well as the vulnerabilities that follow from these. Over 1 billion emails sent over Gmail were examined by Google Research, and the findings are really intriguing: Phishing assaults are 6.2 times more likely to target corporate emails than personal ones, and rogue accounts are 4.3 times more likely, yet spam is only 0.4 times more likely. (Sjouwerman, 2017). Which indicates that the phishing approach is now the attack's primary focus. Attacks continue despite the defenses in place against commercial email fraud, particularly those using social engineering (91% of all cyberattacks start with phishing). (Gatner, 2017). Some of the most frequent and worst errors that employees make to create broken links are giving sensitive information to people without authenticating their identity and access privileges and allowing a stranger within an organization without authorization, which is an example of why there is a need for a human firewall. Sensitive information with a monetary value can be found in corporate inboxes. Phishing targets businesses engaged in banking and entertainment the most. Attackers appear to target organizations based on their size, kind, and activities. (Akamai, 2017). Building a human firewall may sound very similar to team-building and motivational activities that help employees understand how important they are to the success of the company. You are essential to business security! (Proteck, 2017). With phishing attacks, companies cannot deploy security technology quickly enough for remote cybercriminals, which is why the ultimate protection is a combination of security technology and a human (Comtech, 2017). While computer security technology tries to spam and block most emails, cybercriminals use social engineering to target unsuspecting recipients. Criminals send spoofed emails with links that use existing business or person names to extract sensitive information, such as computer login details or personal information. These emails containing malicious links often bypass the usual security measures and are therefore difficult to block. Combining the human firewall with the already existing strategies is a more balanced and proactive approach to preventing BEC fraud, and if companies fail to adopt this strategy, then cyber criminals have already won. Despite very strict data compliance standards, tremendous technological innovation, and increased corporate investment, data breaches are escalating (Sadler, 2021). Previously, security solutions focused on the machine layer of an organization: network points and devices, which primarily provided blunt protection. The most popular security tools in recent days have

focused on perimeter protection by managing terminals and fixing vulnerabilities in the system. But cybercriminals no longer target infrastructure, but humans.

It is the distracted user who clicks on an email attachment or the impatient customer who fills out information in a pixel-perfect phishing page that is vulnerable. It is becoming increasingly evident that regulators and users need to be at the center of strategy when building an approach to cybersecurity in the age of highly sophisticated attacks. (Mark Guntrip, 2020).

Phishing emails contain more contextual information to increase the chances that a recipient will be victimized (Jason, 2012). For example, attackers can include information important to the personal or business interests of the recipient in order to increase the chances of the recipient responding. Such attacks are more and more deployed by criminals who aim to commit financial crimes against specific targets, corporate spies who steal intellectual property and sensitive information, and hacktivists who aim to draw attention to their cause. (APWG, 2014). This solution goes beyond IT; it requires the cultivation of a fresh mindset among employees around cybersecurity, motivated by more than facts and fear, by continually raising awareness and instilling secure actions and decisions at the forefront of the company culture. There are three key elements for building an effective human firewall: making people care about cybersecurity, building awareness and knowledge, and measuring and monitoring (Schablik et al, 2017). A human firewall involves educating individuals within an organization on how to handle their emails, that is, when to click on a link or open an attachment and when to remove it. Education should involve all levels of the organization, not just treat safety training as a compliance-based "checkbox" (Orlando, 2018). There is a lot of debate about the value of safety training. We train users not to click links in unexpected emails, but they do so even after hours of training and publicizing the risks. Spear phishing in particular is a risk that is difficult to explain for many end users due to the nature of well-designed emails and social engineering. Educating users is normally a one-time effort or is rarely directly related to the experience of users in their inbox, thus minimizing human error and preempting human nature (Marcos, 2014). Hackers and spammers exploit human nature through social engineering to gain their trust, for example, by manipulating users to click malicious links in e-mails that appear to be from legitimate ones. Phishing is another attack method that tricks the user into clicking the link. Since some staff may invariably click unsafe links, an important extra layer to protect users who accidentally or by choice do not follow the training and guidance is required. So, when you can get a firewall to protect your network and endpoint detection and response to protect your devices, how do you then protect your organization from such staff? The security of the human layer is the ultimate requirement. meaning there is a lack of inclusivity of behavioral approaches into the already existing security mechanisms. This is why a combination of human firewalls and others, including sophisticated mail gateways, is the best defense to deal with these threats. (Nabila, 2019)

The background study for the development of a human firewall simulator to enhance security awareness against business email compromise (BEC) attacks focuses on the evolving threat landscape of BEC attacks, the limitations of traditional security awareness training, and the potential benefits of experiential learning and simulation-based training methods. BEC attacks represent a formidable and rapidly growing threat to

organizations on a global scale, causing significant financial losses and reputational damage and exploiting human vulnerabilities within organizations. These attacks are characterized by their adept use of social engineering tactics, where cybercriminals manipulate human psychology and organizational dynamics to achieve their malicious goals. The BEC threat landscape highlights the severity and complexity of the threat landscape, including financial impact and reputational damage, social engineering techniques, manipulation of employees, unauthorized actions and information disclosure, impersonation of high-ranking executives, and exploitation of relationships with trusted vendors or partners. Detection challenges are also significant, as BEC attacks are crafted to evade traditional security measures. Human vulnerabilities in cybersecurity are increasingly recognized as a critical factor in the cybersecurity landscape. Cyber attackers skillfully exploit psychological biases and cognitive weaknesses inherent in human behavior to achieve their malicious objectives. These vulnerabilities include exploiting psychological biases, cognitive weaknesses, phishing and social engineering tactics, human error and lack of awareness, insider threats, and the complexity of cyber threats. (Datta, 2021) Addressing human vulnerabilities requires a multifaceted approach, including comprehensive cybersecurity education and training, to equip employees with the knowledge and skills to recognize and respond effectively to various cyber threats. In conclusion, the role of human vulnerabilities in cybersecurity cannot be underestimated. As attackers capitalize on psychological biases, cognitive weaknesses, and the potential for human error, organizations must recognize the importance of education, training, and fostering a culture of cybersecurity awareness among their employees. By understanding these vulnerabilities, organizations can implement strategies to mitigate risks and strengthen their overall security posture. (Acquaye, 2020)

1.2 Statement of the Problem

Organizations face a growing and complex threat from business email compromise in today's interconnected digital landscape (BEC). BEC attacks prey on human weaknesses, employing social engineering strategies to trick staff into disclosing private information, sending money, or carrying out malicious deeds. BEC persists as a problem despite advances in cybersecurity because of its unpredictable strategies and the frequently unintentional participation of employees.

Conventional security awareness training is necessary, but it frequently falls short of enabling staff to recognize and effectively counter the constantly changing BEC attack landscape. The development of the critical skills necessary to recognize increasingly complex phishing attempts and fraudulent activities is hampered by static presentations, theoretical content, and a lack of immersive experiences. To protect their sensitive data, financial assets, and reputations, organizations must close this critical gap in their security strategies.

Additionally, many awareness campaigns are generic in design and do not take into account the variety of organizations, industries, and attack methods that BEC attackers use. It becomes difficult for employees to apply theoretical information to real-world situations due to a lack of customization and context-specific training.

A transformative solution is needed to enhance security awareness against BEC attacks. The research problem addressed by this study is the growing cyberattacks targeting businesses through corporate email and social engineering methods that result in massive financial losses for companies worldwide. Employees are the most vulnerable line of defense and should be part of the messaging system in case attackers pass technical filters. This is the reason why there is a need for organizations to create a "human firewall" as soon as possible because hackers are getting away with millions of shillings (Sjouwerman, 2017). By designing, developing, and evaluating a Human Firewall Simulator using experiential learning, customization, and data-driven insights. Employees are empowered to become effective defenders against BEC attacks, addressing the shortcomings of traditional security awareness training and mitigating risks in the digital age.

1.3 Research Gap

The gap that exists in email security is the lack of inclusivity of behavioral approaches (solutions to social engineering attacks) into the already existing security mechanisms to enhance email security design.

1.4 Main objective

The main objective of this study was to develop a human firewall simulator for enhancing security awareness as the last line of defense in email communication against business email compromise fraud.

1.5 Specific objectives

In order to achieve the main objective of this research study, the following specific objectives were considered:

- i. To identify various social engineering techniques used to compromise corporate email
- ii. To investigate the current solutions for email security in an organization.
- iii. To develop human firewall simulator for enhancing security against business email compromise.
- iv. To test the developed human firewall simulator.

1.6 Research questions

- i. What are the social engineering techniques used to compromise victims in a corporate email?
- ii. What are the current email security solutions applicable in an organization?
- iii. How can a human firewall simulator be developed?
- iv. How can the developed human firewall simulator be tested?

1.7 Significance of the study

The study aims to develop and implement a Human Firewall Simulator to enhance security awareness against Business Email Compromise (BEC) threats. The approach focuses on tackling a persistent threat, incorporating

active learning and experiential training, closing the gap between theory and practice, providing a safe environment for participants to practice identifying and responding to BEC threats, and providing data-driven insights. This approach contributes to building a stronger human firewall, enhancing organizational security posture, and introducing an innovative cybersecurity education approach. By empowering employees to identify and thwart BEC attempts, organizations can potentially avoid substantial financial losses and reputational damage. The study's significance lies in its potential to revolutionize the way organizations educate their workforce about BEC threats and equip them with a powerful strategy to counter the ongoing and evolving challenge of BEC.

1.8 Scope of the Study

In order to improve security awareness against business email compromise (BEC), this study focuses on the design, development, implementation, and evaluation of a human firewall simulator. The study is restricted to the simulator's design, development, and testing in safe situations. It does not cover the whole range of cybersecurity solutions. The objective is to advance our understanding of effective security awareness training and its role in reducing the dangers brought on by BEC assaults.

1.9 Limitation

Human firewall simulators can be valuable tools for enhancing corporate email security, but they have several limitations. These include simplified scenario simulation, a lack of emotional engagement, limited contextual information, a lack of real-time feedback, individual skill variation, and a lack of behavioral change measurement. Simulated training scenarios may not accurately reflect the complexity and diversity of real-world attacks, making employees less prepared to detect and respond to sophisticated or novel threats. Additionally, simulators may not provide real-time guidance during actual attacks, making it harder for employees to recognize subtle signs of phishing or fraud. Additionally, individual skill variations may not be adequately addressed by simulators, as they typically provide a standardized training experience for all participants. Finally, lack of behavioral change measurement can make it challenging to evaluate the effectiveness of training programs. To overcome these limitations, organizations should consider complementing human firewall simulators with other training methods, such as ongoing education, interactive workshops, and real-world case studies. Regular assessments and continuous monitoring can help identify areas for improvement and provide targeted training interventions.

1.10 Contribution to the theory and practice

The concept of a "human firewall simulator" for enhancing security awareness against business email compromise (BEC) involves creating a simulated environment where individuals can learn and practice recognizing and responding to potential BEC attacks. This approach has both theoretical and practical contributions to make to the field of cybersecurity.

Human Firewall Simulator contributes to the theoretical understanding of human behavior in cybersecurity and offers practical benefits by enhancing security awareness, improving incident response, and mitigating the risk of BEC attacks. (Macris, 2011).

1.10.1 Contributions to Theory

Behavioral Understanding: The simulator contributes to our understanding of human behavior in the context of cybersecurity. By simulating real-world BEC scenarios, researchers can observe and analyze how individuals react to different types of attacks. This knowledge can help refine existing theories and models related to cybersecurity behavior.

Learning and Decision-Making Processes: The simulator allows researchers to study the learning and decision-making processes involved in recognizing and responding to BEC attacks. By analyzing participants' actions and choices during the simulation, researchers can gain insights into the cognitive processes underlying effective cybersecurity practices.

Human Factors in Cybersecurity: The simulator sheds light on the role of human factors in cybersecurity. It can help identify vulnerabilities, biases, and cognitive limitations that make individuals susceptible to BEC attacks. This understanding can inform the development of more effective training programs and security measures.

1.10.2 Contributions to Practice

Security Awareness Training: The Human Firewall Simulator provides a practical tool for organizations to train their employees in recognizing and mitigating BEC attacks. It offers a safe environment to learn and practice responding to simulated attacks, helping employees develop a heightened sense of security awareness.

Phishing and Social Engineering Defense: BEC attacks often involve phishing and social engineering techniques. The simulator enables individuals to experience realistic phishing attempts and social engineering tactics, helping them build the skills to identify and resist such attacks in real-world situations.

Incident Response Preparation: By exposing participants to various BEC attack scenarios, the simulator helps organizations prepare their incident response teams. It allows them to practice detecting and mitigating attacks, improving their readiness to respond effectively when a real BEC incident occurs.

Risk Mitigation and Prevention: The simulator assists organizations in reducing the risk of successful BEC attacks by fostering a security-conscious culture. By training employees to be vigilant and proactive, organizations can strengthen their defenses and prevent financial losses associated with BEC incidents.

1.11. Summary of the Background of the Study

Businesses are at risk from the threat of business email compromise (BEC), as attackers pretend to be respected staff in order to trick workers into doing activities that jeopardize security. A staff that is aware of security issues and has strong technical defenses is required to meet this challenge. Human error continues to be a major contributor to successful BEC attacks, underscoring the necessity of fostering an environment where

employees are more security-conscious. As a proactive measure to strengthen an organization's security posture, the idea of a "human firewall" develops. To improve employees' security awareness and their capacity to recognize possible BEC threats, the Human Firewall Simulator was created. Employees can obtain practical experience in identifying and reacting to phishing, social engineering, and other forms of cybercrime by recreating real-world BEC incidents in a controlled setting. imitation-based actions. The simulator offers a secure environment where workers can make mistakes and learn from them without endangering the firm. The Human Firewall Simulator's key features include interactive learning modules, decision-based learning, phishing simulation, progress tracking and reporting, customization, and ongoing learning. Realistic scenarios based on previous attacks are another highlight. Organizations can considerably lessen their susceptibility to BEC attacks by equipping workers with the information and abilities to recognize and thwart efforts. The Human Firewall Simulator is ready to adjust as technology and strategies change, ensuring that employees continue to be the first line of defense against BEC and other social engineering threats.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This chapter focuses on similar work done by other researchers in the past and in the literature. It gives an overview of the research area, allowing the researcher to identify gaps that form the basis of this research.

2.1 Business Email Compromise

Despite the email security practices many organizations have implemented, hackers still manage to get into corporate email, mostly through social engineering attacks.

Fraud by compromise of business emails consists of checking or impersonating the account of a trusted user targeting companies involved in international transfers for the purpose of hijacking payments to an account controlled by the attacker (Berninger, 2018).

These attacks, mostly based on phishing and social engineering, attract cybercriminals because of their relative simplicity. In most cases, BEC fraud involves little or no technical knowledge, malware, or special tools because it is mostly mitigated through social engineering attacks. CEO frauds would likely continue to evolve as the FBI warns that the fraud has cost about \$3.1 billion to businesses and corporations (Hernedy, 2016). For this reason, money is becoming the biggest motivation for the attackers to continue exploiting BEC attacks.

2.1.1 Steps for mitigating Business Email Compromise (BEC)

Step 1: Identifying the business targeted for the attack.

Step 2: Exploring the attack by utilizing engineering tactics to exploit the corporate users through luring and convincing the target of the legitimacy of the transaction.

Step 3: Exchanging the wrong bank account details with the unsuspecting victim.

Step 4: Executing a financial transfer to the dubious account controlled by attackers The more employees an organization hires; the more exposure it gets to digital attackers. This is because it takes only one employee to click on this scam email and let the sensitive data be exposed to the hackers.

A big example is the Anthem Breach, which affected about 80 million people, and when we look at Target, this organization faced a tremendous financial loss of \$162 million (Marianne et al, 2017). This mournful event also happened when a vendor received a phishing email exposing the personal information of an employee to the hacker. While technology also proves to be fruitful to some extent, employees are always the first line of defense. It is the employees who take care of all the machinery and equipment and keep it updated and maintained. Thus, if one wants to improve the security conditions of an organization, the training of employees should be a high priority. Phishing can be a risk that quickly grows in the cyber world and costs web clients billions of dollars each year. It is an illegal movement that employs a group of social innovators to bring together sensitive data from the web. The recognizable evidence of phishing strategies can be found

in different communication strategies like email, instant messages, pop-up messages, or at the web page level. During the period, a number of articles were distributed with procedures and strategies, but it took a long time to distinguish all of them and provide a full understanding. This research presents a hypothetical proof from the IRC (International Rescue Committee) for this risk in an orderly fashion. While it is commonly believed that the phishing attack is to create indistinguishable messages or sites to deceive the web client, this assumption was not used to assess this risk.

2.2 Social Engineering Challenges

It is not only the network configuration but also the well-meaning employees that could be the gateway for hackers (Winder, 2018). Social engineering scams are on the rise and hard to spot, with cybercriminals targeting specific services and users with tailored communications to give the impression they come from a senior manager, a supplier, or a candidate for a job. Social engineering malicious attacks are on the increase and go well beyond just targeting the financial sector. While some organizations are developing employee awareness coaching, requesting penetration tests, or using one of the two, these preventative measures have limitations. "Is security focused on the wrong problem?" (Johnson, 2014).

The problem of social engineering has evolved in recent times at an incredible rate. Until the end of the last century, social engineering was an advanced but ordinary means of attacking dedicated systems, and is it today a methodology common in cybercrime and cyberterrorism? The level of complexity of the attacks, taking advantage of humans, is incredibly high, and often the human layer is the catalyst for subsequent technological attacks (Frumento, 2018).

Phishing emails mainly use social engineering to get the target to respond to decoy messages. (Samani, 2015), but little research has been done on the impact of social engineering. The term "social engineering" refers to the psychological manipulation of people in order to get them to reveal information or commit undesired actions. (Mitnick et al, 2002). Cialdini focuses on three principles: social proof, scarcity, and authority. According to Cialdini, many people tend to comply with requests once they see that others already have them. Emails showing that they have previously been accepted by others are likely to be more persuasive in a phishing environment. Rarity is founded on the premise that most people have just a few unique or limited items. (Cialdini, 2007) As a result, emails claiming that an offer is only accessible for a short time are more likely to impact individuals. People would swiftly comply with a request that appeared to come from a respected authority figure, according to the concept of authority. As a result, an email from the organization's CEO should be more effective than a request from lower-level management. According to a recent study of phishing emails sent between 2013 and December 2013, authority was the most commonly utilized social engineering approach, followed by scarcity, notably in emails asking for account information.

Social engineering techniques are manipulative tactics used by malicious actors to deceive and exploit individuals, often for the purpose of gaining unauthorized access to sensitive information, systems, or

resources. These techniques rely on exploiting human psychology and behavior rather than technical vulnerabilities.

2.2.1 Common social engineering techniques include

- 1. Phishing:** Sending fraudulent emails or messages that appear to be from a legitimate source, enticing recipients to click on malicious links, provide sensitive information, or download malware.
- 2. Spear Phishing:** A targeted form of phishing where attackers tailor their messages to specific individuals or organizations, making them appear more convincing and personalized.
- 3. Pretexting:** Creating a fabricated scenario or pretext to trick individuals into revealing sensitive information or performing certain actions.
- 4. Baiting:** Placing infected physical or digital media (e.g., infected USB drives or fake software downloads) in public areas, hoping individuals will take the bait and unknowingly introduce malware into their systems.
- 5. Quid Pro Quo:** Offering something of value (e.g., free software, support) in exchange for sensitive information, login credentials, or access to a system.
- 6. Tailgating/Piggybacking:** Gaining unauthorized physical access to a restricted area by following an authorized person through access points.
- 7. Impersonation:** Pretending to be someone else, such as a trusted colleague, IT personnel, or customer support representative, to trick individuals into providing information or access.
- 8. Watering Hole Attacks:** Targeting websites frequently visited by a specific group or organization to infect their systems with malware.
- 9. Reverse Social Engineering:** Convincing individuals that the attacker needs their help or expertise to gain access to sensitive information or systems.
- 10. Pharming:** Redirecting website traffic to fraudulent websites by tampering with DNS settings or using malware.
- 11. Tailored Malicious Content:** Using information from social media or other sources to create personalized and convincing messages to deceive targets.
- 12. Elicitation:** Extracting sensitive information through casual conversations or seemingly innocent questions.

Social engineering attacks can be highly effective because they exploit human trust, curiosity, fear, and willingness to help. To defend against social engineering, individuals and organizations should prioritize cybersecurity awareness training, implement strong access controls, and remain vigilant against suspicious communications or requests.

2.3 Techniques in Phishing

Phishing is a rapidly growing threat in the cyber world, causing billions of dollars in damage yearly to Internet users (Shaikh, Shabut, & Hossain, 2016). It's an illegal movement that uses a bunch of social and technological

innovations to collect sensitive data online. The recognizable proof of phishing strategies can be found in different communication strategies, such as mail, instant messages, and contextual or web page-level messages. There have been a number of inquiries about items distributed with various procedures, but they have failed to identify all the dangers to the arrangement. The Research Simulator attempts to assess this crime, examine research perspectives and approaches, and also investigate gaps, thereby attempting to generate phishing attention to stimulate thinking and feedback. actions to improve cybersecurity and gain the trust of business users.

2.3.1 Insights from a targeted phishing

Using highly targeted emails, many leaders fell prey to social engineering attacks known as "spear phishing." Social engineers trick victims into performing unintentional acts by posing as actors. User training with results indicating an individual could increase training effectiveness, hence the potential that organizational training can lead to increased overall spear phishing, even for those who are not directly trained. Despite these promising results, the sensitivity of individuals to highly targeted spear phishing remains a concern for practitioners and researchers. (Shaikh, Shabut, & Hossain, 2016)

2.3.2 What is the prevalence of social engineering as a cyberattack?

According to the newest statistics on the threat environment provided by the European Union Agency for Cybersecurity, social media is now the most widely used attack vector. In order to begin or execute an attack, threat actors prefer to attack humans first rather than security networks and systems.

Indeed, as technology advances and security measures become more difficult to breach, human psychology has stayed constant throughout the millennia, making it easier to attack. Because the stimulus-response effect in human vulnerabilities is constant, these flaws are always successful. Employees are frequently undertrained in social attacks, making it difficult for them to recognize and respond to them. Provoke a vulnerability in the organization that can be exploited (ENISA, 2021).

2.4 How Hackers Steal Email address and Passwords

Hackers frequently steal passwords using various techniques and, more generally, phishing, where they send an official-looking email that later directs the recipient to a fake website.

Once the victim enters a name and a password on the fake site, the hacker recovers the password. The following are the various techniques used in harvesting user names and passwords:

2.4.1 Phishing Attacks

Tab Nabbing: In this technique, a computer hacker sends an official-looking email that directs a victim to a website or fake form. The victim enters a password on the site, which the hacker can then access (Tschabitscher, 2018). A hacker sends an email to someone, indicating the recipient's email password is weak and needs to be replaced. The email would then direct the victim to a fraudulent page that may look exactly

like the one they are mimicking. When the user clicks on the link and arrives on the page, he enters his e-mail address and his password, probably never suspecting that something is wrong. When entering data into the form, the hacker gets both the email address and the password.

A hacker would then log in as a legitimate user and use it to commit fraud.

2.4.1.1 Key Logger Attacks:

This happens when you receive this questionable email, "click on it," then click on a very nice attachment without suspicion, and a JavaScript code is injected into the browser. Every word typed, together with the usernames and passwords, is recorded and given to the hacker without your knowledge (LeClaire, 2006).

2.4.2 Mass Theft

Over 60% of users share their username and password across all of their accounts (Paganini, 2013). Hackers utilize software to collect usernames and passwords from tens of thousands of websites until one is found. After that, they have access to people's accounts and data. If you use the same username and password for all of your accounts, you're exposing yourself to a huge risk.

However, it is nearly impossible to remember all of the complex passwords, so some individuals simply write them down, which defeats the purpose. Others simply use the same password for all of their accounts.

2.4.3 Wi-Fi Traffic Monitoring Attacks

This is where a simple application, downloaded free of charge from the Internet, monitors all traffic on a public Wi-Fi network. Once the username and password have been entered, the software notifies them and the hacker intercepts information.

The username and password have been hacked.

2.4.4 Brute Force Attacks

Most passwords are straightforward and should be guessed after a number of tries."123456" is still the most common password on the planet. (Smith, 2015). Forgetting the password that we used on an account and trying all the passwords we have used in the last years is a common experience. Hackers use tools that can crack passwords by simply entering multiple passwords repeatedly until they are decrypted; these tools can easily be downloaded for free. (Nguyen, 2015)

2.4.5 Network sniffing attacks

This attack involves sniffing passwords on the network especially where https is not enforced. This method also gives out configuration details for example services running, versions, Ip addresses, which would aid phishing attacks.

2.5 Examples of Email attacks mitigated through BEC scams

The examples below indicate the various ways the attackers, under the pretext that they are the CEOs, lure the finance officers into wiring funds to dubious accounts.

Figures 2.1, 2.2, and 2.3 below indicate the various ways the attackers, on the pretext that they are the CEOs, lure the finance officers into wiring funds to dubious accounts. This is a well-organized fraud trend that attackers use with the help of corporate emails to appear like it's coming from a legitimate source.

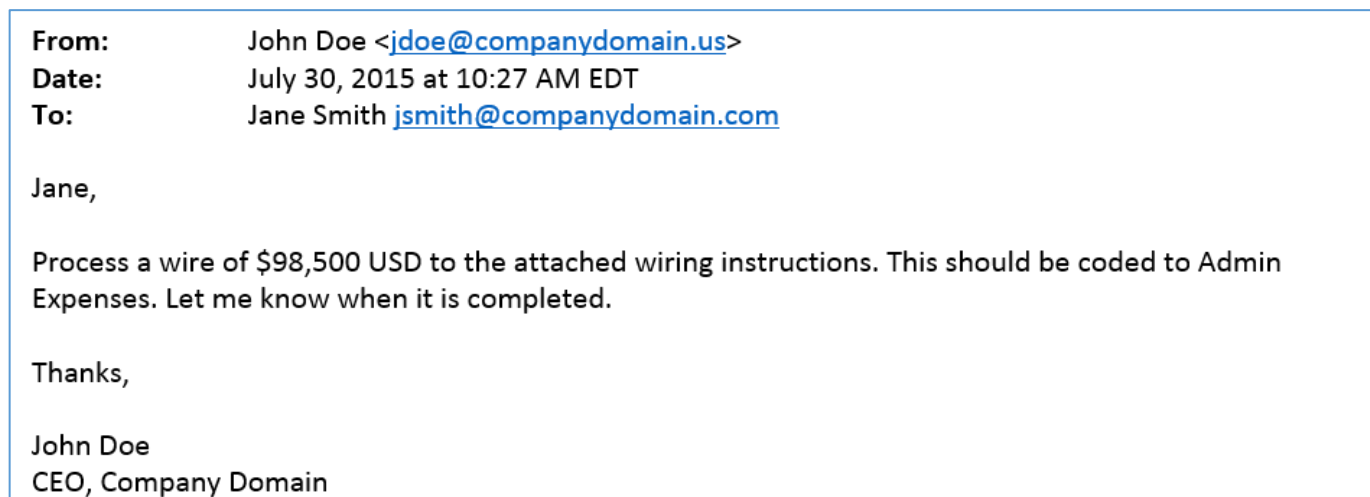


Figure 2.1: BEC scam example 1 (Sabi, 2019)

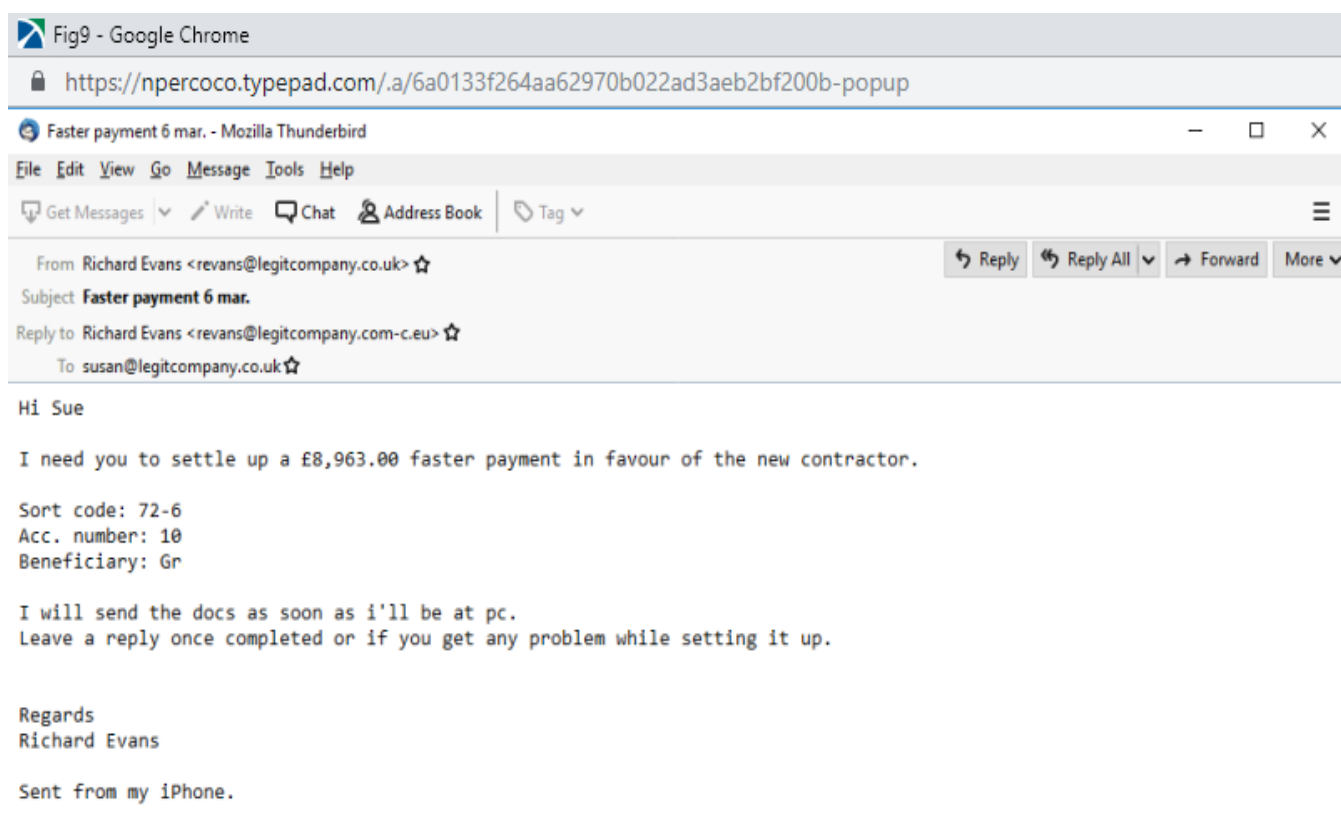


Figure 2.2: BEC scam example 2 (Abbasi, 2018)

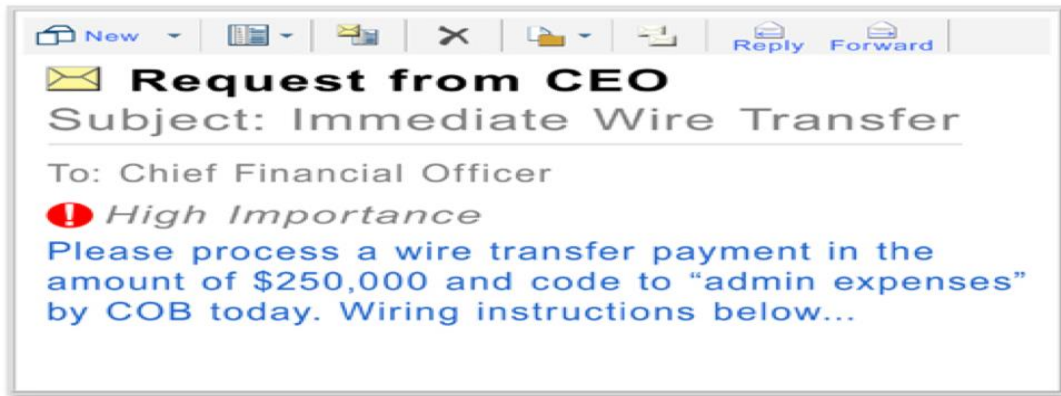


Figure 2.3: BEC scam example 3 (Cloudmark, 2016)

Example 4: Communication from XYZ University

The webmaster of XYZ University warned staff of fake emails in the cooperation email. This is a measure that cannot fully ensure that the employees follow the security procedures. Success cannot be measured in this kind of attempt.. *See Appendix 1*

2.5.1 A thread discussing a real CEO fraud attack

The conversation reproduced below (see Figure 2.4) actually occurred in 2017 between a CEO scammer and the victim successfully scammed, although the names and credentials have been changed (Kaplan, 2018).

Email Thread of an Actual CEO Fraud Attack

From: John Smith
Sent: Monday, 13 November 2017 11:27 AM
To: Susan Brown
Subject: Urgent Attention|

Are you available to handle an international payment this morning?
Have one pending; let me know when to send bank details.

Regards
John Smith
Sent from my iPhone

On Mon, Nov 13, 2017 at 1:33 PM,
Susan Brown wrote:

Hi John,
Sorry was caught up with a project - I'm here now - can I still help?

Susan Brown
Director

On Mon, Nov 13, 2017 at 4:29 PM,
John Smith wrote:

Can you still handle this right now? was very busy earlier.

Regards
John Smith
Sent from my iPhone

On Mon, Nov 13, 2017 at 5:48 PM,
John Smith wrote:

Yes it seem to be a very busy day. The amount is for \$30,120 i am guessing it is very late already for the transfer or can you still get it done today?

Regards
John Smith
Sent from my iPhone

On Mon, Nov 13, 2017 at 6:50 AM,
Susan Brown wrote:

Hi John,
Is it set up ready to go in PC banking? I can't see it there to authorise under international?
Cheers,

Susan Brown

On Mon, Nov 13, 2017 at 5:56 PM,
John Smith wrote:

Oh ok, please find a way around it, my day is really tied. Can i send you the bank details today still?
Can the payment still go out?

Regards
John Smith

On Mon, Nov 13, 2017 at 6:58 AM,
Susan Brown wrote:

Hi John,
I can do my best but will do it from home tonight as have to leave the office now. Think they still go to 8 pm or so.
Send me all the details and I'll try but usually Mary sets them up and we just authorise them. Will see what I can do - it's no trouble as I know I can ask Mary from her home if necessary.
Leave it with us.

Regards
Susan Brown
Director

On Mon, Nov 13, 2017 at 7:02 AM,
John Smith wrote:

Ok then. Thanks
NAME: Acme
SORT CODE: 12341234
ACCOUNT: 123412341234IBAN: ABCD12341234123412341234
SWIFT ABC:ABCD1234BANK: SOME BANK
ADDRESS: 3 Somewhere Place
Send me payment slip once it is completed.

Regards
John Smith
Sent from my iPhone

On Mon, Nov 13, 2017 at 7:14 AM,
John Smith wrote:

Please use this IBAN number for the account.
IBAN: ABCD12341234123412341234123412341
Ensure to send me the slip once its done. Thanks
N.B: confirm receipt of the new IBAN number.

Regards
John Smith

**

Figure 2.4: Email thread of an Actual CEO Fraud Attack (Kaplan, 2018)

2.6 Actions to effectively defend against social engineering attacks

According to Christina Lekati (2020), a psychologist and social engineer, organizations can take advantage of a variety of safeguards and technical controls, such as establishing multi-factor authentication or enforcing least privilege policies. Below are some examples of human factor measures to boost security.:

2.6.1 Social engineering awareness training for employees:

Ignorance is the most exploited factor in social engineering. A person who is unaware of social engineers' techniques and procedures is powerless to combat them. Employees must comprehend not only what to do but why they should do it. They must recognize that security is a shared responsibility and that successful cyberattacks can result in a slew of problems for both themselves and their organizations. However, not all training methods are successful.

It's great to use a strategy that engages employees and is adapted to the needs and surroundings of the company they work for.

2.6.2 Simulations of social engineering attacks:

Employees' talents can be put to the test once they've learned to identify with and respond to social engineering attacks. To see how far a possible stranger could access the premises of a business, phishing email simulations,

phone attack simulations, or person simulations may be required. These simulations assist employees in consolidating their training information and being vigilant.

2.6.3 Conduct an Open-Source Intelligence analysis on the organization:

Companies are frequently unaware of the amount of information about their company that is available on the Internet, the risk that it poses, or the sources that have made it possible. To aid their attacks, social engineers mainly rely on open-source information. Open-source intelligence collection tools aid enterprises in proactively addressing this issue and reducing the risk of vertical attacks and information vulnerabilities. According to Christina Lekati (2020), this analysis is a valuable tool for identifying and addressing specific training requirements. It may be necessary to publish certain potentially dangerous material on the internet. Employees can be trained on how to deal with problems and information that can be used against them, but staying online still exposes them.

2.7 Human Firewall

This involves the involvement of a group of employees who have been trained in the best procedures for detecting and reporting suspicious behavior. The stronger the firewall becomes as more employees commit to being a part of it, the more important this extra layer of human protection becomes. Many violations are due to employee errors. Therefore, a vigilant human firewall can prevent the potential dangers of software errors from occurring.

Although many email filters have been automated through malware scan signatures and blacklists of pattern match domains, most of these controls are known threats.

90% of attacks are preventable because they exploit known vulnerabilities or variations of them (Porter, 2016). While these automated technological defenses are perfect, a percentage still succeeds in specifically traversing threats that have not yet been recognized and for which defenses have been implemented.

If there are some gaps in the firewalls, some of the known vulnerabilities passes on to the users of the organization. This is where the human firewall adds value (Getthreaready, 2017).

Although it may seem far off, the answer to email fraud rests in enlisting the help of employees to create an army of cyber defenders. These are the same people that previously installed shadow IT on the premises, jeopardizing the company's security.

We've seen technology and the "human firewall" work together to safeguard previously susceptible enterprises (Mimecast, 2015).

In building a human firewall for email security, it is important to consider other important security aspects as well. Many organizations face continuous threats from phishing attacks, insider threats, and many other forms of threats. It is obvious that no organization can afford sufficient cybersecurity to mitigate and intercept every risk. The security policy must start with building a culture in which every employee is responsible for the

information. A culture that inspires employees with situational awareness training to identify and respond to incoming threats. This research explores ways to go beyond day-to-day security to create a culture of security. (Amy McLaughlin, 2019).

2.7.1 Defensive First Line

The sensitive data that has to be protected is at the heart of a cybersecurity architecture. The first line of defense should be cyber security technology, but it is not a guarantee of security. Few dangers truly are a breakthrough if a company has deployed the correct ones as targeted protection against risks. This is significant since the "human firewall" is the next line of defense for employees. Employees don't feel threatened if the technology works, and they are less likely to be victims if just a few people break into the infrastructure.

2.7.2 Employees Motivation and Ability

What happens if a threat gets past the "human firewall"? Can staff be able to spot it and respond appropriately? The answer is contingent on the quality of their education.

An example from a cell phone illustrates how to teach employees: there are two reasons why someone wouldn't answer: either they didn't have the capacity to do so or they weren't motivated. In the context of cybersecurity training, "ability" refers to employees' ability to perceive and respond to risks, whereas "motivation" refers to their understanding of the repercussions of any action they take, whether positive or negative. The best training stresses both and does it in easy-to-understand terminology.

2.7.3. Link the Desired Behaviors to Necessary Knowledge

The next stage is to teach staff the new required behavior while using corporate messaging after they are aware of the hazards. Employees require someone to help them recognize their present risky behaviors in order to get there. Clicking on malicious attachment URLs is one example. Alternatives can be determined once these habits have been identified. Rather than clicking on a dangerous link, they identify the link or attachment as such and report it to IT. It is possible to determine exactly the knowledge that employees require regarding email-based hazards by working backwards from this point.

2.8 Theory Supporting Human Firewall Creation

2.8.1 Social Cognitive Theory (SCT)

SCT places a high value on social impact and external and internal social enhancement. This theory describes the unique ways individuals acquire and maintain behaviors, taking into account the social environment in which they operate. This theory takes into account a person's past experiences to determine whether an action is likely to occur. These past experiences influence reinforcement, expectations, and anticipatory attitudes, all of which determine whether and why a person engages in a particular behavior (LaMorte, 2019).

The goal is to describe how humans regulate their behavior through control and reinforcement to achieve sustainable, goal-directed behavior over time. The theory is based on five frameworks.

1. Mutual determinism: refers to the dynamic and interactive interaction of people (individuals with a set of learning experiences), environment (external social context), and behavior (responses to stimuli to achieve goals).

2. Behavioral competence refers to a person's actual ability to perform actions through basic knowledge and skills. In order to act successfully, one must know what to do and how to do it. People learn from the consequences of their actions, which also affect the environment in which they live.
3. Observational Learning: This asserts that people can witness and observe the actions of others and reproduce those actions. This is often indicated by behavioral "modeling." A person who sees a successful demonstration of an action can also successfully complete the action.
4. Reinforcement: refers to an internal or external reaction to an individual's behavior that influences their likelihood of continuing or stopping the behavior.
5. Expectation refers to the expected outcome of a person's actions; people expect their results.

2.9 Human Security Layer

The Human Security Layer automatically detects and prevents threats, including patterns and behaviors in human communication, creating a distinct security identity for each employee over time by increasing their security reflexes. (Tim, 2021)

2.9.1 Need for Human Security Layer

Employees now have power over both your systems and your data, according to Tim Salder. People, on the other hand, make mistakes, break rules, and can be duped (Sadler, 2021). Human error is responsible for 88 percent of data breaches, according to AIG, which states that "human error continues to be a substantial contributor to cyber claims" (Sadler, 2021). With just a few clicks, staff can transfer millions of dollars to a bank account and share medical details in an Excel file over email.

Instead of expecting people to do the right thing 100 percent of the time, we believe it is preferable to prevent errors from occurring in the first place by recognizing and preventing them. Human error is responsible for 88 percent of data breaches, according to AIG, which states that "human errors and behavior continue to be a primary driver of cyber claims" (Sadler, 2021).

2.9.2 People always break the rules

People in every company can break the rules, whether on purpose or by accident. These guidelines might apply to anything from passwords to how sensitive information is maintained. But what about the rules governing data exfiltration? Employees are frequently blissfully unaware. They are unaware of their own policies as well as the policies of bad data management. As a result, people are not hesitant to e-mail company information to their personal email account, for example, to print at home. However, not all employees are well-intentioned, as evidenced by the sale of 68,000 client files to crooks by an employee of a defense cybersecurity firm before the end of 2019. This isn't a one-time occurrence. According to one study, 45 percent of employees say they took work-related documents with them after they were laid off, while more than half of UK employees acknowledged stealing from their employers. For less than £1,000, a fifth of those surveyed would be willing to do so (CISOMAG, 2019). At work, mistakes are unavoidable, ranging from a small typo to a malfunctioning

firewall, and these errors are caused by human error. In fact, 43% of employees say they've made a mistake at work that has harmed their cybersecurity. Regrettably, the repercussions of these errors can be severe. (Sadler, 2021)

If an employee sends a misdirected email, fines may be imposed, confidence may be lost, and the company's reputation may suffer long-term damage. Employees face more than shame and concern as a result of these misdirected emails; they also risk losing their jobs.

2.9.3 People can be tricked

Corporate emails are utilized as a medium of formal communication by organizations of all sizes and sectors with a network of entrepreneurs and clients, making it easy for hackers to pass off as internal and external contacts. Over the last two years, business email compromise attacks have surged by more than 100 percent (Sussman, 2019). So, what if an employee is duped by a spear phishing email and is persuaded into revealing credentials or assisting a hacker in gaining access to your network? The average fine for a violation is \$3.92 million (Brook, 2020). This research intends to curb these costs through the introduction of a human firewall into email security.

2.10 Existing email security solutions Available

Existing email security solutions employ various technologies and strategies to combat social engineering attacks, each with its strengths and weaknesses. Let's compare some common email security solutions:

2.10.1 Spam Filters:

Strengths: Spam filters can effectively block a significant portion of phishing emails and malicious content, reducing the likelihood of successful social engineering attacks. Weaknesses: Advanced social engineering attacks may bypass basic spam filters through tactics like personalized content or spear-phishing techniques.

2.10.2 Anti-Phishing Solutions:

Strengths: Anti-phishing solutions use heuristics and machine learning algorithms to identify and block phishing emails, including those with deceptive URLs or malicious attachments.

Weaknesses: Sophisticated phishing attacks with convincing social engineering tactics might still evade detection by some anti-phishing solutions.

2.10.3 Email Authentication Protocols (SPF, DKIM, DMARC):

Strengths: These protocols help validate the authenticity of incoming emails, reducing the likelihood of domain spoofing and impersonation-based attacks.

Weaknesses: While these protocols improve email authentication, their widespread adoption is not universal, allowing some attackers to exploit domains without proper implementation.

2.10.4 Employee Training and Awareness Programs:

Strengths: Educating employees about social engineering risks can raise awareness and empower them to recognize and report suspicious emails.

Weaknesses: Training alone may not prevent all social engineering attempts, and human error remains a significant vulnerability in phishing attacks.

2.10.5 AI-Driven Threat Intelligence:

Strengths: Artificial Intelligence (AI) and Machine Learning (ML) technologies can identify emerging social engineering patterns and enhance threat detection accuracy.

Weaknesses: AI solutions may produce false positives or negatives, leading to missed threats or legitimate emails being misclassified as malicious.

2.10.6 Behavioral Analysis and Anomaly Detection:

Strengths: Analyzing user behavior and identifying anomalies can help detect account compromise and unauthorized access.

Weaknesses: It may not be effective against sophisticated attackers who mimic legitimate user behavior.

2.10.7 Encryption and Data Loss Prevention (DLP):

Strengths: Encryption and DLP solutions protect sensitive data and prevent inadvertent data leaks, limiting the damage of social engineering attacks.

Weaknesses: Encryption cannot prevent social engineering attacks themselves but can mitigate the impact of successful breaches.

2.10.8 Continuous Monitoring and Incident Response:

Strengths: Real-time monitoring and rapid incident response can identify and mitigate social engineering attacks quickly.

Weaknesses: Lack of resources or delayed responses could lead to significant damage before detection.

Below is a table comparing the strengths and weaknesses of existing email security solutions in solving social engineering attacks:

Table 2.1: comparing the strengths and weaknesses of existing email security solutions in solving social engineering attacks:

Author(s)	Email Security Solution	Beneficiaries	Strengths	Weaknesses
(Zola, 2021)	Spam Filters	Symantec, Sophos Email Security, Barracuda Email Security , Proofpoint, Microsoft	Effectively block a significant portion of phishing emails.	Advanced attacks may bypass basic filters.
(Kl, 2023)	Anti-Phishing Solutions	Cisco Email Security, Proofpoint, Microsoft Defender, Barracuda, Mimecast Email Security	Use heuristics and ML algorithms to identify phishing emails.	Sophisticated attacks may still evade detection.
(Writes, 2023)	Email Authentication Protocols (SPF, DKIM, DMARC)	Cisco Email Security, Proofpoint, Microsoft Defender, Barracuda, Mimecast Email Security, Google Workspace	Validate email authenticity, reducing domain spoofing.	Adoption not universal, some domains may lack proper implementation.

(Samson, 2021)	Employee Training & Awareness Programs	KnowBe4, Cofense, Proofpoint, Mimecast Email Security, SANS, SecurityIQ, Wombat	Educate employees about social engineering risks.	Training alone may not prevent all attacks.
(Alam, 2023)	AI-Driven Threat Intelligence	Darktrace, FireEye, Symantec, Tessian, Vade Secure, GreatHorn	Identify emerging social engineering patterns.	May produce false positives or negatives.
(Stolfo, 2003)	Behavioral Analysis & Anomaly Detection	Cisco Email Security, Proofpoint, Microsoft Defender, Barracuda, Mimecast Email Security, Tessian	Detect account compromise and unauthorized access.	May not be effective against sophisticated attackers.
(Team, 2023)	Encryption & Data Loss Prevention (DLP)	Trend Micro, Egress secure email, Sophos Email Security, Barracuda, Cisco Email Security, Zix Email Encryption	Protect sensitive data and prevent data leaks.	Cannot prevent social engineering attacks themselves.
(Security, 2014)	Continuous Monitoring & Incident Response	FireEye Email Security, Cisco Email Security, Symantec, Mimecast Email Security	Real-time monitoring for quick response.	Lack of resources or delayed response may lead to significant damage.

Organizations must implement a multi-layered defense strategy to combat social engineering attacks. A human firewall simulator, combined with existing solutions, can help reduce the risk of successful attacks. This simulator has a feedback mechanism to assess user awareness and overall organization awareness levels. It integrates with existing solutions to solve phishing attacks and BEC attacks. Despite existing security plans, recent attacks focus on social engineering, making employees part of the security problem. This research designs a simulator that works with existing email security mechanisms, allowing "human" employees to be part of the security, through simulation and policy enforcement.

2.11 Design of the current security model

An email exchange is an email message flow with a variety of mechanisms for spam and antivirus filtering as depicted in Figure 2.5.

Email Message Flow

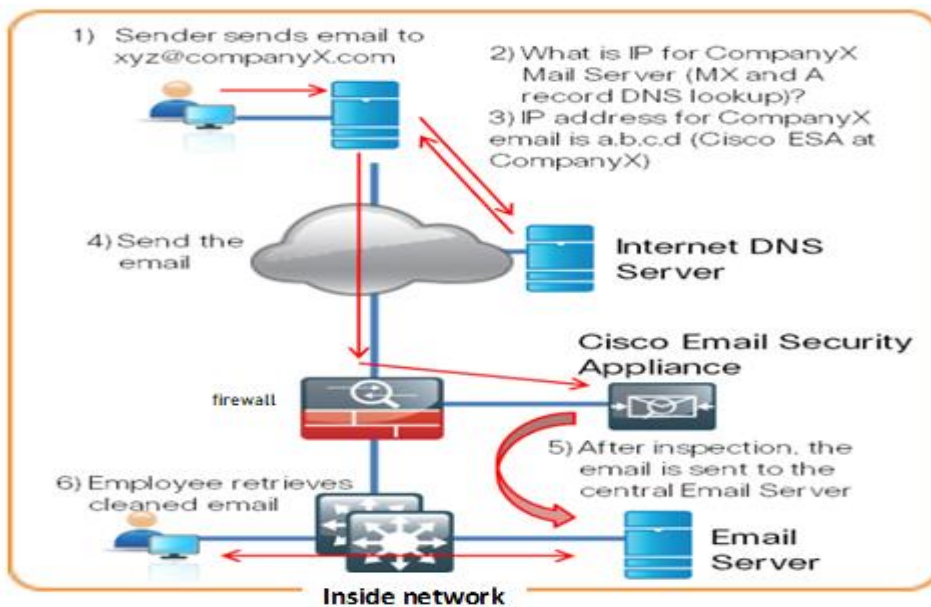


Figure 2.5: Email Message Flow Courtesy of (Cisco, Email Security Deployment Guide, 2010)

Despite all these mechanisms for protection in this design, mostly used to secure emails, corporate emails suffer attacks mostly from social engineering attacks. Social engineering happens at the last stage of message delivery, which is why integrating the security mechanism with a human firewall greatly helps reduce CEO fraud. (See Figure. 5.1)

2.12 How Human firewall works

More than ever, businesses must put cybersecurity first. However, this process calls for a broader approach than the strategy that most businesses had up to this point, which involved investing extensively in security solutions. People are the biggest cybersecurity risk, which is missed if cybersecurity measures are limited to IT-only mitigation. Organizations have traditionally installed firewalls around their technical assets. A firewall is a hardware and software arrangement that monitors and regulates network traffic based on established security criteria. Modern security applications driven by AI have recently been introduced as improvements to the firewall concept. But as sophisticated threats target people and their weaknesses across a larger range of distributed endpoints, a different type of firewall is needed: a human firewall.

2.12.1 What makes a human firewall?

The first line of defense against security risks to a business is its human firewall. A human firewall is a layer of protection for people, as opposed to a technological firewall, which digitally arbitrates network traffic. It is empowered by training and rewards, spanning teams, corporate functions, and technological advancements. A human firewall is not a single individual or "evangelist," it is not restricted to the security team or any other team, it is not the worker's exclusive job, and it is not a "set-and-forget" state.

A human firewall is a layer of protection for people, as opposed to a technological firewall, which digitally arbitrates network traffic.

A human firewall does more than just focus on the conventional "weakest link" in the security "chain." Instead, it is a completely other chain that needs to be encouraged and improved as threats are continuously changing. For instance, prominent phishing risks in five years may not appear the same as those in use now. How many workers actually understand what social engineering is?

Companies must offer staff substantial education, simulation, training, and relevance in order to create a strong human firewall. Training on security awareness should also take into account the individual responsibilities and metrics that each employee plays in addition to the company's primary product or service. This extends far beyond the security team to involve all employees, including managers and call center reps as well as product designers and field colleagues.

2.12.1 Human Firewall components

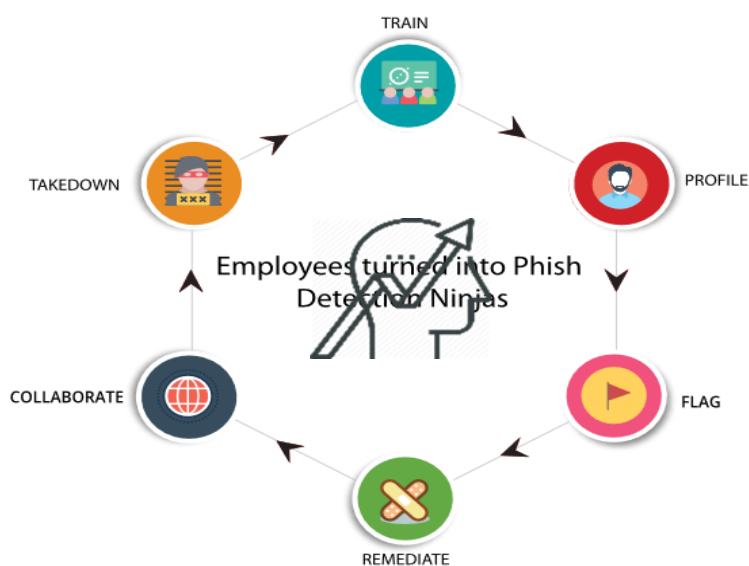


Figure 2.6: Human Firewall components (Gatner, 2017)

- 1. Train:** employees are taken through phishing simulation & awareness training involving. Lessons are given to raise awareness of existing threats to the use of quizzes designed in the LMS.
- 2. Profile:** the system operates on profiling and reporting by the user by monitoring activity by the user and judging individual performance by analyzing behavior and mapping strengths and weaknesses through generating reports to track them.
- 3. Flag:** employees are required to click on the phishing report button which involves a phishing reporting mechanism on Outlook, Email Based and API. Once this is done, the attacks are then handled by the Information Technology department.
- 4. Remediate:** Here, any link or attachment suspected to have a threat is quarantined, deleted from the inbox or server, and shown in a threat alert folder. This is a remedy for Outlook, Google's suite, and many others to ensure that the platform has a user threat.
- 5. Collaborate:** A central repository of global phishing trends and increased phishing detection through crowd wisdom as well as the collaboration of millions of employees globally are to be introduced.

6. Take Down - Collaborations with other international organizations, such as CERT, in some countries ensure that each malicious attempt is located at the source and effectively removed to ensure that it does not affect another employee. A trained employee can report malicious emails and quarantine them to protect the whole organization in real time.

2.13 Summary of Literature Review

The literature review on the development of a human firewall simulator to enhance security awareness against business email compromise (BEC) highlights the growing threat of BEC attacks, their financial impact, and the use of advanced social engineering techniques. Cybersecurity awareness training is crucial for staff members to combat these threats. Conventional training tactics are criticized for their ineffectiveness in changing behavior and adapting to new attack techniques. Experiential learning and simulation have been extensively studied, demonstrating their effectiveness in improving decision-making skills and practical application of knowledge. Human factors play a significant role in cybersecurity, with human error often contributing to successful attacks. Customization and contextualization of training content enhance engagement and relevance, while data-driven training and analysis provide insights into participant behavior, decision-making patterns, and areas for improvement. Simulations that mimic real-world scenarios are deemed effective in enhancing participants' resilience against cyber-attacks. In conclusion, the literature review highlights the need for innovative cybersecurity awareness training, particularly in combating BEC attacks. The incorporation of experiential learning through a human firewall simulator aligns with research findings, focusing on customization, data-driven insights, and practical application.

CHAPTER THREE: RESEARCH METHODOLOGY

3.0 Introduction

In this chapter, the researcher focuses on the methods used in performing research operations and solving research problems systematically.

3.1 Methodology

A quantitative methodology is what distinguishes the research approach used to create the Human Firewall Simulator. This strategy was chosen to fully address the complex issues surrounding raising security awareness against BEC assaults. The quantitative approach makes it easier to monitor results and analyze behavioral data. Behavioral data from participant interactions with the simulator is collected and analyzed as part of the quantitative component. This information consists of choices made, reaction times, and scenario results. The simulator's success is evaluated in terms of improved security awareness, decreased exposure to BEC assaults, and accurate decision-making using the quantitative data (Gogodze, 2019). Reasons for Choosing a Simulation-Based Approach: The necessity for an interactive and immersive learning environment that closely resembles real-world BEC scenarios led to the choice of a simulation-based approach. The interactive aspect of simulations, enables users to actively participate in various BEC attack simulations, is in line with the goal of raising security awareness. This strategy makes use of the principles of experiential learning, according to which learners gain the most knowledge when they actively make decisions and deal with the results of those actions. (Purup, 2020)

3.2 Simulation

Analytical reasoning might be difficult or impossible in the case of complicated models, especially if the specification is nonlinear. In these situations, simulation is frequently the only option. Simulating is the process of moving the model forward in time and seeing what happens.

- i The simulation measures the behaviors of the results that are generated from the simulated data, which is compared to the actual scenario to see if there is a positive effect.
- ii This methodology allows organizations to train and test their employees' responses to cybersecurity incidents in a controlled environment without exposing real data or systems to risk.
- iii. Simulations provide an opportunity to assess user behavior, knowledge, and awareness of cybersecurity best practices. By observing how employees react to simulated cyber threats, organizations can identify areas where further training and awareness programs are needed. This helps in identifying potential weaknesses and gaps in knowledge among employees, enabling organizations to take proactive measures to address them.
- iv. Human firewall simulations create a safe space for employees to make mistakes and learn from them. In real-life scenarios, mistakes can have severe consequences, but simulations allow employees to experiment, fail, and understand the consequences of their actions without affecting the organization's operations. Through

debriefing sessions after the simulation, employees can reflect on their choices and learn from their mistakes, improving their ability to respond effectively to future incidents.

v. Simulations help organizations build and strengthen their incident response capabilities. By immersing employees in realistic scenarios, they gain first-hand experience in identifying and responding to potential threats. This methodology allows organizations to detect areas where their incident response plans or processes might be lacking, enabling them to refine and improve them. It fosters a culture of active defense and encourages employees to stay vigilant against potential cyber threats.

vi. This methodology provide organizations with a measurable way to assess the effectiveness of their cybersecurity training programs. By evaluating how employees perform during simulations, organizations can determine the impact of their training efforts and identify areas for improvement. This methodology enables organizations to fine-tune their training strategies and tailor them to address specific weaknesses or gaps in knowledge. Human firewall simulation methodology replicates realistic scenarios, assesses user behavior and awareness, enables learning from mistakes, helps build response capabilities, and measures the effectiveness of cybersecurity training programs. It provides organizations with valuable insights into their readiness to face cyber threats and allows them to take proactive measures to enhance their overall security posture.

3.2.1 How users are selected to participate in the simulated Training

Selecting the right users to participate in the Human Firewall Simulator is a crucial aspect of its effectiveness. The goal is to ensure that the training reaches those individuals whose roles, responsibilities, and potential exposure to Business Email Compromise (BEC) make them most relevant for the training. However, all corporate users must participate in human-firewall simulated training. Here's how users are typically selected to participate:

1. **Role-Based Selection:** Identify user roles that are more likely to encounter BEC threats due to their involvement in financial transactions, sensitive data handling, or communication with external parties. This might include employees in finance, accounts payable, executive assistants, and procurement.

2. **Departmental Involvement:** Departments that deal with sensitive information, financial transactions, or external communications are often selected for participation. These may include finance, legal, HR, and executive teams.

3. **Risk Profile:** Evaluate the risk profile of different teams or departments. Those that handle higher volumes of financial transactions or sensitive information might be given higher priority for participation.

4. **Phishing Susceptibility:** Consider the susceptibility of users to phishing attacks. Individuals who have a history of falling for phishing attempts might benefit from the training to enhance their vigilance.

5. **Mandatory Training:** Some organizations might mandate certain teams or individuals to undergo the training due to the nature of their work. For example, employees involved in financial transactions might be required to complete the training.

6. **Training Goals:** Align the selection with the goals of the training program. If the aim is to have representatives from all departments, a diverse group of users might be selected.

7. **Pilot Groups:** Start with a smaller pilot group before rolling out the training to a larger audience. This allows you to assess the effectiveness of the training, gather feedback, and make necessary improvements before wider implementation.

8. **Voluntary Participation:** Some organizations might offer the training on a voluntary basis. Users interested in enhancing their security awareness can opt to participate.

9. **Senior Management and Executives:** Including senior management and executives in the training sends a strong message about the organization's commitment to security. Their participation can set an example for others.

10. **Regular Assessment:** Regularly reassess the training needs of different teams or individuals. As roles change or new employees join, consider incorporating them into the training program.

11. **Targeted Approach:** Use data analytics and insights to identify departments or teams that might have a higher likelihood of encountering BEC threats based on historical data.

12. **Refresher Training:** Consider offering refresher training to those who have already undergone the training to reinforce the lessons and keep security awareness high.

The selection process should be well communicated to the participants through training codes which are sent to the participants in good time. Provide them with clear reasons for their selection and the benefits of participating. This can enhance their motivation and engagement during the training process.

3.2.1 The simulation human firewall has two basic steps:

- a. Pre-Assessment of user's knowledge to the social engineering attacks.
- b. Post Assessment Evaluation after integration with human firewall.

3.2.1.1 Assessment of the user's knowledge of the social engineering attacks

Users is tested on various phishing attacks before receiving trainings.

This is done to access knowledge level of the staff in the organization, pointing to the areas of concern to help have a focused based training. Various areas of phishing are;

- i. Phishing awareness: Evaluate if users can identify phishing attacks, their understanding of threats, and their level of awareness of best practices.
- ii. Reporting and response: Evaluate the users' ability to report phishing emails promptly and accurately. This can be assessed by tracking the number of reported incidents and the response time.
- iii. Mobile device security: Test the users' awareness and adherence to secure email practices on mobile devices. This can include evaluating if they use secure email apps, update device software, and understand the risks associated with mobile email usage.
- iv. Password security: Assess the users' password hygiene and knowledge of best practices. This can include evaluating if they use strong and unique passwords, enable two-factor authentication, and understand the importance of regular password changes.

- v. Social engineering attacks: Conduct simulated social engineering attacks to test the users' susceptibility to manipulation through phone calls, messages, voicemail messages, or in-person interactions related to email security.
- vi. Phishing email identification: Evaluate the users' ability to identify signs of phishing emails, such as suspicious sender addresses, grammatical errors, mismatched URLs, requests for personal information, or urgent and threatening language.
- vii. Post-incident evaluation: Assess the users' understanding of the impact and consequences of falling victim to a phishing attack. This can help determine if additional training or remediation is required.

3.2.1.2 Post Assessment Evaluation after integration with human firewall

Awareness training is required based on the analysis from the pre-assessment. Training materials are designed to focus on the weak areas identified during pre-assessment. A training link is sent to the trainees, requesting that they log into a portal with a training button and begin their training based on the test codes sent to them by the administrator. The test codes vary based on clustering from the training needs assessment done at the pre-assessment stage. A link to the training is to be posted on the company's intranet for referral purposes.

The length of the presentation is to be approximately twenty (20) minutes and cover basic topics such as:

- i. The various sorts of phishing scams that exist today.
- ii. How to detect phishing assaults.
- iii. Signs that we've been the victim of a phishing assault.
- iv. How to Avoid Phishing Attacks
- v. information about the hotline, which allows users to report suspects.

The user's knowledge of what has been shared is then tested. By clicking the assessment button, the trainees are taken through tests derived from the training materials that were in the training section. Trainees are taken through a compulsory quiz. If an employee answers all questions correctly, he or she is to be awarded a certificate of completion, but if they fail, it shows the failure rate and the areas of weakness to form the next training.

An overall analysis is graphically displayed for the organization's awareness position. A continuous assessment is done routinely based on statistics provided showing departments and staff most at risk; this is to help achieve the effectiveness of human firewall integration with the email security framework to help reduce business email compromise.

3.3 Instruments

Several tools and instruments were used for the study, including Python for programming tasks, an XAMPP server for local web development and testing, Notepad++ for code editing, a browser and the internet for research and accessing online resources, and an SMTP server for email communication.

- i. Python: Python is a versatile programming language commonly used for data analysis, web development, scientific computing, automation, and more. It provides a wide range of libraries and frameworks that make it suitable for various applications.
- ii. XAMPP Server: XAMPP is a software package that provides a local web server environment for developers. It includes components like the Apache web server, MySQL database, PHP, and Perl. XAMPP allows you to set up a local server on your computer for developing and testing web applications.
- iii. Notepad++: Notepad++ is a free, open-source code editor and text editor for Windows. It supports multiple programming languages, provides syntax highlighting, code folding, and other useful features for code editing and development.
- iv. Browser: A web browser is software used to access and view websites on the internet. Popular web browsers include Google Chrome, Mozilla Firefox, Safari, and Microsoft Edge. Browsers allow you to interact with web-based applications, view web pages, and test web development projects.
- v. Internet: The internet is a global network of interconnected computers and devices that enables communication and access to information worldwide. It is essential for browsing websites, accessing online resources, and connecting to various services.
- vi. SMTP Server: SMTP (Simple Mail Transfer Protocol) is a standard protocol for sending emails. An SMTP server is responsible for sending and routing email messages over the internet. It handles the transfer of outgoing emails from your email client or web application to the recipient's email server.

3.4 Ethical considerations

The research was done under the approval by School of Informatics and Innovative Systems, National Commission for Science, Technology and Innovation, and Board of Postgraduate Studies. See Appendix 4, Appendix 5, and Appendix 6, respectively.

3.5 Summary of Research methodology

The methodology concludes by summarizing the systematic approach taken to design, develop, and implement the Human Firewall Simulator. It emphasizes that the simulator is a dynamic tool that evolves with the changing threat landscape and user needs, fostering a culture of ongoing security awareness and preparedness against BEC attacks.

CHAPTER FOUR: DEVELOPMENT OF HUMAN FIREWALL SIMULATOR

4.0. Introduction

This chapter focuses on the building and development of the simulator, explaining the various stages of the development to the final stage and the tools used.

4.1 Model for Human Firewall Simulator

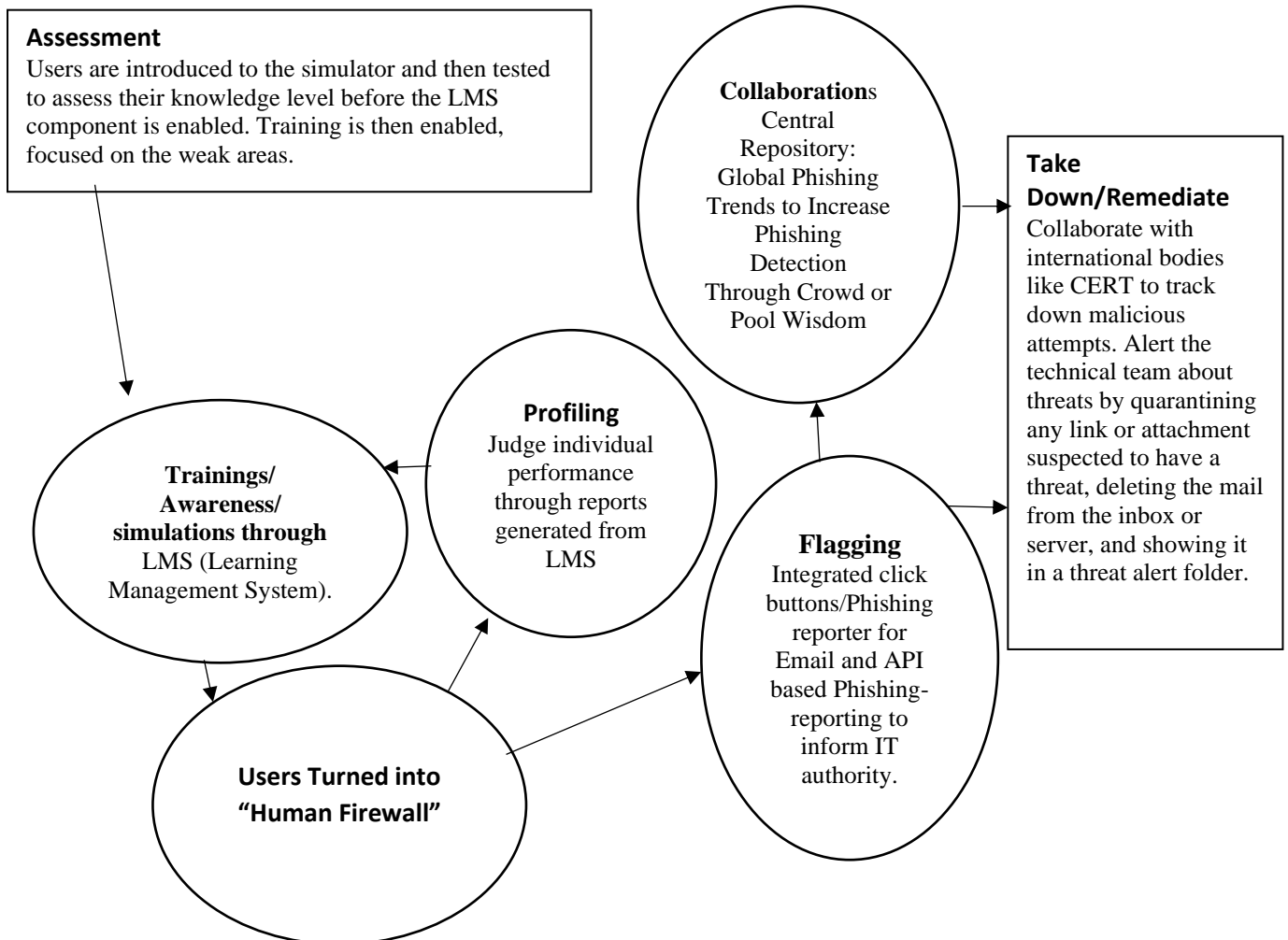


Figure 4.1: Model for Human Firewall simulated (Researcher, 2023)

1. Assessment: Users are introduced to the simulator and then tested to assess their knowledge level; the results are displayed in terms of the number of questions asked correctly, the areas of weakness, as well as the average awareness report on the organization. The training component is then enabled, with training focused on the areas perceived to be the weak points identified by the pre-assessment.

2. Trainings/Awareness/ simulations through LMS (Learning Management System).

This the simulated Human firewall control system that does trainings through LMS, Tests/ Quizzes (The quizzes vary from one trainee to another) are done again to the trainees after the training to see the success

level. This is compared to the previous results found before training. A continuous training and assessment are to be scheduled regularly even to those who had proven to be knowledgeable.

3. Users Turned into “Human Firewall”: Those trained and have met the threshold set for example 100% pass in all the quizzes are considered as part of the security team (Human Firewall). Remember dynamics of attacks changes rapidly because attackers always want to be on top of things. New attack trends adopted by attackers are to be added to the Learning simulator to form part of the new learning materials in the LMS to ensure even the most knowledgeable users are equipped with the latest knowledge. Either test/ quizzes continue periodically to ascertain the knowledge level.

4. Profiling Based on the reports generated by the simulator from the regular quizzes and tests, the system helps with decision-making, i.e., whether a user can be trusted to use the corporate email securely or requires further training; or disciplinary actions as per the organization’s policy. Judge individual performance by analyzing user behavior. For example, if it is determined that a user assumed to flag what was to be flagged or clicked on a malicious link on the corporate email, then this user is to be taken to the training stage once more, and the loop continues.

5. Flagging Integrated click buttons/phishing reporter for email and API-based phishing-reporting to inform IT authority of a suspicious link or communication.

6. Collaborations Involves creation of Central repository global phishing trends to help increase phishing detection through crowd/pool wisdom that informs users of the attack trends users by hackers thus increasing knowledge and awareness on email security.

7. Take Down/Remediate: Collaborate with international bodies like CERT to track down malicious attempts. Alert the technical team about threats by quarantining any link or attachment suspected to have a threat, deleting the mail from the inbox or server, and showing it in a threat alert folder.

4.2. Variables that play a role in the effectiveness of the simulator

Dependent and independent variables that play a role in the effectiveness of the simulator and its impact on security awareness:

4.2.1 Independent Variables:

- i. **Simulator Content:** The various scenarios, simulations, and educational modules provided by the simulator to train employees about BEC tactics and techniques.
- ii. **Feedback Mechanism:** The quality and immediacy of feedback given to users when they interact with simulated phishing emails, helping them understand the reasons behind correct and incorrect decisions.
- iii. **Customization:** The ability of organizations to tailor the simulations to their specific industry, corporate culture, and threat landscape.
- iv. **Frequency and Diversity of Scenarios:** How often new scenarios are introduced and how diverse these scenarios are, which keeps the training fresh and reflective of evolving threats.

- v. **Gamification Elements:** The presence of gamification features like leaderboards, rewards, and achievements to enhance user engagement and motivation.
- vi. **Continuous Learning Approach:** The strategy of introducing new challenges and content over time to ensure that employees maintain a high level of security awareness.

4.2.2 Dependent Variables:

- i. **Security Awareness:** The primary outcome variable, reflecting how well employees understand BEC tactics, can identify suspicious emails, and make informed decisions when faced with potential threats.
- ii. **Phishing Detection Rate:** The percentage of simulated phishing emails correctly identified as suspicious by employees, indicating their ability to recognize potential BEC attacks.
- iii. **Response Rate to Suspicious Emails:** The proportion of times employees take appropriate actions (e.g., not clicking on links, not sharing sensitive information) when faced with simulated suspicious emails.
- iv. **Reduction in Successful BEC Incidents:** The impact of the training on the organization's actual incidence of successful BEC attacks, potentially leading to a decrease in successful breaches.
- v. **User Engagement:** Measured by the frequency of interaction with the simulator, completion rates of modules, and participation in gamified elements.
- vi. **Retention and Application of Knowledge:** The degree to which employees retain and apply the knowledge gained from the simulator in their real-world email interactions.
- vii. **Cultural Shift:** The extent to which the training fosters a security-conscious culture within the organization, leading to long-term changes in employee behavior.
- viii. **Feedback Utilization:** How effectively employees use the feedback provided by the simulator to improve their decision-making in subsequent interactions.

These independent and dependent factors work together to help determine how well the Human Firewall Simulator works to raise security awareness against BEC threats. These factors can be used by organizations to gauge the effectiveness of their cybersecurity training programs and to help them choose the best course of action.

4.3 Human Firewall Simulator Development

This research study involves the development and testing of a human firewall simulator as an appropriate research method to handle the complexities in this research area. The researcher first puts users to the test by testing them through simulating phishing attempts, and then quizzes them (all types of users) to determine the necessity of incorporating a human firewall into the standard email security framework and the value it provides to email security.

4.3.1 Sequence diagram

Sequence diagrams in system design are used to demonstrate different ways users of a system are to interact with the system. It displays the different users that the system has and how those specific users interact with

the system. All users in a system must be captured in this sequence diagram, along with the functions they perform in the system.

4.3.2 Admin sequence diagram

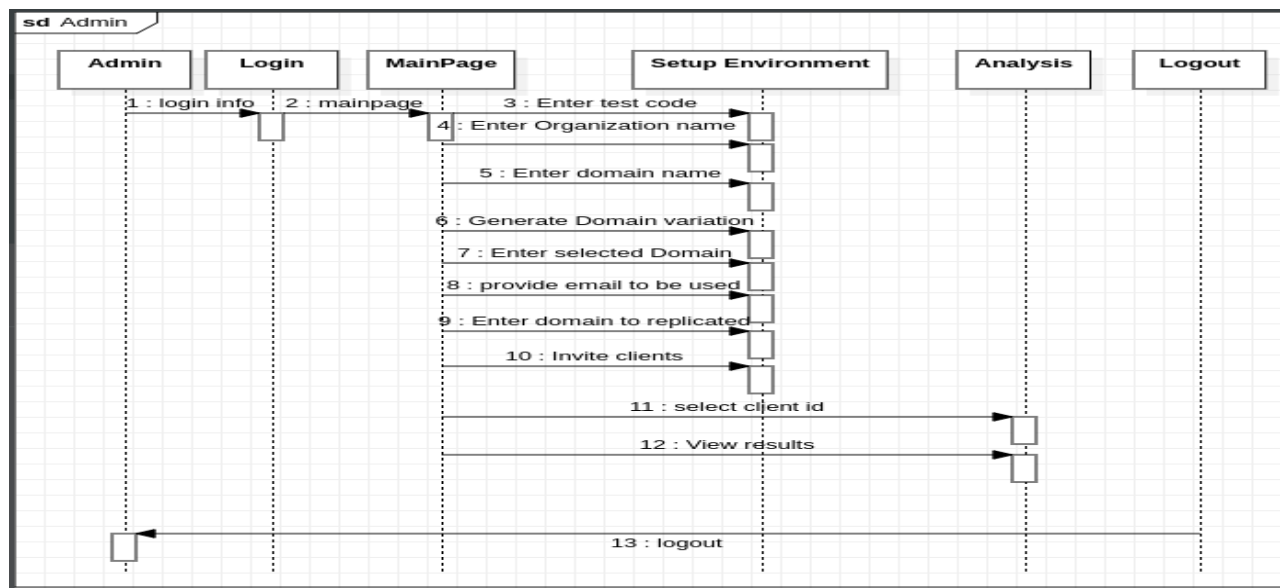


Figure 4.2: Admin sequence diagram (Researcher, 2023)

The admin sequence diagram (figure 4.2) shows the flow of administrator interactions with the system. Upon opening the administrator module, the administrator logs in, takes the system to the main admin page, creates a test code to be sent to the trainees, enters the organization’s name and the domain name of the organization, i.e., www.mail.safaricom.com; the user then generates domain variations that are look-alike, i.e., www.mail.safaricom; the admin then selects one varied domain name for cloning; the admin then provides an email address to be used to send the cloned domain; the admin then enters the domain to be replicated and invites the clients. The administrator then waits for the training and tests to be done by the clients. The analysis is done by selecting the test code that was provided to the clients, viewing the results analyzed, and then logging out.

4.3.3 Client sequence diagram

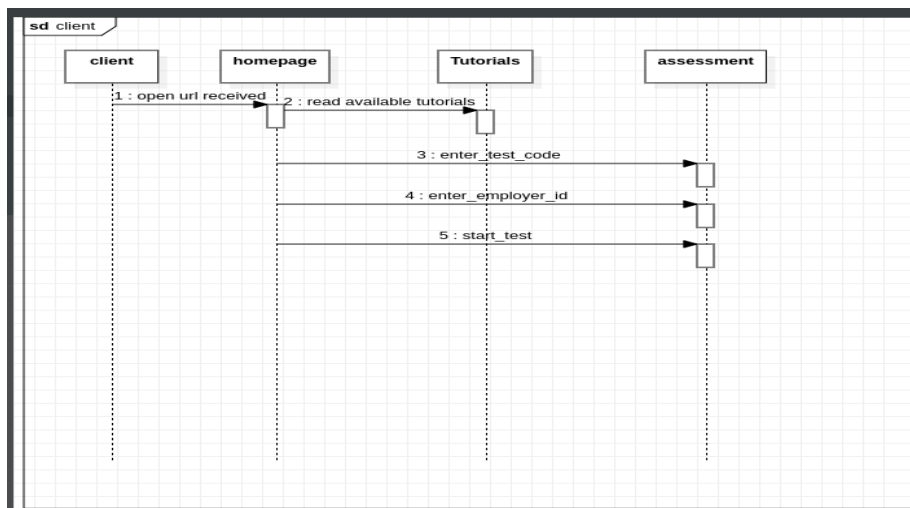


Figure 4.3: Client sequence diagram (Researcher, 2023)

In the client sequence diagram above (Figure 4.3), the client opens the url received on the home page; the url contains the training materials; the client reads the tutorials received; once done, the client enters the test code and employer ID on the assessment button; and the client begins the test.

4.3.4 Use-case Diagram

Another important system design tool is the use-case diagram. They are used mainly to determine different interactions between systems and their actors. They don't describe how the system operates internally; they only identify what the system does and how the system actors use it.

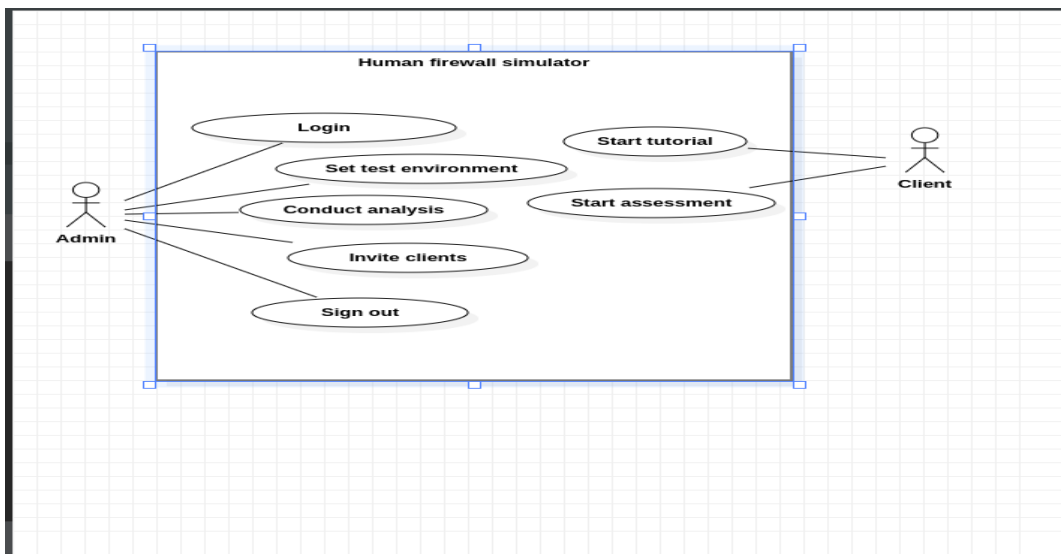


Figure 4.4: Use-case Diagram (Researcher, 2023)

According to figure 4.4, the simulator contains two major parts: the administrator side (Admin) and the client side.

Admin:

- i. log in: Authentication is determined before a user logs in.
- ii. Set test environment: administrator sets the test environment, making sure the main areas of weakness are covered during testing of the clients.
- iii. Conduct analysis: Here, the administrator generated analysis in the form of charts from the tests conducted by the clients.
- iv. Invite clients: The administrator sends invitations to the clients for the scheduled training and testing, and depending on the clustering of the clients, test codes are issued based on the various focused testing areas that have been identified as weak areas of the clients.
- v. Log Out: This is the end stage of system interaction. Logging in comes back when the administrator wants to interact again with the system.

Client:

- i. Start tutorial: Here, the client, upon receipt of an invitation, gets training in the form of presentations, video clips to watch, or live Zoom training. The client or trainee is expected to take the training seriously because an assessment follows. Based on the test code sent to the trainee, the training involves areas the clients are considered weak in or not well knowledgeable about.
- ii. Start assessment: Upon going through the tutorials, the trainee is expected to answer questions
- iii. using the test code provided. If the trainee gets 100% in the training (which is the goal), a certificate is issued instantly on the system; if not, the system analyzes the weak areas where the training failed, which forms the focus of the next training.

4.3.5 Activity Diagram

This is another very important tool in system design; it helps developers of systems understand the flow of events in the system, what constraints the system has, what processes the system has, and the conditions that cause different behaviors in the system. Activity diagrams are key to understanding a high-level overview of what's happening in a system.

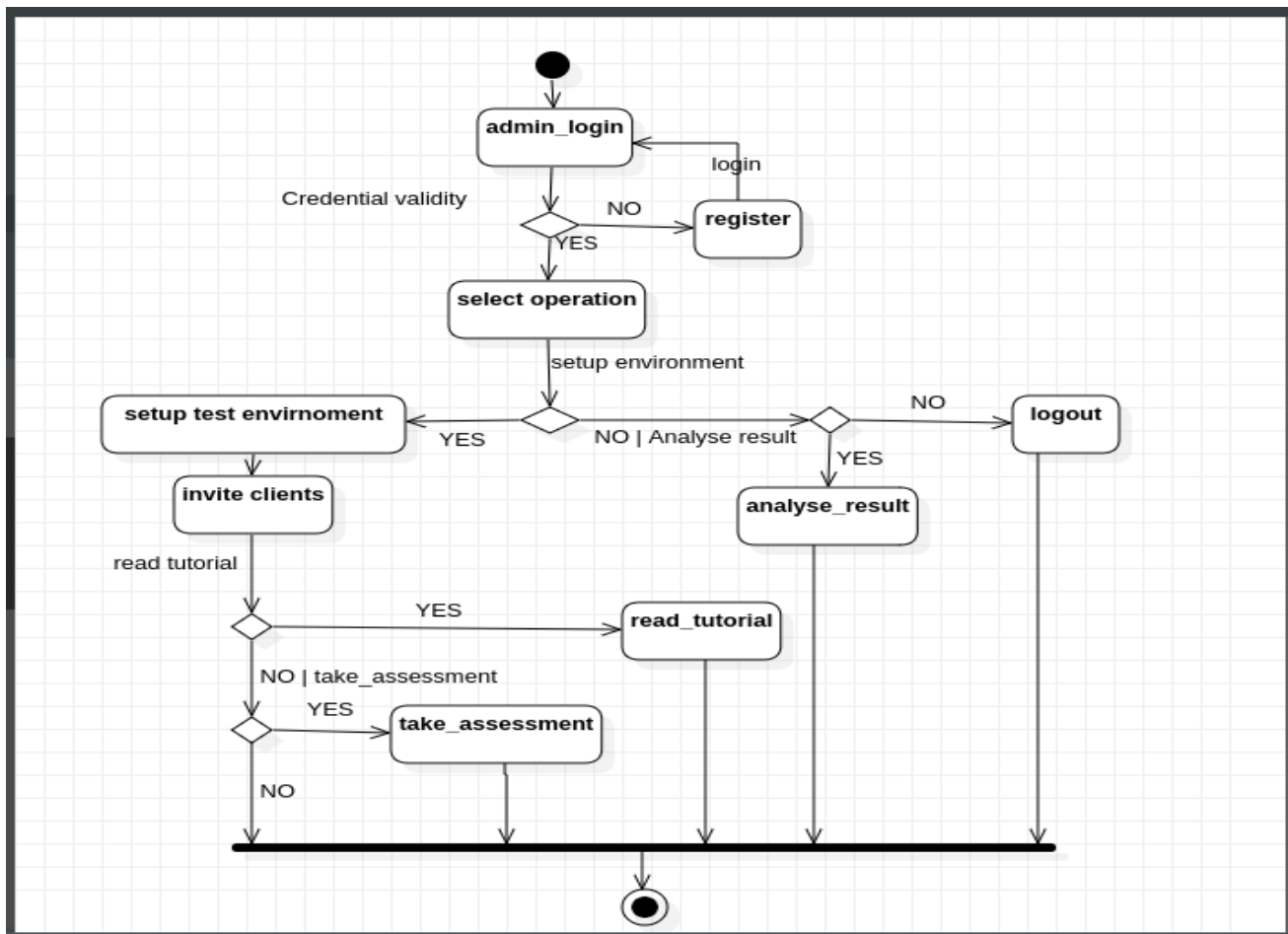


Figure 4.5: Activity Diagram (Researcher, 2023)

From figure 4.5 above, the activity diagram shows admin authentication; if the credentials provided are correct, the system proceeds; otherwise, it takes it back to log in.

Once the administrator is authenticated, the test environment page is displayed. The administrator can choose to proceed to the test environment, analyze existing results using the test codes provided, or logout.

If the administrator chooses to proceed with setting the test environment, clients are invited to read tutorials and then take the assessment. The clients can also be invited to take the assessments without tutorials, especially if the administrator is interested in knowing the knowledge level as a guide for the test environment (pre-assessment). The administrator can then log out.

4.4 Testing and Validation (Results) and Analysis

The simulation tool gives the results of tests or quizzes done by each individual, showing the number of quizzes done, the number of questions answered correctly, and the number of quizzes that failed. The simulator also indicates in which area of email security the user failed, i.e., clicking attachments, responding to suspicious email addresses, or failing to report suspicious email. This shows individual email security awareness.

The total number of people with their unique code or admission number is to be shown in the result charts showing the overall organization's email security position.

The results are relayed in percentage; for example, 75% of users fell victim before integrating email security with a human firewall, or 30% of the users fell victim after integrating a human firewall. The primary goal of phishing simulation is to raise awareness by offering straightforward instruction and a personalized evaluation (without any actual setup—no domain, infrastructure, or email address) to evaluate people's actions in a specific situation and determine their current awareness posture.

The goal of the red team evaluation is to identify IT weaknesses, including people and networks. The majority of organizations take numerous steps to increase perimeter security and patch vulnerabilities discovered, yet people remain the weakest link. Phishing is critical in determining employee security knowledge and enlisting them as members of the security team.

By utilizing engaging and straightforward training sessions, our phishing simulation allows users to grasp email security without actually doing the "real" phishing attack. This simulator provides a personalized environment in which you may create your exam according to your needs, such as making questions unique for each participant, simulating a real-time phishing assault, and making questions targeted and tough to answer.

Once the test is created, anyone in the target population can take it and submit their answers.

At the conclusion of the session, an analysis is offered to help you understand your current awareness posture. because the attackers simply need one click to get through! This makes us think twice about clicking that button. The simulator is designed into two modules: the administrator module and the client module. The admin module has a control panel that updates the database with the most current activities and also invites users to the simulator through email.

4.4.1 Admin Module

Administration module: This module (see figure 4.6) offers access to the configuration test and the analysis of views; it is accessible at the address AdminPanel/login.php (<http://localhost/AdminPanel/login.php>).

“admin” for user name and “admin” for password are the default login credentials.

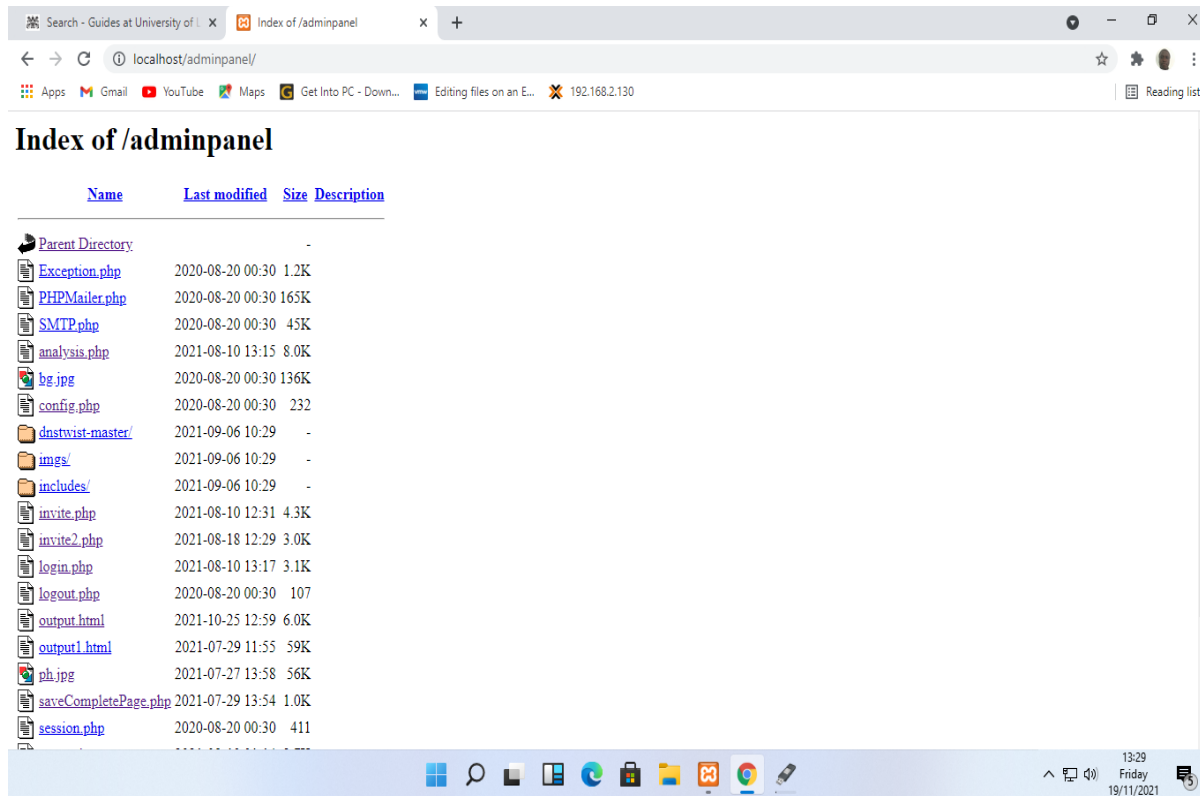


Figure 4.6: Admin-Module (Researcher, 2023)

4.4.1.1 The interface for the phishing simulator login page is as shown below:

Once the credential is placed, the system verifies and authenticates the user or denies access to ensure the security of the system is maintained. This module is controlled by mainly ICT personnel, who are in charge of maintaining and updating the system.

HUMAN FIREWALL SIMULATOR

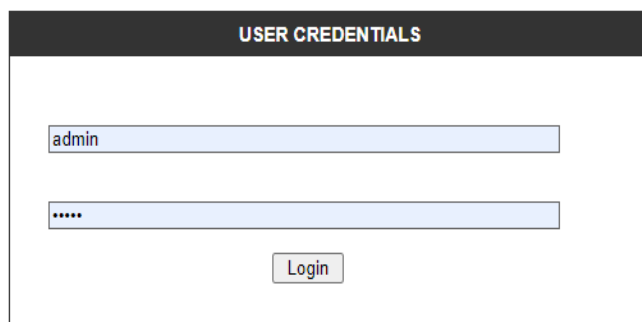
A screenshot of a login interface titled 'USER CREDENTIALS'. It features two input fields: the first contains the text 'admin' and the second contains six dots. Below the input fields is a 'Login' button.

Figure 4.7: Login Interface (Researcher, 2023)

4.4.2 Client Module

This is the module for those who only has access to the tutorial and the evaluation, and is accessed through <http://localhost/phishClient/> from of the panel index.

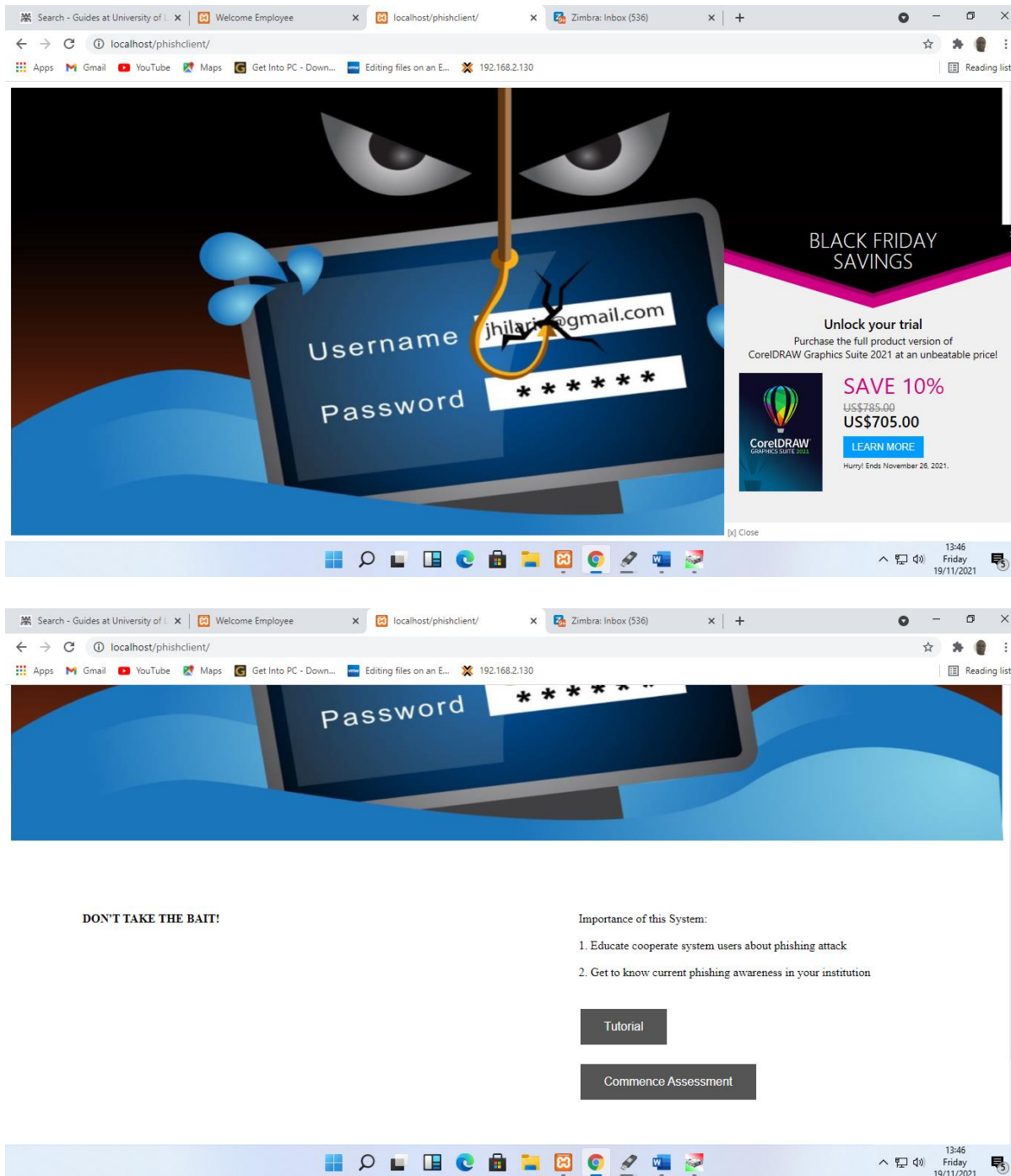


Figure 4.8: client side Interface (Researcher, 2023)

4.4.2.1 Tutorials (Client-Module)

This includes an introduction to phishing along with general tactics for raising awareness and educating people. This section contains presentation documents, links to videos, and links to online trainings, among others.

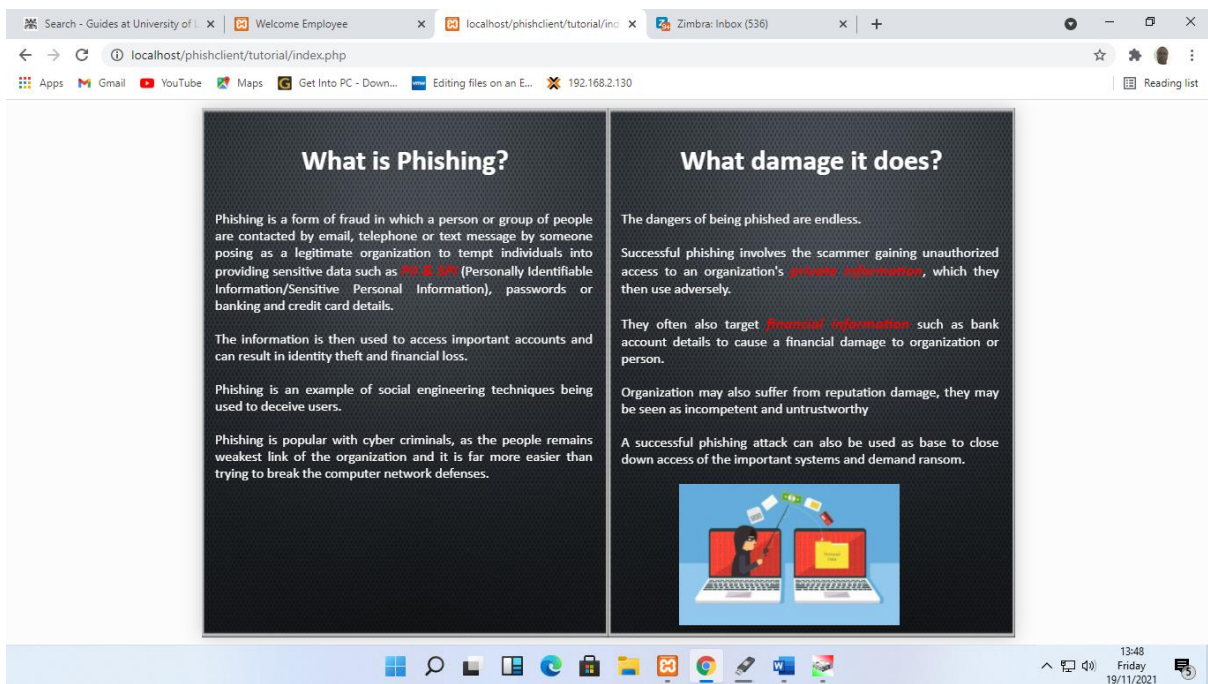
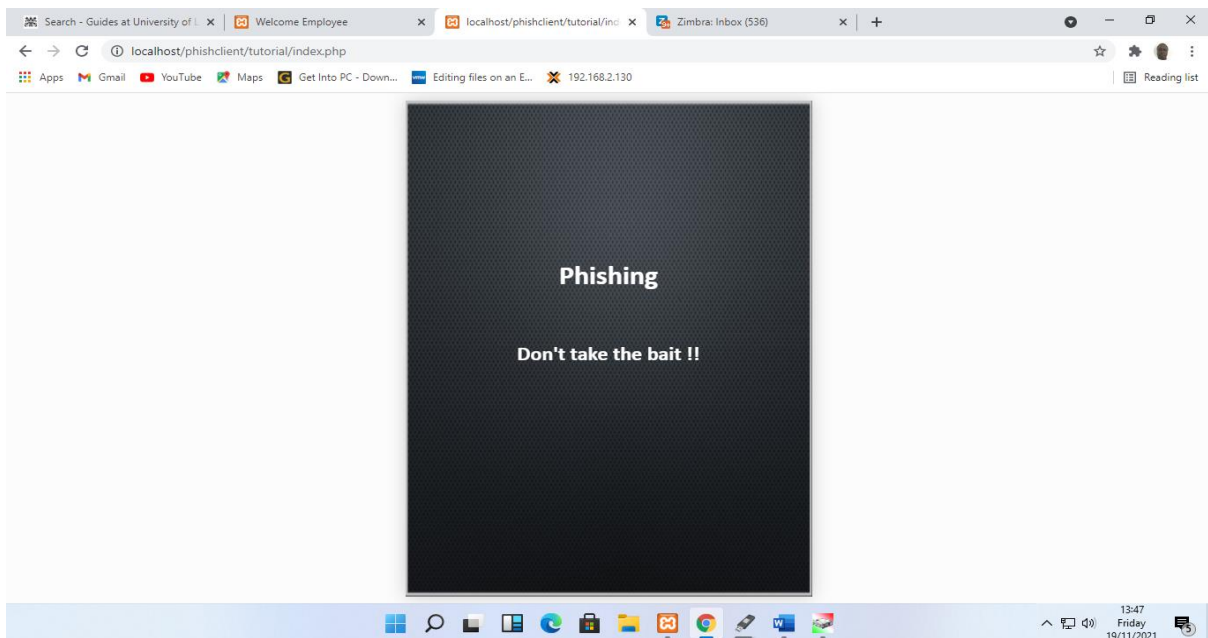


Figure 4.9: Tutorial (Client-side Module) (Researcher, 2023)

4.4.2.2 Evaluation (Client-side Module)

This stage prompts the user to choose between ignoring or reporting phishing or a site or scenario from SMiShing, and the user must choose between ignoring or reporting it. Even if the test code is the same, the questions are different for each user. There is a nice balance of positive and negative questions. Because it only takes one click for an attack to go through, all answers must be correct. When all questions are answered correctly, the system issues a certificate to the students. The certificates are issued in modules, and one must complete one module to move on to the next. See figure 4.10 below.

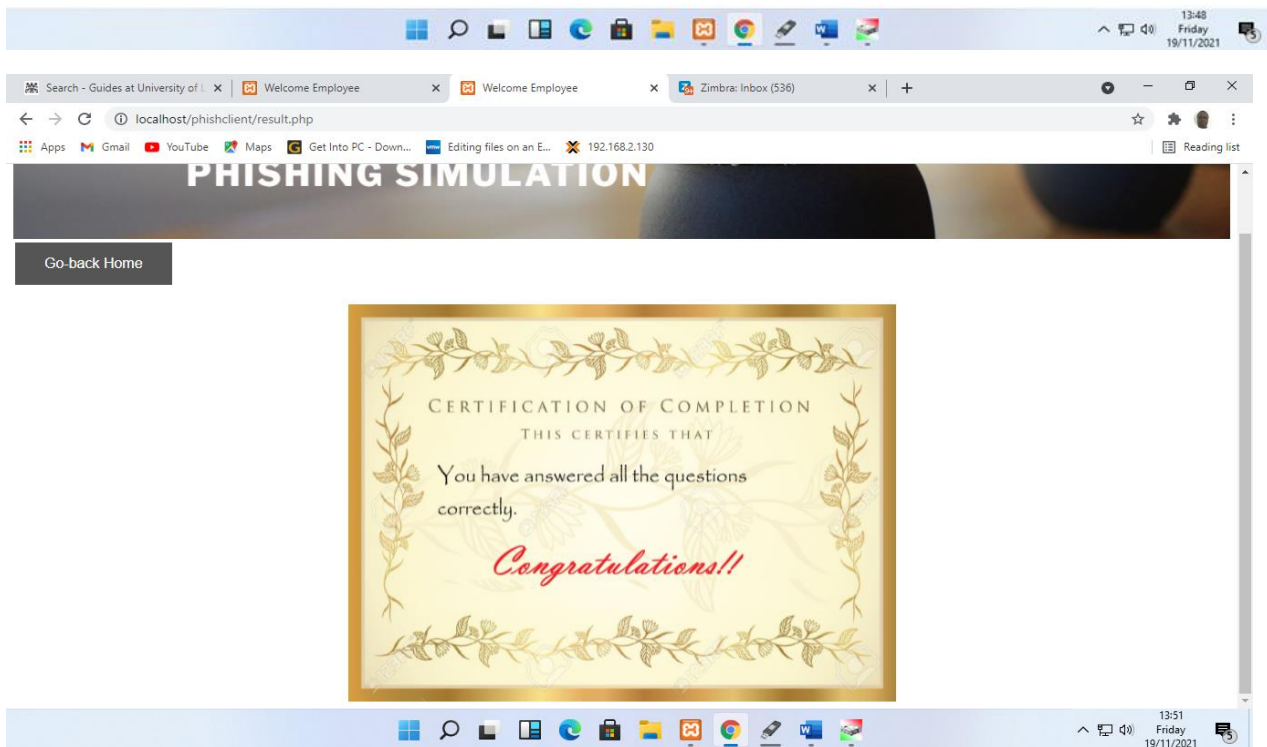
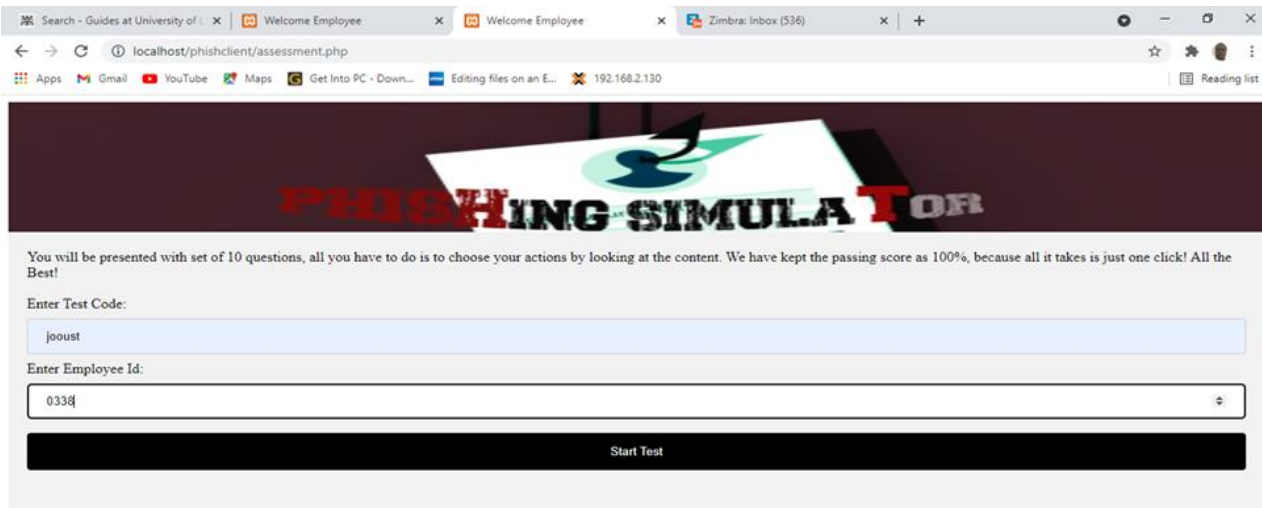


Figure 4.10: Assessment (Client-side Module) (Researcher, 2023)

4.4.3 Test Set up (Administrator Module)

In this section, the simulator asks for some basic information. As an example, enter your domain name here, and the simulator generates a list of comparable domains that attackers can use to target you. You can select

one to use throughout your phishing simulation evaluation.

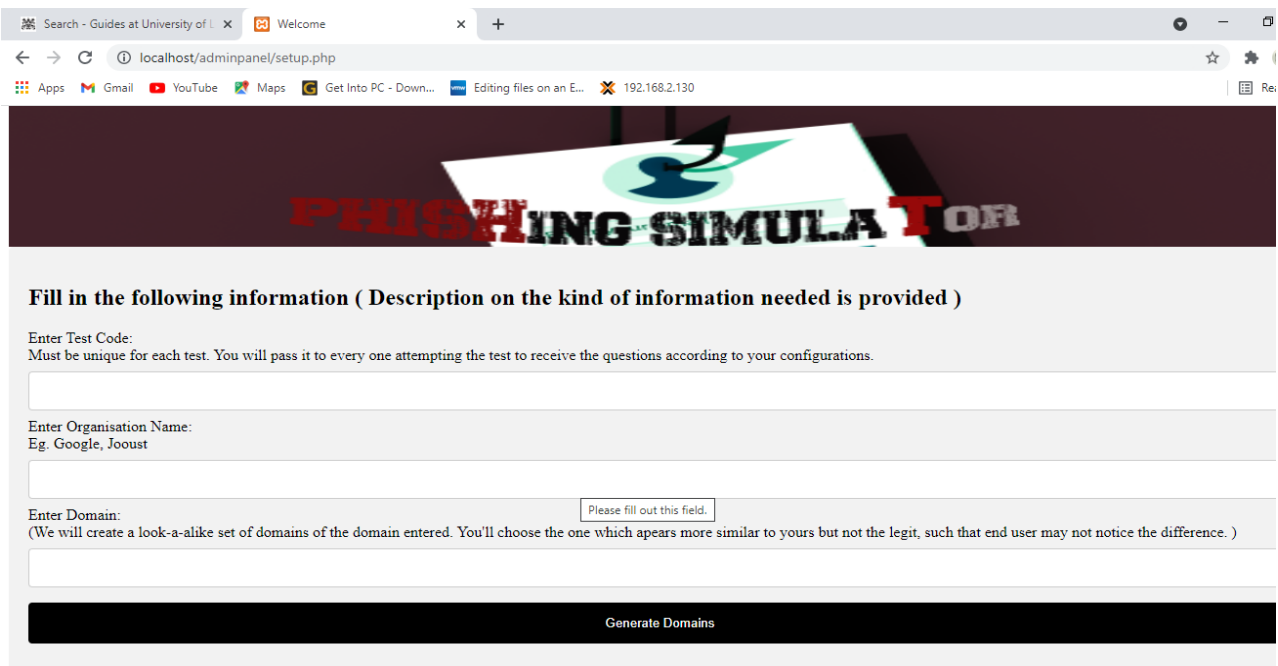
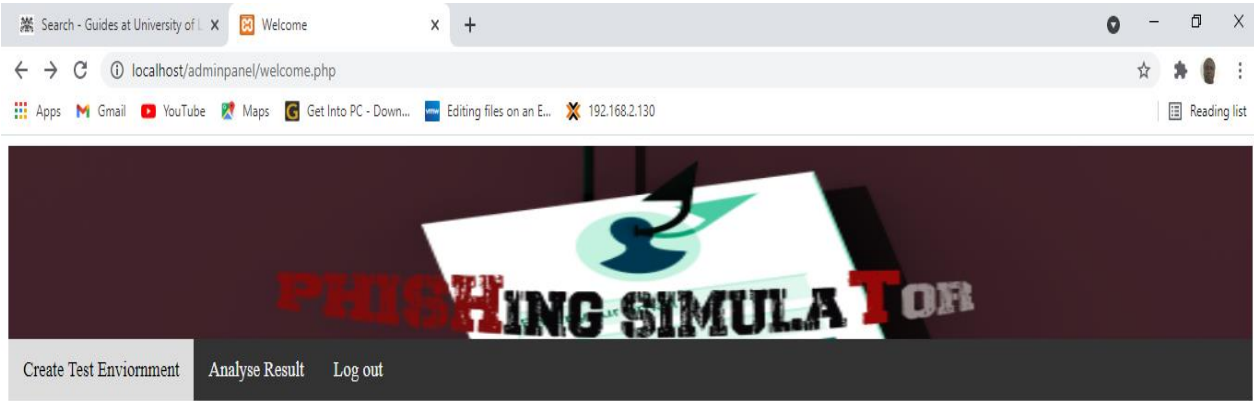


Figure 4.11: Setting up test (Admin Module) (Researcher, 2023)

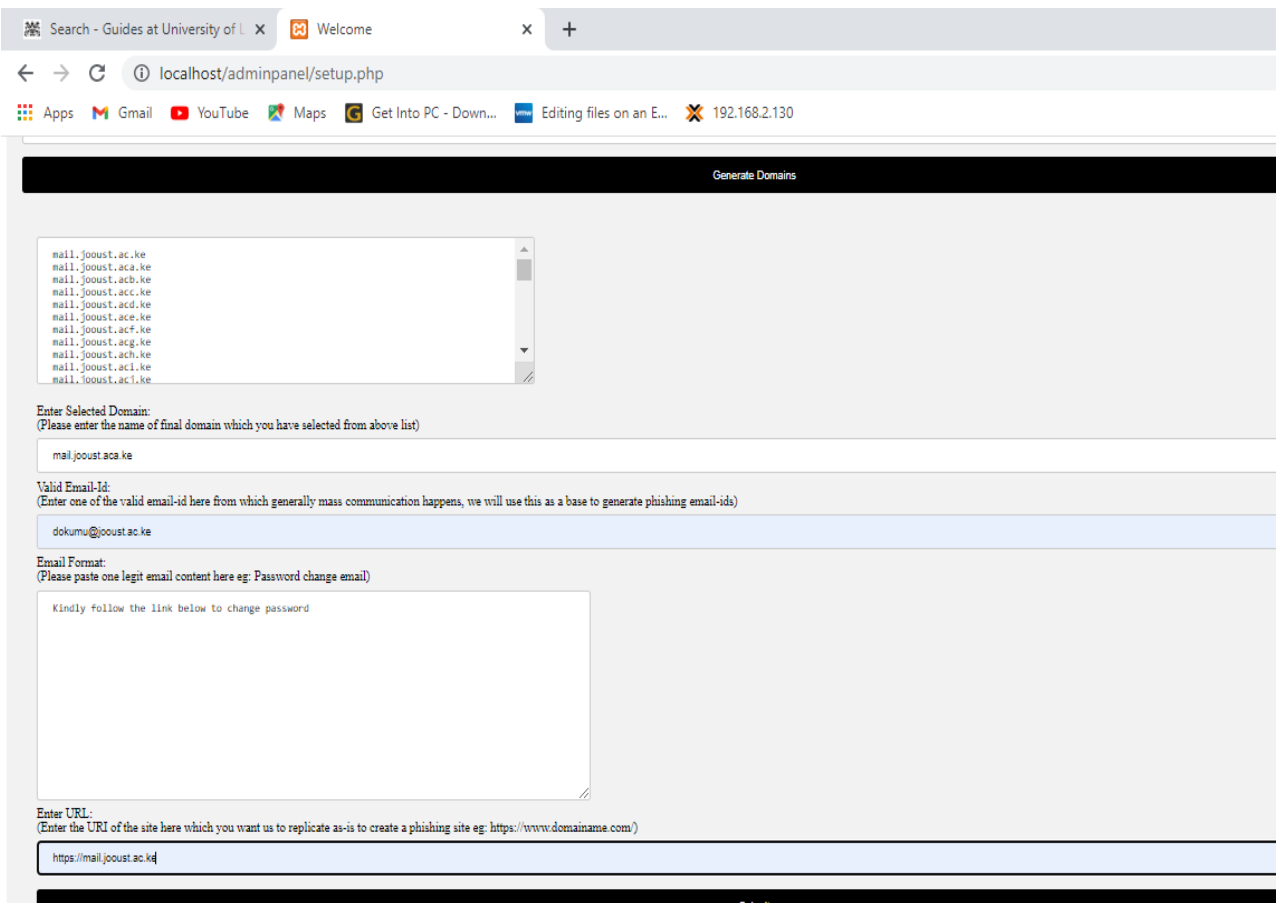


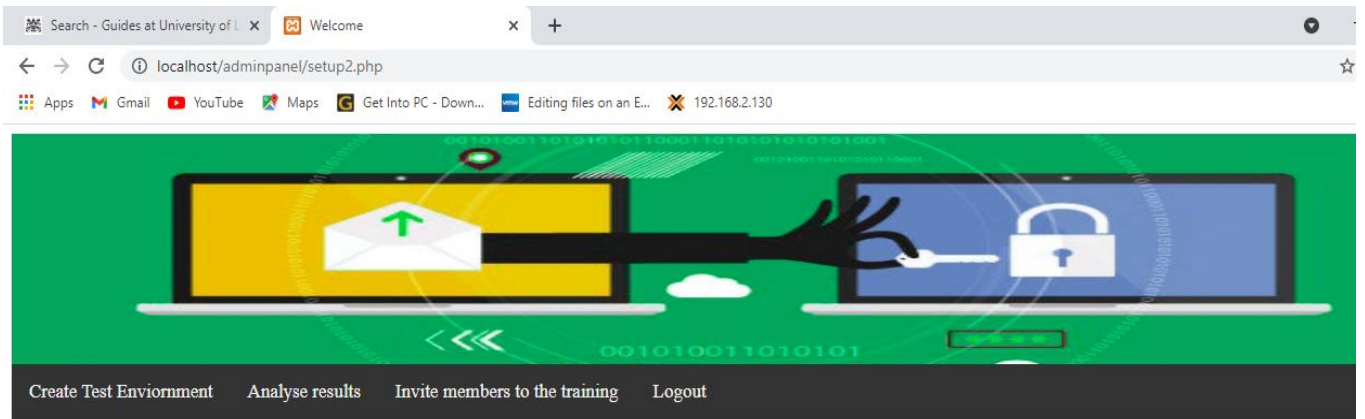
Figure 4.12: Create a similar web site displayed under your domain (Researcher, 2023)

When evaluating, you enter the URI of your most frequently visited websites, and it generates a similar website that is presented under your domain to create a realistic scenario. This is also known as "Typo squatting."

You can construct a test code for each service and a test configuration for each of them so that each receives a different phishing site, making the evaluation even more difficult.

Even if the test is the same, each employee has a separate set of questions.

Email ID: Here you must enter an email ID that is commonly used for mass communication. During the evaluation, the simulator produces more combinations of email addresses. You can see a preview of the phishing web page that we created to look like your original one.



Test Environment has been setup, you can go ahead and launch test
Please be patient, While we create your look a like site. Make sure you allow pop-up to view.
[Preview phised page](#)



Zimbra

Web Client

Username:

Password:

Stay signed in

[Forgot Password](#)

Version:

[Zimbra](#) :: the leader in open source messaging and collaboration :: [Blog](#) - [Wiki](#) - [Forums](#)

Copyright © 2005-2021 Synacor, Inc. All rights reserved. "Zimbra" is a registered trademark of Synacor, Inc.

Figure 4.13: Preview the appearance of the phishing web page that we created to look like the original one. (Researcher, 2023)

4.4.4 Invite (Admin Module)

Admin can upload CSV file and invite the members to take test. See figure 4.14 below.

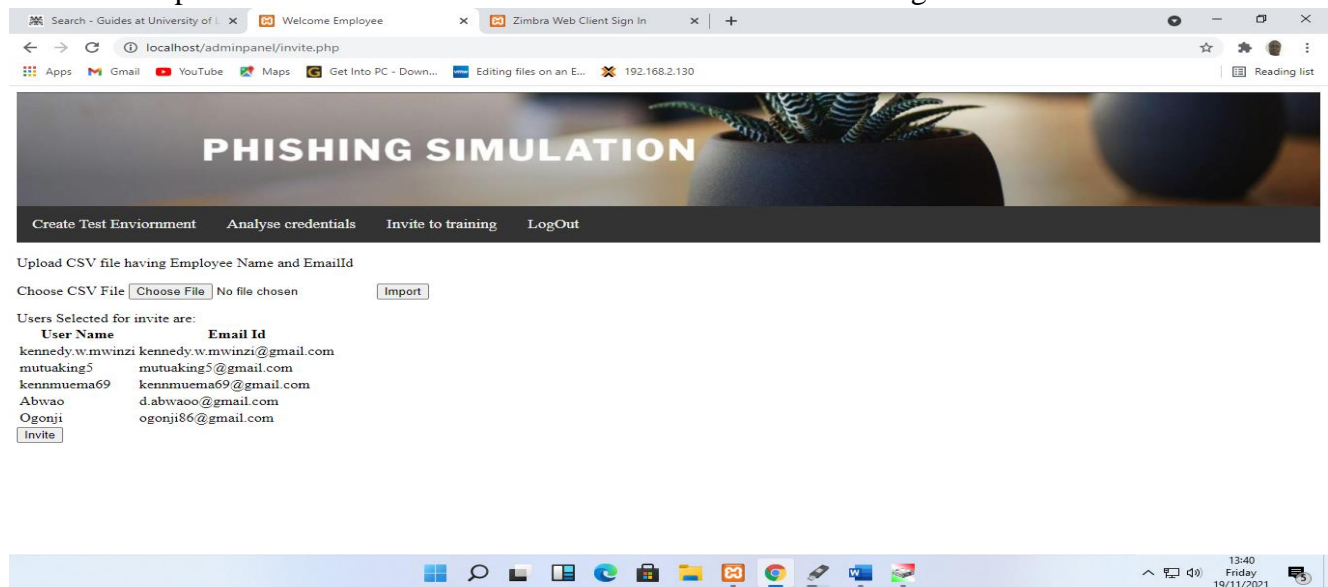


Figure 4.14: Admin can upload CSV file and invite the members to take test. (Researcher, 2023)

Email and contact details of clients to be invited are entered into a CSV Excel file, which is imported into the system for an automated invitation.

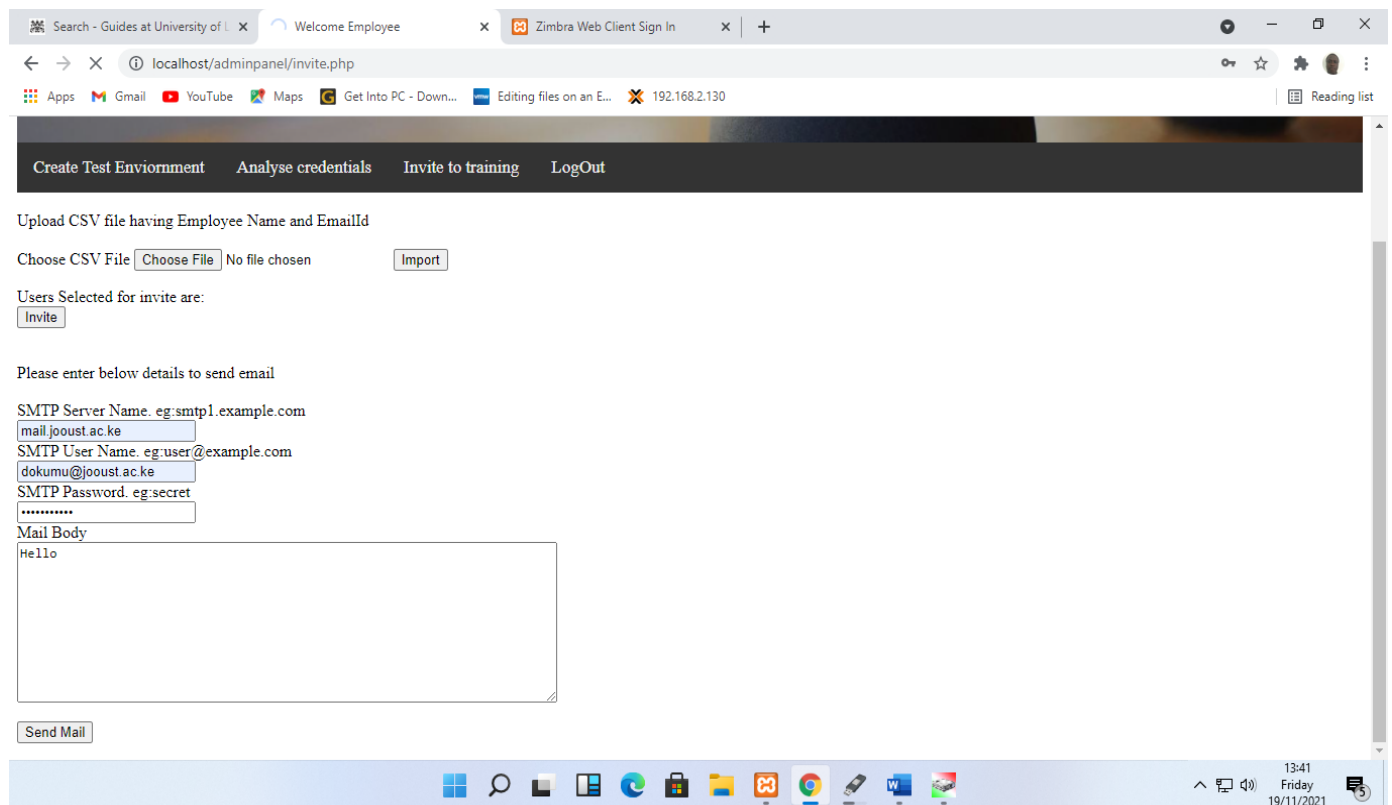


Figure 4.15: Enter SMTP server and administrator's email credentials to invite members. (Researcher, 2023)

4.4.5 Administrator Module (Analysis)

Analysis of data involves examination, categorization, tabulation, testing, and recombination of evidence to solve the research. (Yin, 2003)

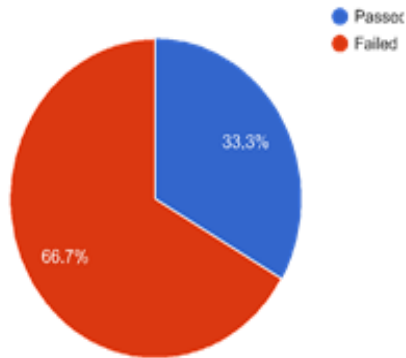
The first step involves pre-assessing user knowledge for social engineering attacks. The second step involves post-assessment assessment after proper training and awareness are given to the staff. In either case, a simulator is embedded in sample users to capture data on pre-assessment and post-assessment. According to Leedy & Ormrod, the data could be organized into tables, figures, and other formats to present information in a compact way. (Leedy, 2005)

The study gives the results in tables, forms, and graphs for representation. It includes a graphical analysis of the various responses provided by the trainees based on the answers provided in the quizzes. This assists in determining the organization's current outreach stance. See figure 4.16.

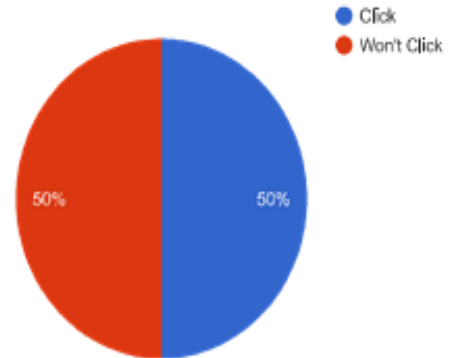
Select testcode for which you want to view analysis:

G1

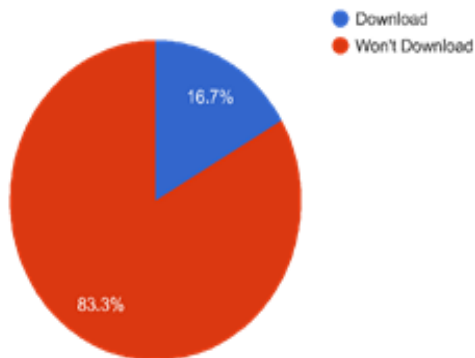
Number of employees who passed test



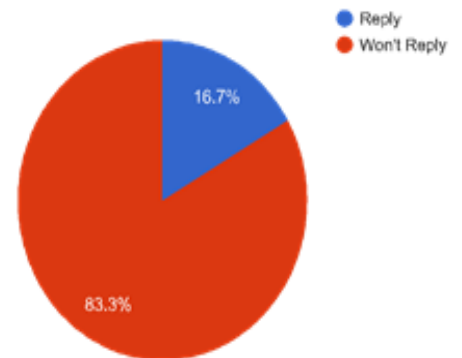
Number of employees who will click on the malicious links



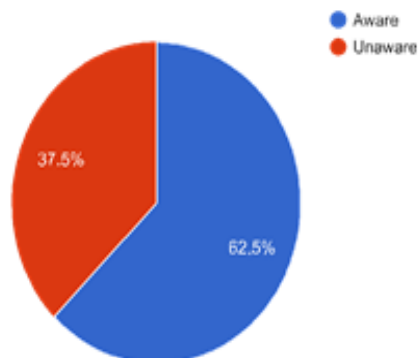
Number of employees who will download the dangerous attachments



Number of employees who will reply to phishing emails



Average awareness of the organisation



Employee wise result

Employee id	No of right answers
339	8
340	9
341	10
342	10
344	6
345	9

Figure 4.16: Analysis/ Results (Researcher, 2023)

4.4.5.1 Analysis of results (from figure 4.16)

1: Number of employees who passed the test: The result indicates the percentage of employees who passed the test versus those who failed. A repeated simulation indicates that the more the users get educated, the higher the percentage of those who pass the tests.

2: Number of employees who clicks on the malicious links: This result is specifically focused on testing employees who click on malicious links to test this area of insecurity. If organizations consider this security area to require more training, then a lot of training is to be focused on this area. The result is relayed in the percentage of those who would click on the malicious link versus those who wouldn't.

3: Number of employees who downloads the dangerous attachments: This result shows the percentage of employees who would download dangerous links compared to those who wouldn't. When a lot of questions are answered correctly in this area, the result indicates that many employees won't click on dangerous attachments. Either way, when a lot of questions in this area are answered wrongly, a higher percentage of employees are likely to click on dangerous attachments. The latter indicates a security threat to the organization.

4: Number of employees who reply to phishing emails: This result shows the percentage of employees who would reply to phishing emails versus those who wouldn't. When a lot of questions are answered correctly in this area, the result indicates that many employees won't reply to phishing emails. Either way, when a lot of questions in this area are answered wrongly, a higher percentage of employees are likely to reply to phishing emails. The latter indicates a security threat to the organization.

5: Average awareness of the organization: This result shows the percentage of employees' average awareness in the above areas tested (malicious links, downloading dangerous attachments, phishing emails). When a lot of questions from the above areas are answered correctly in this area, the result indicates high employees' awareness in terms of percentages. Either way, when a lot of questions in the above areas are answered wrongly, a higher percentage of employees are unaware. This helps guide organizations and corporations on the status of their security at a particular time.

6: Employees Wise results: This indicated how individual employees performed. The employees are identified through their employee ID, and the results are relayed out of ten questions. For example, employee ID 341 scored 10 out of 10 questions compared to employee ID 344, who scored 6 correct out of 10 questions. Tested. How wise the employees are to make the right choice in handling emails is tested through this section of results.

4.5 Summary of Chapter Four

This chapter discusses the technical requirements and setup for deploying the Human Firewall Simulator, including server infrastructure, user authentication mechanisms, database configuration, and system scalability for the organization's workforce.

CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This section discusses the technical requirements and setup for deploying the Human Firewall Simulator, including server infrastructure, user authentication mechanisms, database configuration, and system scalability for the organization's workforce.

5.1 Summary

This research aims to eliminate the need to configure an entire phishing campaign and a "live" environment, to provide a personalized assessment, to train users in targeted attacks, to provide an intuitive interactive interface to exercise the entire process, to involve users in the security team in making the firewall, and to eliminate the need to have a pen-tester or a specialist carry out a phishing campaign. This research also provides options to customize the simulator to adapt to the ever-changing trends in cybersecurity, especially email security. Just with a few clicks, the simulator allows the organization to know its employees in terms of strengths and weaknesses based on the analysis provided.

Employees are the greatest assets in a corporate environment; therefore, with the right education and guidance, they should turn out to be a great part of a robust email security setup. The results achieved above prove the success of the tool (to combat social engineering attacks). When combined with the technical security setups, i.e., firewalls, encryptions, virus scans, and many more, email insecurity threatening BECs and CEOs is tackled effectively.

An integrated email security system therefore ensures security from threats like ransomware, BEC/spear phishing attacks, configuration errors, and malicious links, all of which are now collectively tackled through this new security structure combining human firewalls.

The Human Firewall Simulator is a powerful tool designed to enhance security awareness and protect organizations against business email compromise (BEC) attacks. BEC attacks are a type of cyber threat in which attackers impersonate high-ranking executives or trusted business partners to deceive employees and gain access to sensitive information or financial assets.

The simulator aims to educate employees and strengthen their ability to recognize and respond to BEC attacks effectively. It provides a simulated environment where employees can learn about common BEC tactics, such as email spoofing, social engineering, and phishing. Through interactive exercises and real-world scenarios, employees can practice identifying suspicious emails, verifying sender identities, and detecting fraudulent requests.

The Human Firewall Simulator is a state-of-the-art tool created to promote security awareness and counter the expanding issue of Business Email Compromise (BEC). BEC assaults involve fraudsters posing as reliable organizations in order to trick workers into sending money, disclosing private information, or carrying out

unwanted tasks. By educating them about BEC strategies and teaching them how to spot and efficiently react to questionable emails, this simulator seeks to turn employees into an organization's first line of defense.

The Human Firewall Simulator incorporates various features to engage users and improve their security awareness. It may include interactive modules, quizzes, and educational resources to teach employees about BEC attack techniques and how to defend against them. The simulator may also offer personalized feedback and performance metrics to help employees track their progress and identify areas for improvement.

By using the Human Firewall Simulator, organizations can create a proactive security culture and empower employees to become the first line of defense against BEC attacks. The simulator's immersive and hands-on approach helps employees develop a critical mindset, enabling them to scrutinize emails, verify authenticity, and report suspicious activities promptly. Ultimately, this enhances the overall security posture of the organization and mitigates the risk of falling victim to BEC attacks.

The Human Firewall Simulator is a state-of-the-art tool created to promote security awareness and counter the expanding issue of Business Email Compromise (BEC). BEC assaults involve fraudsters posing as reliable organizations in order to trick workers into sending money, disclosing private information, or carrying out unwanted tasks. By educating them about BEC strategies and teaching them how to spot and efficiently react to questionable emails, this simulator seeks to turn employees into an organization's first line of defense.

Key Features:

1. Realistic Simulations: The simulator simulates a number of BEC scenarios, including CEO fraud, supplier invoicing hoaxes, and urgent fund transfer requests. These simulations closely resemble real BEC attacks, assisting staff members in experiencing and comprehending the strategies employed by fraudsters.

2. Interactive learning modules are offered by the application to educate staff employees on common BEC strategies such as email spoofing, social engineering, and domain impersonation. Users can learn through multimedia presentations, exams, and practical exercises.

3. The simulator maintains a database of emails that seem to be phishing attempts that the business has received. By practicing identifying these phishing attempts in a secure environment, employees can boost their confidence in their capacity to detect hazardous emails.

4. Dynamic Feedback: The simulator gives workers quick feedback on their interactions with simulated phishing emails. This involves pointing out warning signs, describing why an email is suspect, and assisting users in making the best decisions.

5. Customizable Scenarios: Businesses can create simulations that are specific to their industry, corporate culture, and threat environment. The relevance and efficacy of the training are improved by personalization.

6. The simulator tracks individual and team progress, enabling enterprises to evaluate the development of their security awareness as a whole. Managers have access to comprehensive reports that highlight their strengths and highlight areas that need further work.

7. Gamification features: The simulator includes gamification features like leaderboards, achievements, and awards to motivate staff. In order to acquire higher security awareness scores, staff are encouraged to engage in healthy competition.

8. Continuous Learning: By sporadically presenting fresh BEC challenges and scenarios, the Human Firewall Simulator promotes continuous learning. Employees are kept aware and informed about evolving cyber threats as a result.

An effective way to deal with the human factor in cybersecurity is to use the Human Firewall Simulator. Organizations may dramatically lower the risk of falling victim to these scams and improve their overall security posture by providing staff with the information and abilities to spot BEC attacks.

5.1.1 Summary of the objectives

1. Specific Objective 1: To identify various social engineering techniques used to compromise corporate email.

The various techniques used by attackers were identified as well as how they are mitigated. These includes Phishing, Spear Phishing, Pretexting, Baiting, Quid Pro Quo, Tailgating/Piggybacking, Impersonation, Watering Hole Attacks, Reverse Social Engineering, Pharming, Tailored Malicious Content and Elicitation

2. Specific Objective 2: To investigate current email security solutions available.

The email security options available were investigated through qualitative desk-based research, where it was established that the current email solutions available were not focused on turning employees into human firewalls. See table 2.1

3. Specific Objective 3: To develop and test human firewall simulator

Human Simulator was developed and tested. This is clearly shown in chapter four. The researcher designed a model that guided the development of Human Firewall simulator. The model was tested and results analyzed in form of charts and tables.

In summary, the Human Firewall Simulator is a comprehensive tool that leverages simulated environments, educational resources, and interactive exercises to raise security awareness among employees and protect organizations against business email compromise attacks. By training employees to be vigilant and knowledgeable about BEC threats, organizations can significantly reduce the likelihood of successful attacks and safeguard their sensitive information and financial assets.

5.2 Conclusions

The research has a conclusive solution to corporate email security based on the simulator's results, with all employees trained, empowered, and turned into members of the email security team.

Employees' minds are changed to take responsibility for securing the organization, therefore resolving the issue of employees or humans being the weakest link in email security.

The simulator is to be updated with the latest techniques used by hackers to guarantee that company personnel are up-to-date on the latest trends and are part of a global campaign to combat social engineering attacks. To make this simulated tool successful, organizations need to bring better problem-solving skills, faster task completion, competition that drives staff to excel at their jobs. Corporates should also strive to create an environment of teamwork hence increase employee decision-making efficiency. In order to educate users rather than train them (convert them to human firewalls), organizations and corporations should start by organizing security-oriented incentives to motivate the staff to take this education positively. Either there is a need to bring in external security professionals, as they are usually eager to get continuing education from external professionals to add credits to their education. The organization should update its policies to accommodate and reinforce rules for the employees to ensure that the tool is used regularly and actions taken by users are not deemed a threat to organizational email security.

In conclusion, the Human Firewall Simulator is a valuable tool for organizations seeking to enhance security awareness and protect against business email compromise (BEC) attacks. By providing employees with interactive training modules, realistic scenarios, and personalized feedback, the simulator empowers them to become the first line of defense against BEC threats.

Through mandatory training, tailored modules, and a culture of security, organizations can foster a proactive security mindset among employees. By simulating real-world BEC attack scenarios, employees can develop the skills to identify suspicious emails, verify sender identities, and respond appropriately. The gamified elements of the simulator engage employees and encourage active participation, while metrics and analytics allow organizations to measure progress and adapt the training program accordingly.

By integrating the Human Firewall Simulator with existing security measures and staying informed about evolving BEC attack techniques, organizations can establish a robust defense against this type of cyber threat. The simulator acts as a critical component in building a resilient security posture, ultimately safeguarding sensitive information and financial assets from BEC attacks. With continuous updates and a commitment to ongoing training and awareness, organizations can mitigate the risk of falling victim to BEC attacks and create a strong human firewall that serves as an effective defense against cybercriminals.

5.2.1 key assertions that drive this research to its effectiveness in improving an organization's cybersecurity posture

1. Human Vulnerability:

The simulator recognizes that people are frequently the weakest point in a company's cybersecurity defense. Costly security breaches can result from staff members' lack of awareness and vulnerability to social engineering assaults like BEC.

2. Education is empowerment:

The simulator claims that teaching staff about BEC strategies and procedures gives them the power to play a crucial role in the defense against such attacks.

Employees with better knowledge are more likely to recognize questionable emails and take the necessary action.

3. Realistic Simulations: The effectiveness of the simulator depends on the use of accurate BEC simulations. Employees have a better grasp of the strategies utilized by hackers by being exposed to realistic scenarios that mimic genuine attack methods.

4. Building Critical Thinking Skills: The simulator seeks to help workers develop their critical thinking abilities. It cultivates a more skeptical and cautious approach to email exchanges by encouraging them to query the veracity of emails, examine sender information, and consider the context of requests.

5. Continuous Learning: The idea put forth here is that cybersecurity is a continuous activity.

By gradually presenting new scenarios and obstacles, the simulator encourages continual learning and makes sure that staff members are alert and capable of adapting to new risks.

6. Practical Training: The simulator offers practical training in a secure setting. Without worrying about the consequences in the real world, employees can interact with simulated phishing emails, assess potential dangers, and make judgments. This hands-on learning experience strengthens knowledge and boosts self-assurance.

7. Feedback-driven Enhancement: A key element is immediate feedback on how users respond to simulated emails. This feedback process, it is claimed, fosters desirable behaviors and gives workers a chance to constructively learn from their failures.

8. Customization for Relevance: It is said that relevant simulations are more effective at capturing workers' attention. The simulator makes sure that the training is current and relatable by enabling firms to design situations based on their industry, culture, and particular dangers.

9. Behavioral Change: The simulator's overarching objective is to promote behavioral change. It contends that regular exposure to training exercises and simulations might result in a cultural shift within the company where security-conscious conduct is embedded in routine operations.

10. Measurement and Accountability: According to the simulator, keeping track of and reporting on progress is crucial. Organizations may hold workers accountable for their security awareness and pinpoint areas that require improvement by assessing the performance of both individuals and teams.

11. Gamification for Engagement: Using gamification components suggests that competition and engagement can serve as powerful motivators. The simulator promotes active participation and long-lasting interest by making security training interesting and rewarding.

The Human Firewall Simulator builds on these claims to develop a thorough and dynamic strategy to improve security awareness against BEC attacks. By addressing human vulnerabilities, fostering education, and encouraging proactive decision-making, the simulator strengthens an organization's defense against this pervasive cyber threat.

5.3 Recommendations

Eventually, the newly introduced and tested human firewall should be integrated into the already existing email security mechanisms as the last line of defense, bringing about the new email security model shown below in figure 5.1.

5.3.1 Model integrating Human Firewall with existing email security.

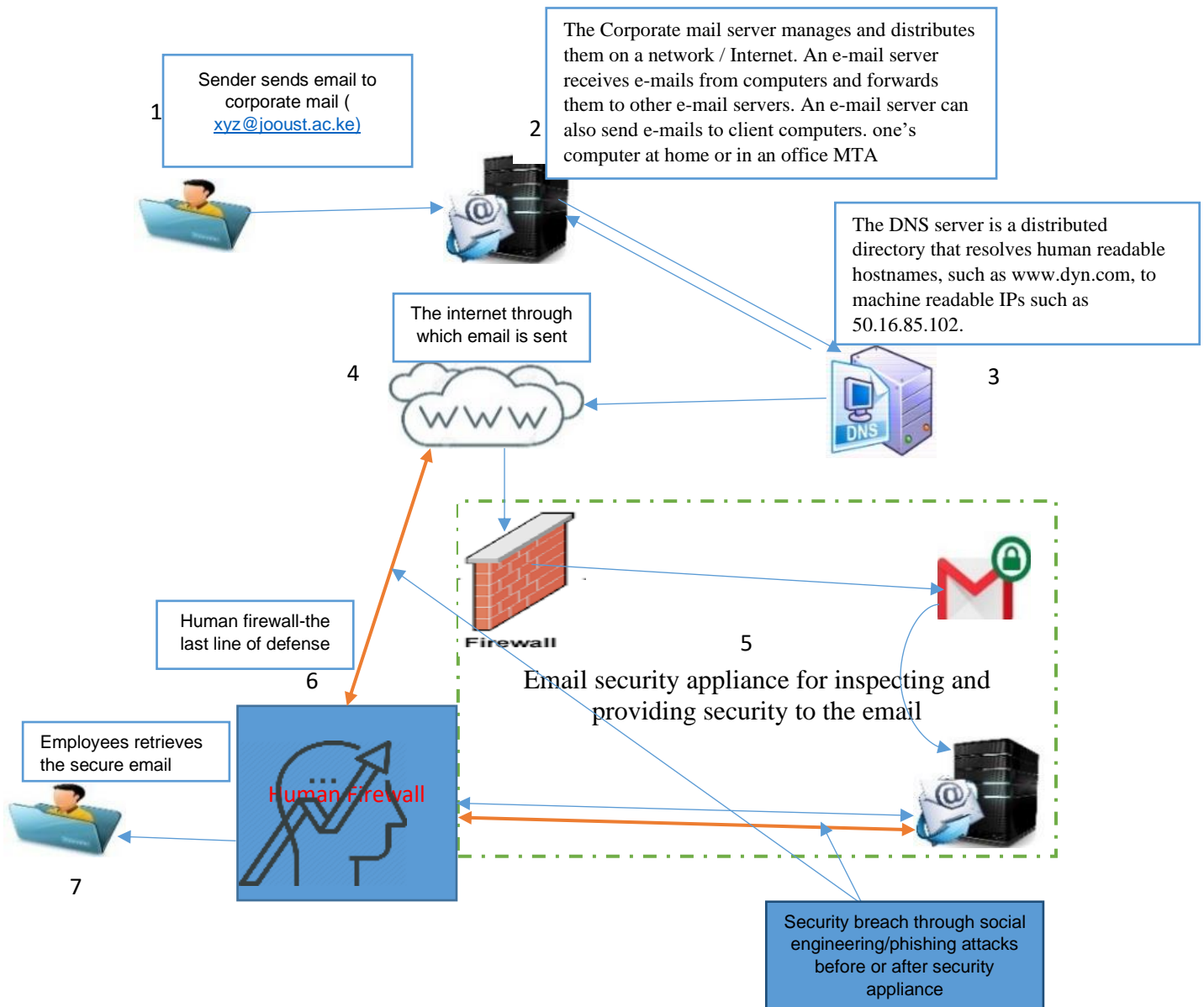


Figure 5.1: Secure email flow integrated with human firewall (Researcher, 2023)

This diagram shows the flow of email from the sender to the receiver. The weakest link is the user, meaning at the receiving point of the email, security goes wrong. Therefore, the need to create a firewall that helps solve problems associated with social engineering attacks—for example, phishing is possible only with the creation of a human firewall, which is the ultimate solution that has been lacking in the already existing logical and physical security measures that have always existed. The problem that has been lacking in email security is caused by human weakness. The human firewall introduces users to being part of the security team by making them responsible for their actions, i.e., avoiding clicking dangerous links by identifying them, flagging them, and being informed of the latest trends in attacks. This ensures security is tackled in totality in the future, and any improvements from the recommendations above would make corporate email even more secure.

To effectively utilize the Human Firewall Simulator for enhancing security awareness against business email compromise (BEC), consider the following recommendations:

1. **Human-Machine Synergy for Improved Defenses:** By linking machine learning to the Human Firewall Simulator, you present a comprehensive approach to cybersecurity training that leverages advanced technology to enhance participants' abilities to counter BEC threats effectively. This integration showcases the potential for combining human understanding and intuition with machine learning's analytical power to create a more resilient and proactive cybersecurity defense
2. **Implement mandatory training:** Make it mandatory for all employees, especially those with access to sensitive information or financial transactions, to complete the Human Firewall Simulator training. Regularly schedule refresher courses to reinforce the knowledge and skills learned.
3. **Tailor training to different roles:** Customize the training modules and scenarios to align with specific job roles and responsibilities within the organization. This ensures that employees receive targeted training relevant to their work and the types of BEC attacks they may encounter.
4. **Foster a culture of security:** Emphasize the importance of security awareness and the role every employee plays in protecting the organization. Encourage open communication and make reporting suspicious emails or incidents a priority. Reward and recognize employees who actively participate in training and demonstrate strong security practices.
5. **Provide real-time feedback:** Offer immediate feedback and guidance to employees as they navigate through the simulator. This helps them understand their strengths and weaknesses, allowing for continuous improvement. Incorporate personalized feedback and recommendations to address specific areas of improvement.
6. **Simulate real-world scenarios:** Develop realistic BEC attack scenarios within the simulator to expose employees to various tactics employed by attackers. This could include scenarios involving urgent payment requests, vendor impersonation, or executive spoofing. By experiencing these scenarios in a safe environment, employees can learn to identify warning signs and respond appropriately.
7. **Engage employees through gamification:** Gamify the training experience by incorporating leaderboards, achievements, and challenges. Encourage healthy competition among employees and departments, motivating them to actively participate in the simulator and improve their security awareness.
8. **Continuously update the simulator:** BEC attacks evolve over time, so ensure that the Human Firewall Simulator stays up-to-date with the latest attack techniques and trends. Regularly update the training modules and incorporate new simulation scenarios to reflect emerging threats.
9. **Measure and track progress:** Implement metrics and analytics to measure the effectiveness of the training program. Track employee performance, completion rates, and the number of reported incidents. Analyze the data to identify areas for improvement and adjust the training content accordingly.

10. Integrate with other security measures: The Human Firewall Simulator should complement other security measures within the organization. Integrate the training program with existing email security solutions, multi-factor authentication systems, and incident response protocols. Reinforce the importance of following security best practices in conjunction with the simulator training.

Stay informed and adapt. Stay updated on the latest trends, best practices, and countermeasures related to BEC attacks. Regularly assess the effectiveness of the human firewall simulator and adapt the training program as necessary to effectively address emerging threats.

By following these recommendations, organizations can maximize the impact of the Human Firewall Simulator in enhancing security awareness against BEC attacks and fortifying their defenses against this prevalent cyber threat.

5.4 Future Research Work

There is a constant need for innovation in security awareness training as the threat landscape changes and technology progresses. Continuous study and innovation in these fields may result in the creation of Human Firewall Simulators that are more efficient and adaptive and that better equip people and organizations to protect themselves from the evolving threat of Business Email Compromise. Here are some prospective study topics for the future:

1. Evaluation of Effectiveness: Conduct extensive research to assess the Human Firewall Simulator's long-term efficacy. Examine how the simulator affects fewer BEC incidences, user behaviour trends, and calculating the return on investment for businesses.
2. Integration with Security Operations: Investigate how the simulator can be integrated with a company's security operations centre (SOC) to facilitate quick incident response in the event of a real BEC threat.

5.5 Summary of Chapter Five

The threat of business email compromise (BEC) continues to pose a significant threat to organizations, prompting the development of the "human firewall" concept. This paper introduces the Human Firewall Simulator, a proactive approach to enhancing security awareness and preparedness among employees. The simulator immerses employees in realistic BEC scenarios, guiding them through decision-making processes to identify potential threats. Interactive modules cover various stages of an attack, including recognizing suspicious email addresses, verifying sender identities, and handling requests for sensitive information. The simulator's customization and continuous learning capabilities ensure its relevance in the face of evolving threats. The Human Firewall Simulator is a pivotal step in mitigating the risk of BEC attacks by providing hands-on experience and immediate feedback. It empowers employees to become vigilant defenders against social engineering tactics, reducing the likelihood of successful BEC attacks driven by human error. It complements technical security measures by addressing the often-overlooked human element, aligning with the principle that security is a shared responsibility. Organizations should integrate the Human Firewall Simulator into their existing security training programs, regularly assess employees' progress, customize the

simulator to reflect industry-specific BEC scenarios and challenges, introduce incentives or rewards for employees who consistently excel in simulator exercises, encourage senior management participation, and continuously update the simulator to address emerging BEC tactics and trends. By investing in this innovative training tool, organizations can significantly strengthen their defense against BEC and similar social engineering attacks.

REFERENCES

- Abbasi, D. F. (2018, September 06). *Advanced Deception with BEC Fraud Attacks*. Retrieved from <https://www.trustwave.com>: <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/advanced-deception-with-bec-fraud-attacks/>
- Acquaye, A. D. (2020). A Study of the Awareness of Security and Safety Culture Among Employees Across Organizations. *TEXILA INTERNATIONAL JOURNAL OF MANAGEMENT*, 115–128. doi:<https://doi.org/10.21522/tijmg.2015.se.19.02.art013>
- Akamai. (2017). *State of the Internet Report*. USA: Akamai. Retrieved from akamai.
- Alam, M. (2023, July 3). *Why You Must Use AI for Email Security Against Cyber Threats*. Retrieved from Ai For Email Security: <https://www.mailmodo.com/guides/ai-for-email-security/>
- Amy McLaughlin. (2019, November 15). *Cyber Security is Not a Department: Building an Information Security Culture*. Retrieved from <https://www.brighttalk.com/webcast>: https://www.brighttalk.com/webcast/288/377659?utm_campaign=knowledge-feed&utm_source=brighttalk-portal&utm_medium=web
- APWG. (2014). *Phishing Activity Trends Report*. Washington DC: APWG.
- Berninger, A. (2018, February 21). *Security intelligence*. Retrieved from IBM X-Force IRIS Uncovers Active Business Email Compromise Campaign Targeting Fortune 500 Companies: <https://securityintelligence.com/ibm-x-force-iris-uncovers-active-business-email-compromise-campaign-targeting-fortune-500-companies/>
- Boote, D. N. (2005). On the Centrality of the Dissertation Literature Review in Research Preparation. *Educational Researcher*. *Scholars Before Researchers*., 3-15. Retrieved from <https://doi.org/10.3102/0013189x034006003>
- Brook, C. (2020, August 18). *What Does a Data Breach Cost in 2020?* Retrieved from digitalguardian: <https://digitalguardian.com/blog/what-does-data-breach-cost-2020>
- Christina Lekati. (2020, September). *CREATING A “HUMAN FIREWALL” FOR IT SECURITY*. Retrieved from dotmagazine: <https://www.dotmagazine.online/issues/securing-the-future/human-firewall-for-it-security>
- Cialdini, R. B. (2007). *The psychology of persuasion*. New York: : Collins.
- Cisco. (2010, 12). *Email Security Deployment Guide*. Retrieved from www.cisco.com: https://www.cisco.com/c/dam/global/en_ca/solutions/strategy/docs/sbaBN_email_secDG.pdf
- Cisco. (2021). Cisco Secure Email. *Cisco Secure*, 3-16.
- CISOMAG. (2019, November 08). *Insider Sold 68K Customer Records to Scammers: Trend Micro*. Retrieved from cisomag.eccouncil.org: <https://cisomag.eccouncil.org/insider-sold-68k-customer-records-to-scammers-trend-micro/>
- Clearswift. (2021). Clearswift Secure Email Gateway. *Secure Email Gateway*, 1-3.
- Cloudmark. (2016, April 14). *The Top 5 CEO Email Wire Fraud Attacks: Rising in Frequency, Increasing in Financial Losses*. Retrieved from <https://blog.cloudmark.com>: <https://blog.cloudmark.com/2016/04/14/the-top-5-email-wire-fraud-email-attacks-rising-in-frequency-increasing-in-financial-losses/>
- Comtech. (2017, February 22). *comtech-networking*. Retrieved from The Human Firewall: <http://www.comtech-networking.com/blog/item/274-the-human-firewall>
- Datta, P. W. (2021). A Perfect Storm. *Digital Threats: Research and Practice*, 1-21. Retrieved from <https://doi.org/10.1145/3428157>

- ENISA. (2021, April 01). *The European Union Agency for Cybersecurity*. Retrieved from ENISA Threat Landscape 2021: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>
- Etal, P. (2021, August 31). *Exchange Online Protection service description*. Retrieved from Microsoft office 365: <https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-protection-service-description/exchange-online-protection-service-description>
- FBI. (2016). *Business E-mail Compromise: The 3.1 Billion Dollar Scam*. New York: This Public Service Announcement (PSA).
- Frumento, E. (2018, July 10). *Social Engineering: an IT Security problem doomed to get worse*. Retrieved from <https://medium.com: https://medium.com/our-insights/social-engineering-an-it-security-problem-doomed-to-get-worst-c9429ccf3330>
- Gatner. (2017, 1 1). *Human firewall*. Retrieved from <https://www.humanfirewall.io: https://www.humanfirewall.io/howit.php#howitwork>
- Gerritsen, J. (2012). HOW TO WRITE AN ARTICLE ABOUT A STUDY FOR A PEER-REVIEWED JOURNAL. *Pediatric Pharmacology*, 46. Retrieved from <https://doi.org/10.15690/pf.v9i2.245>
- Getthreatready. (2017, February 24). *Email And The Human Firewall*. Retrieved from <https://www.getthreatready.com: https://www.getthreatready.com/email-human-firewall/>
- Gogodze, J. (2019). Ranking-Theory Methods for Solving Multicriteria Decision-Making Problems. In *Advances in Operations Research* (pp. 1–7.). Retrieved from <https://doi.org/10.1155/2019/3217949>
- Hernedy, R. (2016, January 11). *Threats 101*. Retrieved from What is Business Email Compromise BEC Attack?: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes>
- Jason. (2012, January 1). *Communication of the ACM*. Retrieved from <https://dl.acm.org/doi/10.1145/2063176.2063197>
- Johnson, S. (2014, March 01). *Social engineering attacks: Is security focused on the wrong problem?* Retrieved from www.Search Security-Techtarget.com: https://searchsecurity.techtarget.com/feature/Social-engineering-attacks-Is-security-focused-on-the-wrong-problem
- Kaplan, D. (2018, April 17). *Here is an Email Thread of an Actual CEO Fraud Attack*. Retrieved from <https://www.trustwave.com: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/here-is-an-email-thread-of-an-actual-ceo-fraud-attack/>
- KI, A. (2023, July 13). *8 Best Anti-Phishing Solutions for Businesses in 2022*. Retrieved from The Sec Master: <https://theseccmaster.com/8-best-anti-phishing-solutions-for-businesses-in-2022/>
- Kohlbacher, F. (2006, January 21). *The Use of Qualitative Content Analysis in Case Study Research*. Retrieved from [Forum Qualitative Sozialforschung / Forum: Qualitative Social Research \(FQS\): https://www.qualitative-research.net/index.php/fqs/article/view/75/153](http://Forum Qualitative Sozialforschung / Forum: Qualitative Social Research (FQS): https://www.qualitative-research.net/index.php/fqs/article/view/75/153)
- LaMorte, W. W. (2019., September 9). *The Social Cognitive Theory*. Retrieved from Behavioral Change Models: <https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangengetheories/BehavioralChangeTheories5.html>
- LeClaire, J. (2006, November 1). *Holiday Scammers' E-Greeting Card Tactics*. Retrieved from MALWARE: <https://www.ecommercetimes.com/story/53889.html>
- Leedy, P. D. (2005). *Practical research*. Saddle River, NJ, USA: Pearson Custom.
- Macris. (2011, july). *Enhancing Enterprise Resource Planning users' understanding through ontology-based training*. Retrieved from Computers in Human Behavior: https://doi.org/10.1016/j.chb.2010.09.013

- Marcos. (2014). "Human error" contributes to nearly all cyber incidents, study finds. *Cybersecurity source*, 1-2.
- Marianne et al. (2017, January 10). *A New In-Depth Analysis of Anthem Breach*. Retrieved from bank info security: <https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>
- Mark Guntrip. (2020, February 27). *Ensuring that Your Users are the Solid Line of Defense Against Cyber Threats*. Retrieved from Bright talk: https://www.brighttalk.com/webcast/13513/382659?player-preauth=VicWfpBwC3YUmgImm%2FhjBP4RONz%2B04I%2B8Yq9%2BKuhRIA%3D&utm_source=brighttalk-recommend&utm_campaign=network_weekly_email&utm_medium=email&utm_content=collab&utm_term=092020
- Mimecast. (2015, August 01). *THREE WAYS TO IMPROVE THE "HUMAN FIREWALL" AND STRENGTHEN EMAIL SECURITY*. Retrieved from <https://www.mimecast.com>: <https://www.mimecast.com/blog/2015/08/three-ways-to-improve-the-human-firewall-and-strengthen-email-security/>
- Mitnick et al. (2002). *THE ART OF DECEPTION*. . Indianapolis:: Wiley.
- Nabila, N. (2019). Toward Detecting Malicious Activities in Online Social Network through User Behavior. *International Journal for Research in Applied Science and Engineering Technology*, 1114–1118. Retrieved from <https://doi.org/10.22214/ijraset.2019.3197>
- Nguyen, D. (2015, March 12). *5 Ways Hackers are Stealing Passwords*. Retrieved from Hypersecu Blog: <https://hypersecu.com/blog/91-5-ways-hackers-are-stealing-passwords>
- Onyango, K. (2018). *Jooust Email Communications*. Bondo: Jooust ICT Directorate.
- Orlando. (2018). The 'human firewall': a more proactive approach to infosec. *The cybersecurity source*, 1-3.
- Paganini, P. (2013). *Two-factor Authentication for SMBs*. Retrieved from securityaffairs: <http://securityaffairs.co/wordpress/15786/security/two-factor-authentication-for-smb.html>
- Pasterfield, L. (2020, February 01). *Build a 'human firewall'*. Retrieved from Cyber security Europe: <https://www.cseurope.info/build-a-human-firewall/>
- Porter, J. (2016). *The CEO's Guide to Navigating the Threat Landscape*. mexico: AT&T Cybersecurity Insights Volume 4. Retrieved from <https://www.business.att.com>.
- Proofpoint. (2020). Proofpoint Email Protection. *Proofpoint*, 1-2.
- Proteck. (2017, May 2). What is a Human Firewall? *What the tech*.
- Purup, P. B. (2020). Research framework for development of building performance simulation tools for early design stages. *Automation in Construction*, 109. Retrieved from <https://doi.org/10.1016/j.autcon.2019.102966>
- Sabi. (2019, March 07). *Scammers' "wire-wire" trick exposed*. Retrieved from www.sabinews.com: <https://www.sabinews.com/scammers-wire-wire-trick-exposed/>
- Sadler, T. (2021, July 08). *Human Layer Security: The Ultimate Guide to Human Layer Security*. Retrieved from www.tessian.com: <https://www.tessian.com/blog/what-is-human-layer-security/>
- Samani, R. a. (2015). "Hacking the Human Operating System: The Role of Social. " <http://www.mcafee.com/au/resources/reports/rp-hackinghuman-os.pdf> Retrieved 1 June, 2015.
- Samson, R. (2021, September 29). *mail Security Awareness Training for Your Employees: The Importance and Reducing the Risks of Successful Cyber Attacks*. Retrieved from ClearNetwork, In: <https://www.clearnetwork.com/email-security-awareness-training/>
- Schablik et al. (2017, November 8). *Threat Ready resources*. Retrieved from www.getthreatready.com: <https://www.getthreatready.com/three-key-elements-building-effective-human-firewall/>

- Security, (. H. (2014, July 30). *Continuous monitoring for enterprise incident response - Help Net Security*. Retrieved from Help Net : <https://www.helpnetsecurity.com/2014/07/30/continuous-monitoring-for-enterprise-incident-response/>
- Shaikh, A. N., Shabut, A. M., & Hossain, M. (2016). A literature review on phishing crime, prevention review and investigation of gaps. *ieeexplore*. Chengdu, China: IEEE.
- Singh, A. S. (2014). SAMPLING TECHNIQUES & DETERMINATION OF SAMPLE SIZE IN APPLIED STATISTICS RESEARCH: AN OVERVIEW. *International Journal of Economics, Commerce and Management*, 15-16.
- Sjouwerman. (2017, February 19). *Security Awareness Training Blog*. Retrieved from knowbe4: <https://blog.knowbe4.com/7-urgent-reasons-for-creating-a-human-firewall>
- Smith, M. (2015, January 20). *25 most commonly used and worst passwords of 2014*. Retrieved from PRIVACY AND SECURITY FANATIC: <https://www.csoonline.com/article/2872085/25-most-commonly-used-and-worst-passwords-of-2014.html>
- Stolfo, S. J. (2003, January 1). *Behavior-Based Approach to Securing Email Systems*. doi:https://doi.org/10.1007/978-3-540-45215-7_5
- Sussman, B. (2019, September 11). *Business Email Compromise Losses Jump 100%*. Retrieved from secureworld: <https://www.secureworld.io/industry-news/new-business-email-compromise-statistics-bec>
- Team, B. (2023, July 23). *What Is Data Loss Prevention? Starter Guide To Email DLP*. Retrieved from Beyond Encryption: <https://www.beyondencryption.com/blog/what-is-data-loss-prevention>
- Tim, S. (2021, July 08). *Human Layer Security*. Retrieved from The Ultimate Guide to Human Layer Security: <https://www.tessian.com/blog/what-is-human-layer-security/>
- Tschabitscher. (2018). *How to Protect Your Password From Getting Stolen*. Retrieved from www.lifewire.com: <https://www.lifewire.com/stealing-a-password-1164408>
- Winder, D. (2018, May 23). *Social engineering: the biggest security risk to your business*. Retrieved from IT Pro: <https://www.itpro.co.uk/social-engineering/30017/social-engineering-the-biggest-security-risk-to-your-business>
- Writes, C. (2023, August 30). *Email Authentication Protocols: SPF, DKIM, and DMARC – A Detailed Guide*. Retrieved from GBHackers - Latest Cyber Security News | Hacker News.: <https://gbhackers.com/email-authentication-protocol/>
- Yin, R. K. (2003). *Designing case studies. Qualitative research*.
- Zola, A. (2021, December 15). *Spam filter*. Retrieved from Security: <https://www.techtarget.com/searchsecurity/definition/spam-filter>

APPENDICES

APPENDIX 1: Communication from XYZ University webmaster

Timbra

dokumu@xyz.ac.ke

Fake JOOUST email communications

From : Kevin Onyango <kenyango@jooust.ac.ke> Fri, Oct 26, 2018 10:28 AM
Subject : Fake JOOUST email communications
To : staffmembers <staffmembers@jooust.ac.ke>

Dear Staff Members,

Please treat all email communication regarding JOOUST services that do not originate from a genuine xyz.ac.ke email address as HOSTILE. Report such communication to the ICT Directorate immediately, in order for us to take action.

Please see the example below:

----- Forwarded Message -----
From: "patodirector@jooust.ac.ke" <patodirector@jooust.ac.ke>
Sent: Friday, October 26, 2018 12:24:37 AM
Subject: New Security 9.5 Update

Important!

According to our records, this account has not been upgraded to the new WebMail 9.5 for Advanced security features Kindly visit the member service area or Sign In to upgrade immediately.

<http://zmcmmncao.tk/> Sign In to upgrade immediately.

-----Disclaimer: The Information contained in this e-mail including attachments is confidential information intended only for the addressee(s). If you have received this communication in error, please notify us and delete or destroy any copies.

--

Kind Regards,
Kevin Onyango,
Directorate of ICT

Kenya Open University of Science & Technology (KOUST).

APPENDIX 2: Coding for the program

Login code

```
1  <?php
2  include("config.php");
3  session_start();
4  $error="";
5  if($_SERVER["REQUEST_METHOD"] == "POST") {
6      // username and password sent from form
7
8      $myusername = mysqli_real_escape_string($db, $_POST['username']);
9      $mypassword = mysqli_real_escape_string($db, $_POST['password']);
10
11     $sql = "SELECT id FROM admin WHERE username = '$myusername' and
password =
    '$p
    '";
12     $result = mysqli_query($db, $sql);
13     $row = mysqli_fetch_array($result MYSQLI_ASSOC);
14     $active = $row['active'];
15
16     $count = mysqli_num_rows($result);
17
18     // If result matched $myusername and $mypassword, table row must be
1 row
19
20     if($count == 1) {
21         // session_register("myusername");
22         $_SESSION['login_error'] = $myusername;
23
24         header("location: welcome.php");
25     }else {
26         $error = "Your Login Name or Password is invalid";
27     }
28 }
29 ?>
30 <html>
31
32 <head>
33 </?></?>
34 <title>Login Page</title>
35
36 <style type = "text/css">
37     body {
38         font-family:arial, Helvetica, sans-serif;
39         font-size:14px;
40         background-image: url("bg.jpg");
41     }
42     label {
43         font-weight:bold;
44         width:100px;
45         font-size:14px;
46     }
47     box {
48         border:#666666 solid 1px;
49     }
```



```

50     </style>
51
52 </head>
53
54 <body bgcolor = "#FFFFFF">
55
56     <div align = "center">
57         <div style = "width:300px; border: solid 1px #333333; " align =
"left">
58             <div style = "background-color:#333333; color:#FFFFFF;
padding: 3px;"><b>Login</b></div>
59
60             <div style = "margin:30px">
61
62                 <form action = "" method = "post">
63                     <label>UserName: <br/></label><input type =
"username"
64                         class = "box"/><br/><br/>
65                     <label>Password: <br/></label><input type = "password"
name = "password" class = "box" /><br/><br/>
66                     <input type = "submit" value = " Submit " /><br/>
67                 </form>
68
69                 <div style = "font-size:11px; color:#cc0000; margin-
top:10px"><?php echo
70                     $name . ?></div>
71
72             </div>
73
74         </div>
75
76     </body>
77 </html>

```

Analysis Code

```

1  <?php
2  error_reporting(0);
3  include ('session.php');
4  include_once 'config.php';
5  ?>
6  <html>
7
8
9
10
11 <title>Welcome Employee</title>
12 
13 <style>
14 <selectBox[

```

```

12 border-radius:4px;border:1px solid #333333;background: none repeat
scroll 0 0 #FFFFFF;
13 background-color: #e0e0e0; height: 23px;
14 ↓
15 ↓ navbar a:hover {
16 background: #ddd;
17 color: black;
18 ↓
19 ↓ navbar a {
20 float: left;
21 display: block;
22 color: #f2f2f2;
23 text-align: center;
24 padding: 14px 16px;
25 text-decoration: none;
26 font-size: 17px;
27 ↓
28 ↓ navbar {
29 overflow: hidden;
30 background-color: #333;
31 top: 0;
32 width: 100%;
33 ↓
34 </style>
35 </head>
36 <body>
37 <div class="navbar">
38 <a href="setup.php">Setup Test Environment</a>
39 <a href="analysis.php">Analysis</a>
40 <a href="invite.php">Invite</a>
41 <a href="logout.php">Sign Out</a>
42
43 </div>
44 Select testcode for which you want to view analysis:
45 <form action="<?-$ _SERVER['PHP_SELF'];?>" method="post">
46 <select name="testcode" class="selectBox">
47 <?php
48 $query = "select distinct testcode from organisation";
49 $result = mysql_query($db, $query);
50 while ($rows = mysql_fetch_array($result))
51 ↓
52 ↓
53 <option value="<?php echo $rows['testcode'];?>"><?php echo
54 $rows['testcode'];?></option>
54 <?php
55 ↓
56 ↓
57 </select>
58 <input type="submit" name="submit" value="analyse">
59 </form>
60 <?php
61 if (isset($_POST['submit'])) {
62 $testcode1 = mysql_real_escape_string($db, $_POST['testcode']);
63 ↓
64
65 $query1 = "select distinct ssid from answer where testcode = '
66 $testcode1'; ";

```

```

66     $query2= "select empid,COUNT(*) as total from answer where
empid=an-actualans and testcode = '$testcode' GROUP by empid HAVING total >
5;";
67     $result1= mysql_query($db,$query1);
68     $result2= mysql_query($db,$query2);
69     $totalemp= mysql_num_rows($result1);
70     $passed= mysql_num_rows($result2);
71     $failed= $totalemp - $passed;
72     <?
73     <script type="text/javascript"
src="https://www.gstatic.com/charts/loader
.js"></script>
74     <script type="text/javascript">
75     google.charts.load('current', {'packages':['corechart']});
76     google.charts.setOnLoadCallback(drawChart);
77
78     function drawChart() {
79         var data = google.visualization.arrayToDataTable([
80             ['Passed','Failed'],
81             <?php
82                 echo ["Passed","Failed"]."1.";
83                 echo ["Failed","Failed"]."1.";
84             >
85         ]);
86         var options = {
87             title: 'Number of employees who passed test'
88         };
89
90         var chart = new
google.visualization.PieChart(
(document.getElementById('piechart')));
91
92         chart.draw(data, options);
93     }
94     </script>
95     <div id="piechart" style="width: 550px; height: 400px;
96     position: absolute;
97     top: 250px;
98     left: 50px;
99     "></div>
100     <?php
101     $query3= "select empid,COUNT(*) as total from answer where
empid=an-actualans and
102     testcode = '$testcode' and mode = 'link' GROUP by empid";
103     $result3= mysql_query($db,$query3);
104     $linkemp= mysql_num_rows($result3);
105     $safe= $totalemp - $linkemp;
106     <?
107     <script type="text/javascript"
src="https://www.gstatic.com/charts/loader.js"></script>
108     <script type="text/javascript">
109     google.charts.load('current', {'packages':['corechart']});
110     google.charts.setOnLoadCallback(drawChart);
111
112     function drawChart() {
113         var data = google.visualization.arrayToDataTable([
114             ['Click','Non Click'],
115             <?php

```

```

116         echo ["'Won't Click'", "$safe-"],";
117     }>
118     });
119     var options = {
120         title: 'Number of employees who will click on the malicious
links'
121     };
122
123     var chart = new
google.visualization.PieChart
(document.getElementById('piechart1'));
124
125     chart.draw(data, options);
126     }
127 </script>
128 <div id="piechart1" style="width: 550px; height: 400px;
129     position: absolute;
130     top: 250px;
131     left: 550px;
132 ></div>
133 <?php
134     $query4 = "select empid,COUNT(*) as total from answer where
empid=emp1-act_alans and
testcode = '$testcode1' and mode = 'attachment' GROUP by empid";
135     $result4 = mysqli_query($db, $query4);
136     $attachemp = mysqli_num_rows($result4);
137     $code_load = $totalemp - $attachemp;
138     }>
139 <script type="text/javascript"
src="https://www.gstatic.com/charts/loader.js"></script>
140 <script type="text/javascript">
141     google.charts.load('current', {'packages':['corechart']});
142     google.charts.setOnLoadCallback(drawChart);
143
144     function drawChart() {
145         var data = google.visualization.arrayToDataTable([
146             ['Download', 'Won't Download'],
147             <?php
148                 echo ["'Download'", "$attachemp-"],";
149                 echo ["'Won't Download'", "$code_load-"],";
150             }>
151             ]);
152         var options = {
153             title: 'Number of employees who will download the dangerous
attachments'
154         };
155
156         var chart = new
google.visualization.PieChart
(document.getElementById('piechart2'));
157
158         chart.draw(data, options);
159     }
160 </script>
161 <div id="piechart2" style="width: 550px; height: 400px;
162     position: absolute;
163     top: 600px;
164     left: 50px;
165 ></div>

```

```

166 <?php
167 $query5 = "select empid COUNT(*) as total from answer where
          empid=empid and
          testcode = '$testcode' and mode = 'email' GROUP by empid";
168 $result5 = mysqli_query($db, $query5);
169 $emailsm = mysqli_num_rows($result5);
170 $reply = $totalsm - $emailsm;
171 ?>
172 <script type="text/javascript"
173 src="https://www.gstatic.com/charts/loader.js"></script>
174 <script type="text/javascript">
175 google.charts.load('current', {'packages':['piechart']});
176 google.charts.setOnLoadCallback(drawChart);
177
178 function drawChart() {
179     var data = google.visualization.arrayToDataTable([
180     ['Reply', 'Won't Reply'],
181     <?php
182         echo ["Reply", "- $reply -"],";
183         echo ["Won't Reply", "- $emailsm -"],";
184     ?>
185     ]);
186     var options = {
187         title: 'Number of employees who will reply to phishing emails'
188     };
189     var chart = new
190     google.visualization.PieChart
191     (document.getElementById('piechart3'));
192     chart.draw(data, options);
193 </script>
194 <div id="piechart3" style="width: 550px; height: 400px;
195     position: absolute;
196     top: 600px;
197     left: 550px;
198 "></div>
199 <?php
200 $average = ($passed + $download + $safe + $reply) / 4;
201 $aware = $totalsm - $average;
202 ?>
203 <script type="text/javascript"
204 src="https://www.gstatic.com/charts/loader.js"></script>
205 <script type="text/javascript">
206 google.charts.load('current', {'packages':['piechart']});
207 google.charts.setOnLoadCallback(drawChart);
208
209 function drawChart() {
210     var data = google.visualization.arrayToDataTable([
211     ['Aware', 'Unaware'],
212     <?php
213         echo ["Aware", "- $average -"],";
214         echo ["Unaware", "- $aware -"],";
215     ?>
216     ]);
217     var options = {
218         title: 'Awareness awareness of the organisation'

```

```

219
220     var chart = new
221     Google.visualization.PieChart
222     (document.getElementById('piechart4'));
223
224     chart.draw(data, options);
225
226 </script>
227 <div id="piechart4" style="width: 550px; height: 400px;
228 position: absolute;
229 top: 920px;
230 left: 50px;
231 "></div>
232 <div id="report" style="
233 position: absolute;
234 top: 970px;
235 left: 600px;
236 ">
237 <?php
238 $download= "select empid,COUNT(*) as NumberOfRightAnswers from answer
239 where
240 answer-actualans and testcode = '$testcode1' GROUP by empid;";
241 $downresult = mysql_query($db,$download); ?>
242 <table border="2" style="background-color: #DCDCDC; color: #000000;
243 margin: 0 auto;" >
244 <thead>
245 <tr>
246 <td colspan="2" style="text-align: center;><b>Employee wise result </b></td></tr>
247 <tr>
248 <th style="text-align: center;>Employee id</th>
249 <th style="text-align: center;>No of right answers</th>
250 </tr>
251 </thead>
252 <tbody>
253 <?php
254 while($row = mysql_fetch_assoc($downresult) ){
255     echo
256     "<tr>
257         <td style="text-align: center;>{$row['empid']}</td>
258         <td style="text-align: center;>{$row['NumberofRightAnswers']}</td>
259     </tr>\n";
260 }
261 </tbody>
262 </table>
263 <?php
264 mysql_close($db); ?>
265 </div>
266 </body>
267 </html>
268

```

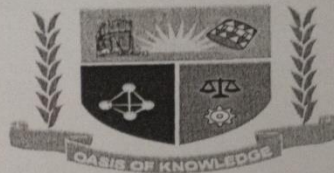
APPENDIX 3: DOCUMENTATION AND MANUAL

Installation Guidelines

Windows Installation Manual

1. Go to <https://www.apachefriends.org/download.html> and download XAMPP.
2. Follow the installation instructions on the screen. It takes care of setting up the web server and MySQL database for you.
3. If you don't want to utilize XAMPP, any web and a standalone installation of should work.
4. Start the 'Apache' and 'MySQL' services in the control panel once you've accomplished steps 1 or 2 depending on your preference.
5. In your browser, go to <http://localhost/phpmyadmin/> or <http://IP/phpmyadmin/>.
6. Click on 'Databases,' and then create a database called phishadmin.
7. Click 'Import' and choose the file phishadmin.sql from the /sql /phishadmin.sql folder.
8. Finish the configuration by copying the accessible source code here to the folder.

APPENDIX 4: Letter from Dean SIIS



**JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS**

P. O BOX 210- 40601
BONDO

Date: 20th February, 2020

Director,
Board of Postgraduate Studies,
JOOUST.

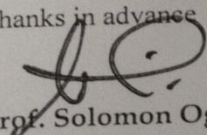
Dear Prof,

RE: LETTER FOR DATA COLLECTION

This is to certify that the following student has addressed all the concerns raised against his proposal oral defense presentation as spelt out in the minutes. Kindly allow him proceed to the next stage of data collection.

1. I152/4262/2016 OKUMU DANIEL ONYANGO

Thanks in advance


Prof. Solomon Ogara
Dean, SIIS

APPENDIX 5: Ethical Review Letter



**JARAMOGI OGINGA ODINGA
UNIVERSITY OF SCIENCE AND TECHNOLOGY
DIVISION OF RESEARCH, INNOVATION AND OUTREACH
JOOUST-ETHICS REVIEW OFFICE**

Tel. 057-2501804
Email: erc@jooust.ac.ke
Website: www.jooust.ac.ke

P.O. BOX 210 - 40601
BONDO

OUR REF: JOOUST/DVC-RIO/ERC/E3

21st December, 2021

Okumu Daniel Onyango,
1152/4262/2016
SIIS
JOOUST

Dear Mr. Okumu',

RE: APPROVAL TO CONDUCT RESEARCH TITLED "HUMAN FIREWALL SIMULATOR FOR ENHANCING SECURITY AGAINST BUSINESS EMAIL COMPROMISE"

This is to inform you that JOOUST ERC has reviewed and approved your above research proposal. Your application approval number is **ERC/21/12/21-03**. The approval period is from 21st December, 2021 – 20th December, 2022.

This approval is subject to compliance with the following requirements:

- i. Only approved documents including (informed consents, study instruments, MTA) will be used.
- ii. All changes including (amendments, deviations and violations) are submitted for review and approval by JOOUST IERC.
- iii. Death and life threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to NACOSTI IERC within 72 hours of notification.
- iv. Any changes, anticipated or otherwise that may increase the risks of affected safety or welfare of study participants and others or affect the integrity of the research must be reported to NACOSTI IERC within 72 hours.
- v. Clearance for export of biological specimens must be obtained from relevant institutions.
- vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.
- vii. Submission of an executive summary report within 90 days upon completion of the study to JOOUST IERC.

Prior to commencing your study, you will be expected to obtain a research permit from National Commission for Science, Technology and Innovation (NACOSTI) <https://oris.nacosti.go.ke> and also obtain other clearances needed.

Yours sincerely,

for
Prof. Francis Anga'wa
Chairman, JOOUST ERC

Copy to: Deputy Vice-Chancellor, RIO Director, BPS Dean, SIIS

APPENDIX 6: Board of Post Graduate Letters



JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE & TECHNOLOGY

BOARD OF POSTGRADUATE STUDIES

Office of the Director

Tel. 057-2501804

Email: bps@jooust.ac.ke

P.O. BOX 210 - 40601

BONDO

Our Ref: I152/4262/2016

Date: 24th February 2020

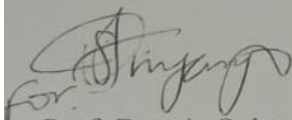
TO WHOM IT MAY CONCERN

RE: OKUMU DANIEL ONYANGO

The above person is a bonafide postgraduate student of Jaramogi Oginga Odinga University of Science and Technology in the School of Informatics and Innovative Systems pursuing Master of Science in Information Technology Security and Audit. He has been authorized by the University to undertake research on the topic: *“Human Firewall Simulator for Enhancing Security Against Business Email Comprise”*.

Any assistance accorded him shall be appreciated.

Thank you.



Prof. Dennis Ochuodho

DIRECTOR, BOARD OF POSTGRADUATE STUDIES

