Received: 19 September 2022 | Revised: 11 January 2023 | Accepted: 17 January 2023 | Published online: 30 January 2023

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2023, Vol. 00(00) 1–24
DOI: 10.47852/bonviewJCCE3202415

BON VIEW PUBLISHING

Human Firewall Simulator for Enhancing Security Awareness against Business Email Compromise

Daniel Onyango Okumu[1], Richard Otieno Omollo[1,*] and George Raburu[1]

[1]*Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Kenya*

Abstract: Chief executive officers (CEOs) can turn out to be the weakest link to an organization's security and attackers know that if they successfully exploit or impersonate someone who has a high level of access like CEOs or chief finance officers (CFOs), they instantly gain great advantage. The problem comes when attacker manages to take control of email accounts of the CEOs and CFOs and sends an email to another staff in the organization, he/she is likely to take it seriously, act accordingly and quickly as possible, and may be wire cash to an account directed by the "CEO/CFO," and/or get away with private or sensitive corporate information. Because of the nature of these attack methods, detection and protection are very difficult since the attackers take advantage of the human weakness which is the weakest link. The main aim of this study is to provide a solution to protect every surface of the organization. By developing a human firewall, working with the already existing technical solutions offers the solution to remaining problem of human weakness. This research developed a simulator to train the users with the latest trends the attackers are using making them do it right (flagging, reporting, not clicking suspicions links) and making email security part of their responsibility. This makes employee become human firewall. The results from the simulator are displayed in charts as number of employees who passed the 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 organization, and how individual employees performed. While organizations have made progress over the years, security is a never-ending process that requires improvement day by day. Since no one in the organization's structure is immune including the top most in the cadre (i.e., CEO), complexity in understanding and awareness creation is more wanting than before. Integrating human firewall into existing security measures as the last line of defense in email communication against business email compromise frauds offers this solution because it has preventive as well as reactive measures both geared toward maximizing email security. A simulation of the attacks to analyze the user involvement to breaching the security followed by an evaluation simulation after integrating human firewall to the organization's email security shows success level. The results from the test show the different success levels, that is, results from pre-assessment definitely show low success level since staff/employees have not been made aware/trained to profile or flag compared to when the employees/staff have gone through the training/awareness. Post-assessment indicates high success level because actions from employees turned into human firewall know how to take proper action, for example, flagging, not clicking malicious links. The organization should update its policies to accommodate and reinforce rules on the employees to ensure that the tool is used regularly and actions taken on user deemed a threat to the organizational email security.

Keywords: human link, impersonation, intercept, business email compromise (BEC), email security, human firewall

1. Introduction

The bad guys get very creative, impersonate leaders of an organization, request documents, or ask payroll employees to bring money to bank accounts. According to the FBI, their efforts were worth an estimated 12 billion dollars, thanks to the compromise of commercial email, known as chief executive officer (CEO) fraud. Defending against these types of phishing attacks is only possible if the security has layers of controls and not just technical (Federal Bureau of Investigation, 2016). Building a human firewall might sound very similar to team building and motivational exercises that make people realize that organizations cannot function without them.

Business security relies on YOU! (Proteck, 2017). With phishing attacks, companies cannot deploy security technology quickly enough for remote cybercriminals, which is why the ultimate protection with 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.

*__Corresponding author:__ Richard Otieno Omollo, Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Kenya. Email: richard.otieno@gmail.com

Criminals send spoofed emails with links that use existing business or personal names to extract sensitive information such as computer login details or personal information. These emails containing malicious links often bypass the usual security and are therefore difficult to block.

A combination of human firewalls with the already existing strategies is a more balanced and proactive approach to prevent business email compromise (BEC) fraud and if companies fail to adopt this strategy, then cybercriminals 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 provide blunt protection.

Most popular security tools in recent days focus 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 the information on 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 (Guntrip, 2020).

Phishing emails contain more contextual information to increase the chances that a recipient will be victimized (Hong, 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, and it requires the cultivation of an employee fresh mindset 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: make people care about cybersecurity, building awareness and knowledge, and measure and monitoring (Schablik et al., 2017). A human firewall creation 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 inboxes, thus minimizing human error involving preempting human nature (Colón et al., 2014). Hackers and spammers exploit human nature through social engineering to gain their trust, for example, by manipulating users to click malicious links in emails that appear to be from legitimate ones.

Phishing is one more 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 accidentally or by choice who do not follow the training and guidance is required. So, when you can get a firewall to protect the network and endpoint detection response to protect your devices, how do you then protect your organization from such staff? Security of the human layer is the ultimate requirement, which means there is a lack of inclusivity of behavioral approach into the already existing security mechanisms

This is why a combination of human firewalls with others including sophisticated mail gateways is the defense to deal with these threats.

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.

The very enormous growth of the Internet, business connectivity, and network and by extension the vulnerabilities coming with them are a very big contributor to growth in cyberattacks.

Google research analyzed over 1 billion of emails passing through Gmail, and the results presented are extremely interesting: corporate emails are 6.2 times more likely to receive phishing attacks, 4.3 times more likely to receive malicious versus personal accounts, but only 0.4 times more likely to receive spam (Sjouwerman, 2017). The meaning focus of the attack is shifting to the phishing method.

Despite the existing mechanism to protect against business email fraud, attack continues especially through social engineering, 91% of all cyberattacks begins with phishing (Gatner, 2017).

Giving sensitive information to people without authenticating their identity and access privileges and allowing a stranger within an organization without authorization are some of the most common and worst mistakes that workers will do to create a broken link is an example of why there is a need for a human firewall. Corporate inboxes contain sensitive information of monetary value. Organizations that are active in finance, and entertainment and are most targeted by phishing. It seems that attackers target organizations by size, type, and operations (Akamai, 2017).

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). 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 mechanism so that email security design is perfect.

2. Literature Review

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 to hijack 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 frauds involve 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 dollars to businesses and corporates (Hernedy, 2016). For this reason, money is becoming the biggest motivation for attackers to continue exploiting BEC attacks.

Steps how BEC is mitigated
Step 1: Identifying the business targeted for the attack.
Step 2: Exploring the attack by utilizing engineering tactics to exploit the corporate users by luring and convincing the target of the legitimacy of the transaction.
Step 3: Exchanging the wrong bank account details to the unsuspecting victim.
Step 4: Executing 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 hackers. A big example is the Anthem Breach which affected about 80 million people and when we look at the target, this organization faced a tremendous financial loss of $162 million (McGee, 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, the employees will always be the first line of defense. It is the employees who take care of all the machinery and equipment and keep them updated and maintained. Thus, if one wants to better the security conditions of an organization, the training of employees should be of high priority.

Phishing can be a risk that quickly grows in the cyber world and causes web clients billions of dollars each year. It is an illegal movement that employs a group of social and innovation to bring together sensitive data from the web. The recognizable evidence of phishing strategies can be 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 took a long fire to distinguish all related and provide a full understanding. This research presents hypothetical proof of International Rescue Committee (IRC) 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 it comes from a senior manager, a supplier, or a candidate for a job. Social engineering malicious attacks are on the increase and well beyond just targeting the financial sector. While some organizations are developing employee awareness coaching or 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 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 for 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 (Kevin and Mitnick 2002).

Cialdini (2007) focuses on three principles: social proof, scarcity, and authority. According to Cialdini (2007), many people tend to comply with the request once they see that others already have it (Cialdini 2007). Emails showing that it has 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.

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 a 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.

2.3. Phishing crime, prevention, and gap investigation

Phishing is a rapidly growing threat in the cyber world causing billions of dollars in damage yearly to Internet users (Shaikh et al., 2016). It is an illegal movement that uses a bunch of social and innovation to collect sensitive data online. The recognizable proof of phishing strategies can be in different communication strategies such as mail, instant messages, contextual, or web page-level messages. There have been a number of inquiries about items distributed with various procedures but 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 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 to perform 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 et al., 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 grow 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 (ENISA, 2021).

2.4. How hackers steal email address and passwords

Hackers frequently steal passwords using various techniques and more generally phishing, where the hacker sends an official-looking email that will later direct the recipient to a fake website. Once the victim enters a name and a password on the fake site, the hacker will recover the password.

The various techniques that are used in harvesting user names and passwords are as follows.

1. Phishing attacks

Tab nabbing: In this technique, a computer hacker sends an official appearing 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 page they are mimicking. When the user clicks on the link and arrives on the page, he enters his email 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 one and use it to commit fraud.

Key logger attacks: This happens when receiving this e-questionable mail, "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. Mass theft: Over 60% of users share their usernames and passwords 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 then, they have access to people's accounts and data.

If you use the same username and password for all of your accounts, you are 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.

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 the information.

The username and password have been hacked.

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 are 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).

5. Network sniffing attacks: This attack involves sniffing passwords on the network, especially where HTTPS is not enforced.

2.5. Examples of email attacks mitigated through BEC scams

The examples below (see Figures 1, 2, 3) 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 which attackers use with the help of corporate emails to appear like it's coming from a legitimate source.

Example 4: Communication from XYZ University

Webmaster of XYZ university warns staff of fake email in the cooperate 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 Figure 4 below.

2.5.1. A thread discussing a real CEO fraud attack

The conversation reproduced below (see Figure 5) actually occurred in 2017 between a CEO scammer and the victim successfully scammed, although the names and credentials have been changed (Kaplan, 2018).

2.6. Actions to effectively defend against social engineering attacks

According to Christina Lekati (2020), psychologist and social engineer, organizations can take 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:

Figure 1
BEC scam example 1 (Sabi, 2019)

Figure 2
BEC scam example 2 (Abbasi, 2018)

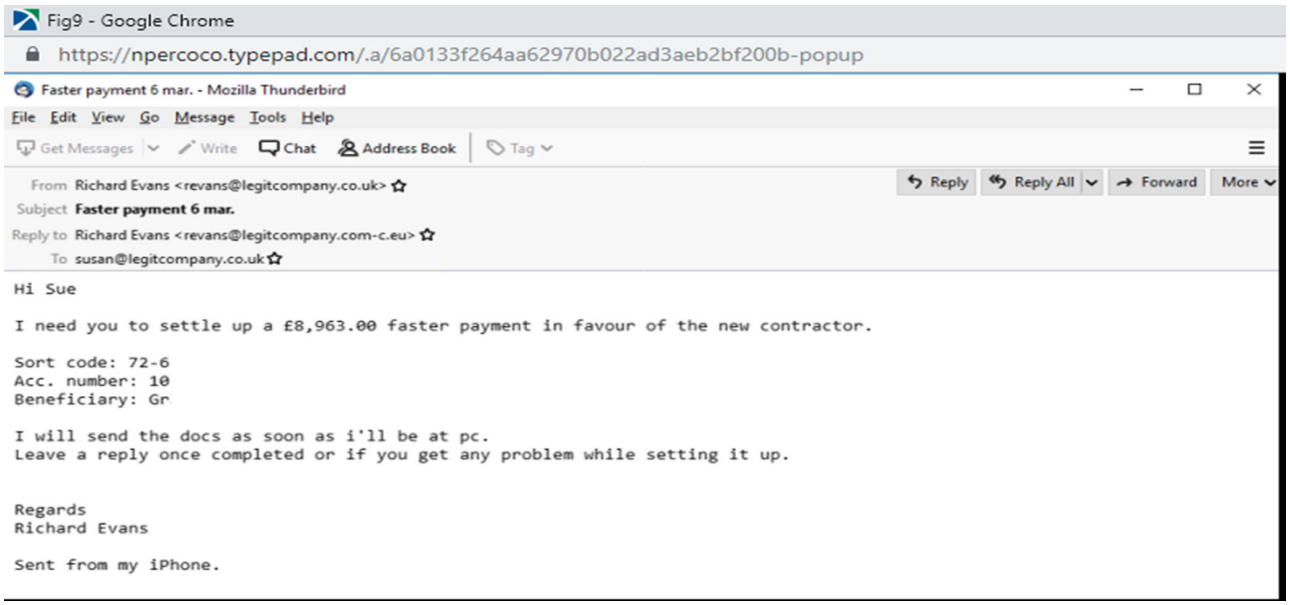
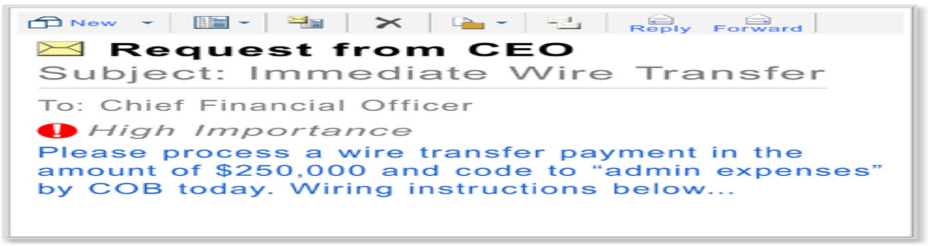


Figure 3
BEC scam example 3 (Cloudmark, 2016)



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

2. Simulations of social engineering attacks:

Employees' talents can be put to the test once they have learned to identify with responding 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.

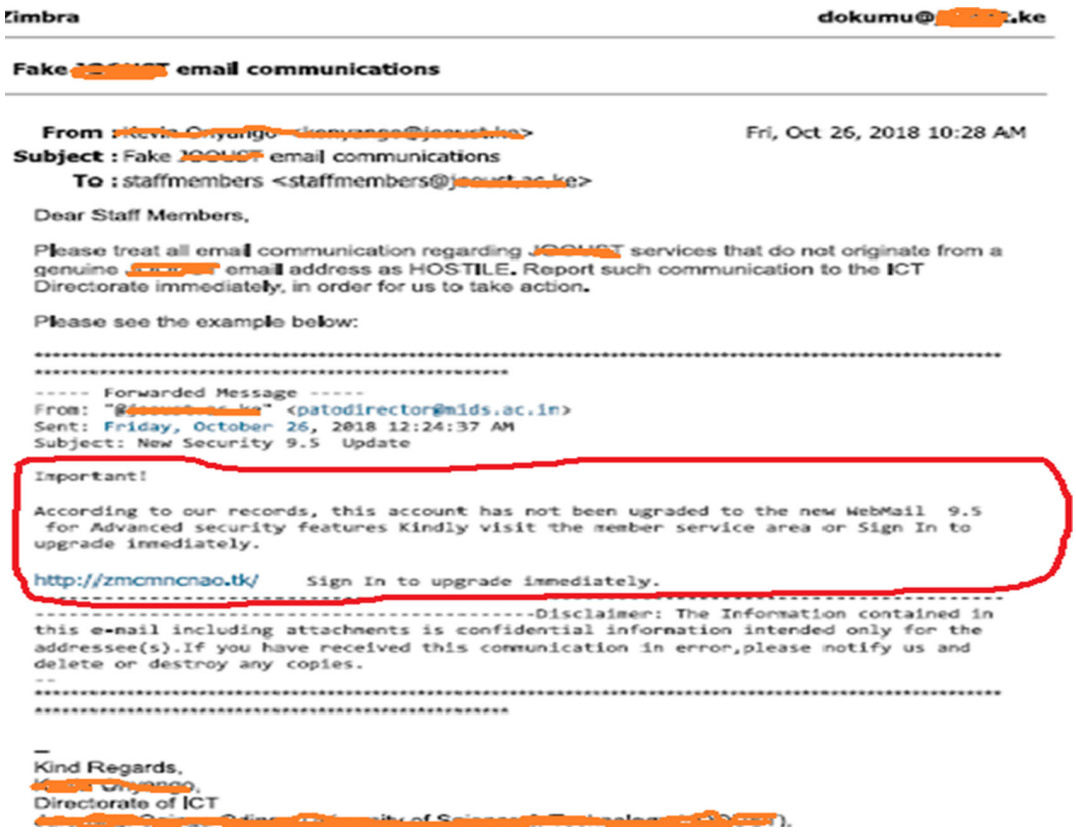
3. Conduct an open-source intelligence analysis on the organization:

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 is 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

Figure 4
Communication from XYZ University webmaster


Zimbra dokumu@[redacted].ke

Fake [redacted] email communications

From : [redacted] Fri, Oct 26, 2018 10:28 AM
Subject : Fake [redacted] email communications
To : staffmembers <staffmembers@[redacted]>

Dear Staff Members,

Please treat all email communication regarding [redacted] services that do not originate from a genuine [redacted] 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: "[redacted]" <patodirector@mids.ac.in>
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://zmcmncnao.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,
[redacted]
Directorate of ICT
[redacted]

commit to being a part of it. The importance of this extra layer of human protection is that many violations are due to employee errors. Therefore, a vigilant human firewall can prevent the potential dangers of software errors and can prevent 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.

Ninety percent of attacks are preventable because they exploit known 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 defenses that have been implemented.

If there are some gaps in the firewalls, some of the known vulnerabilities pass on to users of the organization. This is where the human firewall adds value (Getthreatready, 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 have seen technology and the "human firewall" work together to safeguard previously susceptible enterprises (Mimecast, 2015).

In building a human firewall toward email security, it is important to consider the other important security aspects of security as shown below.

Many organizations face continuous threats from phishing attacks, insider threats, and many forms of threats. It is obvious that no organization can be able to 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 a culture of security (McLaughlin, 2019).

2.7.1. Defensive first line

The sensitive data that have to be protected are at the heart of a cybersecurity architecture. The first line of defense should be cybersecurity technology, but it is not a guarantee of security. Few dangers will truly be 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 will not be threatened if the technology works, and they will be less likely to be victims of a few people breaking into the infrastructure.

2.7.2. Employees' motivation and ability

What happens if a threat gets past the "human firewall"? Will 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 would not answer; either they did not have the capacity to do so or they were not 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 good or negative. The best training stresses both and does it in easy-to-understand terminology.

Figure 5
Email thread of an actual CEO fraud attack

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 pament 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

Ok then. Thanks
NAME: Acme
SORT CODE: 12341234
ACCOUNT: 123412341234IBAN: ABCD123412341234123412341234
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: ABCD123412341234123412341234123412341
Ensure to send me the slip once its done. Thanks
N.B: confirm receipt of the new IBAN number.

Regards
John Smith

**

2.7.3. Link the desired behaviors to necessary knowledge

The next stage is to teach staff the new required behavior while using corporate messages 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 will identify a 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 backward from this point.

2.8. Theories supporting human firewall creation

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 that determine whether an action will 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 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

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

Need for human security layer

Employees now have power over both your systems and your data, according to Tim Sadler.

People, on the other hand, make mistakes, break rules, and can be duped (Sadler, 2021). Human mistake is responsible for 88% of data breaches, according to American International Group, Inc. (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% of the time, we believe it is preferable to prevent errors from occurring in the first place by recognizing and preventing them. Human mistake is responsible for 88% of data breaches, according to AIG, which states that "human errors and behavior continue to be a primary driver of cyber claims" (Sadler, 2021).

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 email 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 is not a one-off occurrence.

According to one study, 45% 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 have made a mistake at work that has harmed their cybersecurity.

Regrettably, the repercussions of these errors can be severe (Sadler, 2021).

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 2 years, BEC attacks have surged by more than 100% (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

Some of the existing email security solutions in the market include the following:

1. Cisco Email Security Appliance
2. Clear swift Secure Email Gateway
3. Microsoft Exchange Online Protection
4. Forcepoint Email Security (formerly Websense)
5. Proofpoint Email Protection.

Out of the many security solutions in a place, none is focused on the user as the biggest link. The simulator as a training tool is what is stressed but not the simulator as a tool to turn users and staff to be part of the security team. The concept of a human firewall is the ultimate solution to corporate email threats like BEC attacks. Many security plans are in place and are replicated by the many security players such as email domain protection, awareness

training, multi-layer anti-virus protection, anti-malware, detection, Sandbox, spam detection, and email encryption among many.

Latest attacks bypass the many security plans in place and instead are focused on social engineering to get into the systems and ultimately cause havoc, and phishing is on the rise hence employees are part of the security problem. Because of this, employees should also be part of the security solutions. Keep in mind that your systems and data are now under the hands of your staff. People, on the other hand, make mistakes, break rules, and can be duped.

The focus of this research is to design a model that works together with other existing tools bringing the "human" employees to be part of the security.

This is well achieved through simulation and policy enforcement.

2.11. Design of the current security models

The email exchange is an email message flow with a variety of mechanisms for spam and antivirus filtering as depicted in Figure 6.

Email message flow

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 and is why integrating the security mechanism with human firewall greatly help reduce CEO fraud (see Figure 7).

2.12. How human firewall works

Train: employees are taken through phishing simulation and awareness training. Lessons are given to raise awareness of existing threats to the use of quizzes designed in the learning management system (LMS).

Profile: the system operates on profiling and reporting by user by monitoring activity by user and judging individual performance by analyzing behavior and mapping strengths and weaknesses through generating reports to track them.

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 IT department.

Figure 6
Email message flow courtesy (Cisco, Email Security Deployment Guide, 2010)

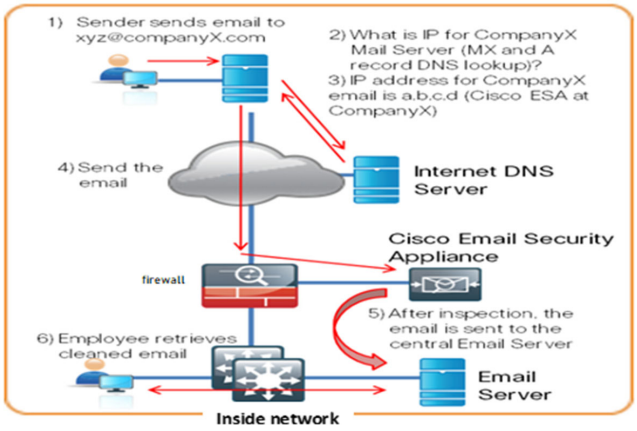
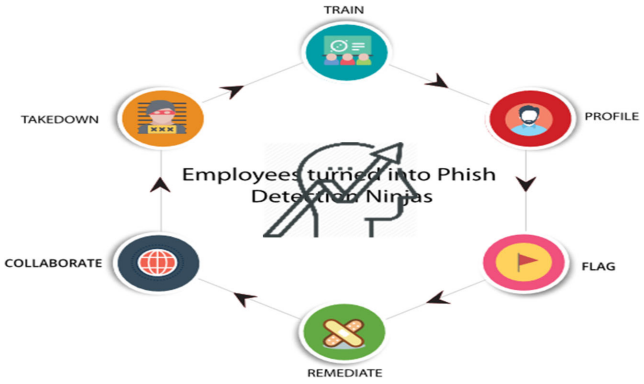


Figure 7
Human firewall components (reprinted from https://www.humanfirewall.io/)



Remediate: here any link or attachment suspected to have threat is quarantined, deleted from the inbox or the server, and shown in a threat alert folder. This is a remedy for Outlook and Google's suite of many others to ensure that the platform has a user threat.

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 is to be introduced.

Take down: collaborations with other international organizations such as Computer Emergency Response Team (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. Model for human firewall

Figure 8 shown above describes how the human firewall model works.

Assessment

Users are introduced to the simulator and then tested to assess their knowledge level, and the result is displayed in terms of the number of questions asked correctly, the areas of weakness, as well as the average awareness report on the organization.

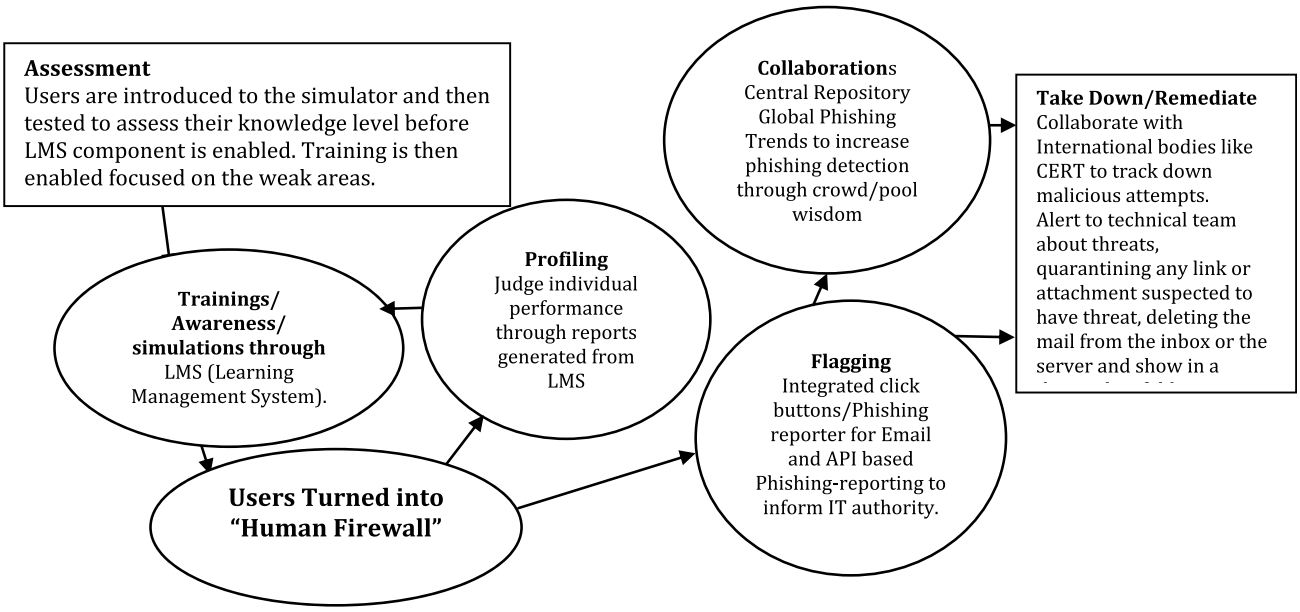
Training component is then enabled with training focused on the areas perceived to be the weak points identified by the pre-assessment.

Trainings/awareness/simulations through LMS.

This is the simulated human firewall control system that does trainings through LMS, and 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.

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

Figure 8
Human firewall model



attackers will be added to the leaning simulator to form part of the new leaning materials in the LMS to ensure even the most knowledgeable users are equipped with the latest knowledge. Either test or quiz continues periodically to ascertain the knowledge level.

Profiling Based on the reports generated by the simulator from the regular quizzes/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 training stage once more and the loop continues.

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

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.
Take down/Remediate

Collaborate with international bodies like CERT to track down malicious attempts.

Alert the technical team about threats, quarantine any link or attachment suspected to have a threat, delete the mail from the inbox or the server, and show it in a threat alert folder

3. Research Methodology

3.1. Simulator

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. The simulation model measures the behaviors of the results that are generated from the simulated data which are compared to the actual scenario to see if there is a positive effect.

The simulation of the current model and the new model using the following steps:

a. Pre-assessment of user's knowledge of social engineering attacks (phishing attacks).
b. Post-assessment evaluation after integration with human firewall.

3.1.1. Pre-assessment of user's knowledge of social engineering attacks (phishing attacks)

Users receive various phishing attacks, at random, at random times over a period of time.

This is done because if they all come on time, they will immediately comprehend what is going on and, rather than recognizing the attacks themselves, will base their actions on those of their colleagues, thanks to a certain form of communication.

The following are some examples of random phishing attempts aimed at users:

1. Employee Directory Update – Employees will get an email that looks to have been received by HR/PR informing them that the employee directory is being updated. Users will update their information by clicking on the URL link. When users click on the link, they will be taken to the XYZ university intranet's home page, where they will be asked to enter their name and password in order to access the form.
2. Corporate (XYZ University) Reorganization Board – Users receive an email informing them that the corporation is in the process of restructuring. To see the updated modifications, please see the pdf attachment.

3. Top-Secret Organization's (XYZ University) Attachment in Microsoft Word TOP – HIGHLY CONFIDENTIAL is the subject of an email sent to users. They find an attachment when they open it. The word attachment appears to provide information about a company's or organization's transportation.
4. See Appendix 1 for an email thread circulated by the webmaster of XYZ university.

3.1.2. Post-assessment evaluation after integration with human firewall

An awareness training is required. Users will be requested to log into a portal when they log in. They will click the play button once they have entered the portal, and a presentation will begin.

The length of the presentation will be approximately 20 minutes and cover basic topics such as:

(1) The various sorts of phishing scams that exist today.
(2) How to detect phishing assaults.
(3) How to detect phishing assaults.
(4) Signs that we have been the victim of a phishing assault.
(5) How to avoid phishing attacks.
(6) Information about the hotline, which allows users to report suspects.

Following that, a link to the training will be posted on the company's intranet for referral purposes.

The user knowledge exam of what has been shared in the will be tested later, after a few days.

The phishing attack approaches listed above will be delivered to users at random over a period of time.

Each attack will include a built-in mechanism for tracking the recipient and determining whether or not he reacted to the attack. This will display a real-time assault vector to the users.

If the user falls victim to the assault and opens the attachment, it will notify them that they have been the victim of a phishing attack and report them in the email that should have informed them about the attack. Finally, users will be asked to take a compulsory quiz.

The exam will include previously received phishing assaults as well as non-attacks, with users being questioned whether they believe it is an attack.

An assessment will be based on statistics provided showing departments and staff most at risk, to achieve the effectiveness of human firewall integration with email security framework. Existing business to reduce BEC.

If an employee answers all questions correctly, he/she will be awarded a certificate of completion but if they failed it will show the failure rate.

An overall analysis will be graphically displayed to the organization's awareness position.

3.2 Instruments

Several tools and instruments shall be used for the study which includes Python program for PHP, Xampp server, Notepad +++, Browser, Internet, and SMTP server.

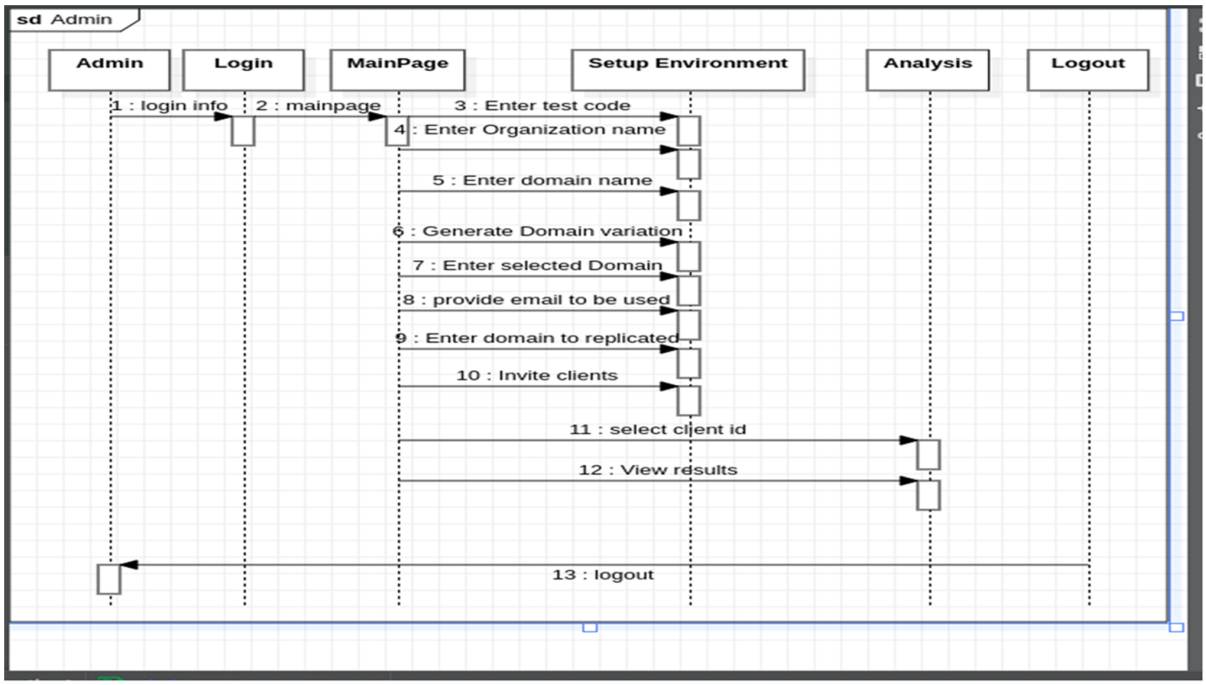
4. System Design

This research study involves the development and simulation of a model as an appropriate research method to handle complexities in this research area. The researcher will first put users to the test by 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.

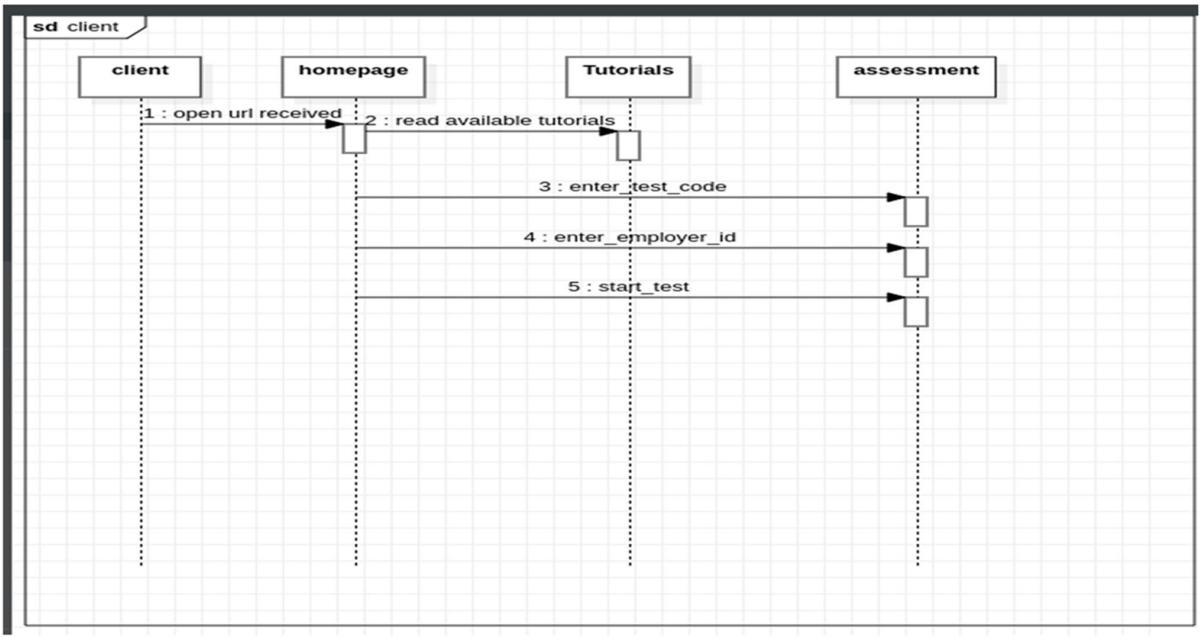
4.1. Sequence diagram

Sequence diagrams in system design are used to demonstrate different ways users of a system will 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 modeling diagram and the functions they perform in the system.

4.1.1. Admin sequence diagram

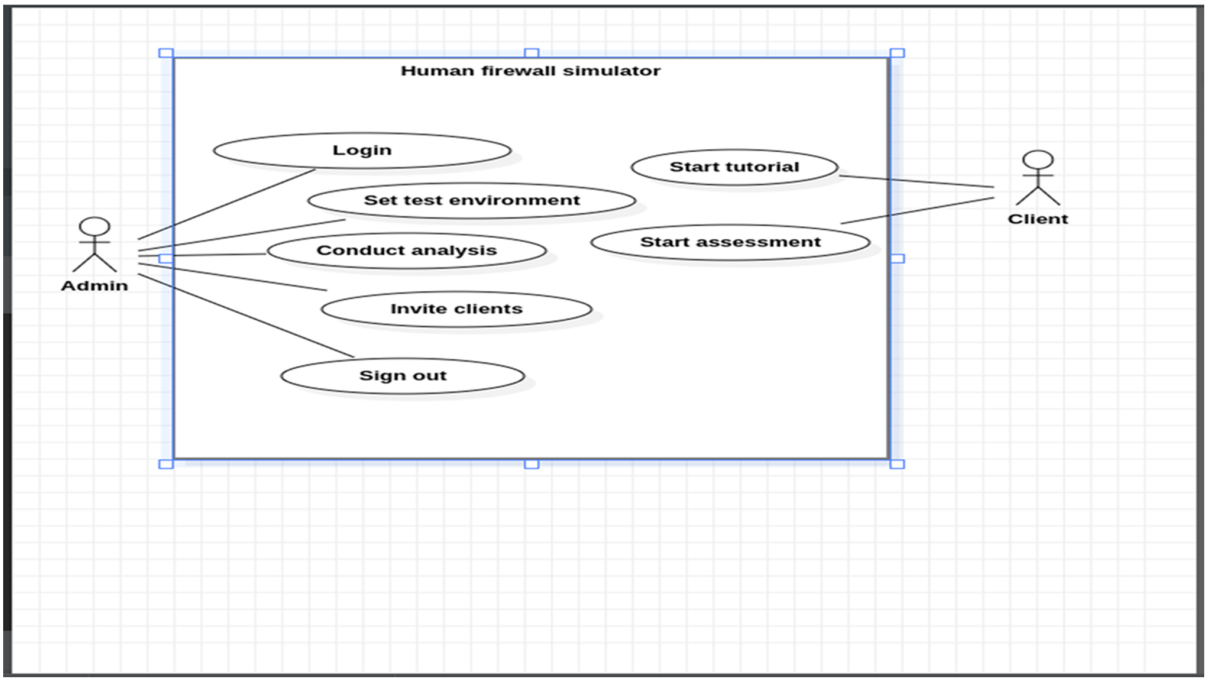


4.1.2. Client sequence diagram



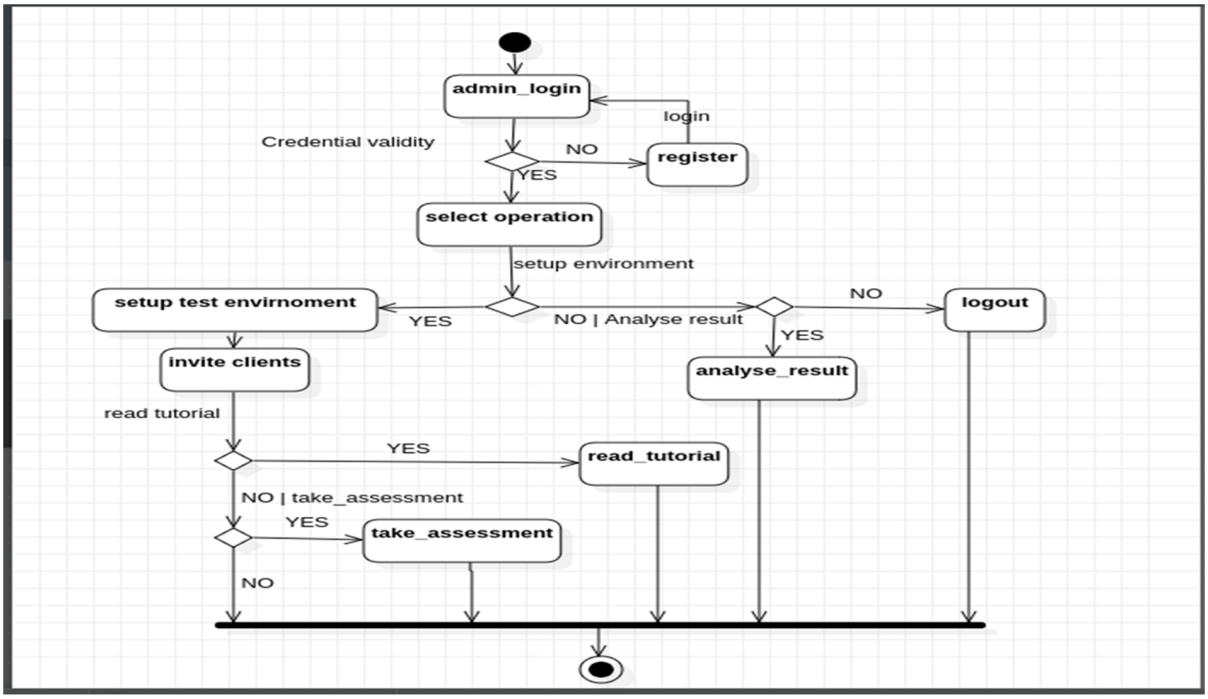
4.2. Use-case diagram

Another important system design tool is the use-case diagram. They are used mainly to determine different interactions between system and its actors. They do not describe how the system operates internally, they only identify what the system does and how the system actors use it



4.3. Activity diagram sequence diagram

This is another very important tool in system designing, it helps developers of systems to 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 the high-level overview of what is happening in a system.



5. Testing and Validation

The simulation tool gives results of test/quizzes done by each individual showing the number of quizzes done, the number of quizzes answered correctly, and the number of quizzes failed. The simulator also indicates which area of email security did the user fail, that is, clicking attachment, responding to wrong suspicious email addresses, or failure to report suspicious email. This shows the individual email security awareness.

Total number of people with their unique code/admission number is to be showed in the result charts showing the overall organizations email security position.

The result will be relayed in percentage, for example, 75% of users fell victims before integrating email security with human firewall or 30% of the users will fall 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.

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 the engaging and straightforward training sessions, our phishing simulation allows users to grasp email security without actually doing the "real" phishing attack.

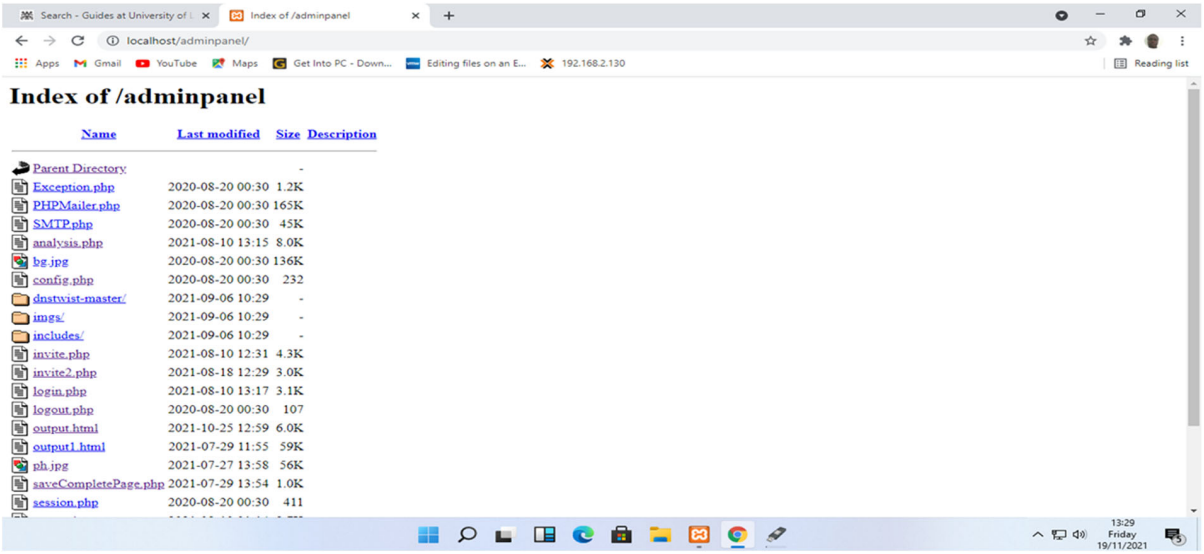
This simulator provides a personalized environment in which you may create your exam according to your needs, such as making questions unique for each participant, simulating a real-time phishing assault, and making questions targeted and tough to answer.

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 will be offered to help you understand your current awareness posture.

Because the attackers simply need one click to get through! This will make us think twice about clicking that button.

Figure 9
Admin module



The simulator is designed in 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.

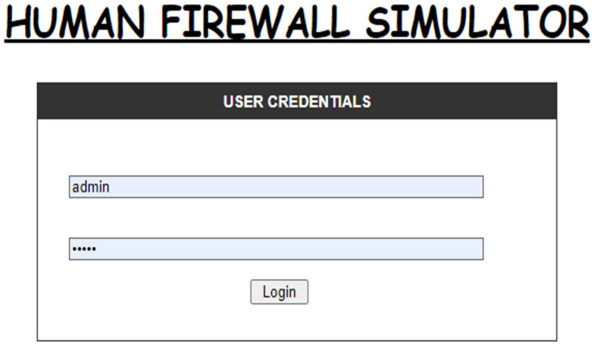
5.1. Admin module

Administration module: This module (See Figure 9) offers access to the configuration test to 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 is the default login credentials.

5.1.1. The interface for the phishing simulator login page is as shown below: see Figure 10

In this section, the simulator will ask you for some basic information. See Figure 11.

Figure 10
Login interface



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

5.2. 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.

5.2.1. Tutorials (client module)

This includes an introduction to phishing along with general tactics for raising awareness and educating people.

5.2.2. Evaluation (client side module)

This stage prompts the user to choose between ignoring or reporting phishing or site or scenario from or SMiShing, and the user must choose between ignoring or reporting it. See Figure 12.

Even if the test code is the same, the questions will be different for each user.

There will be a nice balance of positive and negative questions throughout the questions.

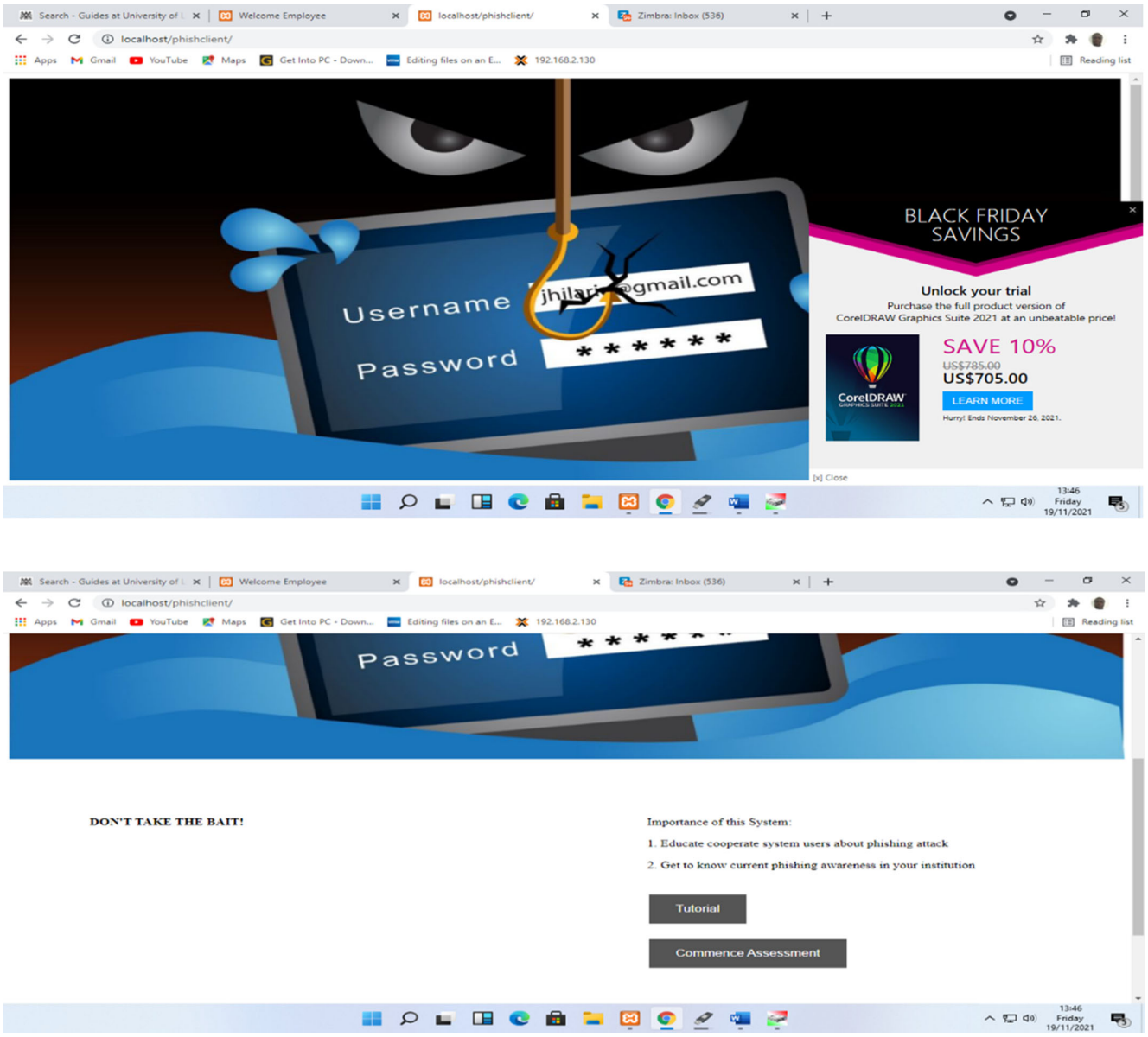
Because it only takes one click to pass the test, all answers must be correct.

Once all the questions are correctly answered, then a certificate will be issued to the trained user but if the user fails, a repeat of the training will be done with focus on the weak areas. For certificate result, see Figure 13.

5.3. Test setup (administrator module)

In this section, the simulator will ask you for some basic information. See Figure 11.

Figure 11
Client side interface



As an example;

Enter your domain name here, and the simulator will generate a list of comparable domains that attackers can use to target you.

You can select one to use throughout your phishing simulation evaluation.

When evaluating (See Figure 14), you will enter the URL of your most frequently visited websites, and we will generate a similar website that will be 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 will have a separate set of questions.

Email ID: Here you must enter an email id that is commonly used for mass communication. During the evaluation, we will produce more combinations of email IDs.

You can see a preview of the phishing web page that we created to look like your original one. See Figure 15.

Admin can upload CSV files and invite the members to take the test as seen in Figure 16.

This web page (see Figure 17) indicates how to enter SMTP server name, SMTP user name, and password to help in sending emails to invite members to the test.

5.4. Invite (admin module)

Admin can upload CSV file and invite the members who have been identified to take test. See Figures 18. The Figure 19 below shows the Assessment screen (client-side module).

Figure 12
Setting up test (admin module)

Figure 13
Assessment (client-side module)

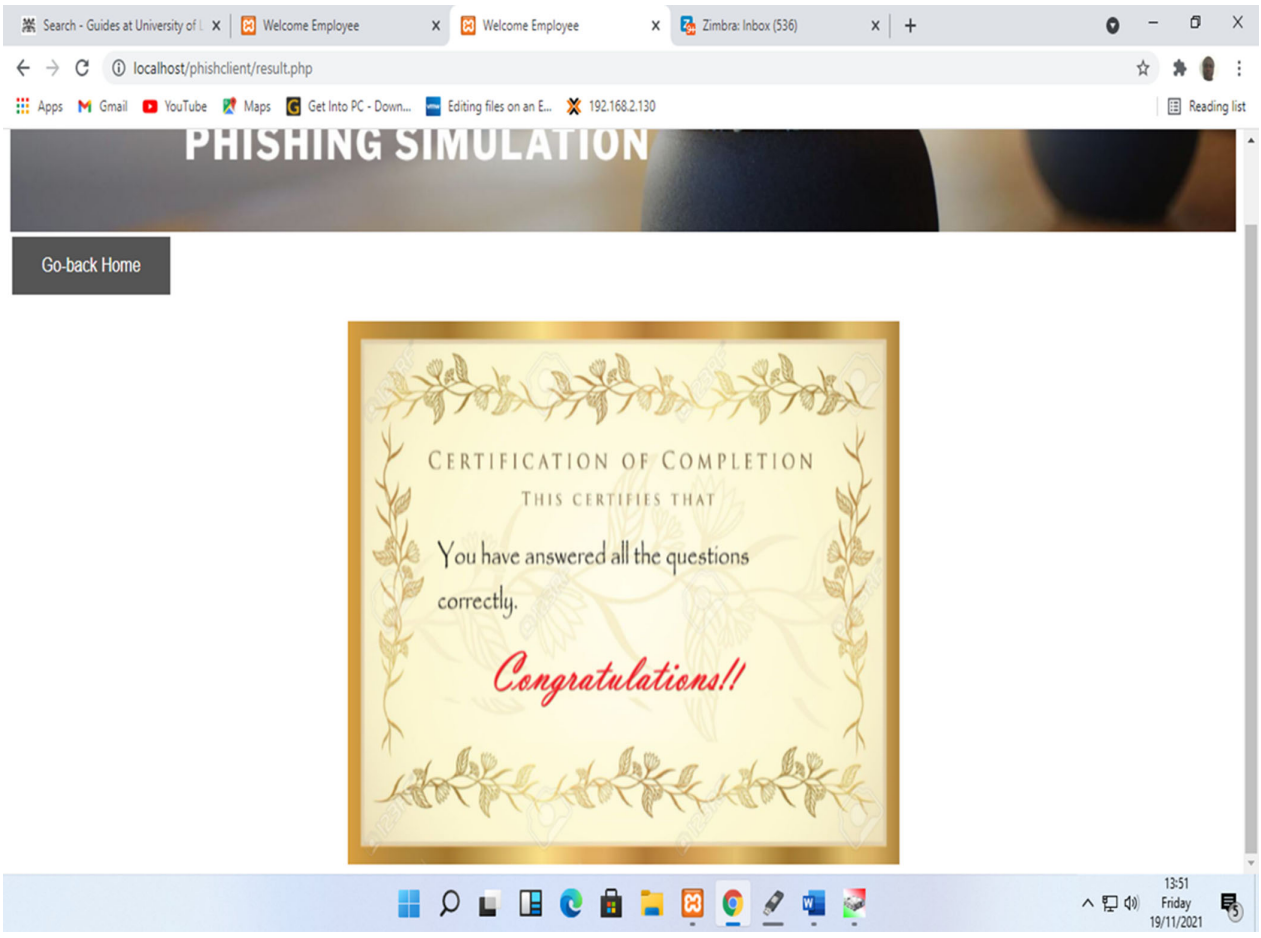


Figure 14
Create a similar website that will be displayed under your domain

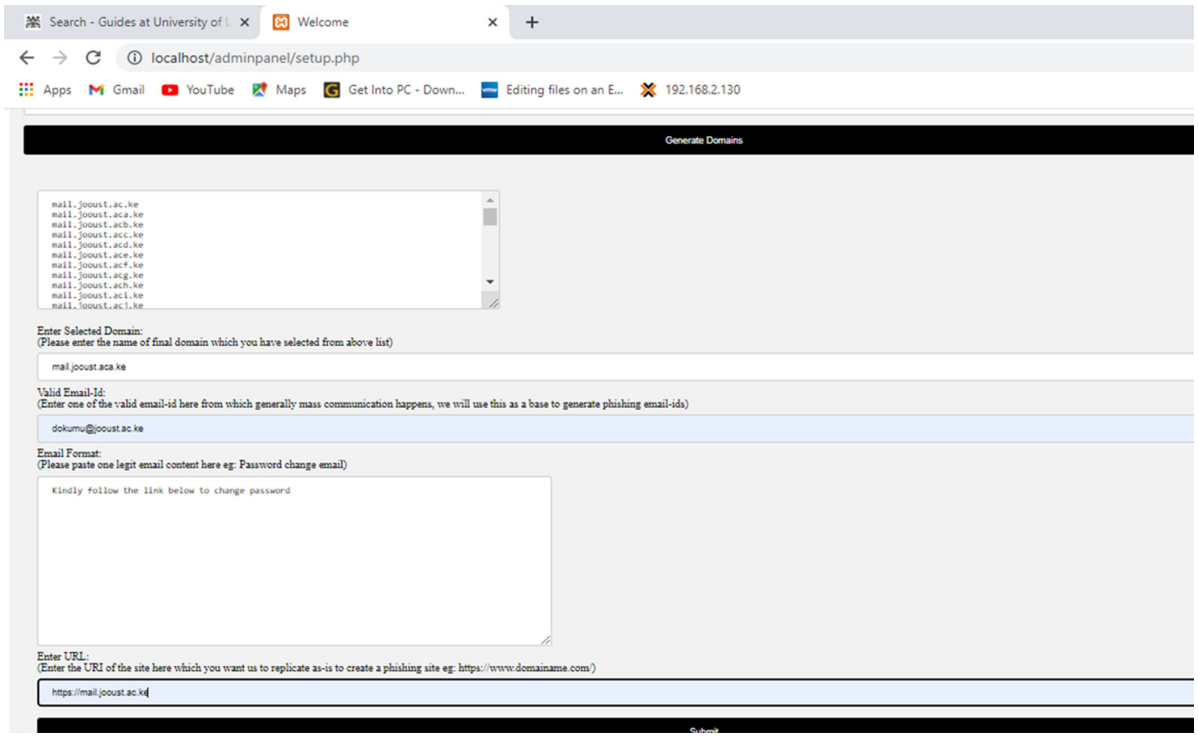


Figure 15
Preview the appearance of the phishing web page that we created to look like the original one

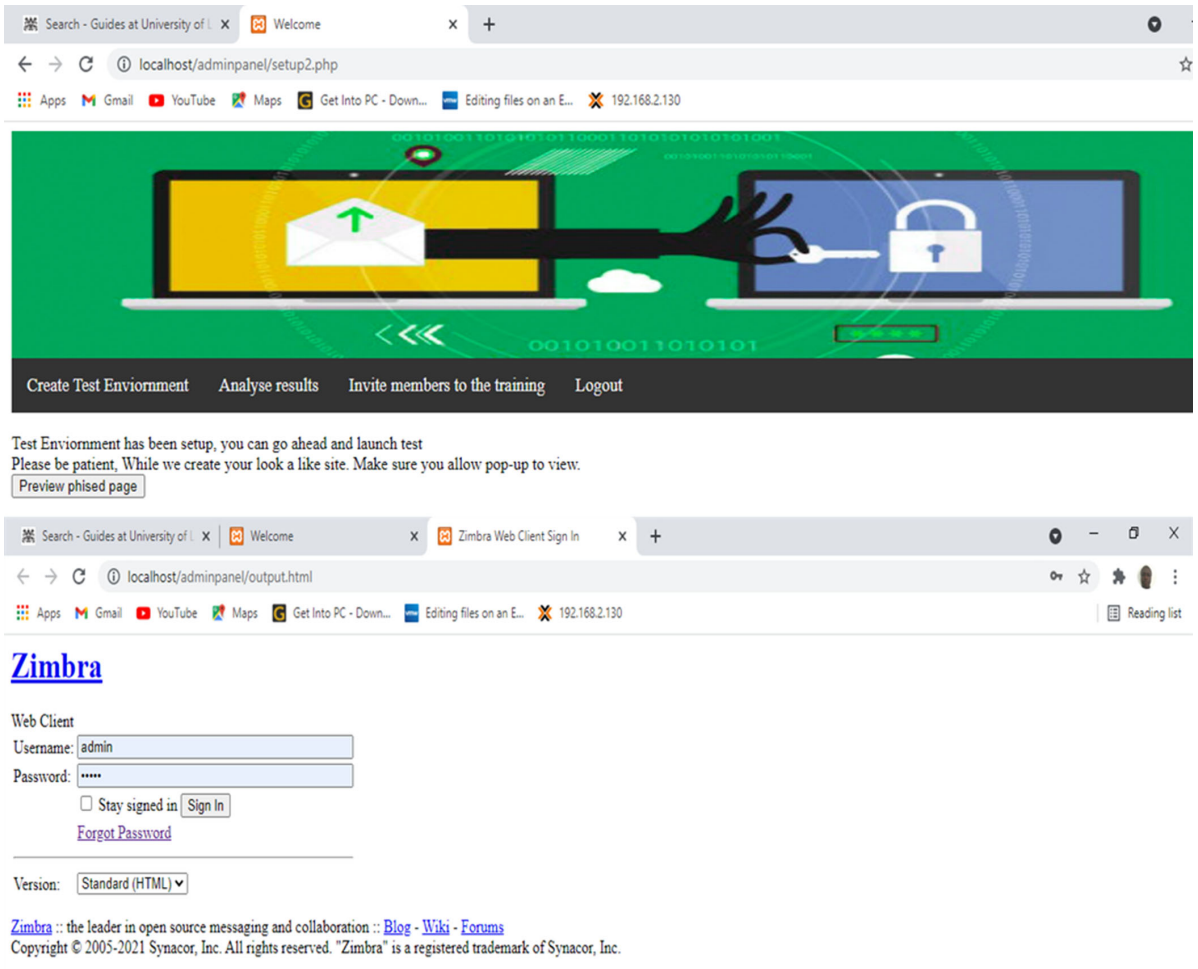


Figure 16
Admin can upload CSV file and invite the members to take test

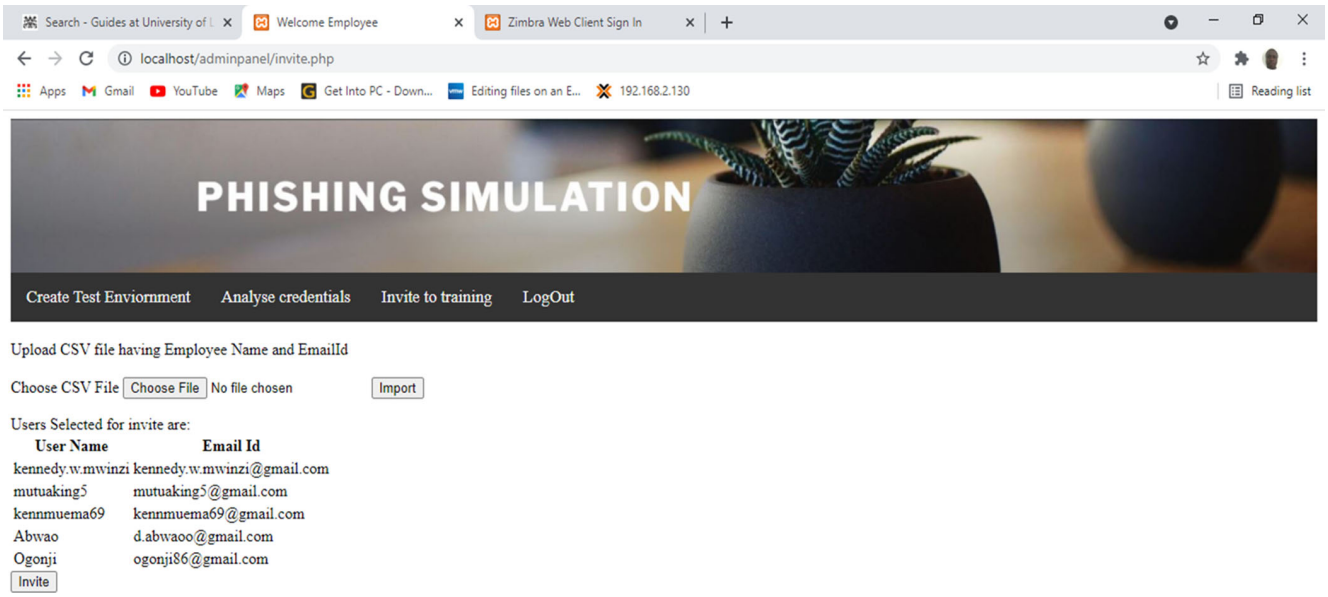
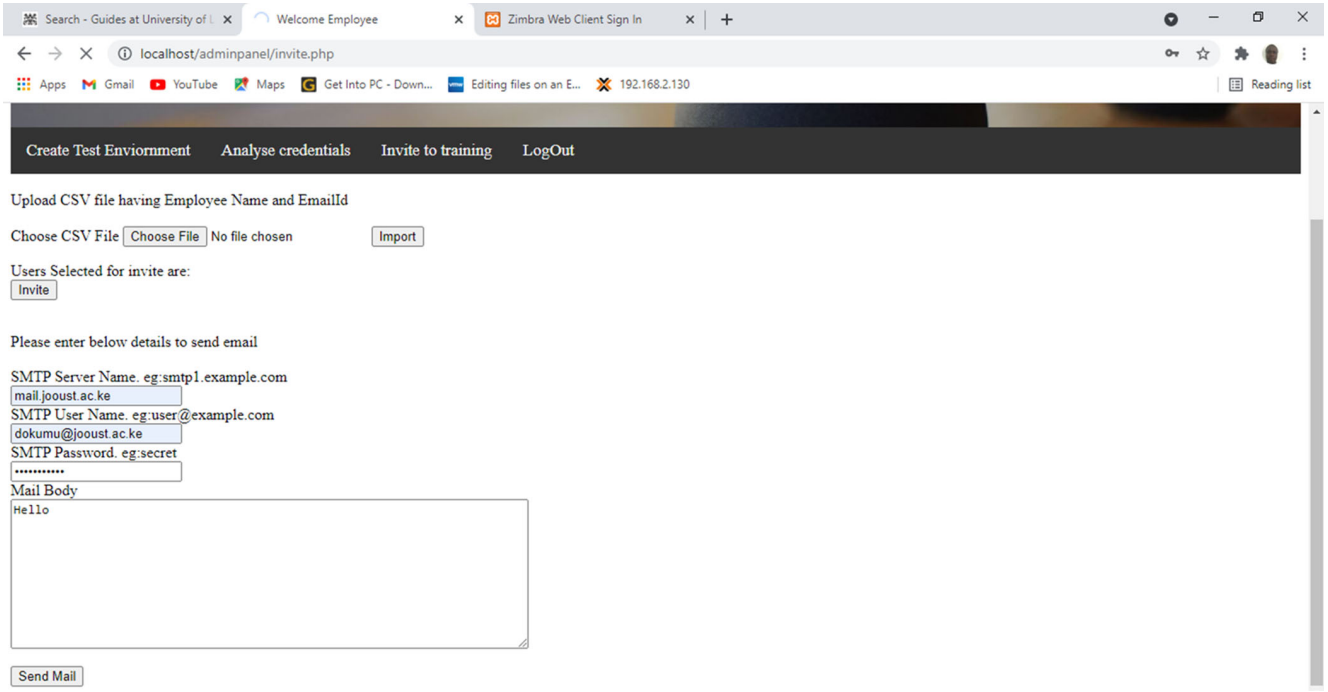


Figure 17
Enter SMTP server and administrator's email credentials to invite members



6. Results and Analysis

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

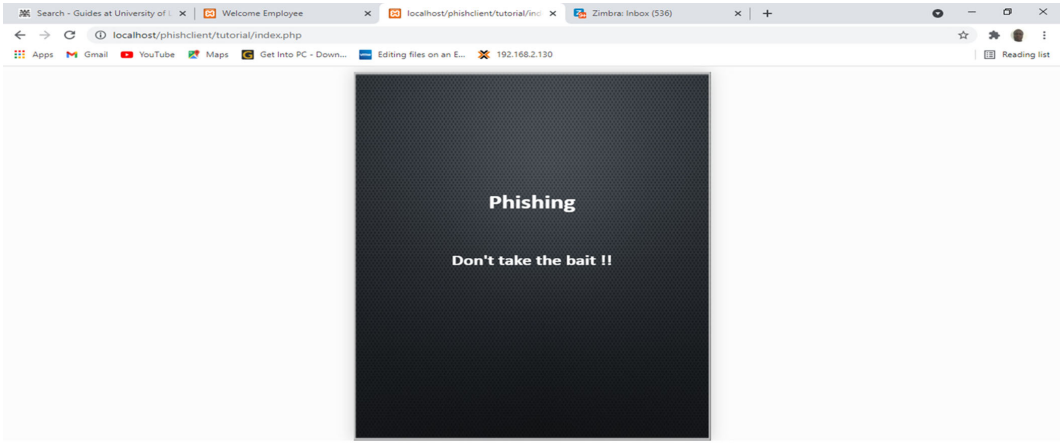
The first step will be on pre-assessing user knowledge for social engineering attacks.

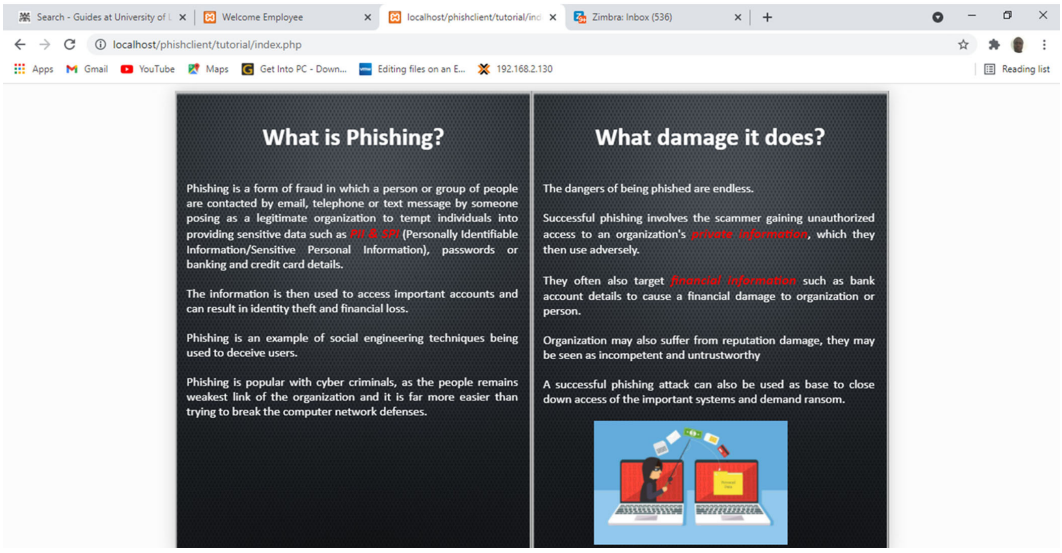
The second step will be the post-assessment assessment after integration with human firewall.

In either case, a simulator will be embedded in sample users to capture data on pre-assessment and post-assessment.

According to Leedy & Ormrod (2005), the data could be organized tables, figures, and other formats to present information in a compact way. The study intends to have

Figure 18
Tutorial (Client-side module)





results in tables, forms, and graphs for representations. The results on the client's module will either show to the user that he/she failed the test or a certificate of success will be awarded as shown below.

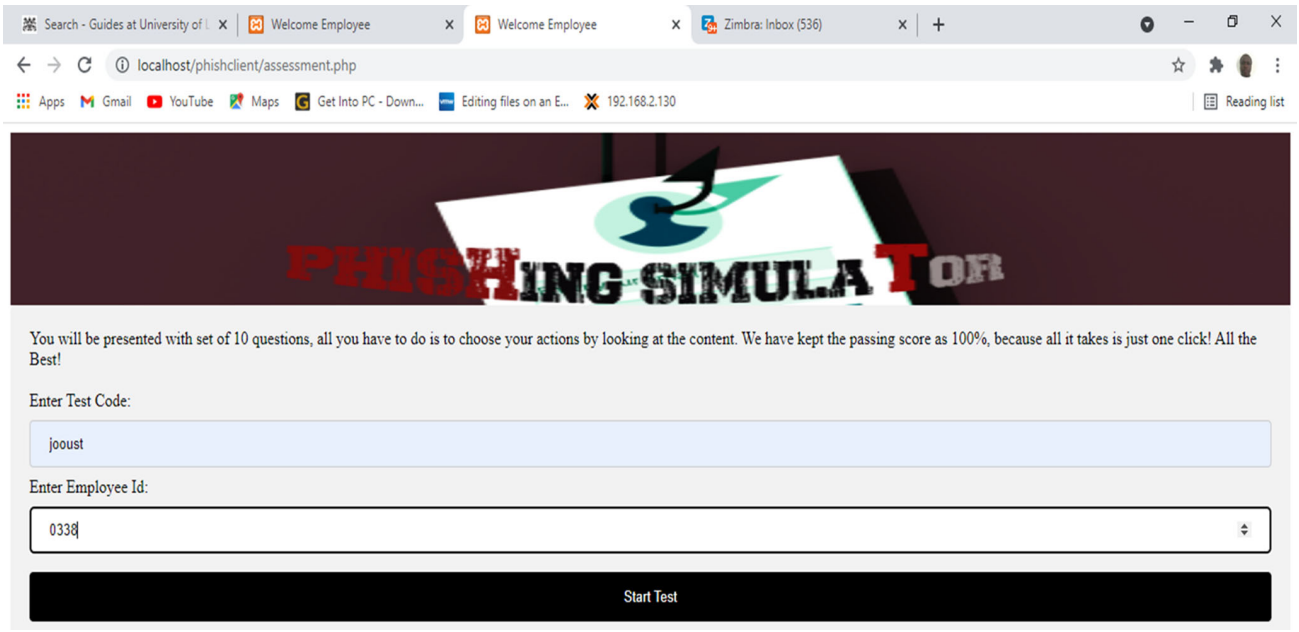
Either from the admin module a more comprehensive result will be analyzed. And based on the result seen below, a user will be scheduled to retake the simulated training immediately focused on the areas of weakness or the user will only be given latest information on phishing from the collaborated central pool and will be tested paradisiacally as demand dictates. The results will be in the form of graphs and a table that analyzes various scenarios based on the model that employees seek to respond to the quizzes. This will assist in determining the organization's current outreach stance.

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

Result 2: Number of employees who will click on the malicious links: This result is specifically focused on testing employees who click on malicious link to test this area of insecurity, incase organizations considered this security area requires more training than a lot of training will be focused in this area. The result is relayed in percentage of those would click on the malicious link verses those who would not.

Result 3: Number of employees who will download the dangerous attachments: This result shows the percentage of employees who would download dangerous links compared to those who would not. When a lot of questions are answered correctly in this area, then the result will indicate that many employees would not click on dangerous attachments. Either when a lot of questions in this area are answered wrongly, then a higher percentage will show employees would click on dangerous attachments. The latter indicates a security threat to the organization.

Figure 19
Assessment (client-side module)



Result 4: Number of employees who will reply to phishing emails: This result shows the percentage of employees who would reply to phishing emails, versus those who would not. When a lot of questions are answered correctly in this area, then the result will indicate that many employees would not reply to phishing emails. Either when a lot of questions in this area are answered wrongly, then a higher percentage will show employees would reply to phishing emails. The latter indicates a security threat to the organization.

Result 5: Average awareness of the organization: This result shows the percentage of employee's average awareness from 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, then result will indicate high employees' awareness in terms of percentages. Either when a lot of questions in the above areas are answered wrongly, then a higher percentage will show employees are unaware. This helps guide organizations/corporates on the status of their security at a particular time.

Result 6: Employees wise results: This indicated how individual employees performed. The employees are identified through Employee Id, and the results are relayed out of 10 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 will be to make the right choice in handling emails will be tested through this section of the result.

7. 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 to 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 clicks, the simulator will allow 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. These results achieved above are proving the success of the tool (to combat social engineering attacks) combined with the technical security setups, that is, firewalls, encryptions, virus scans, and many more, email insecurity threatening BEC and CEOs will be tackled effectively.

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

8. Recommendations

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 will be changed to take responsibility for securing the organization, therefore resolving the issue of employees/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, and competition that drives staff to excel at their jobs. Corporates should also strive to create an environment of teamwork and hence increase employee decision-making efficiency, in order to educate users and rather not to train them (converting them to human firewall), Organizations/corporates should start by organizing security-oriented incentives to motivate the staff to take this education positively. Either there is need to bring in external security professionals as they are usually eager to get continuing education from external professionals to bring credits to education.

The organization should update its policies to accommodate and reinforce rules on the employees to ensure that the tool is used regularly and actions taken on user deemed a threat to the organizational email security.

Eventually, the newly introduced and tested human firewall should then be integrated to the already existing email security mechanisms as the last line of defense bringing a new email security model shown below in Figure 20.

Model integrated human firewall with existing email security.

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 is where security goes wrong. Therefore, the need to create a firewall that will help 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

Figure 20
Charts displaying results

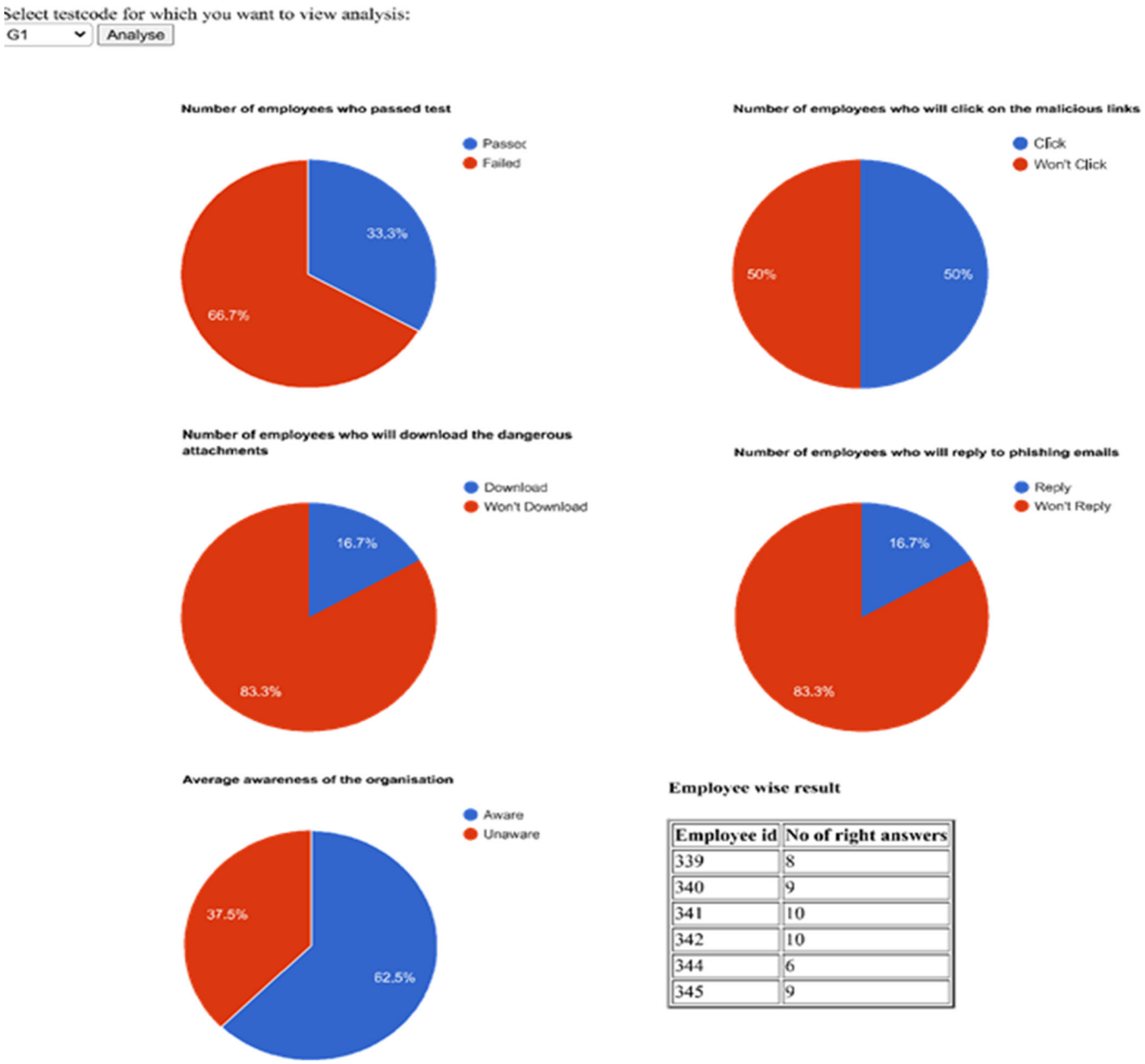
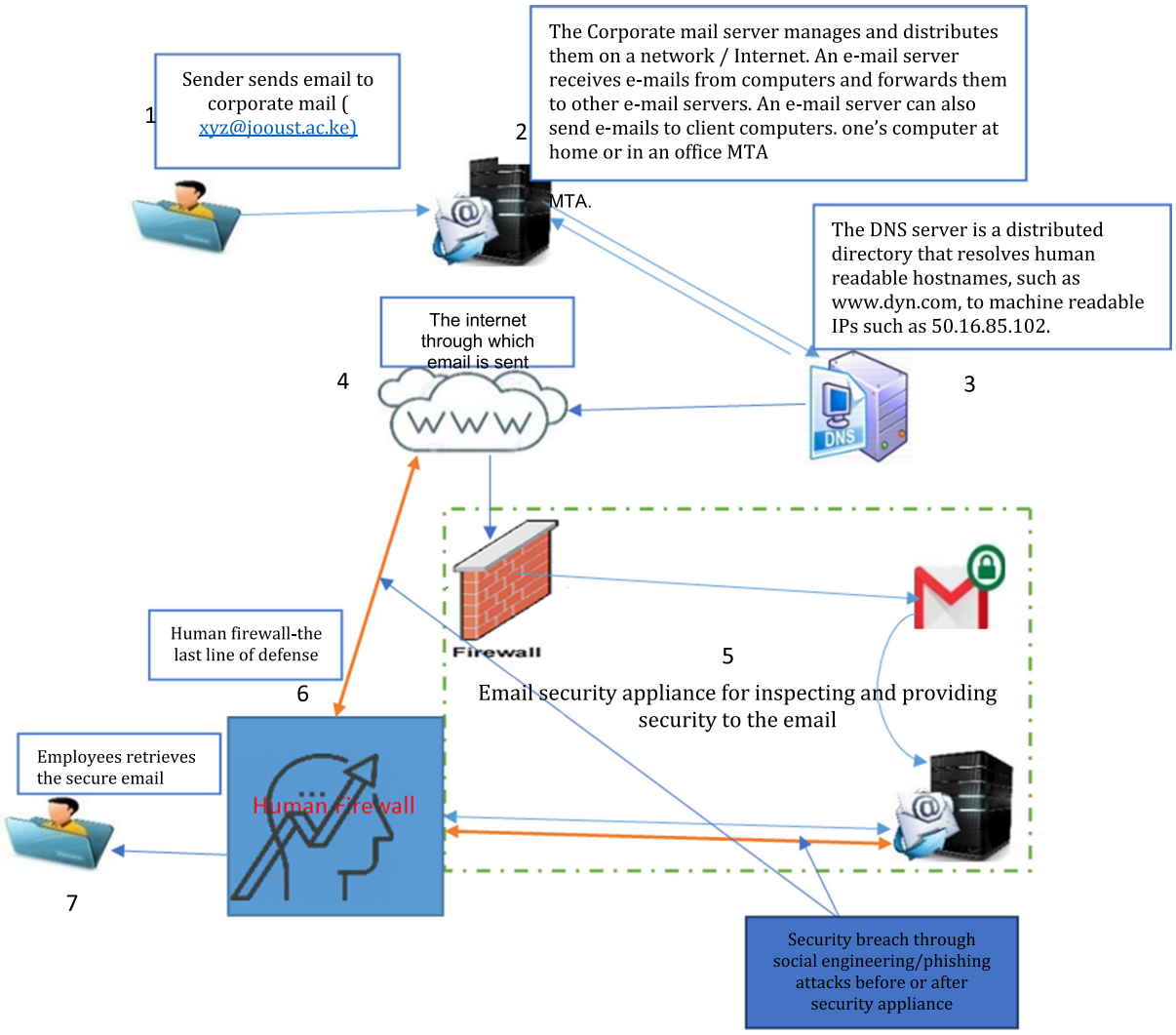


Figure 21
Secure email flow integrated with human firewall



physical security measures that have always existed. The problem that has been lacking in email security was caused by human weakness. Human firewall introduces users to be part of the security team by making them responsible for their actions, that is, avoid clicking dangerous links by identifying them, flagging them, and being informed of the with latest trends in attacks. This will ensure security is tackled in totality. See Figure 21.

9. 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 will take 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 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.

Acknowledgments

This work was supported by Jaramogi Oginga Odinga University of Science and Technology through the School of Informatics and Innovative Systems (SIIS) through varied knowledge and skills availed and a good environment which were very instrumental for this research. Lots of credit go to my Supervisors Dr. Richard Omollo and Prof. George Raburu for the

guidance they offered in this research. Their input is 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 the direction to this research.

Many thanks go to God and to my friends and well-wishers who made indirect input to this research.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

References

Abbasi, D. F. (2018). 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/

Akamai. (2017). State of the internet report. Retrieved from https://www.akamai.com/our-thinking/the-state-of-the-internet

APWG. (2014). Phishing activity trends report. Retrieved from https://apwg.org/trendsreports/

Berninger, A. (2018). Security intelligence. Retrieved from https://securityintelligence.com/ibm-x-force-iris-uncovers-active-business-email-compromise-campaign-targeting-fortune-500-companies/

Brook, C. (2020). What does a data breach cost in 2020? Retrieved from https://digitalguardian.com/blog/what-does-data-breach-cost-2020

Cialdini, R. B. (2007). Influence: The psychology of persuasion (Vol. 55, p. 339). New York: Collins.

Cisco. (2010). Email security deployment guide. Retrieved from https://www.cisco.com/c/dam/global/en_ca/solutions/strategy/docs/sbaBN_email_secDG.pdf

Cisco. (2021). Cisco secure email. Retrieved from: https://www.cisco.com/site/uk/en/products/security/secure-email/index.html

CISOMAG. (2019). Insider sold 68K customer records to scammers: Trend micro. Retrieved from https://cisomag.eccouncil.org/insider-sold-68k-customer-records-to-scammers-trend-micro/

Clearswift. (2021). Clearswift secure email gateway. Retrieved from: https://www.clearswift.com/?code=cmp-0000011446&ls=71771001&gad=1&gclid=Cj0KCQjwsIejBhDOARIsANYqkD1WRlgpvNJUjePooIqeTQ5QPk-RJxw0xsMx7pdO8EWYFkVMd3t-CAAaAt40EALw_wcB

Cloudmark. (2016). 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/

Colón, M. (2014). "Human error" contributes to nearly all cyber incidents, study finds. Cybersecurity Source, 1–2.

Comtech. (2017). Comtech-networking. Retrieved from http://www.comtech-networking.com/blog/item/274-the-human-firewall

ENISA. (2021). The European union agency for cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Federal Bureau of Investigation. (2016). Business e-mail compromise: The 3.1 billion dollar scam. Retrievd from https://www.ic3.gov/Media/Y2016/PSA160614

Frumento, E. (2018). 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). Human firewall. Retrieved from https://www.humanfirewall.io:https://www.humanfirewall.io/howit.php#howitwork

Getthreatready. (2017). Email and the human firewall. Retrieved from https://www.getthreatready.com:https://www.getthreatready.com/email-human-firewall/

Guntrip, M. (2020). Ensuring that your users are the solid line of defense against cyber threats. Retrieved from https://www.brighttalk.com/webcast/13513/382659?player-preauth=VicWfpBwC3YUmgImm%2FhjBP4RONz%2B04I%2B8Yq9%2BKuhRlA%3D&utm_source=brighttalk-recommend&utm_campaign=network_weekly_email&utm_medium=email&utm_content=collab&utm_term=092020

Hernedy, R. (2016). Threats 101. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81. https://dl.acm.org/doi/10.1145/2063176.2063197

Johnson, S. (2014). Social engineering attacks: is security focused on the wrong problem? Retrieved from https://searchsecurity.techtarget.com/feature/Social-engineering-attacks-Is-security-focused-on-the-wrong-problem

Kaplan, D. (2018). 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/

Kevin, D. Mitnick, W. L. (2002). The art of Deception. Indianapolis: Wiley.

LaMorte, W. W. (2019). The social cognitive theory. Retrieved from https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/BehavioralChangeTheories5.html

Leedy, P. D., & Ormrod, J. E. (2005). Practical research (Vol. 108 P. 39). Saddle River, NJ, USA: Pearson Custom.

LeClaire, J. (2006). Holiday scammers' e-greeting card tactics. Retrieved from https://www.ecommercetimes.com/story/53889.html

Lekati, C. (2020). Creating a "human firewall" for it security. Retrieved from https://www.dotmagazine.online/issues/securing-the-future/human-firewall-for-it-security

McGee, M. K. (2017). A new in-depth analysis of anthem breach. Retrieved from https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

McLaughlin, A. (2019). 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

Mimecast. (2015). 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/

Nguyen, D. (2015). 5 ways hackers are stealing passwords. Retrieved from https://hypersecu.com/blog/91-5-ways-hackers-are-stealing-passwords

Orlando, S. (2018). The "human firewall": a more proactive approach to infosec. Retrieved from https://www.scmagazine.com/news/incident-response/the-human-firewall-a-more-proactive-approach-to-infosec

Paganini, P. (2013). Two-factor authentication for SMBs. Retrieved from http://securityaffairs.co/wordpress/15786/security/two-factor-authentication-for-smbs.html

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.

Proteck. (2017). What is a human firewall? Retrieved from https://proteksupport.com/what-is-a-human-firewall/

Sabi. (2019). Scammers' "wire-wire" trick exposed. Retrieved from www.sabinews.com:https://www.sabinews.com/scammers-wire-wire-trick-exposed/

Sadler, T. (2021). 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. Retrieved from http://www.mcafee.com/au/resources/reports/rp-hackinghuman-os.pdf

Schablik, P., *et al.* (2017). Threat Ready resources. Retrieved from www.getthreatready.com:https://www.getthreatready.com/three-key-elements-building-effective-human-firewall/

Shaikh, A. N., Shabut, A. M., & Hossain, M. (2016). *A literature review on phishing crime, prevention review and investigation of gaps*. China: IEEE.

Sjouwerman, S. (2017). Security awareness training blog. Retrieved from https://blog.knowbe4.com/7-urgent-reasons-for-creating-a-human-firewall

Smith, M. (2015). 25 most commonly used and worst passwords of 2014. Retrieved from https://www.csoonline.com/article/2872085/25-most-commonly-used-and-worst-passwords-of-2014.html

Sussman, B. (2019). Business email compromise losses jump 100%. Retrieved from https://www.secureworld.io/industry-news/new-business-email-compromise-statistics-bec

Tim, S. (2021). Human layer security. Retrieved from 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). Social engineering: the biggest security risk to your business. Retrieved from https://www.itpro.co.uk/social-engineering/30017/social-engineering-the-biggest-security-risk-to-your-business

Yin, R. K. (2003). Designing case studies. Qualitative research methods, p. 111 5(14), 359–386.

How to Cite: Okumu, D. O., Omollo, R. O., & Raburu, G. (2023). Human Firewall Simulator for Enhancing Security Awareness against Business Email Compromise. *Journal of Computational and Cognitive Engineering* https://doi.org/10.47852/bonviewJCCE3202415