

Cybercrime and its Psychological Tricks and Traps and Computer Securities

Abstract

Several studies agree that traditional ways of preventing cybercrime, by applying common computer security techniques such as passwords, firewalls and anti-virus, are no longer effective tools/methods for preventing cybercrime. Moreover, the empirical studies evidence that the most effective cybercrime technique is the phishing which is a psychological technique that the cybercriminal use technical tricks and psychological traps to convince or induce the end users to complete the cybercrime plan or mission. In that sense, the individual (victim) became the enabler or catalyst of their own risk (cyberattack). The study establishes Psycho-Cybercrime Solution (PCS) Model that detect tricks and psychological traps in the phishing attack. The PCS model was tested in 40 e-mail messages, 20 from the author's Gmail and 20 from Yahoo accounts and its results show best fits. The study finds that the phishing attack is a psychological attack/issue that still greatly challenges traditional preventive techniques, which are only crafted to detect and prevent cyberspace's technical default or misrule. Moreover, this study finds that technical-based prevention techniques are less effective in reducing phishing attacks. Therefore, we recommend to special program will be developed in the community to address the cybersecurity program by technology vendor or other stakeholders such as financial institutions, law enforcement agencies, revenue authority, learning institutions, communication service companies and government. Moreover, in specific, we recommend to use the Psycho-Cybercrime Solution (PCS) algorithmic Model as a basic awareness learning approach to end users and technology vendors.

Keywords: Cybercrime, Computer Security, Phishing, Cybersecurity, Psychological Traps

1.0 Introduction and Literature Review

Several studies agree that traditional ways of preventing cybercrime, by applying common computer security techniques such as passwords, firewalls, encryption, authentication and anti-virus, are no longer effective tools/methods for preventing cybercrime using modern penetrating tool such as social engineering, sniffing and spoofing, exploitation, vulnerability analysis, password attack, wireless attacks, reverse engineering and phishing (Djenna et al., 2023; Rupesh and Rajasekhar , 2021; Jones, n.d; Abroshan et al., 2018). The empirical studies evidence that most effective penetration techniques is the phishing. Phishing techniques are cybercrime techniques that use the psychological tricks and traps to convince or induce the individual to complete the cybercrime plan or mission. In that sense, the individual (victim) became the catalyst of the crime.

Several scholars evidenced that phishing is the most effective penetration tools, hence, it is

mostly used by cybercriminals (Djenna et al., 2023; Li and Liu, 2021; Muntode and Parwe, 2019). Because the phishing is a cyber-psychological traps, the cybercriminals are prefer to use both phishing techniques (e-mail and voice). The studies on cybercrimes indicate phishing incidence and their effect are higher than other cybercrime techniques. Djenna et al. (2023) studied the effect of cybercrime and found that the economic effect of cybercrime is predicted to be USD 10.5 trillion annually by 2025 in the world. Djenna et al. (2023) also evidenced that the top ten biggest cyber threats is the phishing at the top at 22 per cent, followed by malware at 20 per cent and the remain percentage are shared by other cybercrimes. In addition, in 2022, the USA reported phishing incidences to be about 41.473 percent of the others. Moreover, Djenna et al. (2023) confirmed that cybercriminal activities' effect on the global economy has increased by more than 50 per cent in two years. Therefore, the issue of phishing is still a global challenge that is growing year by year.

Jones (n.d) contends that cybercrime has become a powerful tool for stealing information. The anonymity and convenience of the Internet have enabled criminals to commence highly targeted attacks with minimal effort (Li and Liu, 2021; Muntode and Parwe, 2019; NCSN, 2020; Jones, n.d). The most successful and dangerous of all the cyber-attacks is phishing. Security vendor research found over 94 per cent of detected malware is delivered via e-mail, which makes phishing the number one cyber threat to organizations. With black market demand for information at an all-time high, several companies are experiencing more phishing attacks (Djenna et al., 2023; Reddy and Reddy, 2014). The attacks are becoming more complex, targeted, and increasingly challenging to identify (Hoseini, 2022; Rupesh and Rajasekhar 2021; Jones, n.d). The common adverse of phishing attacks are identity theft, loss of sensitive information (personal or professional), loss of intellectual property, data sold to criminals and third parties, financial losses, unauthorized transactions, exposed usernames and passwords, malware and ransomware installation, backdoors (access to systems) to launch future attacks and reputational damage (Djenna et al. 2023; Hoseini, 2022; Jones, n.d). Hoseini (2022) contended that unlike the ransomware attack, which targets the victim's device and encrypts the files or blocks the whole device, the phishing attack targets the users. Regardless of the high system security or how many firewalls, encryption software, and two-factor authentication mechanisms the system has, individuals can still fall for a phish. Anyone unsuspecting can be the target of an attacker (Hoseini, 2022; Pandey, Kumar, and Singh, 2017; Pande, n.d).

One of the reasons why phishing still works is that some people wish to take a gamble (Broadhurst et al., 2020; Kalakuntla, Vanamala, and Kolipyaka, 2019; Abroshan et al., 2018). Therefore, an attractive prize or endorsement could be enough to get them into a trap. Phishers use an individual's behavioural weaknesses to offer attractive promotions and other techniques to trick the person into fulfilling the desired actions (Kalakuntla et al., 2019; Abroshan et al., 2018). The phishing attacks will not eradicated with a single solution and at one level (Abroshan et al., 2018; Bhavsar et al., 2018; Pande, n.d). A study evidenced that even when utilising modern anti-phishing techniques, over 11 per cent of users read spoofed messages and enter their credentials (Broadhurst et al., 2020; Abroshan et al., 2018). Hoseini (2022) evidenced that many ransomware attacks start with phishing. This type of attack grows daily, and beyond spreading via e-mails, it is also spreading through SMS,

instant messaging, social media sites such as Facebook, and even massively multiplayer games (Hoseini, 2022; Li and Liu, 2021; Abroshan et al., 2018). Human interaction with the Internet is one of the essential aspects of this type of attack. This means the attacker will use psychological tricks to make victims agree to interactions outside their standard patterns (Hoseini, 2022; Abroshan et al., 2018). According to Hoseini (2022), in a study from 2020, more than 91 per cent of cyberattacks, from 2012 onwards, were inundated with phishing attacks. Therefore, they recommended training and knowledge as the most valuable and crucial protection against phishing (Djenna et al., 2023; Hoseini, 2022; Li and Liu, 2021).

A significant challenge of cybersecurity and cybercrime is that the phisher uses convincing messages which psychologically impact the victim and make the victim the catalyst of the crime incident. In that sense, preventing cybercrime becomes difficult because the victim is the catalyst. Notably, phishing is covertly and advanced planned; the end user has no opportunity or time to learn about the phishing tricks, hence becoming vulnerable (Hoseini, 2022; Li and Liu, 2021; Abroshan et al., 2018). Therefore, in this paper we aimed to examine the nature and scope of tricks and traps are commonly used by the cybercriminal attackers. Moreover, the study disclosed how the cybercriminal use tricks to set their traps to the victim, and the victim become the enabler of the crime. In addition, the study provided the techniques and tool of detecting and counter the psychological tricks and traps used by cybercriminals. The study established the Psycho-Cybercrime Solution (PCS) model to prevent and combating the cybercrime. This is the generic model that detect/identify the tricks and untie the traps of the cybercriminal. The next part of the paper are problem identification (trick and traps), Methodology, finding and discussion, and solutions.

2. Problem- Tricks and Traps Defined

One of the challenge of detecting, preventing and combating cybercrimes originated on its technology awareness. In most cases, the cybercrime are committed with skilled people with the awareness of the existing technology. On the other hand, the cybercrime is sometimes lacks commission scene and specific jurisdiction. One of the leading cybercrime is phishing (Hoseini, 2022; NCSN, 2020; Muntode and Parwe, 2019; Abroshan et al., 2018). Conley et al. (n.d) defined phishing as a psychological attack by cybercriminals to trick the end user into giving up information or taking action. Cybercriminals convincingly craft these messages and send them to millions of people around the world. The cybercriminal may send the message to a few targeted individuals. This kind of phishing is called spear phishing. Sometimes, cybercriminals can target a group of higher rank or position in the management; this kind of phishing is known as whale phishing (Rupesh and Rajasekhar, 2021; Li and Liu, 2021; NCSN, 2020; Ollmann, n.d).

Abroshan et al. (2018) identify two ways that phishing attackers may choose to push a victim to fulfil the demand, which is *the peripheral route to persuasion* and the *central route to persuasion*. The central route to persuasion is the method or ways the phishers' message encloses systematic and logical reasoning, inspiring the victim to deem and consider the statements rationally and eventually do anything the phishing attacker wants. The phishing

attacker has carefully designed the situation and the quarrel and knows the victim's conclusion. On the other hand, the peripheral route to persuasion is the method in which a phishing attacker leads the victim to a request without considering it. The phishing attacker uses *mental shortcuts to bypass logical premises*. For example, the victims receive an e-mail informing them that they get thousands of dollars and a costly computer or any valuable commodity in current lottery advertising. This fantastic prize would stimulate many people to give personal.

Moreover, Abroshan et al. (2018) contended that technical tricks and social engineering are two mechanisms phishers use to steal personal and financial credentials. Social engineering aims at individuals, and the result of attacks depends on human decisions, trust, and other cognitive factors (Muntode and Parwe, 2019; Abroshan et al., 2018; Pandey et al., 2017). Fraud is a human endeavour involving deception, rationalisation, violation of trust, the intensity of desire, purposeful intent, risk of apprehension, etc. So, it is important to understand the psychological drives that might control the behaviour of fraud perpetrators (Rupesh and Rajasekhar, 2021; NCSN, 2020; Abroshan et al., 2018). We should study psychological and sociological factors to discover why a user gets caught in a phishing net to analyse the root causes of phishing attacks (Rupesh and Rajasekhar, 2021; Abroshan et al., 2018). We should consider motivational and cognitive sources of errors to assess phishing attackers. A phishing attacker uses errors such as visceral influences, false consensus, reduced motivation for information processing, lack of self-control, preference for confirmation, mood regulation and phantom fixation, authority, sensation seeking, reciprocation, commitment and consistency, reduced cognitive abilities, background knowledge and overconfidence, norm activation, liking and similarity, social proof, alter casting, positive illusions, to phish (Rupesh and Rajasekhar, 2021; Kalakuntla, et al., 2019; Abroshan et al., 2018; Reddy and Reddy, 2014).

Abroshan et al. (2018) evidenced that phishing attackers apply several technical deceit and social engineering practices. In most cases, the cybercriminal must convince the victim to purposely perform a series of activities to offer access to confidential information (Abroshan et al., 2018; Reddy and Reddy, 2014). Phishing is a cybercrime in which the attacker masquerades as a trusted entity (Li and Liu, 2021; Broadhurst et al., 2020; Muntode and Parwe, 2019; Pandey et al, 2017; Pande, n.d). The attacker tries to entice the victim by offering temptations to which the victim easily falls prey (Broadhurst et al., 2020; Muntode and Parwe, 2019). Advanced Persistent Threats (APT) and other cyberattacks begin with phishing (Li and Liu, 2021; Muntode and Parwe, 2019). When the victim opens the malicious e-mail or message and proceeds to perform the requested action, the phishing tools sent by the attacker are activated and complete the required action of stealing information and attacking the victim's financial resources. The phisher uses popular communication channels such as e-mail, webpages, IRC, and instant messaging services (Li and Liu, 2021; Abroshan et al., 2018; Ollmann, n.d). One common trick a phisher uses is impersonating an agent of a legal entity or known person.

Recently, phishers have continued using e-mail with other tricks, such as utilising web banner advertising, message boards, instant chat (IRC), and instant messenger (Li and Liu,

2021; NCSN, 2020; Ollmann, n.d). More recently, phishers used the Voice over IP (VoIP) to deliver their persuasive message and convince victims to either respond with their credentials or drive them to a more sophisticated automated credential-stealing mechanism (Abroshan et al.,2018; Ollmann, n.d). The most popular means for acquiring the victim's information is now through websites designed to represent the real organisation from which the fake message came (Ollmann, n.d). However, in the last few years, phishers have also used exploit material and attachments to deliver specialised payloads such as key loggers, spyware, rootkits, and botnets (Abroshan et al., 2018). Abroshan et al. (2018) contend that phishing is a technique that a scammer uses to deceitfully acquire the victim's bank account information, personal identification, or any other valuable data.

Several anti-phishing techniques and tools are in place, but unfortunately, phishing still works (Li and Liu, 2021; Muntode and Parwe, 2019; Abroshan et al., 2018). One of the reasons for the persistence of phishing is that phishers typically use human behaviour to design and utilise a new phishing technique (NCSN, 2020; Abroshan et al., 2018; Pande, n.d). Therefore, identifying scammers' psychological and sociological factors could help us tackle the root causes of fraudulent phishing attacks (Li and Liu, 2021; Muntode and Parwe, 2019). Abroshan et al. (2018) reviewed the existing anti-phishing techniques and confirmed that most are technically trying to detect and/or prevent phishing attacks. Therefore, they think that focusing on the human psychological and sociological factors that phishing attackers use to scam people would be an effective way to tackle phishing attacks fundamentally. They believe current anti-phishing solutions are functional, though insufficient, as phishers use people's psychological weaknesses to design new phishing attacks.

Phishing prevention is becoming a growing challenge year by year as technology advances. This is because phishers are constantly changing their battlefield. That is, they are continually developing new deceptive techniques to confuse customers and hide the true nature of the message (Li and Liu, 2021; NCSN, 2020). It is increasingly challenging to identify attacks. Hoseini (2022) contended that unlike the ransomware attack, which targets the victim's device and encrypts the files or blocks the whole device, the users of phishing attacks are the users. Regardless of the high system security or how many firewalls, encryption software, and two-factor authentication mechanisms the system has, individuals can still fall for a phish. Anyone unsuspecting can be the target of an attacker (Hoseini, 2022; Rupesh and Rajasekhar, 2021; Abroshan et al.,2018) suggest the preventive mechanism should be involved in three logical layers: the *client side*, which includes the user of the computer or electron or networked device; *the server side*, which consists of the business' Internet visible systems and custom applications, and *enterprise level* which distributed technologies and third-party management services.

On the other hand, Nallaperumal (2018) introduced the Ten Commandments of cybercrime prevention concept. The concept originates from the theological discipline. Nallaperumal (2018) suggests the Ten Commandments for cyber security analytics. It means the company or organisation must follow to be safe from cybercrime. These commandments are: Get which People, Get Money, Get Support; Master your Security Information and Event Management (SIEM); Build an Incident Response Plan (IRP); Implement a Core Next-

Generation Firewall (NGFW); Implement Network-Based Behaviour Analyser Capabilities; Augment Outbound Web Filtering/proxy; Integrate Threat Intelligence into Your SIEM; Upgrade or Augment Endpoint Detection Capabilities; Start Storing Full-Packet Captures (consider converged platform); and Start Hunting for Attacks; rather than waiting for alerts. Critically, the commandments are *doctrine*- based instructions that are *specific and direct* to the target audience, usually the whole populace.

The commandment provides the specific rules and instructions that should be adhered to by the audience. In that sense, these Ten Commandments lack the quality of being commandments. They are too general, technically drafted, not specific, and do not direct the whole populace of the users. They are technically constructed and directed to expert users. In that way, we need to have a simplified model that can detect and prevent cybercrime, particularly phishing attacks, by considering the two distinctive roles: *the user's role and the technology provider's role*.

3. Methodology

This study used the systematic literature review (SLR) and Meta-Analysis. The SLR is used to answer why the phishing is the leading cybercrimes. The researcher applied several studies to answer why the phishing is the leading cybercrime techniques. Meta-Analysis was used to find the solution of phishing by comparing of different studies to suss out any inconsistencies or discrepancies about the cybercrimes (Mengista, Soromessa, and Legese, 2020). Mengista, et al., (2020) defined SLR as a systematic, explicit, and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work made by researchers, scholars, and practitioners. Grant and Booth (2009) suggested the framework of Search, Appraisal, Synthesis, and Analysis (SALSA) is a methodology to determine the search protocols for SLR. The application of SALSA in SLR guarantees methodological accuracy, systematization, exhaustiveness, and reproducibility (Mengista, et al., 2020; Grant and Booth, 2009). Most scientific works such as Malinauskaite, et al. (2019), del Amo et al.2018, Perevochtchikova et al. (2017), and Grant and Booth (2009) applied this methodological approach to reduce risks related to publication bias and to increase its acceptability of the work. Thus, most review works followed the literature search protocol of Preferred Reporting Items for Systematic Reviews and Meta-Analyses and the framework of Search, Appraisal, Synthesis, and Analysis (SASA) (Mengista et al.2020). Thus is, why this study applied both the SLR and Meta-Analysis methods. The study involved 40 e-mail messages sent to the author's Gmail and Yahoo accounts, 20 from Gmail and 20 from Yahoo accounts. The study further classified the 20 Gmail messages; out of 20, 10 are spammed messages, and the remaining 10 are non-spammed messages from Gmail. On the other hand, of 20 Yahoo messages sent to the author's Yahoo accounts, 10 are spammed, and 10 are not spammed (inbox messages).

4. Finding

In this study, we ask the question, from this finding, what are the cause root factors of the phishing attacks? Why are phishing attacks still increasing? What are the leading indicators of the spam message (e-mail)? What are the best combating and preventive methods or

techniques found and recommended by this study? To address these questions, we do analyses and comparison of several studies we find that the cybercriminal (phisher) prefer to phishing techniques because the technique has the psychological impression and technical tricks. The common phishing attack techniques are e-mail and voice or vishing phishing. This technique is effectively used by the cybercrime because the victim induced or psychologically convinced to complete the mission; therefore victim became the enabler or catalyst of the crime.

We find that, phishing attacks still increase because phishing attackers use psychological traps/tricks that cannot be detected and avoided by traditional techniques of cyber security solutions such as passwords, firewalls, and antivirus software. The leading indicator of phishing attacks is the *message content*, which describes the *psychological traps/tricks* using a convincing, or demanding title, promising message, strict deadline, and confidentiality restriction. The study evidences that the best combating and preventing phishing techniques are using the detecting and avoidance algorithm which known as Psycho-Cybercrime Solution (PCS) model suggested by the author in executing the end-user roles of detecting and avoiding and the technology developer or vendors' role of preventing. The PCS Model help both the end user and the vendor to detect early and hence, be aware of the incoming message or voice call from unknown sender. The model provide both technical and non-technical means of detect trick and unties psychological traps.

We applied the study some of the Google and Yahoo mails to shows some of the technical tricks that can be detected at the early stage. Remember the cybercriminal are defacing or hiding their identities, therefore, they use “crafted words or address” to communicate with the victim. Therefore, the close examination of their email address and names reveal some technical issues, e.g., email does not includes the known or nature names, abbreviated names, misspelled names, and the likes. The cybercriminal uses these trick to hide their identities. They can use the fake identities to represent a well-respected personal such as a police officer, a bank officer, pastor or reputable institution such a Bank, church, college, or hide gender etc., when they use phishing they send several message to many people with their dark-email/fake address, they craft message that will impress or even shock the receiver.

The author demonstrate this fact, by using the email message received from Mrs. Wendy Boni (unknown sender), introduced from Bukina Faso. By using the PCS Model we classified the message as a spam message. We do technical and non-technical analysis of the message and detected some trick and traps (Figure 1).

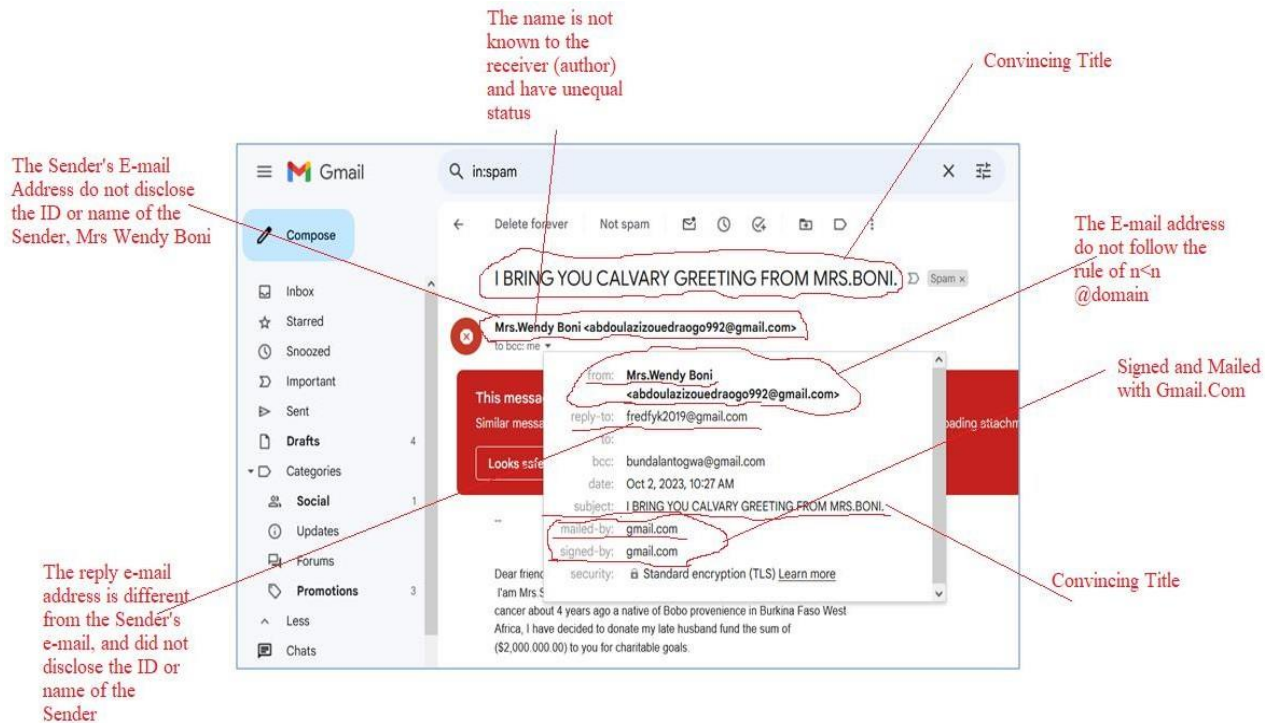


Figure 1: The spammed message from the Mrs Suzan Boni of Burkina Faso

Figure 1 shows the spammed message from a person identified as Mrs Suzani Boni of Burkina Faso. She used the convincing and demanding title “*I bring you Calvary Greeting from Mrs. Boni.*” The word “Calvary” is a psychological trick that convinces the receiver to pay attention to the message of God. The sender tickly hide her identity. In the title, the sender has introduced herself as Mrs Boni, but her names Wendy or Boni do disclose in her e-mail address “*Mrs. Wendy Boni <abdoulazizouedraogo992@gmail.com>*”. This email address discloses nothing about the sender, either her names are not used in the email address. She identifies Abdoulaziz, who is unknown. This sender’s e-mail address does not adhere to the *Authenticity Rule*, that, $n_{1,2} < n_{2,1}@webdomain$. This rule stipulates that for authenticable message the sender’s email address should disclose her/his identities, either first or last name ($n_{1,2}$) should appear before the domain name, or it vice versa ($n_{2,1}$). Moreover, the reply e-mail “*fredfyk2019@gmail.com*” discloses another name, *Fred*, different from the sender's. In that sense, we conclude that the sender or source is unknown.

On the other hand, the message was signed and mailed by the authentic webmail, Gmail. We learn that the main trick is the psychological traps, not the technical issues. We noticed that the e-mail was signed and mailed with the authentic webmail, Gmail, but the e-mail was found to be a phishing attack. Therefore, we must only consider the message content and sender (sources) profile, which describe the psychology, not the technical issue detected or examined in the sender's e-mail address.

In addition, we can analyses furthermore, the psychological contents of the message (e-mail). We aim to disclose the psychological trick/trap constructed by the sender. In the introduction, the

Sender starts with “Dear friend.” It is the convincing welcoming words not officially used in the formal letter. The sender introduces herself as Mrs. Suzan Boni, a 51-year-old *dying woman who was diagnosed for cancer*. The word dying woman is a psychological trap. The sender intends to deceive the receiver that the sender's life is in danger. The diagnosis of *cancer* is an incurable disease. The physiological out is that this woman will die soon because she suffers from an incurable disease. Moreover, the sender explains that she is *widowed* and inherited a lot of *money (\$ 2,000,000.00)* from her *late husband*; because she will die soon, she decided to use the money for *Godly* purposes to serve the needy. Critical analysis of this message content we most of words are psychological premises intended to deceive the receiver into believing that the sender is honest. Notably, all the words in her e-mail, which are coloured, indicate the physiological premises that trap the receivers' minds (Figure 2).

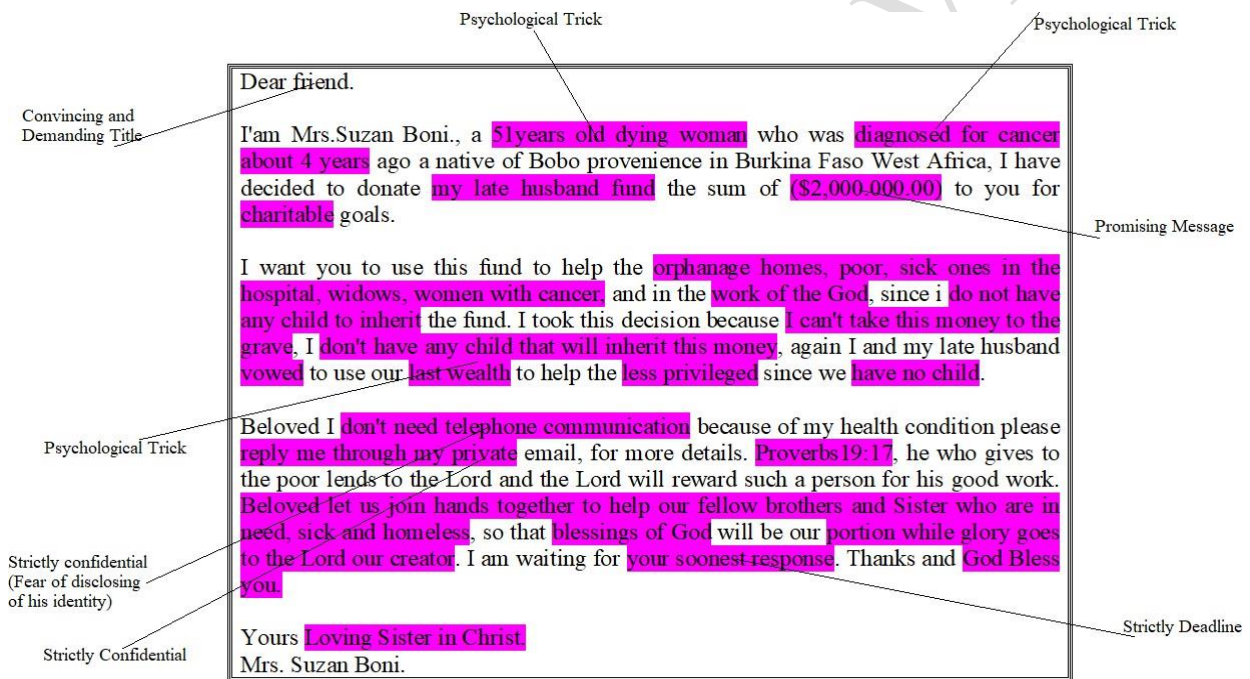


Figure 2: The spammed message from the Mrs Suzan Boni of Burkina Faso

Figure 2 shows the spammed message from the Mrs Suzan Boni of Burkina Faso. The message content analysis by PCS Model and reveals that the message is a phishing attack. However, the sender channeled her message through authentic webmail. The only detection done is through the content analysis, which detects the physiological trap trapped by the sender. In the message, the coloured words show the convincing and promising words that psychologically impact the receivers. For example, the sender says she does not have a child to inherit the money and did not need the telephone communication because of her health problem (notably, the telephone communication will disclose her identity). The provision of the Bible verse, Proverb 19.1, tries to convince the receiver psychologically to believe that a sender is a good man or woman with a religious solid fellow (Christian). Therefore, she has

good faith with the receiver.

5. Solution Provided

The study disclosed the tricks and traps used by cybercriminal. Therefore, the author developed the phishing detecting and avoidance algorithm known as the Psycho-Cybercrime Solution (PCS) model. This model provides a systematic way to detect spam messages. The end users' detection of spam messages increases awareness of the risks of phishing and leads them to avoid phishing risks. The algorithm consists of two main roles: users and technology providers' roles. We describe the role of the end users as the detecting and avoiding roles, and the technology provider has the role of preventing it. The technology provider has the role of educating or informing the end users using the guidelines and caution of the risk associated with the technology or service. Conversely, the end-user has the role of adhering to the technical trick or instruction provided by the technology provider and avoiding the spam message by detecting the psychological and technical trick used by the spammer or phisher.

The model has three decisional dimensions and four decision rules with specific indicators. The model uses the principles of the classification algorithm. The decisional dimension of detecting spammer is the message contents to which the algorithm applies the *Fair-and-Square* (Just and Honest). That is, the message is not intended to cheat or defraud; not deceptive or fraudulent. Therefore, we learn or train the model to learn the indicators of spam: convincing titles, demanding titles, kindly requesting titles, promising messages, strict deadlines, and strict confidentiality, which are labelled suspicious to spam. The second dimension, sender address (channel), applies the authenticity rule. This means the sender's address or channel should be genuine or valid, not fake or forgery. Therefore, we learn or train the model to learn the indicators of spam, that authentic e-mail format or structure is in the form of " $n_{1,2} < n_{2,1}@webdomain$ ". For example, if the message e-mail comes from John Ketwa, the standard e-mail address will be "*John Ketwa > John ...@gmail.com*" or *Ketwa...@gmail.com*. This e-mail address format is labelled as not spam because the e-mail discloses the sender's identity (name or ID). That is, the e-mail provides one or both of names of the sender. The model will label suspicion to spam if the e-mail of John Ketwa, does not disclose either first or last names. For example, *John Ketwa > jajaja897@gmail.com* will be labelled as spam because the e-mail address doesn't disclose or reflect the sender's name. Moreover, the receiver's e-mail and name are not disclosed, and the classifier (model) labels the message as a spam.

Moreover, we train the model that the e-mail not signed and mailed with an authentic domain or organisation, such as Gmail, Yahoo, or other organisation domains, is classified or labelled as spam. On the other hand, if the communication is mobile, the uncommon format of mobile numbers is classified or labelled as spam. The third decisional dimension of the model is the source (sender). The Rule of Equality and Integrity governs the sender. In the communication, the receiver should consider the equitability of the status and integrity of the sender. Therefore, we train the model to learn that if the sender does not disclose the name, legal identity, current status, or location, it classifies as spam. We illustrate the algorithm in Figure 3.

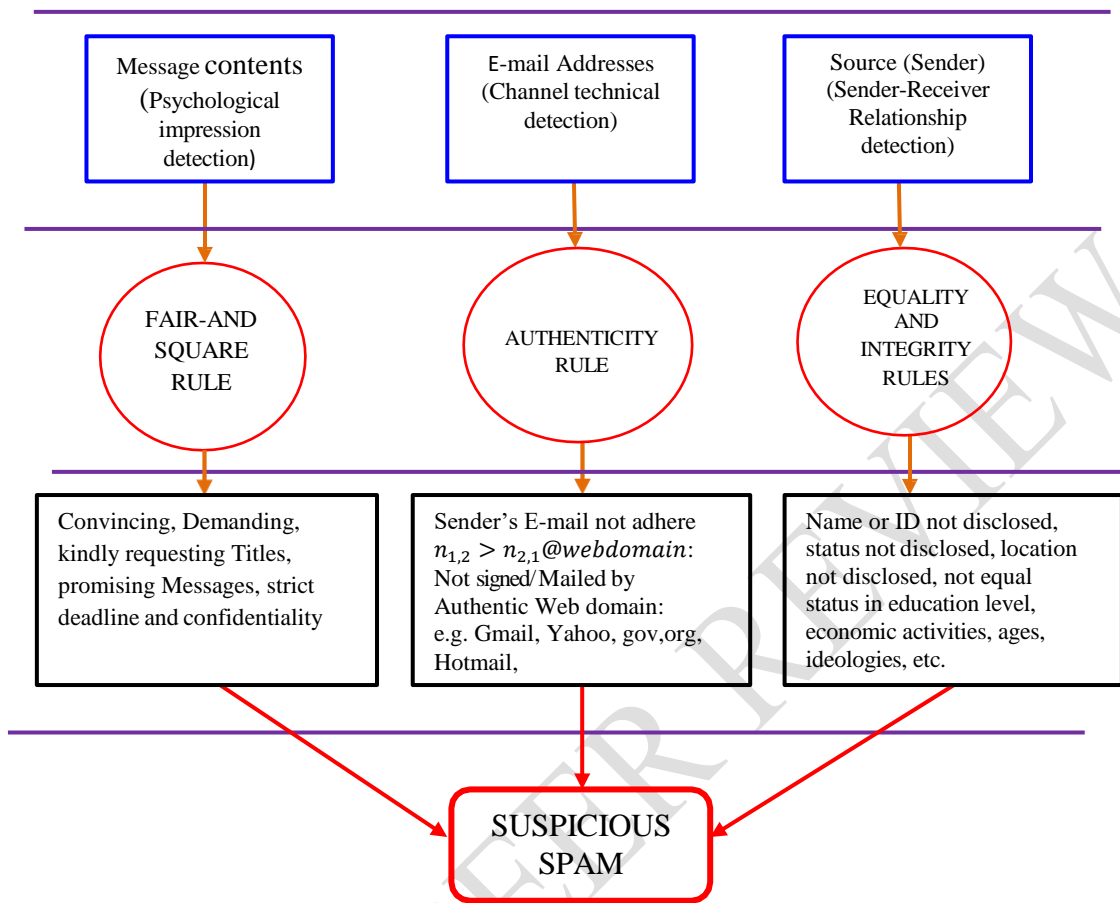


Figure 3: The Psycho-Cybercrime Solution (PCS) Model

The PCS model describe a scientific systematic algorithm of the end users to detect tricks and unstraps the traps of the cybercriminals, particular the phishers or hackers. The model was tested and trained on 40 email, 20 from Google webmail and 20 emails from Yahoo webmail. Notably, the spammed message or e-mail does not mean that it's phishing at 100 per cent. The detecting mechanisms were designed to provide early warning detection of the incoming message; therefore, the receiver can take all necessary measures to verify the spammed message using technical and logical psychological reasoning. The best way to evaluate the spam message is through this model.

6. Discussion

Cybercrime, particularly the phishing attack, still challenges law enforcers worldwide. The techniques the phisher attacker applies to steal information are the major reasons for its difficulty in detection and avoidance. The most studies revealed that most of the techniques and tools prepared in combating cybercrime are highly preventive rather than detecting and that if the threat has penetrated, the effect will continue to harm the system (Goni et al., 2022; Nallaperumal, 2018). In addition, the user has a psychological effect, which is a great challenge because they always trust the technology serves with high quality and safety. This is

also a phishing opportunity. Many victims of cybercrimes are unaware of their being the victims or victimised by the use of technology, which is the real tragedy of many cybercrimes, and cybercrimes are not perceived as heinous crimes on a par with non-cybercrimes by society at large are also catalysts to cybercrimes (Goni et al., 2022; NCSN, 2020; Broadhurst et al., 2020; Nallaperumal, 2018). In that sense, this study introduces how to detect and avoid phishing attacks by users.

The study identifies two roles in combating phishing attacks: the *preventing role* vested in the technology provider or vendor and *detecting and avoiding roles* bestowed to end users. Therefore, this study developed a spam detection algorithm or model that the end users can use to detect phishing attacks or applied by the technology provider/vendor to set or develop the technological user's precaution guideline. We called the spam detection algorithm as the Psycho-Cybercrime Solution (PCS) Model. PCS model consists of three main components that the phisher may use as an *entry*, which are message contents (Psychological impression detection), E-mail Addresses (Channel technical detection) and Source (Sender) (Sender-Receiver Relationship detection). These techniques consider both the *psychological and technical contents* of the e-mail, hence becoming the sensitive tools or techniques to detect phishing attacks.

Some anti-phishing techniques discussed in the literature, such as Access Control and Password Security, Data authentication, anti-virus software and malware scanners, and firewalls, are technically *preventive* rather than *detection*. Moreover, these techniques do not enable the end user to be free from the phishers' deceitful pretenses or psychological traps. The literature suggests that one of the reasons why phishing still works is that some people wish to take a gamble (Li and Liu, 2021; Abroshan et al., 2018; Reddy and Reddy, 2014). Therefore, an attractive prize or endorsement could be enough to get them into a trap. Phishers use an individual's behavioural weaknesses to offer attractive promotions and other techniques to trick the person into fulfilling the desired actions (Muntode and Parwe, 2019; Abroshan et al., 2018). The phishing attacks will not be eradicated with a single solution and at one level (Rupesh and Rajasekhar, 2021; Abroshan et al., 2018).

Literature evidenced that even when utilising modern anti-phishing techniques, over 11 percent of users read spoofed messages and enter their credentials (Li and Liu, 2021; Pandey et al., 2017). Hoseini (2022) evidenced that many ransomware attacks start with phishing. This type of attack grows daily, and beyond spreading via e-mails, it is also spreading through short message service (SMS), instant messaging, social media sites such as Facebook and even massively multiplayer games (Hoseini, 2022; NCSN, 2020; Broadhurst et al., 2020; Muntode and Parwe, 2019). Human interaction with the Internet is one of the essential aspects of this type of attack. This means the attacker will use trick to set the psychological traps to make victims agree to interactions outside their standard patterns (Hoseini, 2022; Rupesh and Rajasekhar, 2021; Kalakuntla, et al., 2019).

In addition, the phisher uses convincing messages which psychologically impact the victim and make the victim the catalyst of the crime incident. In that sense, preventing cybercrime becomes difficult because the victim is the catalyst. Notably, phishing is covertly and advanced planned; the end user has no opportunity or time to learn about the phishing tricks, hence becoming vulnerable. Moreover, the end users are challenged due to the proliferation and advancement of ICT. That is, via technology in which most of the users are less skilled and the technology changing faster, creating a challenge to confining it because the cybercriminal modus operandi changes as the technology changes.

On the other hand, the learning gap of new technology (new technology takes time to be learned and familiar to the end users) forces the end user or community to be ignorant of the technology. Unluckily, the user considers that they are not an owner of the technology or service rendered by that technology, so they pay little consideration to learning its associated risks. The literature explains much about the cybercrime rule and precautionary statements or guidelines to the users. Critical analysis reveals that those rules and instructions are too general, complex, and technically drafted that they become difficult to capture by ordinary users. Consequently, the users ignore the precautionary instructions/guidelines and rules, becoming the victims of cybercrime because they are unaware of the users' guidelines and rules of the technology. Expert end-users effectively apply these cyber security precautionary guidelines and rules. This situation increases cybercrime because most people make transactions through a computer or networked device without cyber security precautions. This is a great challenge!

In that sense, apart from the development of the PCS Model, the awareness training program on the detecting and avoiding roles of the end users will be the best strategy to overcome or reduce the incidence of phishing attacks, particularly for developing countries like Tanzania, which the cybercrime are an active challenge. The PCS Model is the algorithm that fits to be developed as a preliminary precautionary model for the end user, enabling the user to detect and avoid phishing attacks. One advantage of this model is that it can be used easily by individuals with ordinary knowledge of the technology. The model is established because the individual or end user can ask precautionary questions, such as whether they know the sender. Does the message convince or attract the receiver? Does the message promise something valuable to the receiver? These are some of the questions constructed in the algorithmic model to help the end user detect and avoid spammed messages or phishing attacks, even if he or she is not knowledgeable about the technology.

7. Conclusion and Policy and Technical Recommendation

The study proves that the phishing attack is a psychological attack/issue that still greatly challenges traditional preventive techniques, which are only crafted to detect and prevent cyberspace's technical default or misrule. Moreover, this study finds that technical-based prevention techniques are less effective in reducing phishing attacks. It is because the phishers usually use genuine e-mail addresses with authentic web domains such as Gmail, Yahoo, and others to communicate with their targets to convince the victim psychologically. In that sense, we need psychological measures to combat phishing attacks. It

is true! This study found that the main catalyst of the phishing attack is the victim. In other words, the victim is the one who complements or enables the completion of the commission of cybercrime. The end users face the challenge of detecting and avoiding phishing attacks, hence becoming the cybercrime victim.

This paper draws two specific recommendations: policy and technical recommendations. The paper pledge to the decision maker to include the cybercrime security skills or awareness curriculum/program in the lowest level of study to increase the cybersecurity awareness and reduce the cybercrime risks to the community. Moreover, special program will be developed in the community to address the cybersecurity program by technology vendor or other stakeholders such as financial institutions, law enforcement agencies, revenue authority, learning institutions, communication service companies and government. These stakeholders are some of the key beneficiaries of the technology or ICT. This is because, we are living in the world of *digitalize decisions*, we purchase and buy through technology, we communication through technology, we travel through technology. In general we always making *relational or integrative* decision by using ICT. The highly dependency on ICT increases the opportunities for cybercriminals to crimes; hence we become vulnerable to cybersecurity. In specific, we recommend to use the Psycho-Cybercrime Solution (PCS) algorithmic Model as a basic awareness learning approach to end users and technology vendors.

On the other hand, the paper recommend the technical issue of the computer applications. Remember, in the cybercrime, one of the cyberspace components is the computer application or software. In this aspect, we recommend to integrate the computer application with the artificial intelligence (AI) to detect the cybersecurity attacks. The AI is fast grow technology and its integration with other existing or other technologies in the cybersecurity solution is required.

References

- Abroshan.H., Devos.J., Poels.G. and Laermans. E. (2018).Phishing Attacks Root Causes.
- Bhavsar.V., Kadlak.A. and Sharma,S. (2018).Study on Phishing Attacks. *International Journal of Computer Applications*, 182(33), 27-29.
- Broadhurst. R., Skinner.K., Sifniotis. N., Macias. B.M. and Ipsen.Y. (2020). Phishing and cybercrime risks in a university student community. Report to the Criminology Research Advisory Council Grant: CRG 51/16–17. Australian Institute of Criminology.
- Conley. C., Harwood. T., Dudley.T., Powers.E. and Johnson. S. (n.d). Reserved Bank of Atlanta.
- del Amo, I.F., Erkoyuncu, J.A., Roy, R., Palmarini, R. and Onoufriou, D. (2018). A systematic Review of Augmented Reality Content-Related Techniques for Knowledge Transfer in Maintenance Applications, *Comput. Ind.* 103 (2018) 47–71.
- Djenna, A., Barka, E., Benchikh, A. and Khadir, K. (2023). Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics. *Sensors*, 23, 6302. doi.10.3390/s23146302 (Djenna et al., 2023)
- Federal Investigation Agency (FIA). (n.d). Cyber Crime: Risk, Prevention and Legal Remedies, Guidelines for Cyber users. Ministry of Interior. Government of Pakistan.
- Goni. O, Ali, H., Showrov., Alam.M. and Shameem. A.(2023).The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, 1(2), 29–39.

doi./10.5281/zeno do .6499991

- Grant, M.J., Booth, A. (2009). A Typology of Reviews: An Analysis of 14 Review Types and Associated Methodologies, *Health Info. Libr. J.* 26 (2) (2009) 91–108, doi.org/10.1111/j.1471-1842.2009.00848.x.
- Hoseini.A .(2022). Ransomware and Phishing Cyberattacks: Analysing the Public's Perception of these Attacks in Sweden. *Department of Information Technology, Uppsala Universitet.*
- Kalakuntla, R., Vanamala, A.B. and Kolipyaka.R.R.(2019). Cyber Security. *Holistica*, Vol 10, Issue 2, 2019, Pp. 115-128. doi:10.2478/hjbpa-2019-0020.
- Li. Y. and Liu, Q. (2021). A comprehensive review Study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports* 7 (2021) 8176–8186.
- Malinauskaite, L., Cook, D., Davíðsdóttir, B., Ögmundardóttir, H., Roman, J. (2019). Ecosystem Services in the Arctic: A Thematic Review, *Ecosystem Service.* 36,100898, doi.org/10.1016/j.ecoser.2019.100898.
- Mengista, W., Soromessa, T. and Legese, G. (2020). Method for Conducting Systematic Literature Review and Meta-analysis for Environmental Science Research. *MethodsX*, 7, 100777. doi.org/10.1016/j.scitotenv.2019.134581
- Muntode, A.R. and Parwe. S.S(2019). An Overview on Phishing- its Types and Countermeasures. *International Journal of Engineering Research & Technology (IJERT)*, 8(12), 545-548.
- Nallaperumal, K.(2018).CyberSecurity Analytics to Combat Cyber Crimes. 2018 IEEE International Conference on Computational Intelligence and Computing Research. National Cyber Security Centre (NCSN). (2020). Phishing attacks. Crown. UK.
- Ollmann.G. (n.d).The Phishing Guide: Understanding & Preventing Phishing Attacks. *IBM Internet Security Systems.*
- Pande, J.(n.d). Introduction to Cyber Security. School of CS & IT, Uttarakhand Open University, Haldwani.
- Pandey, U.S., Kumar, V. and Singh, H.P. (2017). *Cyber Crimes and Laws*, 1st, Ed. Himalaya Publishing House. Mumbai, India.
- Perevochtchikova, M., De la Mora-De la Mora, G., J.Á Hernández Flores et al., (2019). Systematic Review of Integrated Studies on Functional and Thematic Ecosystem Services in Latin America, 1992–2017, *Ecosystem. Serv.* 36, 100900, doi.org/10.1016/j.ecoser.2019.100900
- Reddy, G.N and Reddy, G.J.U. (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. Chaitanya Bharathi Institute of Technology, Osmania University, Hyderabad., India
- Rupesh, K. and Rajasekhar, A.J. (2021). A Data Analytics Approach to the Cybercrime Underground Economy. *Journal of Engineering Science*, Vol 12, Issue 08, pp. 8-15. SANS institute. Springer International Publishing AG, part of Springer Nature 2018, N. Cuppens et al. (Eds.): CRiSIS 2017, LNCS 10694, pp.187–202. doi.org/10.1007/978-3-319-76687-4_13