Emerging Phishing Attack Trends: A South African Case Study

Jabu Mtsweni[1,2], Precious Maduma[1], Vhuthu Nefale[1], Alex Ramantswana[1], Mfundo Masango[1], and Muyowa Mutemwa[1(✉)]

[1] Council for Scientific and Industrial Research (CSIR), Information and Cyber Security Centre, Pretoria, South Africa
{pntuli1,vnefale,aramantswana,mmasango1,mmutemwa}@csir.co.za
[2] Military Academy, Stellenbosch University, Stellenbosch, South Africa

Abstract. Phishing is a common type of cyber-attack, that uses fraudulent emails or text messages to trick victims into revealing personal information that could further be used to commit actual cyber-crimes. Phishing attacks are prevalent in the cybersecurity space and are becoming complicated and varied as new technologies enter the market. As generative artificial intelligence platforms also become prevalent, we note that phishing attacks become even easier to craft. These attacks pose a real threat and challenge for businesses and individuals, particularly as digital transformation transcends into all spheres of our daily lives. Existing phishing or spam detection techniques do not always evolve as fast as the attack vectors emerge. Further, reporting of phishing emails or fraudulent text messages by users is not engrained in the business culture. The modus operandi of attackers before COVID-19 have changed with new phishing and smishing attack vectors emerging as the different technologies get adopted by users. The objective of this paper is to use phishing data collected from two anonymous South African organizations to technically examine the emerging phishing attack trends. We analyze and map the emerging phishing attacks using thematic analysis, payload analysis, and perceived objectives of the attack which include promoting spam emails, harvesting personal information, hacking into organizations' networks and so on. The paper contributes by developing technical and strategic guidelines on how phishing attacks could be mitigated through a cyber-resilience culture.

Keywords: Cybersecurity · Phishing · Smishing · Spam Emails · Email Security

1 Background and Introduction

1.1 Introduction

Emails are the most preferred mode of communication for businesses today. At the same time, 97% of companies are being targeted email-based phishing attacks [1]. According to Trend Micro, in one year (2020–2021), close to 700 million phishing attacks were detected in Africa with South Africa sharing a third of these attacks. The Interpol report

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 368–382, 2025.
https://doi.org/10.1007/978-3-031-81570-6_24

[2] released in 2021 indicates that the main cyberthreats in Africa are online scams perpetuated by fake emails or text messages that claim to be from legitimate sources and are used to siphon personal information from individuals to commit cyber-fraud. The same report also highlights that Business Email Compromise (BEC) are rife in Africa. These BEC attacks are quite common and are a serious threat to all organizations of any type [3].

Recent research suggest that these types of attacks have increased significantly during the COVID-19 pandemic and with the adoption of many technologies to enable remote work, these attacks are not abating [3], and over 90% of organizations are getting spoofed, meaning that some of the existing security solutions are not aiding in winning the battle.

Figure 1 depicts a Google trend on the topic of "phishing" in South Africa since 2018, which also indicates that phishing is on the upward trajectory (79% on 22 July 2023) compared to (27% on 18 August of 2018) in terms of search interest over time, and this represents a percentage increase of over 193% [4]. These stats were closely comparable with the world-wide picture, confirming that phishing attacks are a serious challenge across the board.

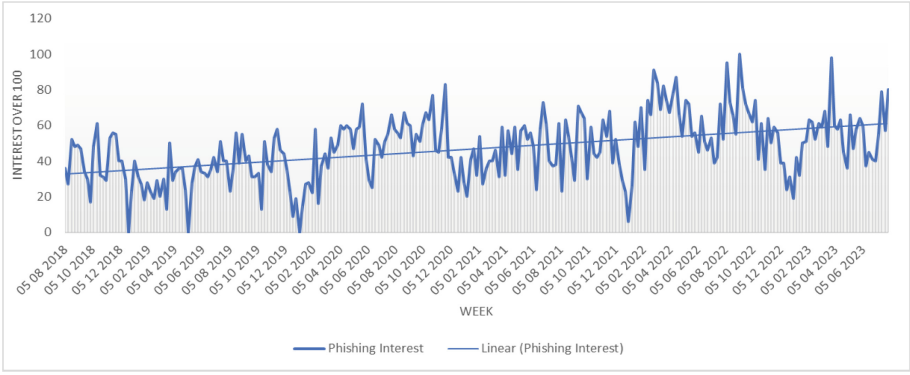

Fig. 1. Google search phishing trends over 5 years

What is also of note is that the types of phishing attacks have moved to text-messages on social media platforms such as WhatsApp, voice messages, as well as video content on social media platforms such as YouTube and TikTok. Of great concern is the maturity of Generative Artificial Intelligent (AI) tools that makes it simpler for anyone, even with no technical skills to generate fraudulent emails that are crafted in any language with limited grammatical and spelling errors, making them even more believable.

What is also evident is that there is a lack of investment in cybersecurity in Africa, but this is costing African countries billions of dollars every year according to [5].

1.2 Background

In this section, we provide background information on phishing and definitions of terminologies used in this research. In general, phishing attacks start with preparation,

followed by execution, and finally exploitation [6]. All these phases evolve as emerging techniques and technologies evolve.

Social Engineering. This is a general term that defines all cybersecurity attacks that rely on human interaction to trick the target into revealing sensitive information either through clicking on a link, opening a malicious email attachment, and/or freely giving information to unauthorized individuals. This type of attack makes humans ignore or forget any precautions before performing a computer related action. The purpose of such messages is to gain access, reveal sensitive information, execute malware, or cause damage to computer systems.

Phishing. This is a type of a social engineering attack that involves sending fraudulent emails or text messages that are meant to give the victim the assurance that they are from a legitimate source, such as a bank or credit card company.

Smishing. Is an attack that involves sending fraudulent text messages to a target with the same intention as phishing e-mails.

Vishing. This attack is different from phishing or smishing in that it uses voice or videos claiming to be an authorized pre-approved trusted person from a reputable and reliable organization (e.g., insurance company or bank) with the hope of tricking the intended victim into revealing sensitive information, such as passwords of pin codes.

Phishing attacks occur in a systematic and planned manner. In [6], a phishing taxonomy is proposed and is aligned to the emerging attack trends. This is shown in Fig. 2 below. Phishing occurs via a communication media, targeting a device of interest such as a mobile device using various techniques like e-mail spoofing. The taxonomy also shows the countermeasures against phishing attacks.

What is lacking in the taxonomy are the phishing intentions or objectives because they are not always common across different attacks. In this study, we attempt to address this aspect. What further makes circumventing phishing attacks difficult lies mostly in the design of the emailing system architecture, where an email can originate from any source using a myriad of tools and platforms and be transported to the destination via different intermediaries. At the same time, email can be transported via legitimate paths carrying payloads that may look innocuous, until obliviously activated by the target.

Figure 3 explains the process of email communication from the sender's email client to the recipient's email client through various email servers. Attackers can use email communications to spread malware by exploiting email security vulnerabilities.

Malware can be sent via email attachments, links or images and can infect one or more devices by spreading ransomware attacks, crashing victims' systems, providing hackers remote device access, steal victim's personal data, destroy files, or add victim's account malicious ad system [7]. Attackers also use phishing emails to trick victims into clicking malicious links or downloading malware-infected attachments.

1.3 Structure of the Paper

The rest of the paper is structured as follows: Sect. 2 discusses the research methodology adopted for this paper. In Sect. 3, the related research work is analyzed and synthesized

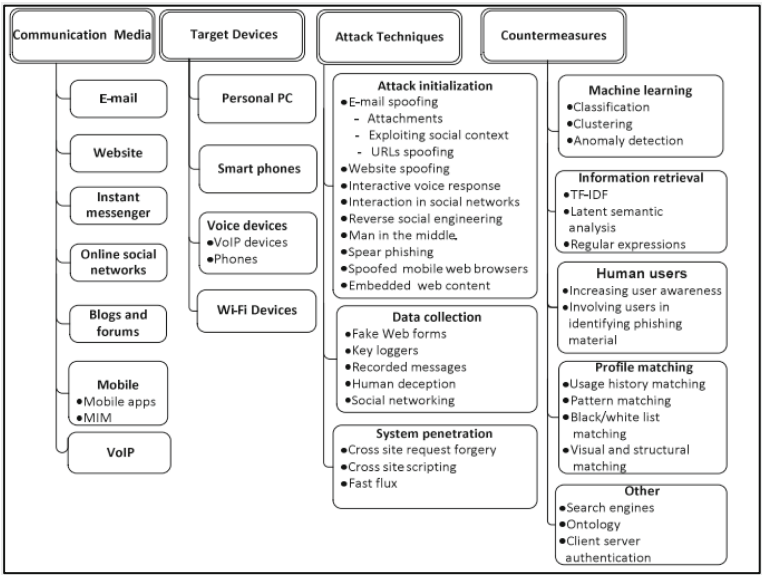

Fig. 2. Phishing attacks taxonomy [6]

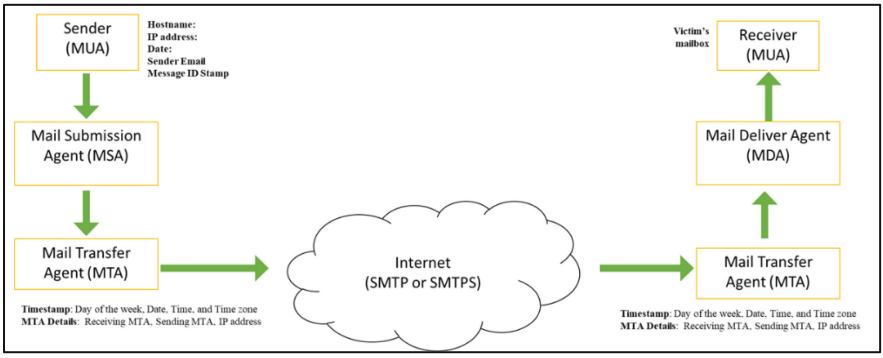

Fig. 3. Email communication system

in relation to our research objective. Section 4 details the data collection process and sampling followed in this study. Section 5 describes the payload attack analysis with selected examples, and Sect. 6 highlights the thematic analysis that provided the emerging phishing attack trends. Section 7 provides technical and strategic guidelines for mitigating phishing attacks, and the paper is concluded with a summary in Sect. 8.

2 Research Methodology

The research conducted for this paper followed a Design Science Research (DSR) approach [8]. The DSR was chosen because it is found to be suitable for research of this nature that deals with a technical subject covering the whole research lifecycle, including

clear problem identification. In addition, DSR tends to accommodate both quantitative and qualitative research methods and can be applied as a problem-driven and solution-driven research approach and can also allow researchers to end-up with different types of artefacts, such as tools, frameworks and/or processes.

This study adopts the research literature review as the first step in fully understanding the challenges in relation to phishing attacks in a general context. A case study approach [9] is adopted to specially focus the research on South Africa. A case study is a widely used approach in research and business for performing in-depth analysis of a subject, which for the purposes of this is a country (South Africa). And there has been several research studies relying on case studies to understand phishing, malware, and intrusion detection datasets.

The South African case study is chosen purely because of readily available (recent) data of phishing emails from two anonymous organizations in South Africa, which could be a challenge to source from other environments due to sensitivity and datedness of such data [10]. In addition, social media engagements on phishing were easily accessed and contextualized with a South African context.

In analyzing the phishing data (from email gateways), payload analysis techniques were employed to identify the patterns and relationships between the data sets at technical level. This was critical in understanding the phishing attack trends from the research data set. Payload analysis refers to technical and statistical techniques for analyzing the payload in events (e.g., phishing email). This technique is used in intrusion detection systems, spam-filters, anti-virus software, and other security tools [11]. Payload analysis may include investigating source of the email, IP (Internet Protocol) address locations, and links or attachments for malicious content. Identifying the features of the payload assists in understanding the objective of the phishing attack [10].

Using phishing data from social media and email-gateways, thematic analysis was also applied. Thematic analysis is qualitative-based and allows for manual identification of themes and patterns within data [12].

3 Related Work: Phishing Attacks

Prior studies have looked closely at attack vectors, social engineering strategies, and technical defenses in the context of phishing attacks. To shed light on the human-centered aspects of this common cybersecurity threat, this study seeks to delve deeper into the psychological factors influencing user susceptibility to phishing.

Phishing is an active research topic across the globe, with varying titles such as social engineering, phishing attacks, business email compromise, and spam. In the table below, we show a selected list of related works spread between 2010–2023. Our research complements these studies by providing a comprehensive analysis of phishing attacks using multiple sources of data (Table 1).

4 Data Collection and Sampling

This paper relied on data collected through “Phish Alert”, where users voluntarily report phishing emails at the organization and from an e-mail gateway detecting phishing emails. In total, over 600 phishing emails were collected from two large organizations in

Table 1. Summary of Related Work

Authors	Title	Year	Contribution
Williams, Hinds, & Johnson [13]	Exploring susceptibility to phishing in the workplace	2018	Authority, urgency, and context impact users' susceptibility to phishing
L'Huiller et al. [14]	Latent semantic analysis and keyword extraction for phishing classification	2010	Use of latent semantic analysis and text mining for characterization of phishing attacks
Pejic-Bach, Jajic, & Kamenjarska [15]	A Bibliometric analysis of phishing in the Big Data Era: high focus on algorithms and low focus on people	2023	Results indicate that real-time data collection and development of effective algorithms are essential in combating phishing attacks
Sharma & Bashir [16]	An analysis of phishing emails and how the human vulnerabilities are exploited	2020	Words used in emails are targeting users' emotional tendencies and triggers for phishing attacks
Burita, Matoulek, Halouzka & Kozak [17]	Analysis of phishing emails	2021	Contribute to the understanding of phishing emails, while adding to the knowledge base on education and training in phishing email defense
Parker & Flowerday [18]	Contributing factors to increased susceptibility to social media phishing attacks	2020	Identify the factors that contribute to an increased susceptibility to social media phishing attacks and propose a model to reduce this susceptibility

South Africa. After pre-processing the data, and removing obvious false positives, the final data for analysis had 587 e-mails.

In addition, phishing reports were collected from social media with the focus on South Africa. This data provides an overview of emerging phishing trends reported by the public on social media. A total of over 415 tweets using the keywords "phishing attacks" (*case insensitive and no-exact match) were collected between 23 June 2023 – 29 July 2023. The analysis is presented in Sect. 6.

5 Payload Attack Analysis

In this section, we highlight the payload attack analysis that was conducted to understand the emerging phishing and smishing attacks. This is done using a multi-prong approach and tools to analyze collected phishing emails. The emails are analyzed using tools such as emails header analyzer to determine origins of the email, path of the email, if it was detected by the existing email server that received it, and if it had any attachments or URLs and whether they were malicious or not, and if anti-virus tools were able to detect it or not.

The payload attack analysis is critical as it gives us insights into emerging techniques used by attackers, as well as payloads that are generally included in the emails and objectives of those payloads. The objective of the payload analysis is to also pick up weaknesses within email security specifically related to phishing and how these weaknesses can be mitigated.

5.1 Tools

The following tools were used for the payload analysis, and they are briefly described.

- **Email Header Analyzer**[1] – this tool was used to extract and analyze email header fields and values to give comprehensive insights on various elements such as source, email servers, network hops, and so on.
- **Whois** – this is the Internet record listing that identifies who owns a domain and IP address blocks.
- **AbuseIPDB**[2] – this is a service used to report and query IP addresses for abuse or other malicious activities.
- **VirusTotal**[3] – it is a Google service used to analyze suspicious files, domains, IPs, and URLs to detect malware and other breaches.
- **Browserling**[4] – we used this as an online browser sandbox that lets one securely open a website in an isolated environment.
- **Splunk SIEM** (Security Incidents and Events Monitoring) - in this context, this tool was used for data ingestion and visualization of phishing data.
- **EML Analyzer**[5] – this tool was used in combination with the Email Header Analyzer to extract email headers, domains, URLs, and attachments within an EML file. EML analyzer also automatically submits contents for relevant checks, for example, URLs are submitted to Virus Total, AbuseIPDB and others.

5.2 Payload Analysis

In this section, we discuss the findings of the analyses performed on the dataset of phishing emails. The summary of the email data points only from two (2) email gateways is tabulated in Table 2 below.

[1] https://www.gaijin.at/en/tools/e-mail-header-analyzer/.
[2] https://www.abuseipdb.com/.
[3] https://www.virustotal.com/.
[4] https://www.browserling.com/.
[5] https://eml-analyzer.herokuapp.com/.

It can be noted there were only 43% of unique email senders with all emails originating from 20 countries. Some of the emails came from the same source, however, targeting different recipients within the two organizations studied. This clearly indicates that spear phishing is also a common attack in many of the phishing emails in South Africa. The trend suggests that phishing emails in South Africa equally exploit both URLs (Uniform Resource Locator) and attachments as payloads.

Table 2. Table captions should be placed above the tables.

	Email Senders	Country of Origin	IP Addresses	URLs in Emails	Attachments in Emails
Totals	587	587	587	280	299
Unique	250	20	190	118	156
%	100%	100%	100%	48%	51%

Email Header Analysis. According to the analysis, 52% of the emails analyzed failed the SPF check. A sender policy framework (SPF) record is a type of DNS TXT record that lists all the servers authorized to send emails from a particular domain [19]. This implies that the email servers from which the phishing emails originated are not permitted to send emails on behalf of the domain. This can be seen as an indication that the domains have been spoofed.

Figure 4 depicts the distribution of the country of origin of the emails based on the sender's email address and message-id. The analysis indicated that 43% of the emails are sent through the United States of America (USA) with South Africa accounting for 32%. South Korea appeared 11% followed by Germany at 3%. From this analysis, it is evident that phishing attacks in South Africa originate from USA servers, and this is not surprising since most of the Internet Service Providers that were analyzed included Google, Microsoft Corporation, and Amazon Technologies, amongst others. All these organizations offer several different internet services that allow for hosting of phishing sites and replaying of emails.

The analysis further revealed at least 56% of the URLs found in 48% of the emails were detected as malicious. Furthermore, on average, only 3.6% of the anti-malware tools found in VirusTotal detected 56% of the URLs in selected e-mails as malicious. This is a concern as this means that if the phishing email gets to the user and the user can open the link, then a larger breach could happen. In addition, the analysis revealed that 57% of the e-mails had attachments. From the analysis, the top 3 identified file extensions that were attached to flagged emails are the Portable Document Format (PDF), which is the leading flagged file extension within the analyzed email data set, followed by docx, which is a Microsoft Word Open Extensible Markup Language (XML) format document file, and lastly zip, which is a file extension for a compressed archive file.

During the analysis of phishing email headers, it was noted that the "Reply-to" headers field are often not the same as the "From" header field. This is due to spoofing of domains and attackers wanting to get the response to the email instead of the email

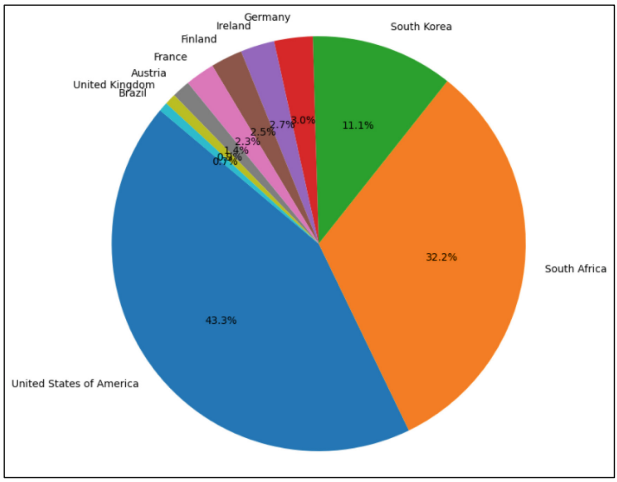

Fig. 4. Distribution of emails per country of origin

being sent to the spoofed email account. It was also noted that emails that pass the SPF alignment check (reply-to domain and from domain headers match) are due to attackers owning that domain, as registering a domain is quite simple.

Figure 5 depicts the top 10 Blocked URL Classifications that were sandboxed. A contrast can be drawn to indicate that most of the blocked URLs are firstly classified as *phishing* as they were requesting for user information or user credentials, the second classification is *dangerous file extension*, the attachments possibly had underlying code or an attached executable which was picked up during the sandboxing process. The third classification of the URLs is *malware*, which is described as a malicious program or code that is harmful to systems. The URLs could be redirected to download, install, or execute the malicious code or program once the user has clicked on the URL contained in e-mail.

The next section focuses on thematic analysis to describe the emerging phishing trends in South Africa using the message title in the email subject as well as content from the social media data.

6 Emerging Phishing Trends

Using the phishing data collected from various sources as well as data from social media collected over a 30-day period, this section discusses the trends of emerging phishing and smishing attacks.

Based on the thematic analysis as shown in Fig. 6, we observed that in South Africa, most of the phishing engagements on social media centers around *banking scams*, *flight bookings*, *smishing via SMS, cloned websites*, *stolen pin-codes, bogus holiday accommodation*, *impersonating attacks*, *ransomware attacks*, *hacked accounts*, *fake support online*, *cyber-crime, use of QR codes to circumvent anti-phishing tools* and many others. The smishing attacks using SMS/MMS consist of a combination of more than just a

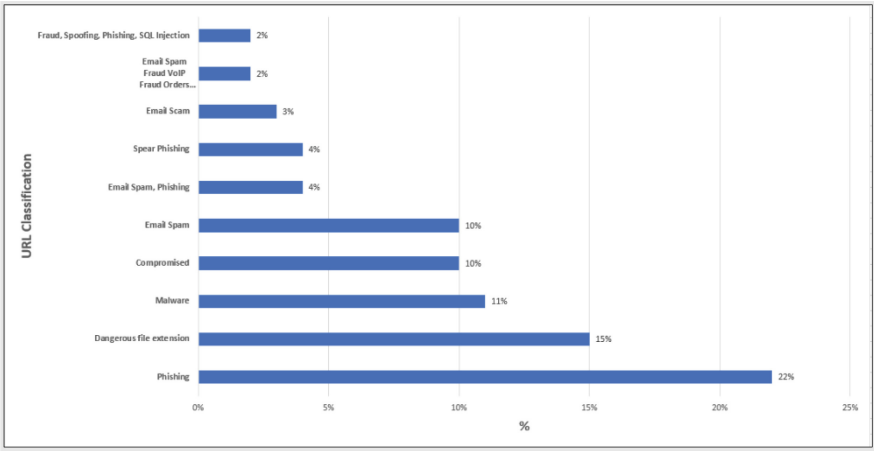

Fig. 5. Top 10 Block URL Classifications

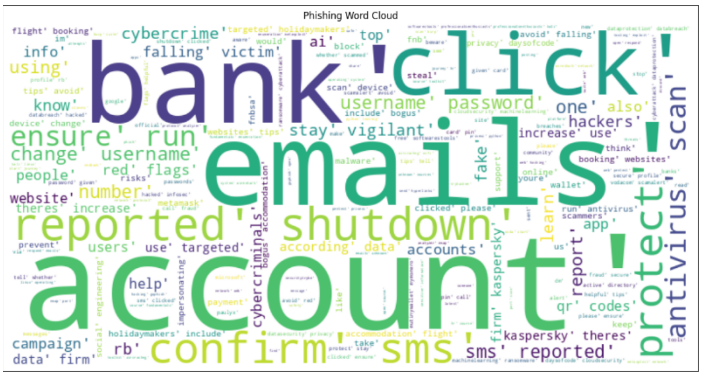

Fig. 6. Social media posts on phishing

malicious URL link that has a payload, this requires legitimizing the contents of the message and making it seem like an actual message from a reputable actor such as a financial or insurance institute.

Figure 7 depicts the common email subjects used by attackers to entice a user to viewing the email as a legitimate email. The email subjects can also be spoofed by an attacker based on information they gathered when doing reconnaissance in the organizations. Based on the analysis, the trends in South Africa suggest that most email subjects focus on the following subjects: *banking, insurance policies, credit cards, purchase orders, bank statements, request for quotations, echo sign signature requests, contract management, shipment, invoicing, payments, mobile rewards, billing, and reminders of different kinds.*

It is evident that phishing attacks tend to be well aligned with the operations of organizations studied. For instance, one organization part of the case study adopted the online signing of documents, and phishing attacks also adapted to this new way of work.

In addition, we have observed that the request for quotations, which when responded to gives away a lot of sensitive information, are used by hackers to extract personal and business information from users.

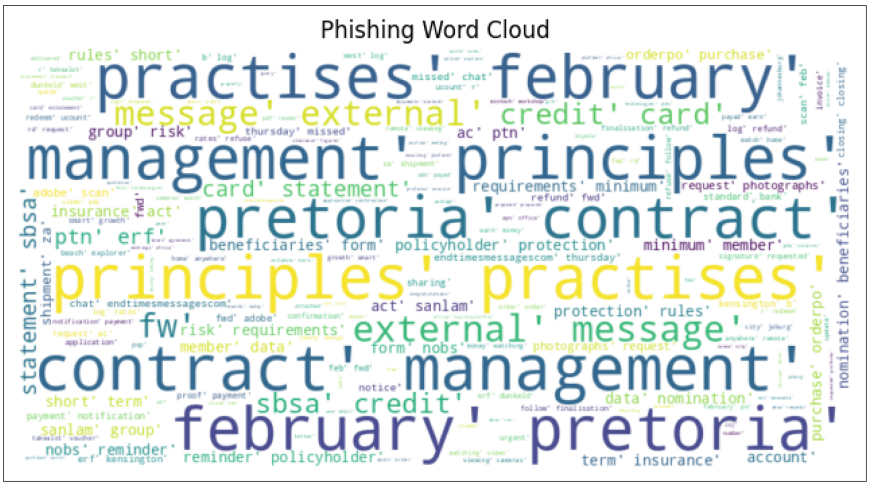

Fig. 7. Common email subjects

Based on the social media data, the analysis shows that raising awareness via social media on phishing is growing in South Africa. Figure 8 depicts the top 10 accounts that have tweeted regarding phishing. Based on the analysis, the South Africa Police Services are leading the engagements about phishing, followed by the South African Government and lastly within the telecommunications and banking sectors, Vodacom and Nedbank formed part of the list as the largest organizations in South Africa promoting anti-phishing campaigns. Additionally, we observed cybersecurity awareness campaigns against phishing by different institutions advising their users what to do and not do when using electronic services.

In this subsection, we also demonstrate that our analysis is aligned to what is already in literature. According to the literature, phishing attacks are indicated to be on the rise. And based on the literature, the following phishing trends are being observed at a global level. Some of these trends were observed in the analysis of the data collected for this research study.

- **Brandjacking.** This is a type of cyberattack in which an attacker impersonates a brand or company to trick victims into sharing personal information or downloading malware, and this can also be done either via email or social media [20].
- **URL Spoofing.** This is the type of attack in which an attacker creates a legitimate-looking phishing web address to trick users into clicking on it and visiting a malicious website. URL spoofing is often used in phishing attacks to trick users into revealing sensitive information or downloading malware.
- **Smishing.** This is a type of phishing attack performed on mobile text messages. And in our analysis of literature and collected data, it is evident that this is an emerging

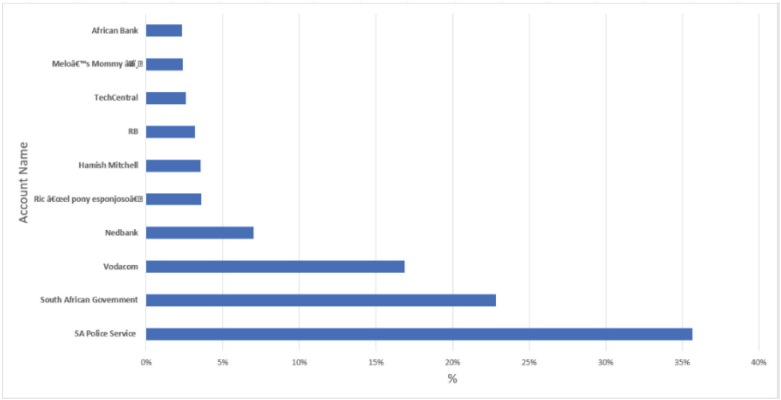

Fig. 8. Top 10 accounts with largest reach

trend, especially for mobile banking and mobile phone rewards targeting users of online banking and mobile phone users.

- **COVID-19 Spoofed Emails** [21]**.** Although, COVID-19 has mostly been tamed across the world, cybercriminals still attempt to impersonate government agencies, healthcare orgs, and financial institutions with the aim to steal personal or financial info or introduce malware into corporate networks.
- **E-mail Metadata Spoofing** [22]**.** Metadata Spoofing refers to an attack pattern in which an adversary changes a resource's metadata, such as a file, directory, or repository, to present a malicious resource as legitimate or trusted. The goal of a metadata spoofing attack is to trick the victim into believing that a malicious resource such as an email is from a trusted source. And this technique is also used to trick anti-phishing tools.

7 Technical and Strategic Guidelines

Email attackers have been introducing new attack vectors to run successful phishing campaigns. One aspect that the attackers focus on is the medium, which is the way the phishing attack is delivered, either through the internet, short message service (SMS)/multimedia messaging service (MMS) or voice. These attacks always have an associated to vector such as email, social networks, websites just to name a few.

This section proposes recommendations related to technical and strategic guidelines (see Fig. 9). To combat phishing and phishing attacks, effective countermeasures, such as cybersecurity awareness training and incorporating technologies to filter, block, or warn about emails or suspicious SMS, are needed. The authors of this paper therefore provide the recommendations summarized in Fig. 9 to minimize phishing attacks and their impact.

Domain-Based Message, Authentication, Reporting and Conformance (DMARC) Enablement. It is recommended that email users, especially enterprises consider enabling DMARC to counter spoofed emails [1]. DMARC authentication acts as a strong protection against phishing assaults and email fraud, fostering trust in email

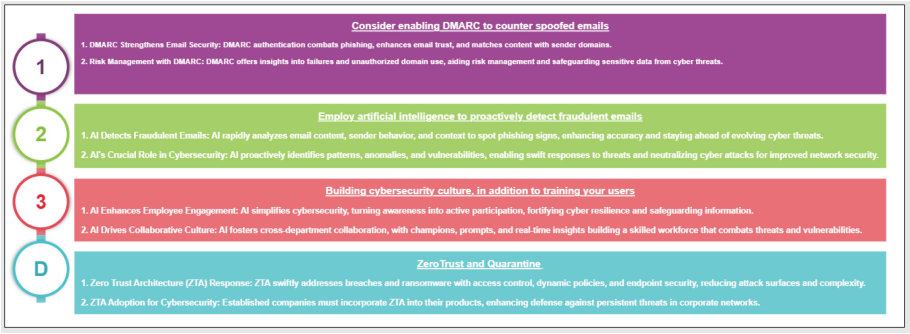

Fig. 9. Technical and strategic guidelines

communications, according to [1]. DMARC does this by matching email content with sender domains and by authenticating messages using cryptographic techniques. Additionally, DMARC offers organizations vital information to manage potential risks and unauthorized domain use through valuable insights into email authentication failures and enforcement actions. Adopting DMARC stands out as a crucial preventative action for protecting sensitive data and email integrity in the face of growing cyber threats.

Artificial Intelligence (AI) Employment. The second is to employ AI enabled security tools to proactively detect fraudulent emails. AI enabled security tools can detect subtle signs of phishing attempts by rapidly analyzing email content, sender behavior, and contextual cues using machine learning algorithms and pattern recognition techniques. This approach not only improves the accuracy of detecting malicious emails, but it also enables organizations to stay ahead of ever-changing cyber threats. Because of AI's ability to learn and adapt, the digital landscape gains a strong defense against fraudulent emails, protecting sensitive information, and improving overall email security.

Build a Cybersecurity Culture. The third recommendation is to build a cybersecurity culture, in addition to training email users. By simplifying difficult terminology and enabling employees and the cybersecurity team to move from awareness to actionable actions. It directs staff members toward particular security procedures, making cybersecurity an active element of daily operations as opposed to a passive idea. Employees become frontline defenders against threats because of this transition, which also strengthens the organization's cyber resilience. As a result, sensitive information and crucial systems are better secured, hence strengthening overall cybersecurity posture [23].

Zero Trust Architecture (ZTA) [24]. This strategic guideline focusses on the use of quarantine and sandboxing. Related to social engineering attacks, a proactive approach of preventing compromised user accounts from gaining access to organizational data and information or executing ransomware attacks is the ZTA. With this approach the aim is to verify the trust relationship of an account or asset before granting access. Assets that are not trusted can be quarantined. And in addition, attachments and URLs can have their trust status verified by sandbox environments. Making use of security technologies

that can execute or open attachments, and URL links in a sandboxed environment, could assist with malicious detections before the emails are delivered to users.

Lastly, organizations could take proactive measures to protect their brand by monitoring social media and online activity for signs of brandjacking and taking legal action against attackers when necessary [25].

8 Summary and Conclusion

The prevalence of email-based phishing attacks has become a significant issue, with over 97% of companies being targeted, particularly in Africa where cyber threats such as online scams and Business Email Compromise (BEC) have become rampant. The use of Generative AI tools has further exacerbated the problem by enabling the creation of sophisticated fraudulent emails. Despite the surge in phishing attacks, there remains a lack of investment in cybersecurity across the continent, resulting in substantial financial losses.

To combat these threats, this paper has demonstrated that in South Africa phishing attacks are continuing to be on the rise, new techniques are being used by the attackers taking advantage of daily operations of the organizations' studied. This paper suggests technical and strategic guidelines based on the payload and thematic analysis, and these include implementing DMARC, utilizing AI for detection, fostering a cybersecurity culture, and adopting a Zero Trust Architecture.

References

1. Mimecast: Cyber Risk Command the C-suite's focus: the state of email security 2023. Mimecast (2023)
2. Interpol: African Cyberthreat Assessment Report: Interpol's key insight into cybercrime in Africa. Interpol (2021)
3. Saud Al-Musib, M., Al-Serhani, F.M., Humayun, M., Jhanjhi, M.H.: Business email compromise (BEC) attacks. Mater. Today Proc. **81**(2), 89 (2023)
4. Google Trends: Google Trends: Phishing. Google, 31 July 2023. https://trends.google.com/trends/explore?date=today%205-y&geo=ZA&q=%2Fm%2F027b9k&hl=en-GB. Accessed 03 Aug 2023
5. IT-Online: Trend Micro tackles rising cybercrime in Africa. IT-Online, 30 June 2022. https://it-online.co.za/2022/06/30/trend-micro-tackles-rising-cybercrime-in-africa/. Accessed 06 Sept 2023
6. Aleroud, A., Zhou, L.: Phishing environments, techniques, and countermeasures: a survey. Comput. Secur. **68,** 160–196 (2017)
7. Proofpoint US: What Is Email Security? - Defining Security of Email, 23 July 2023. https://www.proofpoint.com/us/threat-reference/email-security. Accessed 20 Aug 2023
8. Weber, S., Beck, R., Gregory, R.: Combining design science and design research perspectives–findings of three prototyping projects. In: 45th Hawaii International Conference on System Science (HICSS) (2012)
9. Yin, R.: Case Study Research - Design and Methods, SAGE Publisher, Thousand Oaks (2009)
10. Verma, R., Zeng, V., Faridi, H.: Poster: data quality for security challenges: case studies of phishing, malware and intrusion detection datasets. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019 (2019)

11. Maestre, V., Sandovol, O.A., Garcia, V.L.: Alert correlation framework for malware detection by anomaly-based packet payload analysis. J. Netw. Comput. Appl. **97**, 11–22 (2017)
12. Joffe, H.: Thematic Analysis. Wiley, Hoboken (2011)
13. Williams, E., Hinds, J., Joinson, A.: Exploring susceptibility to phishing in the workplace. Int. J. Hum. Comput. Stud. **120**, 1–13 (2018)
14. L'Huillier, G., Hevia, A., Weber, R., Ríos, S.: Latent semantic analysis and keyword extraction for phishing classification. In: EEE International Conference on Intelligence and Security Informatics: Public Safety and Security (2010)
15. Pejić-Bach, M., Kamenjarska, T., Jajić, I.: A bibliometric analysis of phishing in the big data era: high focus on algorithms and low focus on people. Procedia Comput. Sci. **219**(1), 91–98 (2013)
16. Sharma, T., Bashir, M.: An analysis of phishing emails and how the human vulnerabilities are exploited. In: Advances in Human Factors in Cybersecurity: AHFE 2020 Virtual Conference on Human Factors in Cybersecurity, USA (2020)
17. Burita, L., Halouzka, P., Kozak, P.: Analysis of phishing emails. AIMS Electron. Electr. Eng. **5**(1), 93–116 (2021)
18. Parker, H.J., Flowerday, S.V.: Contributing factors to increased susceptibility to social media phishing attacks. South Afr. J. Inf. Manag. **22**(1), 1–10 (2020)
19. Görling, S.: An overview of the Sender Policy Framework (SPF) as an anti-phishing mechanism. Internet Res. **17**(2), 169–179 (2007)
20. Thakur, K., Hayajneh, T., Tseng, J.: Cyber security in social media: challenges and the way forward. IT Prof. **21**(2), 41–49 (2019)
21. Saleous, H., et al.: COVID-19 pandemic and the cyberthreat landscape: research challenges and opportunities. Digit. Commun. Netw. **9**(1), 211–222 (2023)
22. Jalda, C.S., Nanda, A.K., Pitchai, R.: Spoofing e-mail detection using stacking algorithm. In: 8th International Conference on Smart Structures and Systems (ICSSS) (2022)
23. Mwin, E.N., Mtsweni, J., Chimbo, B.: Conceptual mapping of the cybersecurity culture to human factor domain framework. In: Future of Information and Communication Conference, Switzerland (2023)
24. Pönkänen, P.: Zero trust guidelines for enterprises. JAMK Univ. Appl. Sci. (2023)
25. CISA: COVID-19 exploited by malicious cyber actors. CISA, 8 Apr 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-099a. Accessed 20 Aug 2023
26. Violino, B.: Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them, 23 February 2023