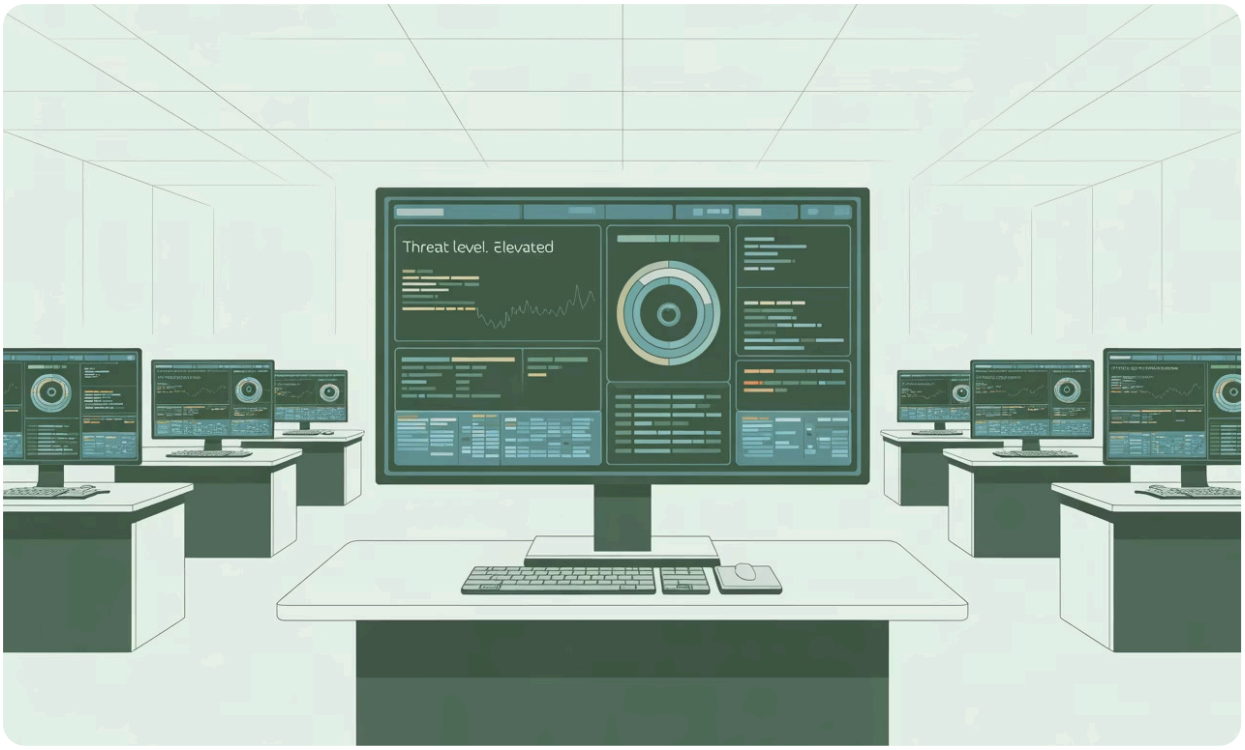
The Role of AI in Crafting Phishing Emails: A Nigerian Political Case Study

RESEARCH ARTICLE

***James Sesugh Iornumbe**
Department of Computer Science, Wesley University, Ondo
📧 james.iornumbe@wesleyuni.edu.ng

Adeleke Adeniyan
Department of Computer Science, Wesley University, Ondo

This article is part of a special issue titled Sustainability, innovation, and development: A Festschrift in honour of Rt. Rev. Prof. Obeka Samuel Sunday.



ABSTRACT

This study investigates the growing threat of AI-generated phishing attacks targeting Nigerian public officials, particularly in the context of rising digital communication within governance. Leveraging a quantitative research approach, 120 responses were analysed from a structured survey distributed across major government institutions. The study found high awareness of phishing among respondents (88.9%; $\chi^2 = 73.64$, $p < 0.001$) but moderate ability to detect AI-generated emails (44.4%; $\chi^2 = 25.36$, $p < 0.001$). Although 66.7% had received suspicious emails ($\chi^2 = 13.34$, $p < 0.001$), only 33.3% had formal training ($\chi^2 = 13.34$, $p < 0.001$). Institutional preparedness was weak, with limited reporting processes and reliance on basic spam filters ($\chi^2 = 106.69$, $p < 0.001$). These results reveal a significant gap between awareness and readiness, underscoring the need for training and AI-driven security measures. Common vulnerabilities include outdated spam filters, lack of reporting channels, and low usage of AI detection systems. The study concludes that Nigerian institutions must adopt proactive, AI-centric cybersecurity strategies to mitigate rising threats posed by generative phishing campaigns.

Research Method

Quantitative survey analysis with 120 responses from Nigerian government institutions

Key Finding

High phishing awareness (88.9%) but moderate AI-detection capability (44.4%)

Main Conclusion

Significant gap between awareness and institutional readiness for AI-generated threats

Keywords: Generative AI, phishing, cybersecurity, Nigerian government, email threats

INTRODUCTION

Phishing, a prevalent global cyber threat, accounted for over 36% of data breaches in 2023 (Verizon, 2023). It uses fraudulent messages to trick recipients into disclosing sensitive information or clicking malicious links. The emergence of generative AI tools like OpenAI's GPT-4 has significantly increased phishing sophistication, enabling AI systems to generate context-aware, grammatically accurate, and highly convincing messages that mimic official communication, making detection increasingly difficult.

Nigerian political figures are highly susceptible to spear phishing and whaling attacks, which use personalised data from social media, news, and public records to craft emails mimicking trusted colleagues or institutions. During an election year, such attacks could leak sensitive documents, discredit candidates, or manipulate voter sentiment. Nigeria's rapidly expanding digital economy, projected to approach USD 27 billion by 2030, has created new vulnerabilities as digital adoption outpaces cybersecurity capacity (Ris-Luamháin, 2025).

01

Traditional Phishing Era

Early phishing attempts featured poor grammar, generic messages, and low success rates before AI.

02

AI Revolution Period

Generative AI tools emerged, enabling sophisticated, context-aware phishing campaigns with higher success rates.

03

Current Threat Landscape

Nigeria faces coordinated AI-powered phishing targeting political figures and public officials with advanced social engineering.

Nigerian authorities have reported significant cyber incidents, and recent law enforcement actions indicate that phishing and fraud rings operate at scale. Microsoft and other agencies have disrupted phishing services tied to Nigerian actors. Nigeria's digital transformation, with increased reliance on email for interdepartmental communication, has exposed public officials to cyber threats. However, national cybersecurity strategies have yet to address specific AI-generated phishing threats. Local cybercriminals are increasingly adopting large language models to draft credible scam emails, often mimicking government tones and referencing current political issues.

Phishing schemes existed long before the internet, with reports dating back to the 19th century. However, large language models (LLMs) have transformed malicious operations by crafting messages that adapt to tone, emotion, and target online footprints. Research shows GPT-4 generated phishing emails achieve higher engagement and click-through rates than traditional messages. This is particularly concerning in politically sensitive environments like Nigeria, where government officials and political candidates are high-value targets due to their access to confidential data and influence over electoral processes.

Nigeria's Evolving Digital Landscape and Cyber Threats

Nigeria is undergoing a rapid digital transformation, characterised by increasing internet penetration, widespread adoption of digital services, and significant e-governance initiatives (NCC, 2022). While this digital evolution promises economic growth and improved public service delivery, it simultaneously broadens the attack surface for cyber adversaries. The nation's growing reliance on digital infrastructure, particularly for critical services and interdepartmental communications, creates fertile ground for sophisticated cyber attacks.

The rise of cybercrime in Nigeria is a significant concern, with various forms of online fraud, including phishing, consistently posing a threat to individuals and institutions. Economic and demographic factors, combined with a burgeoning tech-savvy population, contribute to the prevalence of cybercrime (Economic and Financial Crimes Commission, 2023). Organised phishing and fraud rings, some with international links, operate at scale, as evidenced by recent law enforcement actions and disruptions of phishing services tied to Nigerian actors.

Government digitisation efforts, such as the implementation of e-payment systems, digital identity programmes, and online public service portals, are pivotal for modern governance but inadvertently create new attack vectors. These initiatives, while designed to enhance efficiency and transparency, become prime targets for cybercriminals seeking to exploit vulnerabilities for financial gain or to compromise sensitive data (Federal Government of Nigeria, 2024). The unique geopolitical context and the high-value nature of data held by political figures and public officials further exacerbate these risks, making the development of robust, AI-aware cybersecurity strategies imperative for national security and public trust. Research indicates that Nigerian organisations are experiencing over 4,388 cyber attacks per week, highlighting the urgent need for enhanced cybersecurity measures (Chen, 2025).

Objectives:

1. To identify common techniques used by generative AI tools to enhance phishing attacks.
2. To assess the vulnerability of Nigerian government officials to AI-generated phishing.
3. To evaluate the effectiveness of existing cybersecurity systems in preventing AI-driven phishing.

Research Questions

1. How do generative AI tools enhance the creation of phishing emails?
2. What factors contribute to the vulnerability of Nigerian officials to AI-powered phishing?
3. How effective are existing cybersecurity measures in detecting and mitigating these threats?

Scope of the Study

This study examines AI-generated phishing targeting Nigerian political and public institutions. The study analyses techniques, vulnerabilities, and anti-phishing defences with reference to global trends.

Significance of Study

This study contributes to the understanding of how generative AI is transforming cyber threats in political contexts. For policymakers, it highlights the urgent need to update Nigeria's cybersecurity laws and practices. For cybersecurity professionals, it provides insights into emerging phishing trends and gaps in defence. Academically, the research fills a gap in empirical literature on AI-based phishing in the Global South, providing a foundation for further investigation into political cybersecurity. The study, therefore, examines how generative AI enhances phishing schemes targeting Nigerian government officials. While Global North research dominates, studies from Africa, Asia, and Latin America reveal distinct vulnerabilities such as mobile-based scams, election-related phishing, and financial fraud. By focusing on Nigeria, the study not only exposes local institutional weaknesses but also contributes to global cybersecurity debates by amplifying underrepresented Global South perspectives.

LITERATURE REVIEW

The increasing sophistication of cyberattacks, particularly phishing, is largely attributed to AI integration. Phishing has evolved from crude email scams to highly targeted, contextually tailored messages. Researchers note a sharp increase in AI-driven phishing sophistication and success rates since 2023 (Chen & Lee, 2024). AI-generated phishing emails reportedly achieve up to 54% success, compared to 12% for traditional human-generated attacks (CrowdStrike, 2025). Studies indicate limited AI adoption for cybersecurity in Africa, hindering effective AI-driven defence mechanisms (Nibigira et al., 2024). The Anti-Phishing Working Group (APWG, 2022) highlights the increasing complexity of phishing tactics. In Nigeria, spear phishing, smishing, vishing, and business email compromise, involving executive impersonation for fraudulent transactions, are common and contribute to significant cybersecurity challenges (Olagoke & Alimi, 2024).

Heiding et al. (2024) emphasised the effectiveness of spear-phishing, which targets specific individuals or organisations, yielding higher success rates than generic attempts by exploiting personal information from social media and public records. ML and AI advancements have further enabled adversaries to craft sophisticated phishing emails.

This literature review explores phishing definitions, generative AI's impact, key techniques, conceptual foundations, and empirical studies, focusing on Nigerian political institutions and public sector vulnerabilities.

Definition and Evolution of Phishing

Phishing is fraudulent communication, typically via email, designed to trick individuals into revealing sensitive information or compromising security. The European Union Agency for Cybersecurity (ENISA, 2023) defines it as social engineering that manipulates recipients through trust, urgency, or fear. Early phishing attempts were characterised by poor grammar, generic messages, and low success rates (Alabdan, 2020), but this has changed significantly with machine learning and AI-based text generation.

Generative AI

Generative AI, especially large language models like GPT-3 and GPT-4, has fundamentally altered malicious email campaigns. These models generate human-like text, mimicking target communication styles or organisational language. Comparative studies consistently show AI-generated phishing emails achieve significantly higher engagement rates than manually crafted ones (Miller & Davis, 2025). Studies reveal AI-generated emails are now almost indistinguishable from legitimate ones, leading to significantly higher response rates (Francia et al., 2024; Heiding et al., 2024).

AI-Enhanced Techniques

Spear phishing, whaling, clone phishing, and business email compromise using generative AI automation.

Social Engineering

Real-time manipulation of language to appeal to emotions like urgency, fear, and curiosity.

Nigerian Context

Political vulnerability through digital communication dependence and limited cybersecurity training.

Phishing Techniques Enhanced by AI

The integration of generative AI into phishing has not only improved grammatical quality but has also introduced a new level of personalisation. Common techniques now enhanced by AI include:

- Spear phishing targeting specific individuals using detailed information;
- Whaling aimed at high-profile individuals like government officials;
- Clone phishing duplicating legitimate emails with malicious alterations;
- Business Email Compromise impersonating executives for fund transfers or data theft.

Conceptual Framework: Generative AI as a Cyber Threat Tool

Generative AI's role in phishing can be understood through the lens of social engineering, automation, and digital mimicry. Heiding et al. (2024) argue that LLMs enable real-time manipulation of language to appeal to emotions like urgency, fear, or curiosity. This manipulation, combined with Natural Language Processing (NLP), allows attackers to deceive even cybersecurity-aware individuals.

Generative models can be trained to mimic the email structure of known senders, while Francia et al. (2024) show that these emails are often perceived as more trustworthy than those written by humans.

The capability of generative AI extends to creating complete phishing kits, including website cloning, credential theft, code obfuscation, and automated deployment.

Generative AI and Nigerian Political Vulnerability

Technical advancements in AI are improving rapidly and can be utilised by attackers, while human cognition and mental heuristics remain easily exploitable. Language models, a type of generative AI, allow attackers to create high-quality, human-like text in many different languages for almost no cost. Language model-powered AI assistants like ChatGPT have become commonplace in everyday activities worldwide.

Unique risks in the Nigerian context stem from public sector reliance on digital communication, limited cybersecurity training, and a politically charged environment, making government institutions attractive targets (Oluwole & Bello, 2022). This dependence, coupled with uneven cybersecurity training and a charged political climate, creates openings for phishing and disinformation, potentially disrupting election operations and eroding confidence in results (Adebayo, 2023). These weaknesses also enable account takeovers and payment diversion inside ministries and election bodies, fuelling narratives of incompetence or bias and undermining public trust in governance (Nigerian Cybersecurity Watch, 2021). Local cybersecurity agency reports indicate a rise in phishing attempts ahead of election cycles (CERT-NG, 2024). AI-generated phishing exacerbates this, as local language nuances and public data can be fed into models to enhance authenticity. The African cybersecurity landscape has witnessed a 442% increase in voice phishing attacks driven by AI-generated impersonation tactics (University of Maryland, 2025).

According to Verizon (2023), traditional government spam filters often lack training to detect AI-generated patterns, which differ significantly from previously known malicious signatures, rendering much existing infrastructure ineffective.

THEORETICAL REVIEW

To understand how generative AI transforms phishing, relevant theories explaining attacker behaviour and victim susceptibility must be explored. This section examines four key frameworks contextualising AI-powered phishing within psychological, behavioural, and criminological perspectives, particularly for the Nigerian public sector.

Social Engineering Theory

Social Engineering Theory postulates that attackers exploit human cognitive biases, trust, and emotional responses to manipulate victims into compromising security. Phishing is inherently a social engineering attack. Generative AI intensifies this by crafting messages appealing to emotions like urgency ("your account will be suspended") or authority ("from the office of the president"). Heiding et al. (2024) show that AI-generated phishing emails are more successful when mimicking organisational hierarchies or including political cues, aligning with social engineering principles.

Theory of Planned Behaviour (TPB)

The Theory of Planned Behaviour (Ajzen, 1991) explains how human behaviour is influenced by attitudes, subjective norms, and perceived behavioural control. In phishing, TPB helps understand why individuals fall for or ignore malicious emails. Applying behavioural models to cybersecurity, recent studies in African institutional contexts show that while general phishing awareness may be moderate, limited training and organisational cultures often do not prioritise digital literacy.

Technology Acceptance Model (TAM)

The Technology Acceptance Model (Davis, 1989) explains technology adoption through perceived usefulness and ease of use. TAM clarifies cybercriminals' AI adoption: these tools are accessible, require minimal coding, produce highly convincing content, and lower entry barriers for sophisticated attacks (e.g., Chen & Lee, 2022). Attackers leverage these principles for AI-powered phishing, as AI offers perceived usefulness (enhanced success) and ease of use (automated content generation) (Reynolds, 2025).

Routine Activity Theory (RAT)

Routine Activity Theory (Cohen and Felson, 1979) posits that crime occurs when a motivated offender and a suitable target converge in the absence of a capable guardian. In phishing, generative AI is the "motivated offender," Nigerian officials are "suitable targets," and weak email filters and a lack of real-time monitoring in many Nigerian public institutions represent absent "guardians."

The Theory of Planned Behaviour also informs cybercriminal behaviour, showing attackers' intentions to use AI tools are shaped by attitudes toward the technology, subjective norms within criminal communities, and perceived control over the tools' effectiveness.

Social Engineering

Exploits human cognitive biases and emotional responses. AI intensifies manipulation through organisational mimicry and political cues.

Planned Behaviour

Attitudes, norms, and control influence phishing susceptibility. Limited training reduces threat perception and detection ability.

Technology Acceptance

AI tool adoption by criminals driven by usefulness and ease of use. Low barriers enable sophisticated attacks by non-experts.

Routine Activity

Crime occurs with motivated offenders, suitable targets, and absent guardians. Nigeria's weak defences create ideal attack conditions.

EMPIRICAL REVIEW

Researchers have empirically examined the intersection of large language models (LLMs) and phishing attacks. LLMs' rapid improvement in creating realistic, coherent, and persuasive text makes them excellent phishing tools. This review incorporates global research alongside findings specific to Nigeria and other developing countries.

Global Empirical Evidence

Francia et al. (2024) experimentally compared AI-generated and human-written spear phishing messages. AI-generated content achieved a 54% click-through rate versus 38% for human-written emails, with most participants failing to distinguish them, confirming AI's persuasive capability.

Heiding et al. (2024) conducted simulated phishing attacks using GPT-4 on professionals, crafting emails to mimic internal communication. Conventional spam filters detected only 18%, underscoring current technologies' inability to identify syntactically and semantically correct AI-generated phishing content. Similarly, research by Okonkwo and Okonkwor (2025) documented the substantial surge in cyber-attacks on Nigerian financial institutions, with phishing representing a primary attack vector causing notable financial losses and operational disruptions.

Chen and Wu (2023) explored the psychological impact of AI-generated phishing. They found that messages tailored by generative AI exploited cognitive biases more effectively than human-crafted ones, leading to higher perceived credibility and elevated success rates in AI-powered social engineering campaigns.

Empirical Evidence in African and Nigerian Contexts

The Nigerian public sector faces significant cybersecurity challenges, lacking robust defences against evolving cyber threats. Public institutions often lack real-time monitoring tools, making them particularly vulnerable to sophisticated phishing campaigns. Cybersecurity assessments highlight the urgent need for enhanced security infrastructure and awareness programmes within government ministries, departments, and agencies.

A cybersecurity assessment by the National Information Technology Development Agency revealed that fewer than 30% of federal ministries, departments, and agencies had any form of AI-aware email filtering system. Most relied on outdated blacklists and could not detect newer, adaptive phishing formats.

Research Design

This study employed a quantitative research design to assess the awareness, exposure, and institutional response to AI-generated phishing attacks among Nigerian government officials. The quantitative approach enabled the collection of measurable and analysable data using structured questionnaires.

Population and Sample Size

The population comprised political office holders and key administrative staff working in public sector institutions across Nigeria. A sample of 120 respondents was selected through purposive sampling to reflect individuals with likely exposure to phishing attempts and organisational security protocols. This sample size was determined based on a statistical power analysis, aiming for a 95% confidence level and a 5% margin of error, to ensure robust and generalisable findings within the target population.

Instrument for Data Collection

A structured questionnaire, divided into four sections (general awareness, personal exposure, institutional preparedness, and cybersecurity infrastructure), was developed using Google Forms. The instrument featured closed-ended questions, Likert-scale items, and multiple-choice responses. A pilot test was conducted to refine the instrument, ensuring clarity and reliability.

Method of Data Collection

The questionnaires were distributed online and physically in government secretariats and ministries in Abuja (Federal Capital Territory) and Lagos State, targeting participants with direct or indirect experience in cybersecurity. Of the 130 questionnaires distributed, 120 were completed, yielding a 92.3% response rate. While the high response rate is commendable, the purposive sampling approach and potential hesitancy from some political office holders to participate in sensitive, security-related surveys may introduce a degree of selection bias, favouring respondents more amenable to discussing cybersecurity issues.

Method of Data Analysis

Responses were coded and analysed using descriptive statistics such as frequency counts, percentages, and mean scores. Key variables like phishing awareness, institutional preparedness, and tool effectiveness were analysed using SPSS. Charts and tables were used for visual representation. Inferential statistics, such as chi-square tests and correlation analysis, were used to determine significant relationships between respondent demographics and phishing awareness.

Validity and Reliability of the Instrument

To ensure validity, the questionnaire was reviewed by cybersecurity experts and academic professionals. Reliability testing using Cronbach's Alpha yielded a value of 0.84, confirming strong internal consistency among the questionnaire items.

Ethical Considerations

The research received ethical clearance from relevant institutional review boards. Respondents gave informed consent and were assured of anonymity and data confidentiality. No personal identifiers were recorded, and participation was voluntary.

Limitations of the Study

While the study achieved a high response rate (92.3% from 130 distributed questionnaires), potential non-response bias remains a consideration. The initial challenges and hesitations from some political office holders to participate may indicate that those who did respond were already more engaged with or aware of cybersecurity issues, potentially skewing the findings towards higher awareness and preparedness than what truly exists across the broader population of Nigerian government officials.

Geographically, the study was confined to government institutions within urban centres (Abuja and Lagos State). This significantly limits the generalisability of the findings to rural areas, where infrastructure, access to technology, and exposure to specific types of cyber threats, as well as levels of cybersecurity awareness and institutional capacity, may differ substantially. Future research should strive for broader geographical coverage to capture a more representative national perspective.

The reported hesitations from some political office holders also introduce a potential data validity concern. Officials in positions of power might be more inclined to provide socially desirable responses or underreport vulnerabilities due to perceived political or professional repercussions, even with assurances of anonymity. This could lead to an overestimation of preparedness or awareness within higher echelons of government.

Furthermore, the study's findings are inherently temporal, reflecting the situation during the specific data collection period. The dynamic nature of AI-generated phishing threats and evolving cybersecurity policies means that awareness and institutional responses can change rapidly. The timing of data collection relative to significant cybersecurity incidents, policy announcements, or political cycles could influence respondent perceptions and current practices, making long-term applicability subject to re-evaluation.

Finally, while purposive sampling aimed to include individuals with relevant exposure, the representativeness of the sample across various government levels and diverse departments may not be perfectly balanced. An uneven distribution could mean that the findings reflect the realities of certain governmental sectors more heavily than others, limiting a comprehensive understanding of the national landscape of AI-generated phishing defence.

In addition to these points, responses were self-reported, which inherently introduces the potential for social desirability bias and memory recall issues, thereby limiting the accuracy of reported behaviours and perceptions. Since no simulated phishing tests were used, actual behavioural susceptibility to AI-generated attacks remains unmeasured. Future research should combine surveys with experimental methods such as controlled or field-based phishing simulations to capture real-world responses and provide stronger evidence for designing more effective training programmes and robust institutional defences.

RESULTS

The research questions were divided into clear indices to aid respondents' comprehension. The results and discussion of each are shown below.

Table 1: Awareness of Phishing and AI-Generated Emails

Item	Yes (%)	No (%)	Maybe (%)	χ^2	df	p-value
Are you familiar with phishing emails?	88.9	11.1	—	73.64	1	<0.001
Can you distinguish between human- and AI-generated phishing emails?	44.4	44.4	11.1	25.36	2	<0.001
Aware of AI-generated phishing emails? (Scale 1–5)	Avg. 3.3	—	—	—	—	—
Believe AI tools have increased phishing threats?	66.7	11.1	22.2	62.46	2	<0.001

Source: Field Survey (2025)

The analysis revealed a very high level of awareness of phishing among respondents, with 88.9% indicating familiarity ($\chi^2 = 73.64$, $p < 0.001$). This aligns with global trends where phishing is widely recognised as a dominant cyber threat. However, the ability to distinguish between human- and AI-generated phishing emails was moderate (44.4% Yes, 44.4% No, 11.1% Maybe), with the Chi-square test confirming a significant imbalance ($\chi^2 = 25.36$, $p < 0.001$). This indicates that while officials recognise phishing generally, they struggle to identify the more sophisticated AI-driven variants. Furthermore, a majority (66.7%) indicated that AI has increased phishing threats ($\chi^2 = 62.46$, $p < 0.001$), underscoring growing concern about AI's role in amplifying cyber risks.

Table 2: Personal Exposure to Phishing (Frequency of Suspicious Emails)

Daily (%)	Weekly (%)	Monthly (%)	Rarely (%)	χ^2	df	p-value
22.2	22.2	11.1	44.4	27.86	3	<0.001

Two-thirds (66.7%) of respondents reported receiving phishing emails in the past year, a finding that was statistically significant ($\chi^2 = 13.34$, $p < 0.001$). This demonstrates the high prevalence of phishing targeting public sector employees. The frequency of suspicious emails varied, but the distribution was significantly skewed towards "rarely" (44.4%) compared to daily or weekly exposure ($\chi^2 = 27.86$, $p < 0.001$). Notably, the average convincing level of AI phishing emails was rated 4.1/5, suggesting that even infrequent attempts are highly deceptive and potentially successful.

AI Features Observed in Phishing Emails

Common features noticed:

i. Perfect grammar

ii. Mimicked internal department tone

iii. Personalised names/roles

iv. References to real government projects

Table 3: Institutional Readiness and Training

Item	Yes (%)	No (%)	Maybe (%)	χ^2	df	p-value
Trained to identify AI-phishing	33.3	66.7	—	13.34	1	<0.001
Confidence spotting AI-phishing (Scale 1–5)	Avg. 3.2	—	—	—	—	—
Clear phishing reporting process	33.3	44.4	22.2	8.46	2	<0.05

Table 3 reflects the low institutional preparedness, with only one-third of respondents (33.3%) had received training to identify AI phishing. This is a significant deviation from expected levels ($\chi^2 = 13.34$, $p < 0.001$). Confidence in spotting AI phishing was modest (avg. 3.2/5). The lack of structured reporting processes further compounds the issue: only 33.3% confirmed the existence of a clear reporting process, while 44.4% reported none and 22.2% were unsure ($\chi^2 = 8.46$, $p < 0.05$).

These results highlight institutional weaknesses in both prevention and response mechanisms, leaving organisations vulnerable to advanced phishing threats.

Institutional Vulnerabilities (Multiple Responses)

Commonly reported issues:

i. Lack of cybersecurity training (100%)

ii. Pressure to respond quickly (88.9%)

iii. Outdated email filters (66.7%)

iv. High-value targeting and publicly available info (44.4%)

Table 4: Email Security Systems and Effectiveness

Security System	Usage (%)	χ^2	df	p-value
Basic spam filters	77.8	106.69	2	<0.001
AI-driven detection	11.1			
Other	11.1			

Effectiveness Rating (Scale 1-5): Avg. 3.0

Table 4 shows that 77.8% of institutions rely on basic spam filters as their primary line of **defence**, with only 11.1% adopting AI-driven detection systems. The Chi-square test (χ^2 = 106.69, $p < 0.001$) indicates an overwhelming dependence on outdated or limited tools, which are inadequate against AI-generated phishing attacks. This reliance is particularly concerning given the sophistication of current phishing campaigns, which often bypass traditional spam filters. Security experts warn that traditional signature-based filters are increasingly ineffective against AI-generated attacks, which employ polymorphic methods and automated A/B testing to constantly evolve and bypass detection systems (Slavin, 2025).

Table 5: Reported Phishing Incidents

Item	Yes (%)	No (%)	Maybe (%)	χ^2	df	p-value
Institutions suffered phishing in past year	33.3	22.2	44.4	8.46	2	<0.05

Table 5 depicts that in the past year, 33.3% of institutions reported phishing incidents, while 22.2% denied such experiences and 44.4% were unsure ($\chi^2 = 8.46$, $p < 0.05$). The high proportion of uncertainty suggests weaknesses in monitoring and incident reporting systems, which may lead to underreporting and delayed responses.

Suggested Improvements include the following

i. Cybersecurity training (100%)

ii. AI-powered detection systems (88.9%)

iii. Dedicated cybersecurity team (66.7%)

iv. Mandatory reporting mechanisms (44.4%)

Interpretation of Findings

Analysis reveals high phishing awareness, but moderate ability to distinguish AI-generated attacks, coupled with low confidence and minimal formal training. Institutional mechanisms, such as reporting processes and advanced filtering tools, are lacking. These findings highlight a gap between awareness and preparedness, necessitating targeted interventions in Nigerian public institutions.

Summary of Findings

This study offers critical insights into Nigerian government officials' awareness, exposure, and institutional preparedness concerning phishing, especially AI-generated threats.

Respondents showed high phishing awareness (88.9% familiar, $\chi^2 = 73.64$, $p < 0.001$). However, distinguishing human- vs. AI-generated phishing emails was moderate (44.4% Yes, 44.4% No, 11.1% Maybe; $\chi^2 = 25.36$, $p < 0.001$), indicating difficulty with AI-driven variants. A majority (66.7%) believed AI increased phishing threats ($\chi^2 = 62.46$, $p < 0.001$), reflecting concern over AI's role in cyber risks.

Two-thirds (66.7%) of respondents reported receiving phishing emails in the past year ($\chi^2 = 13.34$, $p < 0.001$), showing high prevalence amongst public sector employees. Suspicious email frequency was skewed towards "rarely" (44.4%) ($\chi^2 = 27.86$, $p < 0.001$). Notably, AI phishing emails averaged 4.1/5 for convincingness, indicating high deceptiveness.

Institutional preparedness was critically low. Only one-third (33.3%) had received AI phishing training ($\chi^2 = 13.34$, $p < 0.001$), with modest confidence (avg. 3.2/5). A clear reporting process existed for only 33.3%; 44.4% reported none, and 22.2% were unsure ($\chi^2 = 8.46$, $p < 0.05$). These results underscore institutional weaknesses in prevention and response, leaving organisations vulnerable.

Institutions primarily rely on basic spam filters (77.8%), with only 11.1% using AI-driven detection systems. The Chi-squared test ($\chi^2 = 106.69$, $p < 0.001$) highlights an overwhelming dependence on outdated tools, inadequate against sophisticated AI-generated phishing attacks.

In the past year, 33.3% of institutions reported phishing incidents, 22.2% denied, and 44.4% were unsure ($\chi^2 = 8.46$, $p < 0.05$). This high uncertainty points to weak monitoring and reporting systems, potentially leading to underreporting and delayed responses. These findings align with broader African cybersecurity challenges, where the integration of AI into both attack and **defence** strategies remains a critical concern for continental security frameworks (Momoh, 2025).

CONCLUSION

The findings reveal a disconnect between growing exposure to AI-generated phishing and institutional readiness in Nigeria's public sector. The sophistication of these attacks, enhanced by AI's ability to craft realistic and persuasive messages, outpaces the **defence** mechanisms currently in place. General challenges exist in Nigerian cybersecurity, highlighting vulnerabilities. Bridging this gap requires targeted reforms of Nigeria's cybersecurity strategies, incorporating AI-specific awareness, detection tools, and responsive governance frameworks to protect sensitive systems and officials.

RECOMMENDATIONS

Based on the research findings, the following recommendations are proposed:

1. Cybersecurity Training: Introduce continuous training programmes focused on AI-generated phishing for all public officials. Research emphasises that traditional security awareness training must be enhanced to address AI-generated threats, as 67.4% of phishing attacks now utilise AI technologies (University of Maryland, 2025).

2. AI-Powered Detection Tools: Deploy machine learning-based anti-phishing systems in all public institutions.

3. Clear Reporting Channels: Establish and mandate phishing incident reporting procedures across ministries. This will help create auditable records of who reported what, when, and how the issue was handled, enabling oversight bodies to verify responses, spot systemic gaps, and ensure transparency

4. **Policy Reform:** Update the National Cybersecurity Strategy to include generative AI as a threat category.

5. Public-Private Partnerships: Encourage collaboration with tech firms and academia to develop adaptive detection models. Initiatives like the United States' National Cyber Forensics and Training Alliance (NCFTA), which fosters collaboration between government, private companies, and universities, have successfully co-developed threat intelligence and tools to combat cybercrime.

Resource Allocation: Invest in cybersecurity infrastructure and recruit dedicated threat response teams. Investments must be distributed so ministries, agencies, regulators, universities, and hospitals outside major cities receive the same as those in Abuja, Lagos, and Port Harcourt.

ACKNOWLEDGEMENT

Not Applicable

CONFLICTS OF INTEREST

The author declares no conflict of interest.

FUNDING

This research received no funding from any agency.

REFERENCES

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

Chen, Y. (2025). Cybersecurity in Nigeria: Emerging issues, domestic governance and international co-operation. World Journal of Advanced Research and Reviews, 26(2), 935-942.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588 - 608.

CrowdStrike. (2025). Global threat report 2025. CrowdStrike Inc.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319 - 340.

Francia, J., Hansen, D., Schooley, B., Taylor, M., Murray, S., & Snow, G. (2024). Assessing AI vs. human-authored spear phishing SMS attacks: An empirical study using the TRAPD method. *arXiv preprint arXiv:2406.13049*.

Heiding, F., Lermen, S., Kao, A., Schneier, B., & Vishwanath, A. (2024). Evaluating large language models' capability to launch fully automated spear phishing campaigns: Validated on human subjects. *arXiv preprint arXiv:2412.00586*.

Momoh, Z. (2025). Artificial intelligence and the challenges of cybersecurity in Africa: A critical examination. Global Network for Advancement of Integrity, Transparency and Accountability.

Nibigira, N., Havyarimana, V., & Xiao, Z. (2024). Artificial intelligence adoption for cybersecurity in Africa. Journal of Information Security, 15(2), 145-162.

Okonkwo, C. J., & Okonkwor, O. S. (2025). The impact of cyber-attacks on Nigerian banks and strategies for mitigation. International Journal of Science and Research Archive, 15(2), 758-761.

Reynolds, P. (2025). How AI-generated content is fuelling next-gen phishing and BEC attacks: Detection and defence strategies. Security Boulevard.

Ris-Luamháin, A. (2025, June 20). *The rising threat of AI-powered cybercrime in Nigeria.* Bloomsbury Institute for Security and Intelligence. **https://bisi.org.uk/reports/the-rising-threat-of-ai-powered-cybercrime-in-nigeria**

Slavin, B. (2025). AI-powered phishing in 2025: How intelligent attacks are outsmarting cybersecurity defences. DMARC Report.

University of Maryland. (2025). Cybersecurity Awareness Month: AI and Deepfakes. The Elm.

Verizon. (2023). *2023 Data Breach Investigations Report*.

ABOUT THE AUTHOR(S)

James Sesugh Iornumbe

Department of Computer Science, Wesley University, Ondo, Nigeria

📧 James.iornumbe@wesleyuni.edu.ng

Adeleke Adeniyan

Department of Computer Science, Wesley University, Ondo, Nigeria

Received: July 25, 2025

Accepted: August 28, 2025

Published: November 19, 2025

Citation:

Iornumbe J. S. & Adeniyan A. (2025). The Role of AI in Crafting Phishing Emails: A Nigerian Political Case Study. *SustainE, 3*(3), 684 - 703. In A. A. Atowoju, E. O. Oyekanmi, A. A. Akinsemolu, & D. M. Duyil (Eds.), *Sustainability, innovation, and development: A Festschrift in honour of Rt. Rev. Prof. Obeka Samuel Sunday* [Special issue]. https://doi.org/10.55366/suse.v3i3.33