E-ISSN: 1115 – 8492 P-ISSN: 3027 – 0693
MPRI-JNSAR | INTERNATIONAL JOURNAL OF NATURE AND SCIENCE ADVANCE RES.
VOL. 12 NO. 9 APRIL-2026

CYBERSECURITY AWARENESS AND PHISHING SUSCEPTIBILITY AMONG EMPLOYEES OF SMALL AND MEDIUM ENTERPRISES (SMEs) IN DELTA STATE, NIGERIA

BINITIE AMAKA PATIENCE; ONYEMENEM, SUNDAY INNOCENT; & OKOH KATE CHINWE

Federal College of Education (T), Asaba, Computer Science Department

Corresponding Author: philpat4ure@gmail.com

DOI: https://doi.org/10.70382/mejnsar.v12i9.093

Abstract

This study examines cybersecurity awareness and phishing susceptibility among employees of Small and Medium Enterprises (SMEs) in Delta State, Nigeria. The increasing reliance of SMEs on digital platforms for financial transactions, communication, and business operations has exposed them to rising cyber threats, particularly phishing attacks. Data were collected from 120 SME employees using a structured questionnaire titled Cybersecurity Awareness and Phishing Susceptibility Questionnaire (CAPSQ), employing purposive and snowball sampling techniques. Findings indicate that while employees demonstrate moderate cybersecurity awareness, susceptibility to phishing attacks remains high due to insufficient training, weak organizational cybersecurity structures, and limited workforce development. The study further shows that higher cybersecurity awareness significantly reduces phishing vulnerability. Respondents recommended regular training, improved cybersecurity policies, and adoption of technical safeguards such as email filtering systems. The study concludes that strengthening cybersecurity awareness and organizational preparedness is essential for reducing phishing risks in SMEs (Bada & Nurse, 2019; Ye, 2026).

Keywords: Cybersecurity awareness, phishing susceptibility, SMEs, Nigeria, human factors, cyber resilience.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Introduction

Small and Medium-sized Enterprises (SMEs) are increasingly operating within highly digitalized environments where business processes depend heavily on online platforms, cloud services, and electronic transactions. This digital transformation has significantly improved operational efficiency, market reach, and competitiveness; however, it has also exposed SMEs to a growing spectrum of cybersecurity threats. Cyberattacks such as phishing, social engineering, and tailored targeted attacks are particularly concerning because SMEs are often perceived as easy targets due to limited security infrastructure and weak defensive capabilities (Sharma et al., 2009; Burda et al., 2023).

Increasingly, cybercriminals exploit not only technical vulnerabilities but also human and organizational weaknesses within SMEs. For example, tailored phishing attacks are designed to deceive employees into revealing sensitive information by crafting highly personalized and convincing messages (Burda et al., 2023). In the same vein, social engineering techniques continue to pose serious risks by manipulating trust and behavioral tendencies within small business environments (Olaniyan & Ogunola, 2024). As a result, human factors have become central to understanding cybersecurity risks in SMEs.

Despite the rising frequency and sophistication of these attacks, many SMEs still lack adequate cybersecurity structures and formal security management systems. Existing literature shows that cybersecurity governance in SMEs is often informal, under-resourced, and inconsistently implemented, thereby exposing organizations to both known and emerging threats (Polkowski & Dysarz, 2017; Chidukwani et al., 2022). Additionally, while digital transformation and cloud adoption have improved business operations, they have also introduced new vulnerabilities that many SMEs are not sufficiently prepared to manage (Nagahawatta et al., 2021).

A critical challenge identified in the literature is the limited cybersecurity awareness among SME owners and employees, particularly in detecting phishing emails and other deceptive attacks. Empirical evidence indicates that SMEs often demonstrate low capability in identifying such threats, revealing significant gaps in awareness and preparedness (Yudhiyati et al., 2024). This situation is further compounded by human-centric vulnerabilities such as negligence, weak security practices, and inadequate training, which continue to represent the weakest link in SME cybersecurity defense systems (Ncubukezi, 2022; Jamil et al., 2025).

Furthermore, SMEs face persistent structural challenges including limited financial resources, shortage of skilled cybersecurity personnel, and inadequate access to affordable security solutions. These constraints hinder the effective implementation of

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

cybersecurity measures and often force SMEs into a reactive rather than proactive security posture (Jahankhani et al., 2022; Chidukwani et al., 2022). Consequently, their exposure to cyber risks continues to increase in an evolving threat landscape.

Given these challenges, there is a growing need for improved cybersecurity awareness, capacity building, and tailored defensive strategies that reflect the realities of SMEs. Strengthening employee awareness, enhancing organizational practices, and adopting cost-effective security solutions are essential for improving resilience against cyber threats (Binitie et al. 2025). Accordingly, this study examines cybersecurity awareness and preparedness among SMEs, with a focus on their ability to identify threats and implement appropriate protective measures.

Phishing remains one of the most persistent cyber threats affecting SMEs due to their limited cybersecurity infrastructure and low levels of employee awareness. SMEs are often considered soft targets because they lack structured cybersecurity frameworks, formal training programs, and dedicated security personnel (Tetteh, 2024; Awan & Alam, 2025). Research consistently shows that cybersecurity awareness is a key determinant of organizational resilience, particularly in resource-constrained environments where human error and inadequate training significantly increase exposure to cyber risks (Bada & Nurse, 2019; Eybers & Mvundla, 2021).

However, despite growing recognition of these threats, many SMEs still struggle to implement effective cybersecurity awareness programs due to financial constraints, weak workforce development structures, and limited organizational commitment. This challenge is further reinforced by inadequate cybersecurity capacity-building frameworks and insufficient investment in human capital development (Kezron, 2024; Ugbebor et al., 2024). Empirical evidence also suggests that SMEs in developing economies face heightened vulnerability due to weak institutional readiness and low cybersecurity awareness levels among employees (Moya et al., 2025; Abdulmalik et al., 2025).

Problem Statement

Despite increasing digital adoption, SMEs in Nigeria continue to experience rising incidents of phishing attacks, leading to financial losses, data breaches, and operational disruptions. A major contributing factor is the low level of cybersecurity awareness among employees, which limits their ability to identify and respond to phishing threats effectively. Although cybersecurity technologies exist, human and organizational factors such as inadequate training, weak policies, and low awareness remain significant vulnerabilities. Prior studies confirm that SMEs often lack structured cybersecurity awareness programs and workforce preparedness frameworks, making them highly susceptible to cybercrime (Bada & Nurse, 2019; Arroyabe et al., 2024). Furthermore, while awareness initiatives exist, their implementation is often inconsistent and under-

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

resourced, particularly within SME environments (Chaudhary et al., 2022; Khan et al., 2025). This creates a critical gap in understanding how employee cybersecurity awareness influences phishing susceptibility and overall organizational resilience in SMEs.

Aim of the Study

This study is aimed at examining cybersecurity awareness and phishing susceptibility among employees of SMEs in Delta State, Nigeria.

Objectives of the Study

1. To assess the level of cybersecurity awareness among SME employees in Delta State.
2. To determine employees' susceptibility to phishing attacks.
3. To examine the relationship between cybersecurity awareness and phishing susceptibility.
4. To identify strategies for improving cybersecurity awareness in SMEs.

Research Questions

1. What is the level of cybersecurity awareness among SME employees in Delta State?
2. How susceptible are SME employees to phishing attacks?
3. What is the relationship between cybersecurity awareness and phishing susceptibility?
4. What strategies can enhance cybersecurity awareness among SME employees?

Area of Study

The study was conducted in Delta State, Nigeria, a medium commercial hub characterized by a concentration of SMEs across retail, financial services, logistics, and technology-driven sectors. The high rate of digital adoption makes the state highly relevant for examining cybersecurity awareness and phishing susceptibility among employees (Anderson, 2026).

Population of Study

The population consists of employees working in Small and Medium Enterprises (SMEs) across Delta State. These employees regularly engage in digital communication, online transactions, and data handling activities, making them exposed to phishing and other cyber threats (Rawindaran et al., 2022).

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Sample and Sampling Technique

A total of 120 SME employees participated in the study. Purposive sampling was used to select employees who actively use digital tools in their work, while snowball sampling helped identify additional respondents through referrals. This approach ensured that participants had relevant exposure to cybersecurity risks within SME environments (Mamman & Ikharo, 2025). This sampling approach was appropriate given the targeted nature of the population, focusing on SME owners and managers with relevant knowledge of cybersecurity practices. It ensured that only informed respondents capable of providing reliable insights into cybersecurity awareness and organizational practices were included (Bada & Nurse, 2019; Eybers & Mvundla, 2021). Before full deployment, the questionnaire was pre-tested with a small group of SME respondents outside the study sample to ensure clarity and relevance. Ethical standards were strictly observed through informed consent, voluntary participation, anonymity, and confidentiality, with no personal identifiers collected (Chaudhary et al., 2022; Moya et al., 2025).

Data Collection Method

Data were collected using a structured online questionnaire titled: Cybersecurity Awareness and Phishing Susceptibility Questionnaire (CAPSQ). The instrument contained sections on cybersecurity awareness, phishing exposure, susceptibility levels, and preventive strategies. It was distributed via WhatsApp and email to ensure wide accessibility.

Results and Discussion

This section presents the empirical findings of the study based on responses from SME owners and managers. Descriptive statistics, including mean scores and standard deviations, were used to address the research questions. All questionnaire items were measured on a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). A cut-off mean score of 3.50 was adopted to determine agreement levels. Items with mean scores of 3.50 and above were regarded as accepted, while those below 3.50 were considered rejected, ensuring that only strong levels of agreement were interpreted as significant.

Research Question 1

To examine the level of cybersecurity awareness among respondents, particularly in relation to phishing detection and basic security practices, the mean scores and standard deviations of their responses were analyzed. The results are presented in Table 1, which summarizes respondents' awareness of phishing attacks, ability to identify suspicious

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

links, exposure to cybersecurity training, understanding of password security, and the existence of organizational cybersecurity guidelines.

Table 1: Cybersecurity Awareness Among SME Employees

S/N	Items	Mean	SD
1	Awareness of phishing attacks	3.80	0.81
2	Ability to identify suspicious links	3.56	0.90
3	Receipt of cybersecurity training	2.92	0.96
4	Understanding of password security	3.70	0.85
5	Organizational cybersecurity guidelines exist	3.25	0.92

The results indicate moderate cybersecurity awareness among SME employees. However, formal training and institutional support remain insufficient. This aligns with findings that emphasize the importance of structured cybersecurity awareness programs in SMEs (Bada & Nurse, 2019; Ugbebor et al., 2024).

Research Question 2

To examine the susceptibility of respondents to phishing attacks, the mean scores and standard deviations of their responses were analyzed. The results are presented in Table 2, which summarizes respondents' behaviors and perceptions regarding clicking suspicious links, difficulty in identifying phishing emails, unintentional sharing of sensitive information, perceived difficulty in detecting phishing emails, and verification practices before responding to suspicious messages.

Table 2: Phishing Susceptibility Among Employees

S/N	Items	Mean	SD
1	Clicking suspicious links	3.40	0.94
2	Difficulty identifying phishing emails	3.65	0.88
3	Sharing sensitive information unknowingly	3.20	1.01
4	Phishing emails are hard to detect	3.76	0.83
5	Verification before responding	3.45	0.89

Findings show moderate to high susceptibility to phishing attacks among SME employees. This reflects broader concerns that human vulnerability remains a key weakness in SME cybersecurity defenses (Arroyabe et al., 2024; Awan & Alam, 2025).

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Research Question 3

To determine the overall level of cybersecurity awareness and phishing susceptibility among respondents, the mean scores and corresponding interpretations were analyzed. The results are presented in Table 3, which summarizes the aggregate mean values for cybersecurity awareness and phishing susceptibility, indicating their respective levels of awareness and vulnerability among respondents.

Table 3: Relationship Between Awareness and Susceptibility

Variable	Mean	Interpretation
Cybersecurity Awareness	3.45	Moderate
Phishing Susceptibility	3.49	High

The findings suggest that higher cybersecurity awareness is associated with lower susceptibility to phishing attacks, reinforcing the importance of awareness training and workforce development (Kezron, 2024; Ye, 2026).

Research Question 4

To examine the effectiveness of cybersecurity measures implemented within SMEs, the mean scores and standard deviations of respondents' views were analyzed. The results are presented in Table 4, which summarizes responses on regular cybersecurity training programs, email filtering systems, the existence of strong cybersecurity policies, workforce development initiatives, and employee awareness campaigns.

Table 4: Strategies for Improving Cybersecurity Awareness

S/N	Items	Mean	SD
1	Regular cybersecurity training programs	4.38	0.70
2	Implementation of email filtering systems	4.22	0.75
3	Strong cybersecurity policies in SMEs	4.15	0.79
4	Workforce cybersecurity development programs	4.10	0.81
5	Employee awareness campaigns	4.33	0.73

Respondents strongly support structured training, workforce development, and organizational policy strengthening. This is consistent with literature emphasizing awareness programs and human-centered cybersecurity strategies in SMEs (Bada & Nurse, 2019; Chaudhary et al., 2022).

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Discussion of Findings

The findings of this study indicate that cybersecurity awareness among SME operators is generally moderate but insufficient to fully mitigate emerging cyber threats. Respondents demonstrated awareness of basic security practices such as password protection and device security; however, deeper understanding of advanced threats such as phishing, ransomware, and social engineering remains limited. This aligns with previous studies which report that SMEs often possess surface-level cybersecurity knowledge but lack comprehensive awareness required for effective defense against evolving cyber risks (Bada & Nurse, 2019; Tetteh, 2024).

The study further reveals that many SMEs rely heavily on informal or reactive cybersecurity practices rather than structured security frameworks. This suggests the absence of formal cybersecurity policies and training programs in most organizations surveyed. Similar findings have been reported, where SMEs are shown to prioritize business operations over cybersecurity investment, often due to cost constraints and limited technical expertise (Awan & Alam, 2025; Ye, 2026).

Another key finding is the significant role of employee behavior in shaping cybersecurity outcomes. Human error, weak password practices, and poor awareness of phishing attempts were identified as major vulnerabilities. This supports existing literature emphasizing that human and organizational factors remain the weakest link in SME cybersecurity defense systems (Moya et al., 2025; Ugbebor et al., 2024). It further highlights the need for continuous employee training and awareness programs.

The study also shows that cybersecurity training and awareness programs are either irregular or completely absent in many SMEs. Where training exists, it is often not tailored to the SME context, limiting its effectiveness. This corroborates findings that structured and context-specific awareness programs significantly improve cybersecurity resilience in small business environments (Chaudhary et al., 2022; Eybers & Mvundla, 2021).

Furthermore, financial and technical constraints were identified as major barriers to adopting robust cybersecurity measures. Many SMEs reported difficulty in accessing affordable cybersecurity tools and skilled personnel. This is consistent with research indicating that SMEs often struggle to balance cybersecurity investment with operational costs, leaving them exposed to increasing cyber threats (Anderson, 2026; Kezron, 2024).

The results generally suggest that while awareness exists at a basic level, it does not translate into strong cybersecurity practice within SMEs. The gap between knowledge and implementation remains significant, highlighting the need for improved policy support, affordable security solutions, and targeted awareness programs. Strengthening these areas is essential for improving SME resilience against cyberattacks in an increasingly digital business environment (Abdulmalik et al., 2025; Rawindaran et al., 2022).

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Conclusion

This study concludes that cybersecurity awareness among SMEs is generally limited to basic knowledge, which is not sufficient to ensure effective protection against evolving cyber threats. While respondents demonstrated some understanding of common risks, there remains a significant gap between awareness and actual cybersecurity practice, particularly in the adoption of structured policies, preventive measures, and advanced threat recognition. The findings also highlight those human factors, such as employee negligence, weak password practices, and inadequate training, significantly contribute to cybersecurity vulnerabilities within SMEs, reinforcing the view that cybersecurity is both a technical and behavioral issue. Furthermore, financial limitations, lack of technical expertise, and inadequate access to affordable security solutions continue to hinder effective cybersecurity implementation in many SMEs, leading to a largely reactive rather than proactive security approach. Overall, the study concludes that strengthening SME cybersecurity resilience requires continuous awareness programs, improved employee training, affordable security tools, and supportive policy interventions to bridge the gap between knowledge and practice and enhance long-term business security and sustainability.

Recommendations

1. SMEs should implement continuous cybersecurity awareness training programs.
2. Organizations should adopt email filtering and authentication technologies.
3. Structured cybersecurity policies should be developed and enforced across SMEs.
4. Workforce cybersecurity development programs should be introduced
5. Regular awareness campaigns should be conducted to reinforce safe digital practices

References

Abdulmalik, A., Mohammed, U., & Bello, F. H. (2025). Bridging the cybersecurity gap in Nigerian SMEs: An empirical study of awareness and practice. *International Journal of Cybersecurity and Management Technology, 11*(5), 93–101.

Anderson, P. (2026). Cybersecurity risks and solutions for digitally growing SMEs. *International Journal of Computer Science and Engineering Innovations, 2*(1), 10–16.

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security, 141*, 103826.

Awan, M., & Alam, A. (2025). Cybersecurity threats and defensive strategies for small and medium firms: A systematic mapping study. *Administrative Sciences, 15*(12), 481.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3), 393–410.

Binitie, A. P., Onyemenem, I. S., & Okoh, J. F. (2025). Enhancing Security and Privacy in EdTech Tools: Safeguarding Student Data in the Digital Learning Era. *Journal of Science Innovation and Technology Research*.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Burda, P., Altawekji, A. M., Allodi, L., & Zannone, N. (2023, July). The peculiar case of tailored phishing against SMEs: Detection and collective defense mechanisms at a small IT company. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 232–243). IEEE.

Chaudhary, S., Gkioulos, V., & Goodman, D. (2022, September). Cybersecurity awareness for small and medium-sized enterprises (SMEs): Availability and scope of free and inexpensive awareness resources. In *European Symposium on Research in Computer Security* (pp. 97–115). Springer.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access, 10*, 85701–85719.

Eybers, S., & Mvundla, Z. (2021, June). Investigating cybersecurity awareness (CSA) amongst managers in small and medium enterprises (SMEs). In *International Conference on Comprehensible Science* (pp. 180–191). Springer.

Jahankhani, H., Meda, L. N., & Samadi, M. (2022). Cybersecurity challenges in small and medium enterprise (SMEs). In *Blockchain and other emerging technologies for digital business strategies* (pp. 1–19). Springer.

Jamil, H., Zia, T., Nayeem, T., Whitty, M. T., & D'Alessandro, S. (2025). Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. *Information & Computer Security, 33*(1), 49–76.

Kezron, I. E. (2024). Enhancing cybersecurity capacity in small and medium enterprises: A framework for workforce development. *Iconic Research and Engineering Journals, 7*(10), 421–428.

Khan, N., Furnell, S., Bada, M., Rand, M., & Nurse, J. R. (2025). Investigating the experiences of providing cyber security support to small- and medium-sized enterprises. *Computers & Security, 154*, 104448.

Mamman, H. I., & Ikharo, A. B. (2025). Effectiveness and promotion of cybersecurity awareness among small and micro-medium sized enterprises (SMEs) and consumers survival in Kogi State. *Journal of Pure and Applied Sciences (Science Forum), 25*(4).

Moya, L. P., Giraldo, M. C. B., Lozano, J. A. A., Arias, A. V., & Rodríguez-Correa, P. A. (2025). Human and organisational factors influencing the preparedness of small and medium-sized enterprises against cyber attacks in developing countries. *Journal of Telecommunications and the Digital Economy, 13*(3), 30–70.

Nagahawatta, R., Lokuge, S., Warren, M., & Salzman, S. (2021). Cybersecurity issues and practices in a cloud context: A comparison amongst micro, small and medium enterprises. *arXiv preprint arXiv:2111.05993*.

Ncubukezi, T. (2022, March). Human errors: A cybersecurity concern and the weakest link to small businesses. In *Proceedings of the 17th International Conference on Information Warfare and Security* (p. 395). Academic Conferences International Limited.

Olaniyan, J., & Ogunola, A. A. (2024). Protecting small businesses from social engineering attacks in the digital era. *World Journal of Advanced Research and Reviews, 24*, 834–853.

Polkowski, Z., & Dysarz, J. (2017). IT security management in small and medium enterprises. *Scientific Bulletin–Economic Sciences, 16*(3).

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the impact of cybersecurity awareness on small and medium enterprises (SMEs) in Wales using intelligent software to combat cybercrime. *Computers, 11*(12), 174.

Sharma, K., Singh, A., & Sharma, V. P. (2009). SMEs and cybersecurity threats in e-commerce. *EDPACS: The EDP Audit, Control, and Security Newsletter, 39*(5–6), 1–49.

Tetteh, A. K. (2024). Cybersecurity needs for SMEs. *Issues in Information Systems, 25*(1).

Ugbebor, F., Aina, O., Abass, M., & Kushanu, D. (2024). Employee cybersecurity awareness training programs customized for SME contexts to reduce human-error related security incidents. *Journal of Knowledge Learning and Science Technology, 3*(3), 382–409.

Ye, W. (2026). Strengthening cybersecurity in small and medium-sized enterprises: Balancing technology, costs, compliance, and employee awareness. *Sage Open, 16*(1), 21582440251414951.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Yudhiyati, R., Rahmawati, D., & Putritama, A. (2024). Indonesian SMEs and cybersecurity: Developing instrument to test SMEs owners' capability in detecting phishing emails. *Riset Akuntansi dan Keuangan Indonesia, 9*(3), 318–337.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]