International Journal of Criminology & Justice (IJCJ)

VOLUME 1 ISSUE 1 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

International Journal of Criminology & Justice (IJCJ)

Volume 1 Issue 1, Year 2025
https://journals.e-palli.com/home/index.php/ijcj

Malware, Data Theft and Emotional Distress as Risk Factors of Phishing in Nigeria

Lateef Junior Adeyemo[1*], Isaiah Oden David[1], Tirimisiyu Yemi Olabulo[1]

Article Information

Received: April 07, 2025

Accepted: May 06, 2025

Published: September 16, 2025

Keywords

Cybersecurity, Data Theft, Emotional Distress, Phishing Attacks, Social Media

ABSTRACT

This study investigates malware, data theft, and emotional distress as risk factors contributing to phishing vulnerability among Nigerian internet users. Data were collected from 2,016 participants through purposive and convenience sampling, using a quantitative cross-sectional survey design. The analyses focused on platform exposure, behavioural patterns, and sociodemographic predictors of emotional reactions to phishing incidents. Findings revealed that phishing threats vary across social media, with Instagram, Twitter, and Facebook being most affected. Emotional distress is highest when users experience real consequences, while overconfidence and exposure fatigue reduce vigilance. Sociodemographic factors such as age, gender, education, and occupation significantly predict emotional reactions to attacks. It is therefore recommended that phishing prevention in Nigeria requires joint efforts from various agencies, associations, and the Ministry of Health to implement cybersecurity education, block threats in real time, train self-employed users, provide emotional support, and involve technology companies in user protection through reporting systems, safety tools, and targeted awareness initiatives.

INTRODUCTION

Phishing has emerged as a global dominant and evolving cyber threat, characterised by deceptive digital communication designed to extract sensitive information or deliver malicious software. Eliot and Maxime (2025) report that 64% of organisations experienced Business Email Compromise (BEC) attacks in 2024, while 80%–95% of all cyberattacks originated from phishing attempts. Approximately 80% of phishing campaigns are intended to steal user credentials, and nearly 80% of phishing websites now use HTTPS, making them appear secure and more difficult for users to detect. The attack surface has also expanded, with 40% of phishing campaigns now targeting platforms like Slack, Microsoft Teams, and social media, beyond traditional email channels. Phishing emails impersonating tax agencies such as the IRS or global counterparts have increased by 35%, and brand impersonation remains widespread, with over 44,750 phishing domains reported to have used Facebook's name to deceive users. The availability of phishing kits on the dark web has grown by 50%, enabling less-skilled actors to carry out advanced schemes. These developments have coincided with a 4,151% surge in phishing attacks since the public release of ChatGPT in 2022, reflecting the rapid evolution of phishing tactics. Furthermore, 68% of data breaches now involve the human element, and the average cost of a phishing-related breach is estimated at $4.88 million. These attacks typically combine social engineering with technical tools, such as malware, to exploit system vulnerabilities and user behaviour. The increasing sophistication of phishing now extends beyond technical manipulation to include psychological and emotional exploitation, often targeting users with limited awareness or emotional resilience.

In Africa, this challenge is intensified by the continent's rapid digital growth outpacing cybersecurity readiness. The 2021 INTERPOL Cybercrime Assessment reported an estimated 500 million internet users across Africa, only 38% of the population and highlighting significant potential for further expansion. The report identified phishing, including online scams like fake emails, messages, and BEC, as one of the most prevalent cyber threats, attributing this to weak regulatory frameworks, low public awareness, and heavy reliance on mobile technology (INTERPOL, 2021). Social media platforms and messaging applications, widely used for both personal and commercial communication, have become common entry points for phishing actors seeking to exploit behavioural and emotional vulnerabilities among unprotected users.

Nigeria presents a particularly urgent case within this continental context. As of January 2023, the country had over 122.5 million internet users and 36.6 million active social media accounts, placing it among Africa's most digitally connected populations (DataReportal, 2023). However, this high connectivity has made users more vulnerable to phishing campaigns disguised as online job offers, investment opportunities, or banking alerts (Mangut & Datukun, 2021). These threats are delivered through malware, malicious software designed to steal, disrupt, or monitor data, and are increasingly accompanied by large-scale data theft, involving the unauthorised collection of personal, financial, and login credentials (Alabdan, 2020).

While these technical dimensions are well documented in cybersecurity literature, growing evidence (Cheng *et al.*

[1] Department of Sociology, University of Ibadan, Nigeria
[*] Corresponding author's e-mail: lateefadejunior@gmail.com

2020; Ghani *et al.* 2023) suggests that emotional distress is an equally significant but overlooked risk factor. Emotional states such as anxiety, stress, and fatigue can reduce users' attentiveness and increase susceptibility to phishing attempts. In a context like Nigeria, where economic hardship, information overload, and low digital literacy prevail, emotional distress may substantially increase user vulnerability. Nevertheless, most local interventions remain focused on technical defences, and ignore the emotional aspects of user risk. Additionally, there is limited research exploring how malware, data theft, and emotional distress function collectively as risk factors for phishing, particularly across diverse user groups. Sociodemographic characteristics, such as age, gender, education level, and occupation, may influence not only the likelihood of exposure to phishing attacks but also the emotional consequences of being victimised. This study addresses this gap by examining phishing as a multidimensional threat. It investigates (i) the social media platforms most commonly associated with suspicious link exposure; (ii) the relative influence of malware and data theft on emotional distress; and (iii) the role of sociodemographic variables in predicting emotional responses to phishing incidents.

LITERATURE REVIEW

Emotional distress has been identified as a significant risk factor for phishing and other forms of cybercrime, as it influences individuals' susceptibility to various cyber threats. The rise of social media platforms, such as Facebook, Instagram, Twitter, and Snapchat, has shifted the landscape of phishing attacks. Vila *et al.* (2021) argue that social media has become a prime target for cybercriminals due to users' limited awareness of security risks and poor threat management. These platforms expose a large number of users to phishing attacks because they often rely on emotional engagement with content, which diminishes their ability to recognise and respond to suspicious activity. Emotional responses, such as excitement or curiosity about a post, may lead individuals to click on phishing links or disclose personal information without considering the consequences. Thus, the emotional connection that users develop with social media contributes significantly to their vulnerability to phishing attacks. In addition to emotional engagement, Silic and Back (2016) found that phishing risks on social media are heightened by employees' susceptibility to psychological triggers, weak organisational control measures, inadequate security policies, and poor user authentication. These factors, when combined with individuals' emotional responses to social media content, create an environment where phishing attacks are more likely to succeed. Employees, for example, may be more likely to trust a phishing attempt if it evokes a sense of urgency, fear, or excitement. Furthermore, weak organisational control measures mean that users may not be adequately trained to identify phishing threats, or they may not be encouraged to follow cybersecurity best practices. The lack of emotional resilience and security training increases the likelihood of falling for phishing scams, which highlight the role of emotional distress in these incidents. Badescu (2024) discusses how phishing has evolved, with attackers exploiting human psychological and technical vulnerabilities. Social engineering techniques, which manipulate users emotionally, have become particularly effective. The study explains that phishing attacks often target users' emotions, such as fear of missing out or the allure of a reward. These psychological manipulations lead to poor decision-making, with users providing personal information or downloading harmful software under the influence of these emotional triggers. The emotional manipulation involved in phishing is critical in understanding why individuals are often tricked into compromising their security, as these emotions cloud their judgement and lead to impulsive actions. Bada and Nurse (2020) contribute to the discourse by exploring the broader social and psychological effects of cyber-attacks. They suggest that the emotional responses elicited by cyber-attacks influence how individuals perceive online risks and how they engage with online threats. Public perceptions of cybercrime often lead to heightened emotional responses, such as fear or anxiety, which can shape an individual's approach to cybersecurity. These emotional responses influence their risk perception, motivation to protect themselves, and overall psychological well-being. The emotional distress caused by cyber-attacks can lead to cognitive biases that may affect decision-making and make individuals more likely to fall victim to future phishing attacks. Budimir *et al.* (2021) examined the emotional responses triggered by cybersecurity breaches, noting that these incidents often elicit strong emotional reactions, such as anxiety, fear, and frustration. These emotional responses are not uniform but vary depending on individual personality traits, such as resilience, emotional stability, and how individuals cope with stress. The study found that individuals with lower emotional resilience are more likely to experience long-term mental health effects following a cybersecurity breach. These emotional responses can increase vulnerability to future cybercrime, as individuals may become more anxious and less trusting of online systems. In this context, emotional distress, particularly in response to cybercrime, can reduce individuals' ability to protect themselves effectively, leaving them open to further phishing attacks. Ghani *et al.* (2023) explored the emotional outcomes of cyberbullying and online fraud, particularly among women on social media, finding that such experiences lead to significant emotional distress. Women affected by online fraud or cyberbullying often experience anxiety, stress, trauma, and a decline in self-confidence. These emotional impacts can lead to negative thinking patterns and reduced capacity for critical thinking, which can make individuals more susceptible to phishing attacks. The findings emphasise that the emotional toll of cybercrime is not only a consequence of the immediate incident but

also affects an individual's long-term psychological state. Emotional distress, particularly in the form of anxiety and fear, can lead individuals to make hasty decisions or neglect cybersecurity measures, thus increasing their risk of falling for future cybercrimes, including phishing.

Theoretical Framework

Technology Threat Avoidance Theory

The Technology Threat Avoidance Theory (TTAT), introduced by Liang and Xue (2009), is a behavioural theory used to explain how people react to threats related to technology, especially when it comes to cybersecurity problems like malware, phishing, and identity theft. TTAT posits that individuals evaluate technology threats through two main thinking processes : threat appraisal and coping appraisal, which then affect how motivated they are to avoid the threat and what actions they take. In the threat appraisal process, people look at perceived severity, which is how serious the threat's consequences are; perceived susceptibility, which is how likely they think they are to be affected; and perceived maladaptive rewards, which are the possible benefits of not avoiding the threat (Liang & Xue, 2009). These help shape how dangerous a threat seems. In the coping appraisal process, individuals consider their self-efficacy, which is their belief in their ability to take protective action; response efficacy, which is how well they think the protective action will work; and response cost, which is the effort, time, or money required to deal with the threat (Carpenter *et al.,* 2019). These threat and coping appraisals influence avoidance motivation, which is the intention to do something about the threat; this motivation leads to avoidance behaviour, which means taking real actions like installing antivirus software or turning on two-factor authentication (Boysen *et al.,* 2019). In the context of phishing in Nigeria, TTAT can explain how social media users react to risks like malware, data theft, and emotional distress. If users believe they are likely to be targeted and that the effects, like losing personal data or feeling emotionally stressed, are serious, they may become more alert. Their decision to avoid phishing links depends on how confident they are in spotting scams, whether they believe safety precautions will work, and how hard or costly it is to take those steps. When these users feel prepared and believe protective actions are worth it, they are more likely to avoid phishing attempts.

MATERIALS AND METHODS

This study adopted a quantitative cross-sectional survey design. This design was appropriate because it allowed the researcher to collect data at a single point from a large population. The survey method was chosen for its efficiency in reaching a wide pool of internet users across different regions. It also supports the use of statistical tools such as logistic and multiple regression analyses to test hypotheses and assess predictive relationships. The study involved 2,016 Nigerian internet users who completed and returned the questionnaire. The population comprised Nigerian residents who actively use the internet for communication, banking, shopping, or work. Nigeria was selected because it presents a high-risk environment for phishing due to its expanding digital economy, low cybersecurity awareness, and increased use of online services such as banking, e-commerce, and social networking. The sample size was adequate for statistical analysis and ensured a broad representation of users across various demographics and internet habits. The study used a combination of purposive and convenience sampling techniques. Purposive sampling enabled the selection of participants who were most likely to have experienced or encountered phishing-related activities, such as email users, online shoppers, and social media users. Convenience sampling made it possible to reach participants who were readily available and willing to respond, especially via online platforms. This combination increased the likelihood of including respondents with diverse experiences for efficient data collection. Data were gathered using a structured questionnaire designed to obtain relevant information on the key variables. The questionnaire included items on demographic characteristics, phishing exposure, experiences with malware and data breaches, and emotional distress. The instrument was pilot-tested to ensure clarity and relevance. It was administered electronically through email and social media platforms to enhance reach and convenience. The data were analysed using IBM SPSS Statistics Version 27. Descriptive statistics, such as simple percentages, were used to summarise the data. To test the influence of malware and data theft on phishing victimisation, a binary logistic regression model was employed. In addition, multiple regression analysis was used to determine the predictive effect of emotional distress and other continuous variables on phishing risk. These methods allowed the researcher to examine both categorical and continuous predictors of phishing incidents. Analyses were conducted at a significance level of $p < 0.05$.

RESULTS AND DISCUSSION

The sociodemographic characteristics of the respondents (N = 2016) reveal a predominantly youthful sample. As shown in Table 1, a majority of respondents (51.1%) were aged between 18 and 24 years, followed by those aged 25 to 34 years who constituted 42.0% of the sample. Smaller proportions were recorded for the age brackets of 35 to 44 years (4.5%), 45 to 54 years (2.0%), and those aged 55 and above (0.5%). This distribution indicates that over 93% of the respondents were under the age of 35, suggesting that the study primarily engaged a younger demographic likely to be active on social media platforms. In terms of gender, the majority of respondents identified as female (60.3%), while 38.9% identified as male. A very small fraction (0.8%) preferred not to disclose their gender. This suggests that women were more represented in the sample, which may have implications for interpreting behaviours and attitudes towards social media usage and online security threats. Regarding educational attainment,

Table 1: Sociodemographic Profile of the Respondents (n=2016)

Characteristics	Categories	Frequency	Percentage (%)
Age Group	18–24	1030	51.1
	25–34	846	42.0
	35–44	90	4.5
	45–54	40	2.0
	55 and above	10	0.5
Gender	Female	1216	60.3
	Male	784	38.9
	Prefer not to say	16	0.8
Highest Level of Education	No formal education	76	3.8
	Primary school	38	1.9
	Secondary school	404	20.0
	Tertiary education	1342	66.6
	Postgraduate studies	156	7.7
Occupation	Employed (Full time)	180	8.9
	Employed (Part-time)	244	12.1
	Self-employed	1240	61.5
	Student	324	16.1
	Unemployed	28	1.4
	Total	2016	100.0

most of the respondents reported having achieved tertiary education (66.6%), while 20.0% had completed secondary school education. A smaller segment indicated postgraduate studies (7.7%), whereas 3.8% had no formal education, and 1.9% reported completing only primary school. These findings indicate that the majority of the respondents were well-educated, with nearly three-quarters having completed tertiary or postgraduate education. This educational profile suggests a higher level of digital literacy within the sample, which could influence their awareness and responses to phishing attempts encountered online. The respondents' current occupational status further contextualises their social media usage patterns. Most participants were self-employed (61.5%), indicating a strong entrepreneurial presence within the sample. Students accounted for 16.1% of the respondents, while those employed part-time and full-time constituted 12.1% and 8.9% respectively. Only a small fraction (1.4%) reported being unemployed. The dominance of self-employed individuals may point to a frequent use of digital platforms for business promotion or operations, which could explain their exposure to link-based phishing attacks. The sociodemographic profile suggests that the study population is predominantly young, female, well-educated, and self-employed. This composition is particularly relevant in the context of the research, as these characteristics are likely to influence respondents' engagement with social media, their exposure to cyber threats, and their capacity to recognise and respond to phishing attempts.

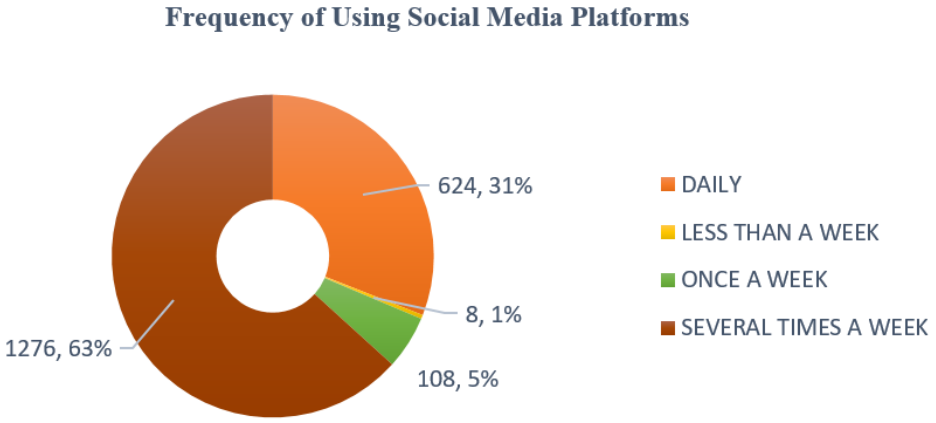
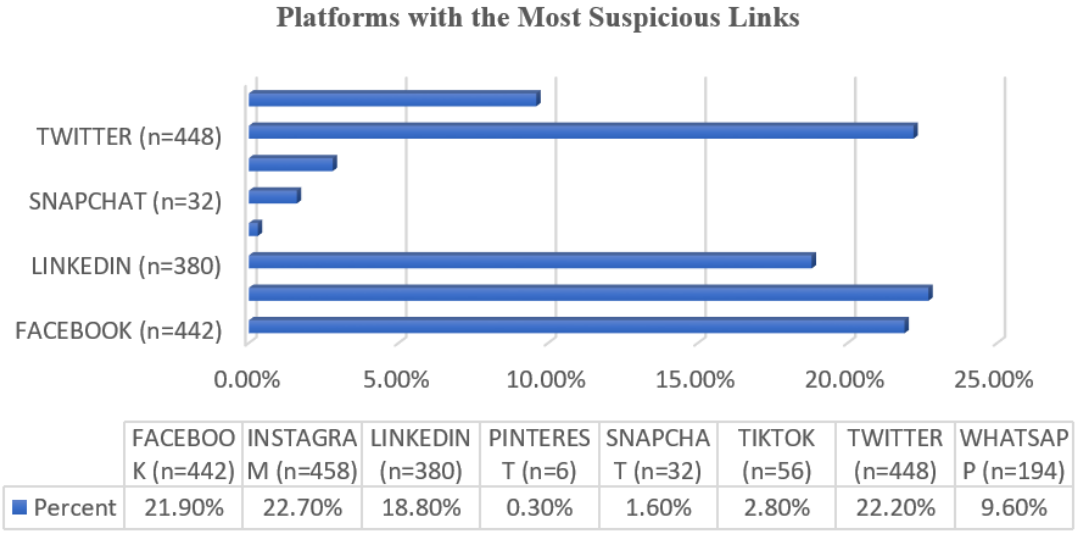


Figure 1: Frequent use of social media platforms.

Figure 1 displays a descriptive analysis of the frequency of social media platform use among participants. Results indicated that the majority of respondents (n = 1,276, 63%) reported using social media several times a week. Additionally, 624 participants (31%) indicated that they used social media daily. A smaller proportion of respondents reported using social media once a week (n = 108, 5%) or less than once a week (n = 8, 1%). These findings suggest that social media usage is highly frequent among the majority of participants, with nearly all individuals engaging with these platforms at least weekly. As seen in Figure 2, the platforms where users encountered



	FACEBOOK (n=442)	INSTAGRAM (n=458)	LINKEDIN (n=380)	PINTEREST (n=6)	SNAPCHAT (n=32)	TIKTOK (n=56)	TWITTER (n=448)	WHATSAPP (n=194)
Percent	21.90%	22.70%	18.80%	0.30%	1.60%	2.80%	22.20%	9.60%

Figure 2: Platforms with the Most Suspicious Links

the most suspicious links revealed n differences across social media sites. Instagram was reported as the platform with the highest percentage of suspicious link encounters (22.7%), followed closely by Facebook (21.9%) and Twitter (22.2%). LinkedIn accounted for 18.8% of suspicious link encounters. Comparatively lower percentages were recorded for TikTok (2.8%), Snapchat (1.6%), and Pinterest (0.3%). WhatsApp accounted for 9.6% of the suspicious links reported. These findings suggest that while suspicious links are present across multiple platforms, users are most likely to encounter them on Instagram, Facebook, and Twitter.

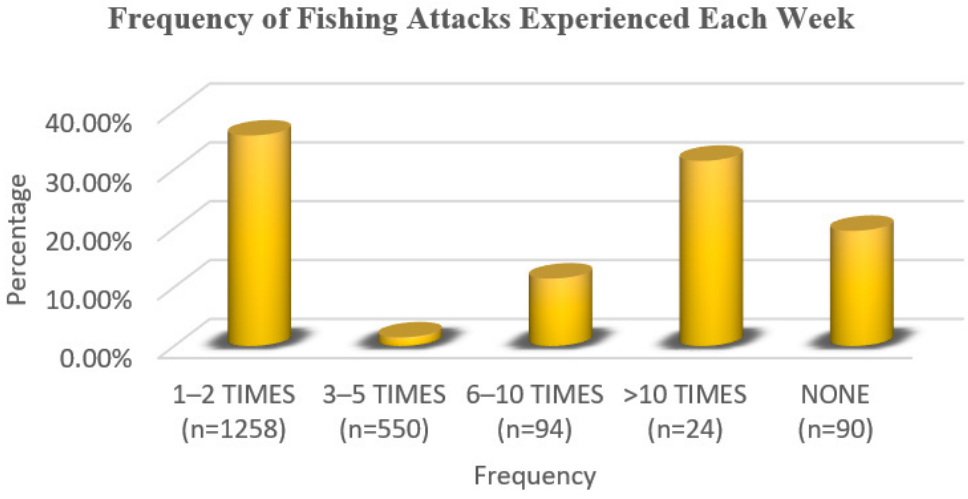


Figure 3: Frequency of Fishing Attacks Experienced Each Week

As seen in Figure 3, the analysis of phishing attacks experienced each week indicated varying levels of exposure among respondents. The majority reported encountering phishing attacks 1–2 times per week (39.7%, n = 1258). Additionally, 17.4% (n = 550) experienced phishing attempts 3–5 times weekly, while 3.0% (n = 94) encountered attacks 6–10 times weekly. A smaller proportion of participants (0.8%, n = 24) experienced phishing attacks more than 10 times per week. Notably, 12.5% (n = 90) reported experiencing no phishing attacks during the observed period. These results highlight that phishing threats are a frequent challenge for most social media users, with a significant portion encountering them multiple times each week.

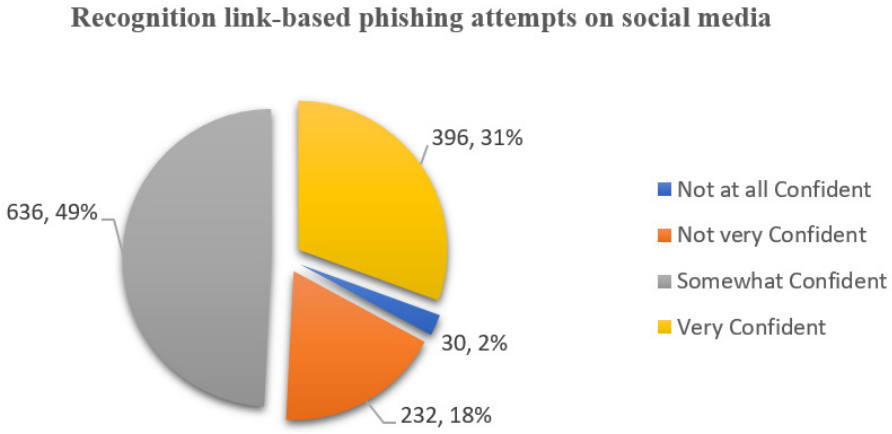


Figure 4: Confidence in recognising link-based phishing attempts on social media

The pie chart (Figure 4) displays respondents' self-reported confidence levels in recognising link-based phishing attempts on social media platforms (N = 1,294). Results indicate that approximately half of the respondents (49%, n = 636) reported feeling "Somewhat Confident" in their ability to identify such threats. Nearly one-third of participants (31%, n = 396) indicated they were "Very Confident" in their phishing recognition abilities. In contrast, a smaller proportion of respondents expressed limited confidence, with 18% (n = 232) reporting they were "Not Very Confident" and only 2% (n = 30) stating they were "Not at All Confident" in recognising link-based phishing attempts on social media. These findings suggest that while the majority of participants (80%) report at least some level of confidence in their ability to identify social media phishing attempts, a substantial minority (20%) acknowledge significant vulnerability in this area.

Table 2: Binary Logistic Regression Predicting the experience of Malware as a Risk Factor of Emotional Distress across Socio-demographic Groups

Characteristic	Category		P	Odd Ratio OR	95% CI (Lower – Upper)
Age Group	18–24	Ref	–	–	–
	25–34		.000	39.972	[6.221 – 256.823]
	35–44		.001	25.263	[4.040 – 157.970]
	45–54		.020	9.647	[1.435 – 64.855]
	55 and above		.034	9.056	[1.181 – 69.437]
Gender	Female	Ref	–	–	–
	Male		.040	4.885	[1.073 – 22.236]
	Prefer not to say		.049	4.491	[1.003 – 20.102]
Level of Education	No formal education	Ref	–	–	–
	Primary School		.026	8.569	[1.290 – 56.927]
	Secondary School		.056	0.515	[0.261 – 1.016]
	Tertiary Education		.127	3.399	[0.706 – 16.358]
	Postgraduate Studies		.000	10.218	[3.473 – 30.065]
Current Occupation	Employed (Full time)	Ref	–	–	–
	Employed (Part time)		.009	2.389	[1.246 – 4.581]
	Self-employed		.000	70.882	[24.020 – 209.166]
	Student		.013	3.032	[1.263 – 7.276]
	Unemployed		.962	1.030	[0.302 – 3.513]

A binary logistic regression was conducted to examine the predictive influence of various socio-demographic characteristics on the likelihood of experiencing emotional distress due to phishing attacks. The results, presented in Table 2, revealed several statistically significant predictors. First off, age was a strong predictor of emotional distress. Compared to respondents aged 18–24 years (reference category), those aged 25–34 years were significantly more likely to experience emotional distress due to phishing attacks (OR = 39.972, 95% CI

[6.221, 256.823], p < .001). Similarly, individuals aged 35–44 years (OR = 25.263, 95% CI [4.040, 157.970], p = .001), 45–54 years (OR = 9.647, 95% CI [1.435, 64.855], p = .020), and those aged 55 years and above (OR = 9.056, 95% CI [1.181, 69.437], p = .034) were also significantly more likely to report emotional distress compared to the youngest age group. This pattern suggests an increasing vulnerability to emotional distress with advancing age among the respondents. Gender also emerged as a significant predictor. Compared to females (reference category), males had significantly higher odds of reporting emotional distress (OR = 4.885, 95% CI [1.073, 22.236], p = .040). Respondents who preferred not to disclose their gender were similarly more likely to experience emotional distress (OR = 4.491, 95% CI [1.003, 20.102], p = .049). These findings indicate that emotional distress is not confined to one gender but may be higher among males and individuals who choose not to disclose their gender identity. Educational attainment showed a mixed pattern. Using respondents with no formal education as the reference group, those with primary school education were significantly more likely to experience emotional distress (OR = 8.569, 95% CI [1.290, 56.927], p = .026). Although secondary school education was associated with a lower likelihood of emotional distress (OR = 0.515, 95% CI [0.261, 1.016]), this association did not reach conventional significance (p = .056). Tertiary education was not a statistically significant predictor (OR = 3.399, 95% CI [0.706, 16.358], p = .127), while respondents with postgraduate studies were significantly more likely to experience emotional distress (OR = 10.218, 95% CI [3.473, 30.065], p < .001). These results suggest that while basic education (primary level) and higher education (postgraduate level) are associated with higher odds of emotional distress, secondary education may have a slightly protective effect, although not conclusively. Occupation was another significant predictor. Relative to respondents employed full-time (reference group), those employed part-time were more likely to report emotional distress (OR = 2.389, 95% CI [1.246, 4.581], p = .009). Self-employed individuals had dramatically higher odds of experiencing emotional distress (OR = 70.882, 95% CI [24.020, 209.166], p < .001), highlighting a particularly vulnerable group. Students were also more likely to report emotional distress (OR = 3.032, 95% CI [1.263, 7.276], p = .013). Conversely, unemployment status did not significantly predict emotional distress (OR = 1.030, 95% CI [0.302, 3.513], p = .962), suggesting that among this sample, unemployment per se was not a unique driver of emotional distress compared to being employed full-time. These findings indicate that emotional distress among the respondents is significantly shaped by age, gender,

Table 3: Multiple Regression Analysis Predicting the relative factors of Data Theft and Malware Attacks on Emotional Distress

Model Summary								
Model	**Multiple R**	**R Square**	**Adjusted R Square**			**Std. Error of the Estimate**		
1	.210a	.044	.041			.341		
ANOVA[a]								
Model		**SS**		**df**	**MS**	**F**	**p**	
1	Regression	10.845		6	1.807	15.500	.000[b]	
	Residual	234.280		2009	.117			
	Total	245.125		2015				
Coefficients								
Model					**t**	**Sig.**	**95.0% CI**	
		B	**S.E**	**Beta**			**Lower**	**Upper**
1	(Constant)	1.449	.054		26.695	.000	1.342	1.555
	Encountering suspicious links on social media	-.040	.008	-.111	-5.022	.000	-.055	-.024
	Lack of cybersecurity awareness	-.007	.046	-.004	-.162	.871	-.097	.082
	Clicks	-.096	.048	-.052	-1.989	.047	-.190	-.001
	Inability to take action	-.005	.004	-.023	-1.032	.302	-.013	.004
	Experienced negative consequences	-.274	.052	-.146	-5.270	.000	-.376	-.172

a. Dependent Variable: Emotional Distress

education, and employment status. Older respondents, males, those with primary or postgraduate education, self-employed individuals, and students were particularly at elevated risk.

A multiple regression analysis was conducted to examine the predictive impact of relative factors related to data theft and malware attacks on emotional distress. The overall model was statistically significant, $F(6, 2009) = 15.50$, $p < .001$, indicating that the set of predictors explained a significant proportion of the variance in emotional distress. The model accounted for approximately 4.4% of the variance in emotional distress ($R^2 = .044$, Adjusted $R^2 = .041$), with a standard error of the estimate of .341. Examining the individual predictors, encountering suspicious links on social media significantly predicted emotional distress ($B = -0.040$, $SE = 0.008$, $\beta = -0.111$, $t = -5.022$, $p < .001$), suggesting that increased encounters with suspicious links were associated with a slight decrease in emotional distress, although the negative direction may require further contextual explanation. Lack of cybersecurity awareness was not a significant predictor ($B = -0.007$, $SE = 0.046$, $\beta = -0.004$, $t = -0.162$, $p = .871$), indicating that cybersecurity knowledge, as measured, did not significantly impact emotional distress. Clicking on suspicious links was found to significantly predict emotional distress ($B = -0.096$, $SE = 0.048$, $\beta = -0.052$, $t = -1.989$, $p = .047$), albeit with a small negative effect size. The inability to take action after a malware-related incident did not significantly predict emotional distress ($B = -0.005$, $SE = 0.004$, $\beta = -0.023$, $t = -1.032$, $p = .302$). Importantly, experiencing negative consequences after clicking a suspicious link was a strong and significant predictor of emotional distress ($B = -0.274$, $SE = 0.052$, $\beta = -0.146$, $t = -5.270$, $p < .001$). This finding indicates that individuals who experienced tangible negative outcomes were significantly more likely to report heightened emotional distress. These results suggest that while encountering suspicious links and clicking behaviours contribute modestly to emotional distress, the experience of negative consequences has the most substantial impact among the variables assessed.

Discussion

Social Media Platforms Most Susceptible to Suspicious Links

The findings of the study indicate that the risk of encountering suspicious links is widespread across several popular social media platforms, with notable variations in platform-specific exposure. The most frequently cited platforms for suspicious link encounters were Instagram, Twitter, and Facebook. This outcome corresponds with prior research by Silic and Back (2018), who observed that platforms designed for high interactivity and information sharing tend to attract a higher concentration of phishing activities. Users' heavy engagement on these platforms creates ideal opportunities for malicious actors to exploit human trust and social connectivity. The study further revealed that LinkedIn, a platform traditionally associated with professional networking, also reported a considerable number of suspicious link exposures. This finding challenges assumptions that professional or formal platforms are inherently more secure. It aligns with the observation made by Badescu (2024) that phishing strategies are increasingly adaptive and infiltrate diverse social media environments regardless of their intended purpose. Platforms like TikTok, Snapchat, and Pinterest, although recording lower exposure rates, should not be dismissed as safe, as their growing popularity could eventually make them attractive targets for cybercriminals. The intense frequency of social media use among participants adds another layer of concern. The majority reported accessing social media platforms either daily or several times weekly. This finding is consistent with the position of Parker and Flowerday (2020), who stated that high-frequency users are naturally at an elevated risk due to increased opportunities for exposure. Constant engagement creates habitual patterns that may lower users' vigilance over time, which is a critical concern when viewed through the lens of the Technology Threat Avoidance Theory. When users perceive themselves as less susceptible because of familiarity with the platform, their motivation to avoid risky interactions, such as clicking suspicious links, may decline, thereby increasing vulnerability. Findings also revealed overconfidence in users' ability to detect phishing links. While many respondents expressed being "somewhat confident" or "very confident" in recognising phishing threats, this confidence appears inconsistent with the high volume of phishing exposures reported. This discrepancy may signal an overestimation of skill, where users feel more capable than they actually are, which results in reduced vigilance. Vila *et al.* (2021) noted that overconfidence in cybersecurity often weakens protective behaviours. In this case, users' beliefs that they can identify malicious content may discourage them from scrutinising links carefully, and this increases their actual risk. This pattern may also reflect a broader issue of behavioural complacency due to routine exposure. When users encounter phishing attempts frequently across various platforms but do not experience immediate harm, they may begin to normalise these risks. Egelman and Peer (2015) explained that repeated exposure without tangible consequences leads to desensitisation that reduces users' perceived severity of the threat. Under technology threat avoidance theory, this affects both threat appraisal and avoidance motivation, particularly if individuals begin to see phishing as an unavoidable or non-serious aspect of social media use.

It is important to stress that the presence of phishing threats is not uniform across all platforms but varies based on user engagement styles, platform security protocols, and content dynamics. The detection of a notable amount of phishing on WhatsApp further broadens the understanding that messaging services, not just social feeds, can be major vectors for attacks. As evidenced in the report of Andrey *et al.* (2021), the private nature of messaging applications fosters a false sense of

security among users that reduces their critical scrutiny of incoming content. The study's revelation that no platform is entirely immune calls for a recalibration of users' security expectations across all online environments. It also reinforces the importance of cross-platform cybersecurity awareness initiatives. Without sustained and platform-specific interventions, the evolving tactics of cybercriminals will continue to exploit gaps in user perception and behaviour.

Relative Factors Predicting Malware and Data Theft Attacks on Emotional Distress

The study's findings uncovered important factors related to how malware and data theft attacks influence emotional distress among social media users. It was clear that exposure to suspicious links alone did not have a straightforward relationship with emotional reactions. Although encountering suspicious links on social media was significantly associated with emotional distress, the relationship was not as strong as initially expected. This observation supports the position of Baillon *et al.* (2019) that mere exposure does not always equate to harm, especially when users perceive themselves to be capable of handling such risks. However, the presence of frequent suspicious links still creates an environment of uncertainty, which over time can lower users' emotional resilience. Findings also show that clicking on suspicious links slightly predicted emotional distress. However, the small effect suggests that the action of clicking, in itself, does not necessarily produce immediate or intense emotional consequences unless it results in tangible harm. This insight mirrors the observations of Gainsbury *et al.* (2019) that users often engage in risky online behaviours without fully appreciating the potential psychological costs unless they suffer direct negative outcomes. The Technology Threat Avoidance Theory also demonstrated a strong correlation between users' avoidance behaviours and their perceptions of the effectiveness of coping responses. If users believe that they can recover easily or that clicking a link is unlikely to cause serious damage, their motivation to avoid such behaviours diminishes, thereby maintaining their emotional equilibrium until a negative event occurs.

Importantly, the study revealed that the strongest predictor of emotional distress was the experience of negative consequences following phishing incidents. This outcome is supported by earlier work by Bada and Nurse (2020), which emphasised that the emotional impact of cyberattacks escalates dramatically once the victim suffers real losses, such as identity theft, financial theft, or reputational harm. In this context, Technology Threat Avoidance Theory explains that the perceived severity of the threat is amplified once consequences are felt, and this heightened perception triggers emotional distress more than theoretical risks ever could. Emotional distress, therefore, appears less related to theoretical exposure and more intensely tied to concrete experiences of damage. The findings also indicated that lack of cybersecurity awareness and inability to take protective action after encountering threats were not significant predictors of emotional distress. This aligns with the perspective offered by Budimir *et al.* (2021): awareness, in isolation, does not guarantee behavioural change or emotional protection. Knowledge without application seems insufficient to shield users emotionally from the consequences of cyberattacks. Furthermore, from the standpoint of Technology Threat Avoidance Theory, users may cognitively understand threats but fail to translate their knowledge into motivated avoidance if they do not feel personally vulnerable or do not perceive their coping mechanisms as effective. Another critical insight that adds nuance to these findings is the idea of exposure fatigue. Users who reported high-frequency exposure to suspicious links may have developed a psychological tolerance or emotional numbness toward digital threats. The result is a desensitisation process, where repeated exposure without immediate negative outcomes causes individuals to normalise the presence of threats and stop reacting with urgency, as seen in media violence (Stadler, 2013). This pattern could explain why some predictors, such as general exposure and link-clicking behaviour, show only weak associations with emotional distress. Within the Technology Threat Avoidance Theory, this trend reflects a weakening of threat appraisal over time. When users cease to see phishing as an unusual or pressing danger, their motivation to take protective action and their emotional responses both diminish, even if the objective risk remains high.

The analysis of sociodemographic factors provided critical insights into how characteristics such as age, gender, education, and occupation predict emotional distress in response to phishing and malware attacks. The findings indicated that age was a major predictor, with older respondents more likely to report emotional distress compared to younger participants. This finding challenges the common belief that older individuals, due to their presumed caution and life experience, are less susceptible to emotional impacts from cyber threats. Budimir *et al.* (2021) have similarly established that younger individuals, although technically more savvy, may be less emotionally reactive to cyber incidents because of greater familiarity with online risks. As age increases, users may perceive themselves as more vulnerable or less adaptable to fast-changing digital threats, which leads to heightened emotional reactions when attacked.

Gender also emerged as a significant predictor of emotional distress, with males and those who preferred not to disclose their gender more likely to report distress compared to females. This finding stands in contrast to some earlier research, such as that of Lindsay *et al.* (2016), which often associates higher emotional responses to online threats with female users. However, the present study's result supports the idea that gendered experiences of digital risk are complex and evolving. Male users may experience greater emotional distress, not because of greater vulnerability but possibly because of a reluctance

to seek help or discuss security breaches, which leads to internalised stress responses.

Educational attainment showed a non-linear relationship with emotional distress. Surprisingly, respondents with primary school education and those with postgraduate studies were significantly more distressed than those with no formal education or tertiary education. Secondary education was associated with a slightly protective effect, although not conclusively. These findings suggest that emotional vulnerability does not decrease consistently with higher education levels. This complexity validates the argument of Petrauskaite (2020) that education can increase knowledge without necessarily building emotional resilience to modern threats such as cyber attacks. Users with postgraduate education might experience higher emotional distress because their increased awareness of potential threats magnifies their perceived severity. They may have a deeper understanding of the far-reaching consequences of cyberattacks, which heightens the perceived severity of each incident. On the other hand, users with only primary education may feel less equipped to respond to threats which enhance their perceived vulnerability and emotional strain.

Occupation was revealed as a particularly powerful predictor of emotional distress. Self-employed individuals were significantly more likely to report high levels of distress, a finding consistent with the work of Arroyabe *et al.* (2024) that highlighted the deep psychological and financial impacts of cyberattacks on entrepreneurs and small business owners. For self-employed individuals, a phishing attack could directly threaten their livelihood and intensify emotional responses. However, another layer of vulnerability may lie in emotional isolation. Unlike full-time employees, self-employed individuals lack institutional support structures such as IT teams, mental health services, or formal peer groups. This absence of professional backup may force them to handle the full emotional burden of an attack alone. Without guidance or reassurance, emotional responses may intensify, which contributes to prolonged distress and a sense of helplessness not always visible in technical or economic data.

Similarly, students and part-time workers also exhibited elevated levels of distress, possibly due to precarious financial situations or transitional life stages that magnify the perceived severity of digital threats. Full-time employees showed comparatively lower distress levels, perhaps reflecting greater institutional support structures that can mitigate the emotional fallout from cyber incidents. Interestingly, unemployment did not significantly predict emotional distress, suggesting that individuals disengaged from active work or study may perceive less immediate risk or consequence from phishing attacks. This lack of emotional impact among unemployed users may stem from lower digital activity or fewer financial transactions online. Without regular interaction with digital platforms tied to work, income, or communication, unemployed individuals might not view phishing threats as directly threatening, which in turn dampens their emotional responses. Their lower emotional distress may therefore be less about resilience and more about perceived detachment from the online environments where such attacks occur.

CONCLUSION

Phishing thrives within a complex network of social, emotional, and behavioural vulnerabilities that are usually underestimated. Emotional distress, often dismissed or invisible in cybersecurity discussions, emerges as a crucial driver of risk. It is not simply a consequence of phishing but a condition that shapes how users respond to, cope with, or ignore potential threats. When distress is persistent, unaddressed, or amplified by socioeconomic pressures, users may become emotionally fatigued, disengaged, or overconfident, all of which create ideal conditions for phishing attacks to succeed. In contexts like Nigeria, where structural digital education gaps coexist with rapid online adoption, emotional distress cannot be treated as a passive outcome. It must be acknowledged as an active and dynamic part of the threat landscape. As long as emotional responses are excluded from national cybersecurity strategies, and as long as malware and data theft continue to be treated only as technological disruptions, the human dimension of phishing will remain neglected. This reality shows the need for a shift from controlling the tools of attack to understanding the state of the user. Building protection against phishing in Nigeria will require more than just improved systems; it will also require efforts to support and prepare individuals in practical and emotional ways.

Recommendations

In order to effectively reduce the risks associated with phishing in Nigeria, a coordinated and multidimensional approach is necessary, and this must involve collaboration among government agencies, educational institutions, cybersecurity experts, and digital platform providers. The National Information Technology Development Agency (NITDA) should lead the development of a national cybersecurity awareness curriculum that addresses not only technical threats but also the emotional and psychological dimensions of phishing. This curriculum should be integrated into secondary and tertiary education through partnerships with the Federal Ministry of Education, National Universities Commission (NUC) and relevant curriculum bodies. At the same time, the Nigerian Communications Commission (NCC) should work with internet service providers and mobile network operators to detect and block suspicious links in real time, while also mandating safer default settings on mobile applications and browsers.

For the business sector, the Small and Medium Enterprises Development Agency of Nigeria (SMEDAN) can initiate targeted digital safety training for self-employed individuals and microbusinesses, many of whom use social media platforms for daily transactions but lack the resources to manage online risks. Emotional

support mechanisms should also be considered; the Federal Ministry of Health, in collaboration with non-governmental organisations, can introduce digital mental health campaigns aimed at helping victims of cyber crimes cope with stress and anxiety. In addition, technology companies operating in Nigeria, including social media platforms and digital payment providers, must be engaged in creating responsive reporting systems, flagging tools, and transparent user education policies.

REFERENCE

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet, 12*(10), 168. https://doi.org/10.3390/fi12100168

Andrey, S., Rand, A., Masoodi, M. J. & Tran, S. (2021). *Private Messaging, Public Harms*. Retrieved from https://www.cybersecurepolicy.ca/privatemessaging

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. https://doi.org/10.1016/j.cose.2024.103826

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92). Academic press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

Badescu, R. (2024). Phishing Threats in the Age of Social Media: A User-Centric Approach. *Informatica Economica, 28*(4), 83-101. https://doi.org/10.24818/issn14531305/28.4.2024.07

Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. *PloS one, 14*(12), e0224216. https://doi.org/10.1371/journal.pone.0224216

Boysen, S., Hewitt, B., Gibbs, D., & McLeod, A. (2019). Refining the threat calculus of technology threat avoidance theory. *Communications of the Association for Information Systems, 45*(5), 95-115. https://doi.org/10.17705/1CAIS.04505

Budimir, S., Fontaine, J. R., Huijts, N. M., Haans, A., Loukas, G., & Roesch, E. B. (2021). Emotional reactions to cybersecurity breach situations: scenario-based survey study. *Journal of medical Internet research, 23*(5), e24879. https://doi.org/10.2196/24879

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*(22), 380-407. https://doi.org/10.17705/1CAIS.04422

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior, 108*, 106311. https://doi.org/10.1016/j.chb.2020.106311

DataReportal (2023). *Digital 2023: Nigeria*. Retrieved from https://datareportal.com/reports/digital-2023-nigeria

Eliot, B. and Maxime, C. (2024). *Phishing Trends Report* (Updated for 2024). [online] Hoxhunt.com. Retrieved from https://hoxhunt.com/guide/phishing-trends-report.

Gainsbury, S. M., Browne, M., & Rockloff, M. (2019). Identifying risky Internet use: Associating negative online experience with specific online behaviours. *New Media & Society, 21*(6), 1232-1252. https://doi.org/10.1177/1461444818815442

Ghani, N. M., Bakar, M. A. A., & Rosli, H. (2023). Cybercrime experience's impact on women's emotions: A case study in Penang. *Malaysian Journal of Tropical Geography (MJTG), 49*(2), 48-67.

INTERPOL (2021). *INTERPOL report identifies top cyberthreats in Africa*. [online] www.interpol.int. Retrieved from https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71-90. https://doi.org/10.2307/20650279

Lindsay, M., Booth, J. M., Messing, J. T., & Thaller, J. (2016). Experiences of online harassment among emerging adults: Emotional reactions and the mediating role of fear. *Journal of Interpersonal Violence, 31*(19), 3174-3195. https://doi.org/10.1177/0886260515584344

Mangut, P. N., & Datukun, K. A. (2021). The current phishing techniques–perspective of the Nigerian environment. *World Journal of Innovative Research, 10*(1). https://doi.org/10.31871/WJIR.10.1.9

Parker, H. J., & Flowerday, S. V. (2020). Contributing factors to increased susceptibility to social media phishing attacks. *South African Journal of Information Management, 22*(1), 1-10.

Petrauskaite, A. (2020). Society resilience to contemporary threats: The impact of education. *Public Security and Public Order, 24*, 329-337. https://doi.org/10.13165/PSPO-20-24-20

Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior, 60*, 35-43. https://doi.org/10.1016/j.chb.2016.02.050

Stadler, J. (2013). Screen media violence and the socialisation of young viewers. *Youth violence: Sources and solutions in South Africa,* 319-345.

Vila, J., Briggs, P., Branley-Bell, D., Gomez, Y., & Coventry, L. (2021). Behavioural issues in cybersecurity. In *Security Risk Models for Cyber Insurance* (pp. 27-48). 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742: CRC Press.