Published by The College of Agriculture and Hospitality Management (COAHM), TASFUED, vol. 1, no. 1, pp. 82-87

JOAHM, TASFUED
Journal of Agriculture and Hospitality Management

The Role of Cyber-Security in Curbing Online Agricultural Frauds among Small-Scale Farmers in Ogun State, Nigeria

[1]Abiala, A. A.; [1]Adewale, I. A.; [2]Olawumi, A. T.; [3]Abiala, O. M. & [1]Jimoh, J. B.
[1]Department of Agricultural Economics and Extension, Tai Solarin Federal University of Education, Ijagun, Ogun State, Nigeria
[2]Department of Tourism and Hospitality Management, Tai Solarin Federal University of Education, Ijagun, Ogun State, Nigeria
[3]Library Department, Ogun State Polytechnic of Health & Allied Sciences, Ilese-Ijebu, Ogun State, Nigeria
Corresponding author: *abialaaa@tasued.edu.ng*

Abstract
This study examined the role of cyber-security in curbing online agricultural frauds among small-scale farmers in Ogun State, Nigeria. The rapid expansion of mobile phone ownership, mobile money and digital agricultural platforms in Nigeria has created new opportunities for farmers to access market information, inputs, and credit, but has simultaneously exposed them to various online agricultural frauds. A descriptive survey design was adopted, employing a multistage sampling procedure to select 150 small-scale farmers across the four ADP zones of Ogun State. Primary data were collected using a structured questionnaire and analysed using descriptive and inferential statistics. The findings from this study confirmed that there is a significant correlation between respondents' socio-economic characteristics and cyber-security awareness ($r = 0.31$, $p = 0.004$). There is a negative correlation between respondents' vulnerability to fraud and cyber-security awareness ($r = -0.52$, $p = 0.000$) and there is a significant relationship between frequent and infrequent platform users and cyber-security awareness ($r = 0.94$, $p = 0.016$) while constraints to the adoption cyber-security practices showed a negative correlation ($r = -0.36$, $p = 0.001$) in Ogun State. The study concludes that higher cyber-security awareness and adoption of protective digital practices were significantly associated with lower vulnerability to online agricultural frauds, but awareness levels among small-scale farmers in Ogun State remain generally low, constrained by limited digital literacy, weak extension messaging on cyber-security, and low access to formal cybercrime reporting channels. The study recommends the integration of cyber-security literacy into agricultural extension programmes, and collaborations with consumer-protection agencies.

Keywords: Cyber-security, online fraud, small-scale farmers, digital agriculture

1. Introduction

The last decade has witnessed a rapid expansion of digital technology use across Nigeria's agricultural sector. Mobile phones are now widely used by farmers to access market price information, communicate with buyers, receive extension advice and make and receive payments through mobile money and bank transfer platforms (Nwosu, 2022). Building on this expansion, a wave of agricultural technology (agritech) platforms emerged from around 2016 onward, offering Nigerians the opportunity to invest in farmland, livestock or crop production in exchange for promised returns, and marketing themselves as a solution to the agricultural sector's chronic financing gap. At their peak, these agric-crowd-funding platforms had reportedly mobilised over ₦20 billion from Nigerian investors (Nwachukwu, 2025).

Abiala, A. A., Adewale, I. A., Olawumi, A. T., Abiala, O. M. & Jimoh, J. B. (2026). The Role of Cyber-Security in Curbing Online Agricultural Frauds among Small-Scale Farmers in Ogun State, Nigeria, *Journal of Agriculture and Hospitality Management (JOAHM),* vol. 1, no. 1, pp. 82-87.
©COAHM, Vol. 1, No. 1, Oct 2026.

However, beginning around 2020, many of these platforms began to default on payments to investors, and a number were subsequently associated with fraud and Ponzi-scheme allegations; industry commentary has since described the period as one in which "agriculture became fraud," with technology serving as the enabler. Nigeria's Economic and Financial Crimes Commission (EFCC) and Nigeria Financial Intelligence Unit (NFIU) have published advisories naming dozens of agriculture-branded companies among suspected Ponzi schemes operating in the country, with the National Deposit Insurance Corporation estimating that Nigerians lost hundreds of billions of naira to Ponzi-related schemes over roughly two decades (EFCC, 2025 & NFIU, 2025). Beyond investment fraud, small-scale farmers, like other Nigerians, are also exposed to other forms of online and mobile-based fraud, including SIM-swap fraud, phishing messages impersonating banks or mobile money providers, fake input-supplier and produce-buyer scams on social media and messaging platforms, and card-related and account-takeover fraud targeting the savings of everyday bank and mobile-money

customers, including farmers (Food Ingredients First, 2025).

Cyber-security, understood broadly as the set of technologies, practices and behaviours aimed at protecting devices, accounts, data and transactions from unauthorised access or exploitation, is central to curbing this exposure. In urban and formal-sector contexts, cyber-security awareness campaigns, two-factor authentication, and regulatory oversight of digital platforms have become increasingly common. Rural and semi-rural small-scale farmers, however, often have comparatively lower levels of digital literacy, are more reliant on informal information networks (including social media and word-of-mouth) for investment and market decisions, and may have less access to formal channels for verifying the legitimacy of a digital platform or reporting a suspected fraud, potentially leaving them disproportionately vulnerable to online agricultural fraud despite their growing use of mobile and digital financial tools (Industrial Ransonware (IR), 2026).

Ogun State is located in south-western Nigeria and bordering Lagos State, has a large population of small-scale farmers engaged in the production of crops such as cassava, maize, vegetables, oil palm and root and tuber crops, alongside growing mobile phone penetration and increasing farmer engagement with mobile money, social media-based agricultural marketing, and agric-investment platforms, given the state's proximity to Lagos, Nigeria's commercial and fintech hub. Understanding how cyber-security awareness and practices among small-scale farmers in Ogun State relate to their exposure to, and experience of, online agricultural fraud is therefore both timely and relevant to informing extension policy, financial consumer protection and rural digital-literacy interventions.

It is against this background that this study investigates the role of cyber-security in curbing online agricultural frauds among small-scale farmers in Ogun State. As small-scale farmers in Ogun State increasingly engage with mobile money, social media-based agricultural marketing and online agric-investment opportunities, they become correspondingly exposed to the risk of online fraud, ranging from fraudulent agric-investment/crowd-funding schemes to phishing, SIM-swap and impersonation scams targeting their mobile money and bank accounts (Davis, 2021). National-level evidence indicates that agriculture-branded Ponzi schemes and digital fraud have affected large numbers of Nigerians, including small-scale farmers, resulting in substantial financial losses, eroded trust in digital financial platforms and, in some documented cases, farmers losing savings accumulated over several years. Despite this exposure, it is unclear to what extent small-scale farmers in Ogun State are aware of common online agricultural fraud tactics, what specific forms of online fraud they have experienced or are most vulnerable to, what cyber-security practices (if any) they currently apply to protect themselves, and whether and how their level of cyber-security awareness is related to their actual vulnerability to online agricultural fraud (Ajayi, 2024). Agricultural extension programming in Nigeria has traditionally focused on production, marketing and input-use messaging, with comparatively little systematic attention paid to digital/cyber-security literacy as a component of farmer support services. Without empirical evidence specific to small-scale farmers in Ogun State, extension planners, financial regulators and rural development agencies lack the locally grounded information needed to design effective interventions to curb online agricultural fraud in Ogun State.

1.2 Objectives of the Study

i. Describe the socio-economic characteristics of small-scale farmers in Ogun State.
ii. Determine the frequency of use of digital/online platforms for agricultural transactions among farmers in Ogun State.
iii. Identify the types and perceived prevalence of online agricultural fraud experienced by farmers in Ogun State.
iv. Assess farmers' cyber-security awareness and the protective digital practices currently adopted in Ogun State.
v. Identify the constraints to the adoption of cyber-security practices among small-scale farmers in Ogun State.

1.3 Hypotheses

$H0_1$: There is no significant relationship between the respondents' socio-economic characteristics and their cyber-security awareness in Ogun State.

$H0_2$: There is no significant relationship between the respondents' vulnerability to fraud and their cyber-security awareness in Ogun State.

$H0_3$: There is no significant relationship between the respondents' frequent or infrequent platform users and their cyber-security awareness in Ogun State.

$H0_4$: There is no significant relationship between the respondents' constraints and to the adoption of cyber-security practices in Ogun State.

2. Methodology

This study was carried out in Ogun State, located in the south-western geopolitical zone of Nigeria. Ogun State is on 7°00'0.00" N 3°34'59.99" E on DMS coordinates and shares boundaries with Lagos State to the south, Oyo and Osun States to the north, Ondo State to the east, and the Republic of Benin to the west, giving it a strategically important location along major trade corridors linking Lagos to the rest of Nigeria and to West Africa. The state comprises twenty local government areas and is home to a substantial agrarian population engaged in the production of crops such as cassava, maize, vegetables, oil palm, kolanut and root and tuber crops, alongside a fast-growing industrial and residential corridor closest to Lagos. The Ogun State

Agricultural Development Programme coordinates extension services to farmers across the state's local government areas. Given its proximity to Lagos, Nigeria's commercial and fintech hub, Ogun State's farming population has relatively high exposure to mobile phone networks, mobile money agents and social media-based commerce, providing a relevant context for examining online agricultural fraud and cyber-security awareness among small-scale farmers.

The study adopted a descriptive survey research design, considered appropriate for systematically describing farmers' characteristics, digital platform use, and fraud experience and cyber-security awareness. The population of the study comprised of all small-scale farmers in Ogun State, including farmers who have experienced online agricultural fraud and those who have not.

A multistage sampling procedure was used for the selection of respondents. Firstly, Ogun State was stratified into four agricultural zones namely Remo, Ijebu, Yewa/Awori and Egba (following ADP's zonal structure). Secondly, two local government areas were randomly selected from each zone. Thirdly, two communities were randomly selected from each of the chosen local government areas. Fourthly, 10 small-scale farming households who had experience online agricultural frauds were randomly selected from 16 communities totaling 160 respondents as sample size but only 150 questionnaire copies were recovered. A structured questionnaire was used as the main instrument for primary data collection. The instrument was divided into sections covering: (a) socio-economic characteristics of respondents, (b) use of digital/online platforms for agricultural transactions, (c) types and prevalence of online agricultural fraud experienced or perceived, measured through a checklist of fraud types drawn from the literature reviewed (d) cyber-security awareness and protective practices, measured using a Likert-type rating scale, and (e) constraints to the adoption of cyber-security practices. Reliability was established through a pilot test administered to a small sample of small-scale farmers outside Ogun State, with the resulting data subjected to Cronbach's alpha reliability analysis of 0.74.

Primary data were collected through the administration of the structured questionnaire/interview schedule by the researcher, with the assistance of trained enumerators and extension agents familiar with the study communities, to ensure clarity of interpretation, sensitivity in discussing fraud victimisation, and a high response rate. Secondary data were obtained from relevant published and unpublished sources, including ADP records, EFCC/NFIU advisories, journal articles and institutional reports, to support the background and literature review sections of the study. Data collected were analysed using both descriptive and inferential statistics. Descriptive statistics, including frequency counts, percentages, means and standard deviation, were used to summarise respondents' socio-economic characteristics, digital platform use, and fraud experience and cyber-security awareness. Inferential statistics was used to test the study's hypotheses 1, 2, 3 and 4 were tested using PPMC.

3. Results and Discussions

3.1 Socio-economic characteristics of the small-scale farmers in Ogun State

The results in Table 1 present the socio-economic characteristics of the small-scale farmers in which the majority of respondents were male (64.0%), 30.7% were within the middle age bracket (41–50 years), 87.3% had formal education, and 36.7% had between 11 and 20 years of farming experience, 41.3% cultivating between 1 and 2 hectares of farmland. Notably, about three-quarters (74.7%) of the total respondents reported owning a smartphone, indicating a farming population with substantial exposure to mobile-based digital platforms and, correspondingly, to online fraud risk. This result supports the findings of Ajayi (2024) who found out that both male and female farmers are prone to online agricultural frauds and there is need for individual farmers to protect themselves against online frauds that may request for their personal data.

3.2 Frequency of use of digital/online platforms among the small-scale farmers in Ogun State

The results in Table 2 show that the respondents' frequency of use of different categories of digital/online platforms. 59.3% frequently used mobile money/bank transfer apps, 50.7% frequently used social media-based produce/input trading are the most frequently used platform types, while 65.3% never used formal agric-investment/crowd-funding platforms and 50.7% never used online input marketplaces are used less frequently, though a non-trivial minority of respondents report at least occasional use of agric-investment platforms. This supports the findings of Nwachuwkwu (2025) and Nwosu (2022) who found out that rapid growth of mobile money, social media-based agricultural marketing and agric-investment/crowd-funding platforms in Nigeria, the well-documented collapse of numerous agric-crowd-funding platforms into fraud and Ponzi-scheme allegations from around 2020 onward, and the need for location-specific evidence on how cyber-security awareness relates to small-scale farmers' vulnerability to online agricultural fraud.

3.3 Types and perceived prevalence of online agricultural fraud experienced by farmers in Ogun State

The results in Table 3 present the types and perceived prevalence of online agricultural fraud, 24.0% personally experienced phishing messages/calls impersonating banks or mobile-money providers, 20.7% fake input-seller scams show the highest rates of personal victimisation, while awareness of fraudulent agric-investment schemes (whether personally experienced or known through a victim) is reported by a majority of respondents, consistent with the scale of

Table 1: Socio-economic Characteristics of Respondents

Variable	Category	Frequency	Percentage
Sex	Male	96	64.0
	Female	54	36.0
Age	≤ 30 years	22	14.7
	31–40 years	41	27.3
	41–50 years	46	30.7
	51–60 years	27	18.0
	> 60 years	14	9.3
Educational Level	No formal education	19	12.7
	Primary education	34	22.7
	Secondary education	66	44.0
	Tertiary education	31	20.7
Farming Experience	≤ 5 years	24	16.0
	6–10 years	39	26.0
	11–20 years	55	36.7
	> 20 years	32	21.3
Farm Size	< 1 hectare	58	38.7
	1–2 hectares	62	41.3
	> 2 hectares	30	20.0
Smartphone Ownership	Yes	112	74.7
	No (basic phone only)	38	25.3

Source: Field Survey, 2026

Table 2: Frequency of Use of Digital/Online Platforms for Agricultural Transaction

Platform Types	Frequently Used	Occasionally Used	Never Used
Mobile money/bank transfer apps	89 (59.3%)	41 (27.3%)	20 (13.4%)
Social media for buying/selling produce or inputs (WhatsApp, Facebook)	76 (50.7%)	48 (32.0%)	26 (17.3%)
Agric-investment/crowd-funding platforms	18 (12.0%)	34 (22.7%)	98 (65.3%)
Online marketplaces for farm inputs	29 (19.3%)	45 (30.0%)	76 (50.7%)

Source: Field Survey, 2026

Table 3: Types and Prevalence of Online Agricultural Frauds

Type of Online Fraud	Personally Experienced	Heard of/Know a Victim	Neither
Fraudulent agric-investment/crowd-funding scheme	22 (14.7%)	84 (56.0%)	44 (29.3%)
Fake input-seller scam (paid, goods not delivered)	31 (20.7%)	69 (46.0%)	50 (33.3%)
Fake produce-buyer scam	18 (12.0%)	58 (38.7%)	74 (49.3%)
Phishing messages/calls impersonating banks	36 (24.0%)	77 (51.3%)	37 (24.7%)
SIM-swap / unauthorised account access	14 (9.3%)	49 (32.7%)	87 (58.0%)

Source: Field Survey, 2026

agric-crowd-funding fraud reported at the national level. This is in line with the findings of Cohen & Felson (2024) reported that phishing messages/calls impersonating banks or mobile-money providers and fake input-seller scams were very common among rural farming households who had smartphones and were not aware of online agricultural frauds in eastern part of Nigeria.

3.4 Farmers' cyber-security awareness and the protective digital practices adopted in Ogun State

The results in Table 4 present that respondents showed (3.48) strong awareness of basic protective norms (such as not sharing PINs/OTPs) but weaker confidence in recognising phishing messages (2.44) and, notably, low awareness of where to report online fraud (2.15), suggesting reporting-channel awareness as a specific area for intervention. This agrees with the findings of EFCC, (2025) and NFIU (2025) who found out that there was a relatively high rates of awareness of, or personal experience with, fraudulent agric-investment schemes mirror the scale of agric-crowdfunding fraud documented at the national level and that numerous agriculture-branded companies as suspected Ponzi schemes.

Table 4: Farmers' Cyber-security Awareness and Protective Practices

Cyber-security Awareness/Practice Statement	Mean Score	Remark
I know that I should never share my PIN or OTP with anyone	3.48	Agree
I verify an investment opportunity before sending money	2.86	Agree
I use a strong/unique password for my mobile banking apps	2.61	Agree
I am confident I can recognise a phishing message	2.44	Disagree
I know where to report online fraud if it happens to me	2.15	Disagree

Source: Field Survey, 2026 (Strongly Disagree = 1 to Strongly Agree = 4), mean = 2.50

Table 5: Constraints to the Adoption of Cyber-security Practices as Perceived by Farmers

Constraints	Mean	Rank
Low digital/cyber-security literacy and technical understanding	3.55	1st
Extension agents rarely discuss online fraud/cyber-security during visits	3.40	2nd
Lack of a clear, accessible channel to report suspected online fraud	3.33	3rd
Cost/inaccessibility of smartphones with adequate security features	2.92	4th
Peer/social pressure to join popular agric-investment schemes	2.77	5th
Language barrier in security alerts/instructions from banks and apps	2.58	6th

Sources: Field Survey, 2026 (SD = 1 to SA= 4), mean = 2.50

Table 6: Hypotheses Testing

Hypotheses	Statistical Tool	Computed Value	P-value	Decision (α=0.05)
$H0_1$: Socio-economic characteristics vs. cyber-security awareness	PPMC	r = 0.31	0.004	Reject H0
$H0_2$: Vulnerability to frauds vs. cyber-security awareness	PPMC	r = -0.52	0.000	Reject H0
$H0_3$: frequent or infrequent platform users vs. cyber-security awareness	PPMC	r= 0.94	0.016	Reject H0
$H0_4$: Constraints to adoption of cyber-security practices	PPMC	r = -0.36	0.001	Reject H0

Source: Field Survey, 2026 5% level of significance

3.5 Constraints to the adoption of cyber-security practices among farmers in Ogun State

The results in Table 5 present that low digital/cyber-security literacy and technical understanding was ranked 1st (3.55), and the limited attention given to online fraud/cyber-security during routine extension visits was ranked 2nd (3.40) as the most severe constraints, followed by the absence of a clear, accessible channel through which farmers can report suspected online fraud was ranked 3rd (3.33). This is in consonance with the findings of NDPC (2025) and CBN (2025) who also identified low digital literacy and weak integration of cyber-security messaging into routine extension contact as leading constraints echoes concerns raised in the Ekiti State smart-farming cyber-security study and in grassroots digital-literacy initiatives documented in rural northern Nigeria, both of which emphasise the value of structured, community-based cyber-security training in reducing farmer victimisation.

3.6 Effect of cyber-security awareness and online agricultural frauds

The results in Table 6 summarise the effect of cyber-security awareness on farmers' vulnerability to online agricultural fraud; and results of the statistical tests conducted for the four null hypotheses 1-4 were rejected. Cyber-security awareness shows a significant correlation with respondents' socio-economic characteristics (r = 0.31, p = 0.004). This supports the findings of Nwosu (2022) who found out that age, education and experience are predictors of adoption and usage of digital technologies in agriculture. There is a negative correlation between respondents' vulnerability to frauds and cyber-security awareness (r = -0.52, p = 0.000). This corroborates the findings of Ajayi (2024) who found out that awareness and adoption of modern technologies are capable of boosting agricultural outputs. More so, there is a significant difference between frequent and infrequent platform users and cyber-security awareness (r = 0.94, p = 0.016), this finding agrees with the findings of Nwachuckwu (2025) who reported that platform users are more likely not vulnerable to online agricultural frauds because they can identify fraud messages. It also correlates with Cohen & Felson (2024) found out that farmers with greater "capable guardianship," in the form of cyber-security knowledge and protective practice, appear less likely to be victimised even where their exposure to digital platforms while constraints showed a negative correlation to the adoption of cyber-security practices (r = -0.36, p = 0.001) in the study area. This finding is in consonance with the findings of Davis (2021) who found out that farmers with higher cyber-security awareness report lower vulnerability to online agricultural fraud, that fraudulent agric-investment schemes and phishing scams are the most widely encountered fraud types, and that low digital literacy and weak integration of cyber-security content into extension services constitute the leading constraints to farmers adopting protective practices.

4. Conclusion

It is concluded that cyber-security awareness played a significant, protective role in curbing online

agricultural fraud among small-scale farmers in Ogun State, by reducing the likelihood that farmers' growing engagement with digital agricultural and financial platforms translates into actual fraud victimisation. However, the realised protective effect of cyber-security awareness is likely to be constrained by generally low digital literacy levels and by the limited extent to which cyber-security content is currently integrated into agricultural extension service delivery in the study area.

5. Recommendations

i. Agricultural extension organisations, including ADP, should integrate basic cyber-security/digital-literacy content covering topics such as recognising phishing messages, protecting PINs and OTPs, and verifying investment opportunities into routine extension training and farmer-group meetings in Ogun State.

ii. Financial regulators and law-enforcement agencies, including the Central Bank of Nigeria, the Securities and Exchange Commission and the Economic and Financial Crimes Commission, should collaborate with state agricultural agencies to disseminate targeted, farmer-friendly public-awareness materials (in local languages, where appropriate) warning against specific agric-investment fraud tactics and listing verified, legitimate agricultural investment/financing channels.

iii. A simplified, widely publicised channel (e.g., a toll-free helpline or USSD code) should be established or promoted for farmers to verify the legitimacy of an agric-investment opportunity and to report suspected online fraud, given the low awareness of reporting channels identified as a key constraint.

iv. Mobile network operators and financial service providers should strengthen consumer-facing security defaults (such as mandatory transaction alerts and simplified two-factor authentication) for the mobile money and banking products most commonly used by small-scale farmers.

v. Farmer cooperative and association structures should be leveraged as peer-to-peer channels for sharing verified information about agric-investment opportunities and warning members about specific scams circulating within the community, given the significant role of social networks in both spreading fraud and potentially countering it.

Acknowledgements

We want to thank the State Coordinator, zonal leaders and small-scale farmers under the Ogun State Agricultural Development Programmes for their unwavering supports and maximum cooperations before, during and after the data collection for this study.

References

Ajayi, D. (2024). Rising cases of digital fraud threaten Nigeria's financial inclusion goals. *Journal of technology and science*, 14 (3): 23-43.

Central Bank of Nigeria (CBN) (2025). Cyber-security awareness programme for financial institutions in Nigeria. CBN Publications 7: 1-10.

Cohen, L. E., & Felson, M. (2024). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4): 588–608.

Davis, F. D. (2021). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3): 319–340.

Economic and Financial Crimes Commission (EFCC). (2025). Public alert: List of suspected Ponzi scheme companies. Abuja: EFCC: 23-38. Retrieved July 21, 2026

Industrial Ransomware (2026). Cyber-security and Its Application to Industrial Analysis. IR Publication May 2026: 11-18.

Food Ingredients First (2025). Creating Cyber-security Awareness and Adoption. FIF Bullention July, 2025: 1-11.

Nigeria Financial Intelligence Unit (NFIU) (2025). Advisory on Ponzi schemes in Nigeria (Update). Abuja: NFIU: 25-43.

Nwachukwu, C. (2025). Accessing the impact of smart farming on cyber-security and food security among rural farmers in Ekiti State, Southwest Nigeria. (Conference/working paper): 54-78.

Nwosu, U. (2022). Socio-economic and technological factors influencing financial inclusion among indigenous peoples in Bauchi State, Nigeria: 22-35.

Nigeria Data Protection Commission (NDPC) (2025). Cyber Frauds Protection. NDPC Publication June 2025: 23-30.