International Journal of Agricultural Extension and Rural Development Studies, 13 (1),1-9, 2025
Print ISSN: ISSN 2058-9093
Online ISSN: ISSN 2058-9107
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Assessing Cybersecurity Awareness Among Farmers: A Survey-Based Analysis of Digital Access and Structural Barriers

A.B. Ale, F.O. Aladekomo, A.R. Akinnate and F. Oke
Department of Agricultural Science, Adeyemi Federal University of Education, Ondo, Nigeria
Corresponding author: aleab@afued.edu.ng

doi: https://doi.org/10.37745/ijaerds.15/vol13n119 Published March 14, 2026

Citation: Ale A.B., Aladekomo F.O., Akinnate A.R. and Oke F. (2026) Assessing Cybersecurity Awareness Among Farmers: A Survey-Based Analysis of Digital Access and Structural Barriers, *International Journal of Agricultural Extension and Rural Development Studies*, 13 (1),1-9

Abstract: The growing use of digital technologies in agriculture exposes farmers to increasing cybersecurity risks. This study assessed cybersecurity awareness among farmers in Ondo State, Nigeria, and examined factors associated with awareness levels. A cross sectional survey of 117 farmers was conducted using a structured questionnaire. Results show a moderate level of cybersecurity awareness (grand mean = 3.41). Farmers demonstrated stronger awareness of common cyber threats, particularly risks of sharing personal information online (mean = 4.07) and social media account compromise (mean = 3.94), but weaker knowledge of reporting cybercrime (mean = 2.57). Key challenges to safe digital participation include limited digital safety knowledge (mean = 2.47), poor internet connectivity (mean = 2.45), and irregular power supply (mean = 2.37). Chi square analysis indicated that awareness differed significantly across age groups ($\chi^2 = 26.19$, $p = 0.003$). Multiple regression showed no statistically significant independent predictors. The findings highlight the need for practical digital safety training and improved rural digital infrastructure.

Keywords: cybersecurity awareness, rural farmers, digital access, structural barriers, Nigeria

INTRODUCTION

Digital technologies are becoming deeply embedded in agricultural livelihoods. Farmers increasingly use mobile phones, internet platforms, digital payment systems, and online advisory services to access markets, financial services, climate information, and extension support. These tools create important opportunities for productivity, inclusion, and resilience. At the same time, they expose rural populations to rising cybersecurity risks such as phishing attacks, identity theft, financial fraud, misinformation, and data breaches (Kshetri & Voas, 2022).

Cybersecurity awareness refers to the knowledge and everyday practices that enable individuals to recognize digital threats and protect themselves online. It is now a critical requirement for safe participation in the digital economy. However, preparedness remains uneven, particularly in rural and agricultural communities where digital adoption often advances faster than digital safety capacity.

Recent global assessments emphasize that human vulnerability remains one of the most persistent cybersecurity weaknesses. Limited user awareness, unsafe digital behavior, and poor knowledge of reporting mechanisms continue to increase exposure to cyber risks (European Union Agency for Cybersecurity [ENISA], 2022).

Cybersecurity readiness is shaped not only by individual knowledge but also by broader structural conditions. Access to reliable internet, affordability of connectivity, digital literacy, and institutional support systems influence how individuals engage with digital technologies and manage cyber risks (Organisation for Economic Co-operation and Development [OECD], 2023). Where infrastructure is unreliable and digital skills are limited, exposure to online threats increases.

These challenges are especially visible in agricultural communities. The rapid growth of digital agriculture, mobile money systems, precision farming tools, and online produce markets has expanded farmers' digital footprints. At the same time, rural users often operate in resource constrained environments characterized by weak connectivity, unstable electricity supply, and limited training opportunities (Food and Agriculture Organization [FAO], 2022; International Telecommunication Union [ITU], 2022). These conditions restrict the ability of farmers to adopt secure digital practices.

Emerging research shows that agriculture is becoming an increasingly attractive target for cybercrime due to its growing reliance on connected technologies and digital supply chains. Disruptions to digital systems can threaten farm operations, financial transactions, food logistics, and market access (Kshetri & Voas, 2022). Studies also note that small scale farmers face disproportionate risks because they often lack cybersecurity training and institutional support (Chaudhary et al., 2023).

Capacity building and institutional support play an essential role in strengthening digital safety in rural sectors. Practical digital literacy programs, community based training, and extension services have been shown to improve secure technology use and digital confidence (United Nations Development Programme [UNDP], 2023). Hands on learning approaches are consistently more effective than passive awareness campaigns in promoting safer online behavior.

Specifically, the study:

i. examined relationships among digital access, structural barriers, intervention support, and cybersecurity awareness
ii. assessed whether awareness differs across demographic groups
iii. identified the strongest predictors of cybersecurity awareness using multivariate regression analysis

RESEARCH METHODS

This study employed a quantitative cross-sectional survey design to investigate the predictors of cybersecurity awareness among farmers. A multi-stage sampling method was used. From each of the three agroecological zones in the state, 4 communities were randomly selected, and ten farmers were randomly selected making a total of 120 respondents. However only 117 interviews scheduled

The instrument comprised closed-ended items organized into five domains: demographic characteristics, cybersecurity awareness, digital access and exposure, structural barriers, and intervention and support measures. Cybersecurity awareness was measured using multiple indicators assessing knowledge of cyber threats and protective practices, including phishing awareness, safe mobile banking behavior, password security, identification of fraudulent digital portals, public Wi-Fi risk awareness, reporting of cybercrime, and awareness of government cybersecurity initiatives.

Digital access and exposure variables captured access to internet-enabled devices, internet use frequency, digital literacy, extension service exposure, peer influence, education-related capacity, and affordability of data services. Structural barriers assessed infrastructural and capacity constraints such as poor internet connectivity, unreliable power supply, high costs of digital services and secure devices, limited digital safety knowledge, etc. Intervention measures evaluated the perceived importance of capacity-building initiatives, including extension-based training, digital literacy programs, mobile cybersecurity alerts, local-language awareness campaigns, affordable secure devices, and broadcast media campaigns. Most variables were measured using five-point Likert-type scales.

Data analysis was conducted using statistical software and spreadsheet tools. Descriptive statistics, including means and standard deviations, were used to summarize response patterns. Internal consistency of multi-item constructs was assessed using Cronbach's alpha reliability coefficients. Pearson correlation analysis examined associations among the major constructs. Group differences in cybersecurity awareness were tested using an independent samples t-test (gender) and one-way analysis of variance (education level). Multiple linear regression analysis was performed to identify predictors of cybersecurity awareness, with the model specified as:

$$Awareness = \beta 0 + \beta 1(Access) + \beta 2(Barriers) + \beta 3(Interventions) + \beta 4(Education) + \beta 5(\text{Internet Use}) + \varepsilon$$

where Awareness represents the cybersecurity awareness index; Access denotes digital access conditions; Barriers represents the structural constraints index; Interventions captures support and capacity-building measures; Education represents education level; Internet Use reflects usage frequency; β_0 is the intercept; β_1–β_5 are regression coefficients; and ε is the error term. Additionally, a chi-square test of independence assessed the association between gender and internet use frequency. Participation was voluntary, and respondents were informed of the study purpose and assured of confidentiality.

RESULTS AND DISCUSSION

Frequency of Use of the Internet

The frequency of internet use, as shown in Figure 1, revealed that 67% of the Farmers use the Internet for one reason or another, indicating that cybersecurity knowledge would be beneficial to them. Notably, 17% of the respondents never use the internet. It is therefore necessary to raise awareness of the many advantages they could gain from accessing the internet.

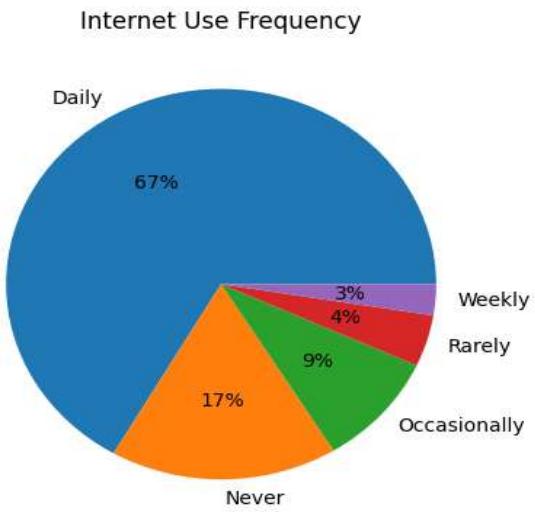

Figure 2: Frequency of Internet Use Source: Field survey, 2025

Engagement with Online Activities

The results from Figure 2 Figure 2 shows farmers' use of online facilities. Email (70.9%) and mobile banking or e-wallet services (78.6%) are the most widely used platforms. Social media and messaging services are also common, used by 63.2% of respondents, while 58.1% engage in e-commerce and online market activities. In contrast, the use of more formal digital services is limited. Only 36.0% use government or NGO portals, and cloud storage or online backup services have the lowest usage at 15.4%. Overall, farmers rely more on communication and financial platforms than on formal information systems and data protection tools.

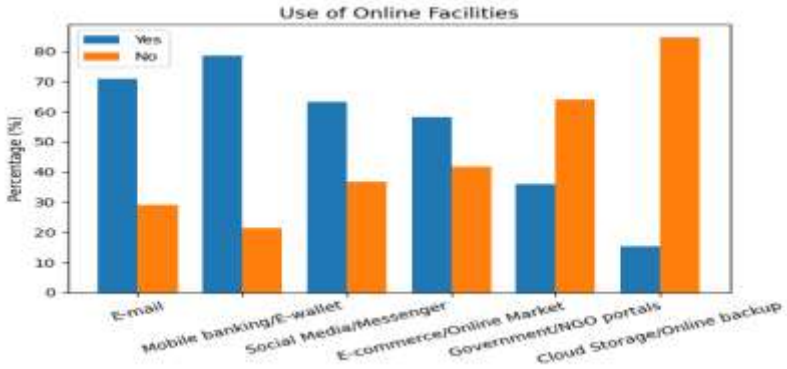

Figure 2: Dichotomous Response Distribution for the Use of Online Facilities for Agricultural or Personal Activities Source: Field survey, 2025

Perceived Factors Influencing Cybersecurity Awareness

Table 1 shows a moderate overall level of cybersecurity awareness among farmers (grand mean = 3.41). Respondents demonstrate stronger awareness of common and experience-based risks, particularly the dangers of sharing personal or banking information online (mean = 4.07) and the possibility of social media account compromise (mean = 3.94). Awareness of general cybersecurity

concepts, phishing scams, and public Wi-Fi risks is also relatively high. In contrast, knowledge of formal procedures and practical protective skills is weaker. Awareness of how to report cybercrime records the lowest score (mean = 2.57), while understanding of strong password management and mobile banking protection remains modest. This pattern suggests that farmers are more familiar with widely publicized cyber threats than with institutional processes and advanced safety practices. Similar trends have been reported in rural digital user studies, where experiential awareness exceeds procedural cybersecurity knowledge (ENISA, 2022; ITU, 2022; Kshetri & Voas, 2022).

Table 1: Cybersecurity Awareness Levels Among Farmers

Item	Mean	SD
I understand what cybersecurity means	3.70	1.08
I am aware of email scams and phishing messages	3.63	1.10
I know how to protect my mobile banking or e-wallet app	3.42	1.11
I know my social media accounts can be hacked	3.94	0.98
I can identify fake grant or registration portals	3.52	1.10
I am aware that using a public Wi-Fi can expose my data.	3.74	1.12
I understand how to create and manage a strong password.	3.45	1.17
I am aware of how to report a cyberattack or online fraud.	2.57	1.23
I am aware of the risks of sharing personal / banking information with strangers online	4.07	0.92
I am aware of government or agricultural agencies promoting cybersecurity awareness.	3.21	1.20
Grand Level of Awareness ($\bar{x}$)	**3.41**	**1.23**

Source: Field survey, 2025

Factors Influencing Cybersecurity Awareness

Table 2 highlights key factors influencing cybersecurity awareness among smallholder farmers. Digital literacy level emerged as the most important factor, followed closely by education level and access to internet-enabled devices. This confirms that awareness is strongly linked to users' ability to understand and navigate digital technologies safely. Exposure to extension agents also plays a significant role, suggesting that agricultural extension services can serve as effective channels for cybersecurity education. Peer influence further indicates that farmers learn cybersecurity behaviors through social interactions within their communities. Conversely, the relatively lower importance attached to the cost of data suggests that awareness is more constrained by skills and knowledge than by financial barriers alone. These findings support earlier research emphasizing the role of education, training, and institutional support in cybersecurity awareness (ITU, 2022).

Table 2: Perceived Importance of Factors Influencing Cybersecurity Awareness Among Farmers

Factor	Mean	SD
Access to internet-enabled phones	4.15	0.86
Education level	4.31	0.74
Exposure to extension agents	4.17	0.82
Peer/farmer influence	3.79	0.92
Cost of data	3.52	1.03
Digital literacy level	4.35	0.86

Source: Field survey, 2025 (VI – Very Important; I – Important; N – Neutral; LI – Less Important)

Challenges to the Adoption of Cybersecurity Practices

Table 3 highlights the main challenges limiting farmers' adoption of cybersecurity practices. The most severe constraint is limited digital safety knowledge (mean = 2.47), followed closely by poor internet connectivity (mean = 2.45) and irregular power supply (mean = 2.37). These findings indicate that both skill gaps and infrastructural weaknesses hinder safe digital participation. Financial barriers, including the high cost of data services and secure devices, are also notable constraints, alongside the lack of farmer-focused cybersecurity training. Language and literacy barriers present additional difficulties, while shame in reporting cyber fraud is the least severe challenge. The results show that cybersecurity adoption is constrained more by knowledge and infrastructure gaps than by social stigma. Similar barriers to safe digital engagement in rural communities have been widely documented (FAO, 2022; ITU, 2022; World Bank, 2021).

Table 3: Challenges Confronting the Adoption of Cybersecurity practices in the study area (ranked in descending order of severity)

Constraint	Mean	SD
Limited knowledge of digital safety	2.47	0.62
Poor internet connectivity	2.45	0.64
Irregular power supply	2.37	0.68
High cost of data/services	2.18	0.80
High cost of secure devices	2.17	0.80
Lack of farmer-focused cybersecurity training	2.18	0.77
Language/literacy barriers	1.99	0.85
Shame in reporting cyber fraud	1.92	0.86

Source: Field survey, 2025 *(NC – Not a Constraint; MC – Mild Constraint; SC – Severe Constraint)*

Socioeconomic Differences in Cybersecurity Awareness

The chi square results show that age is the only socioeconomic factor significantly linked to cybersecurity awareness ($\chi^2 = 26.192$, $p = 0.003$), meaning awareness differs across age groups. This suggests that younger farmers may feel more confident using digital tools, while older farmers may depend more on informal learning and past experience. Similar age related patterns in digital skills and online safety behavior have been widely reported (OECD, 2023; ITU, 2022). In contrast, awareness does not differ significantly by sex, education level, or farming experience. Male and female farmers show comparable understanding of cybersecurity, reflecting evidence that gender gaps in digital competence are narrowing as mobile access expands (UNDP, 2023). The weak role of formal education also suggests that schooling alone does not guarantee practical cybersecurity knowledge, since digital safety skills are rarely emphasized in general curricula (ENISA, 2022).

Table 4: Association Between Socio-economic Characteristics and Cybersecurity Awareness

Variables	Chi-square	df	p-value
Age vs Awareness	26.192	10	0.003
Sex vs Awareness	0.628	2	0.730
Education vs Awareness	8.401	8	0.395
Farming Experience vs Awareness	2.555	6	0.862

Source: Field survey, 2025

Multivariate Analysis of Factors Associated with Cybersecurity Awareness

The multiple regression results provide important insight into the factors shaping cybersecurity awareness among farmers. While the overall model indicates that respondents demonstrate a meaningful baseline level of awareness, none of the examined predictors showed statistically significant independent effects. Digital access, which is often assumed to strengthen online safety, displayed a small negative and non significant relationship with awareness, suggesting that having internet access or digital devices alone does not necessarily translate into safer digital behavior. This supports growing evidence that connectivity without adequate digital safety training can increase exposure to cyber risks rather than reduce them (OECD, 2023; ITU, 2022). Structural conditions showed a weak positive association after reverse coding, implying that fewer infrastructural and capacity constraints may slightly support awareness development, although the effect remains limited. This aligns with research highlighting how unreliable connectivity and power supply continue to hinder secure digital participation in rural settings (FAO, 2022).

Institutional interventions, including training programs and awareness initiatives, also demonstrated minimal influence, reinforcing findings that passive or irregular programs rarely produce measurable improvements unless they are practical, continuous, and locally relevant (UNDP, 2023). Education level and internet use frequency similarly exhibited small, non significant effects, indicating that general schooling and time spent online do not automatically build cybersecurity competence. Prior studies note that digital experience without guided learning can normalize unsafe practices rather than

improve protective behavior (Kshetri & Voas, 2022), and that formal education does not always include digital safety skills (ENISA, 2022). Taken together, the results suggest that cybersecurity awareness in agricultural communities is shaped by a broader mix of social, contextual, and experiential factors that extend beyond infrastructure and access alone. Improving preparedness therefore requires integrated strategies that combine hands on digital safety training, community based learning approaches, continuous engagement, and context specific risk communication tailored to rural users.

Table 5: Multiple Regression Analysis of Factors Associated with Cybersecurity Awareness

Predictor	Coef.	Std.Err.	t	P>|t|	[0.025	0.975]
Intercept	3.250	0.650	4.996	0.000	1.961	4.539
Access	-0.106	0.115	-0.923	0.358	-0.333	0.121
Barriers	0.069	0.117	0.592	0.555	-0.162	0.300
Interventions	0.019	0.110	0.176	0.861	-0.198	0.236
Education_level_factor	0.047	0.045	1.044	0.299	-0.042	0.136
Internet_use	0.007	0.026	0.285	0.776	-0.044	0.058

Source: Field survey, 2025

CONCLUSION AND RECOMMENDATIONS

The study shows that farmers are increasingly using digital technologies for farming and daily activities. While many respondents are aware of common cyber threats, gaps remain in practical areas such as reporting cybercrime and applying strong security practices. Ongoing challenges including poor internet connectivity, unstable electricity, limited digital safety knowledge, and high device costs make safe online participation difficult. Awareness also varies across age groups. Overall, digital engagement among farmers is growing faster than their preparedness to stay safe online.To strengthen cybersecurity awareness among farmers the following recommendations are made:

- Organize regular, practical training on digital literacy and online safety
- Use agricultural extension services to deliver hands-on cybersecurity education in local languages
- Improve rural internet connectivity and electricity supply
- Promote access to affordable and secure digital devices
- Encourage collaboration among government, extension agencies, farmer groups, and technology providers

REFERENCES

Chaudhary, P., Rehman, A., & Alotaibi, Y. (2023). Cybersecurity challenges in smart agriculture: Risks, vulnerabilities, and protection strategies. *Computers and Electronics in Agriculture, 205*, 107630.https://doi.org/10.1016j.compag.2022.107630

European Union Agency for Cybersecurity. (2022). *Cybersecurity skills development in the EU*. Publications Office of the European Union. https://doi.org/10.2824/834686

Food and Agriculture Organization of the United Nations. (2022). *The state of food and agriculture 2022: Leveraging automation in agriculture for transforming agrifood systems*. FAO. https://doi.org/10.4060/cb9479en

International Telecommunication Union. (2022). *Global cybersecurity index 2021*. ITU Publications. https://doi.org/10.35917/9789210015054

Kshetri, N., & Voas, J. (2022). Securing the agriculture sector's expanding digital footprint. *Computer, 55*(4), 78–83. https://doi.org/10.1109/MC.2022.3142877

Organisation for Economic Co-operation and Development. (2023). *OECD digital economy outlook 2023*. OECD Publishing. https://doi.org/10.1787/b1e5cced-en

United Nations Development Programme. (2023). *Digital strategy 2022–2025: Building inclusive digital ecosystems*. UNDP. https://doi.org/10.18356/789210021543

World Bank. (2021). *World development report 2021: Data for better lives*. World Bank. https://doi.org/10.1596/978-1-4648-1600-0