

Assessment of Cybersecurity Practices in Electronic Banking among Agro-Entrepreneurs in Obio/Akpor L.G.A, Rivers State, Nigeria

Ugwuja V.C* and Ekpo M. E

*Department of Agricultural Economics and Extension, University of Port Harcourt, Nigeria
Corresponding author**

Abstract: The study assessed cyber security practices adopted by agro-entrepreneurs in Obio/Akpor L.G.A, Rivers State. The specific objectives were to describe the socio-economic characteristics of agro-entrepreneurs in Obio/Akpor L.G.A, identify electronic banking products accessed by agro-entrepreneurs, ascertain fraud experiences of agro-entrepreneurs in accessing electronic banking products, identify cybersecurity control measures adopted by agro-entrepreneurs, and to ascertain factors that influence level of adoption of cybersecurity measures among agro-entrepreneurs. Data were collected with the aid of structured questionnaire, administered on 90 respondents using two-stage sampling procedure. The data were analyzed with the use of descriptive statistics and regression analysis. The finding showed that 83.3% of the respondents were male, 43.3% of the respondents were in the age bracket of 31-40 years, and married agro entrepreneurs were 71.1%. Electronic banking products mostly utilized by the respondents were SMS Alert, online fund transfer, balance enquiry, Debit card and Automated Teller machine (ATM). Agro-entrepreneurs experienced risks of unsuccessful transaction through POS in which their accounts were debited, they also experienced threats such as smishing in which they released their banking details through SMS and money was debited from their account. Agro-entrepreneurs adopted cybersecurity measures such as avoiding lonely ATM, ignoring text messages and email that request for banking details. Also, the regression result on the rate of adoption of cybersecurity measures by agro entrepreneurs indicate that farming status, cooperative membership, annual income and internet access were significant factors influencing rate of adoption of cybersecurity measures. The study recommends that Central Bank of Nigeria should impose on banks with the responsibility of educating customers deeply not only superficially on the risk involved in electronic banking, and banks should provide financial products and services that will expose customers to mild risks.

Keywords: Electronic banking; Cybersecurity; Agro-entrepreneurs; Financial Products and Services

I. INTRODUCTION

Agriculture is a major contributor to Nigeria's gross domestic product (GDP) and small scale agro-entrepreneurs play a dominant role in this contribution (Mgbenka et al 2015). Agro-entrepreneurship is the process of backward or forward value addition whereby farmers use creative ways of improving the quality and quantity of agricultural produce or get involved in agro-based industry

activities. These creative ways are usually enhanced by the use of Information and Communication Technology (ICT).

The term ICT according to Zuppo (2012), can be defined as a combination of communication applications, procedures and devices that include phones, computer and network hardware and software. Information and communication technologies have been implemented in various sectors in the economy such as the education sector, health care, financial sector to aid in service delivery. Information communication and technology has been customized over the years to fit in all sectors as it is needed based on the services that each sector provides.

According to (Reynolds et al, 2003), human beings are transitioning from manual operations to increasing dependence on digital communication and other innovations in the information and communication industry. In the financial sector ICT has been influential in enabling financial institutions in extending its services through financial inclusion of people unreachable by this services and also diversifying its services (Pilat & Van 2003). Agboola (2007) noted that in this day an era of people which includes Agro-entrepreneur can now access simple services such as cash deposit and withdrawal, payment of bills and payment of other daily services from their phones, computers and other electronic devices that are being developed on a daily basis. Therefore, connectivity has enabled people to access market information, and relevant services which is helping to make life easier for people.

Information communication technology has contributed to the concept of global economic shrinkage in terms of allowing connectivity for people from any point on the globe (Avgerou, 2003). Today, businesses and financial institutions that invest heavily in information and communication technology have a competitive edge in terms of being more productive, growing faster, more investment opportunities and more profits (Agboola 2007). This has birthed electronic banking.

Electronic banking (e-banking) is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic and interactive communication channels. E-banking includes the systems that enable financial institutions, customers, individuals or

businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet. Customers access e-banking services using intelligent electronic devices, such as a personal computer (PC), personal digital assistant (PDA), smart phones/tablets, automated teller machine (ATM), kiosk, or Touch Tone telephone. The electronic banking services are aimed at improving the market share and business growth of the financial industry.

Kshetri (2005) explained that despite all the benefits accruing to the extensive usage of information technologies, the increased dependency on it has also translated into a growing rate of criminal activities conducted via the same ICT platforms. The major problem of electronic banking is that it has so much associated risks. Empirical evidence has shown that cyber risks that are of most concern to Digital financial service (DFS) providers are insider and third-party threats, data breaches, identity theft, and system downtimes (CGAP 2018). Risks in internet banking are more diversified and there is an effect of risk intensification, it could then be seen that risks in online finance are more difficult to avoid (Gujun, 2013). Given the risks in digital finance, the risk control and management procedures must be strengthened, otherwise, the existence and further development of electronic banking will be severely threatened. Schaeffer (2009) stated that prior to the year 2001, the phenomenon of cyber-crime was not globally associated with Nigeria. This resonates with the fact that in Nigeria we came into realization of the full potential of the internet right about that time. Since then, however, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet. Kshetri(2005) reported that while organizations and individuals are exploiting its business benefits, they may not realize that cyberspace confers the same benefits on those who wish to attack them. Therefore, it is pertinent to study how agro-entrepreneurs have been affected by these risks and the strategy they are using to combat it, hence the need for the study.

II. OBJECTIVES OF THE STUDY

The general objective of the study was to assess cyber-security practices adopted by agro-entrepreneurs for safer banking. The study was specifically carried out to;

- i. Describe the socio-economic characteristics of agro-entrepreneurs in Obio/Akpor L.G.A.
- ii. Identify electronic banking products accessed by agro-entrepreneurs in the study area.
- iii. Ascertain fraud experiences of agro-entrepreneurs in accessing electronic banking services in the study area.
- iv. Identify cybersecurity control measures adopted by agro-entrepreneurs in the study area.
- v. Ascertain factors that influence adoption of cybersecurity control measures among agro-entrepreneurs in the study area.

Hypothesis of the Study

H_0 : There is no significant relationship between socio-economic characteristics of agro entrepreneur and rate of adoption of cybersecurity measures.

III. METHODOLOGY

The study was conducted in Obio/Akpor Local government area in River state. The people in the area are involved in agriculture in its different forms ranging from farming, processing of agro-products, and buying and selling of agro-products. The population of the study included all the agro-entrepreneurs who accessed electronic banking products in Obio/Akpor LGA. A two-stage sampling procedure was employed in the selection of the respondents for this study. The first stage was a purposive selection of three communities based on high concentration of economic activities which are agro- based and availability of financial institutions. The second stage was a purposive selection of 30 agro-entrepreneurs that are accessing electronic banking products from each community,. making-up a total of 90 agro-entrepreneurs for the entire study. Data for this study were collected from primary source with the aid of structured questionnaire. Descriptive statistics and regression model were used to achieve the objectives of the study.

Model Specification

Ordinary Least Square Regression analysis was used to test for significant relationship between socioeconomic characteristics of the agro entrepreneurs and the rate of adoption of cyber-security measures. The implicit form of the linear regression is

$Y = f(X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8, X_9) + e$, where Y will be = Rate of adoption of cyber-security measures

Y was derived as $U/V \times 100$,

U=Number of cyber-security measures adopted by an agro entrepreneur

V= Total number of cyber-security measures

X_1 = Age (Years)

X_2 = Household Size (Number)

X_3 = Educational Status (Years)

X_4 = Marital Status (Years)

X_5 = Farming status (Full-time= 1, Part-time= 0)

X_6 = Cooperative Membership (Dummy; Yes =1, No=0)

X_7 = Business experience (Years)

X_8 = Internet access (Dummy; Yes= 1, No= 0)

X_9 = Annual income (Naira)

X_{10} = Extension Services

e = Stochastic error term.

The relationship between the dependent and each of the independent variable was examined using the four functional forms, Linear, semi-log, Exponential and double-log

Linear function: $Y = \beta_0 + \beta_1X\beta_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \beta_5X_5 + \beta_6X_6 + \beta_7X_7 + \beta_8X_8 + \beta_9X_9 + \beta_{10}X_{10} + e$

Exponential function: $Y = \beta_0 + \beta_1\log X\beta_1 + \beta_2\log X_2 + \beta_3\log X_3 + \beta_4\log X_4 + \beta_5\log X_5 + \beta_6\log X_6 + \beta_7\log X_7 + \beta_8\log X_8 + \beta_9\log X_9 + \beta_{10}\log X_{10} + e$

Semi-log function: $\log Y = \beta_0 + \beta_1X\beta_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \beta_5X_5 + \beta_6X_6 + \beta_7X_7 + \beta_8X_8 + \beta_9X_9 + \beta_{10}X_{10} + e$

Double Log function: $\log Y = \beta_0 + \beta_1\log X\beta_1 + \beta_2\log X_2 + \beta_3\log X_3 + \beta_4\log X_4 + \beta_5\log X_5 + \beta_6\log X_6 + \beta_7\log X_7 + \beta_8\log X_8 + \beta_9\log X_9 + \beta_{10}\log X_{10} + e$

Where B_0 =intercept

B_1 to B_{10} =Estimated coefficients.

IV. RESULTS AND DISCUSSION

Socio economic characteristics of agro-based entrepreneurs

The result showed a higher ratio for males than females, which showed that 83.3% of the respondents were male while 16.7% of the respondents were females. The study also revealed that 43.3% were in the age bracket of 31-40 years, while 28.9% were in the age bracket of 41-50 years. Most of the respondents been within the age brackets of 31-40 years, indicates that they are in their middle active ages of production. Married individuals were the highest among the respondents with the percentage of 71.1%,while 28.9% were single.

A breakdown of the educational status indicated that 14.4% had secondary education while 85.6% had attained tertiary education, and this was the highest level of education attained. About 72.2% had a family size of 1-4, while 27.8% had a family size of 5-8 which showed that the family size of 1-4 were the most dominant in the study area hence had the highest frequency. The respondents which were into full-time farming were the most dominant in the study with a percentage of 84.4% while 15.6% were part-time agro entrepreneurs. About 24.4% were into crop production, 6% were into agro-processing, 4.4% were into livestock, 2.2% were into agricultural produce marketing, 4.4% were into agricultural service while 57.8% where into fish farming.

Table 1 shows the result of the socio-economic characteristics of agro-based entrepreneurs.

Table 1: Distribution of Farmers Socio-economic Characteristics

Socio economic characteristics	Frequency (n=90)	Percentage (%)
Gender		
Male	75	83.3
Female	15	16.7

Age		
21-30	6	6.7
31-40	39	43.3
41-50	26	28.9
51-60	15	16.7
61-70	4	4.4
Marital status		
Single	26	28.9
Married	64	71.1
Level of educational status		
Primary	0	0.0
Secondary	13	14.4
Tertiary	77	85.6
Family size		
01-Apr	65	72.2
05-Aug	25	27.8
Farming status		
Full time	76	84.4
Part time	14	15.6
Enterprise type		
Livestock	4	4.4
Crop	22	24.4
Agro processing		
Fish Farming	52	57.8
Agricultural produce marketing	2	2.2
Agricultural service	4	4.4
Business experience		
01-May	64	71.1
06-Oct	24	26.7
Nov-15	2	2.2
Average annual income (₦)		
50,000-150,000	8	8.9
151,000-250,000	8	8.9
251,000-500,000	33	36.7
501,000-1,000,000	20	22.2
1,000,000 & above	21	23.3
Annual savings (₦)		
50,000-150,000	34	37.8
151,000-250,000	21	23.3
251,000-500,000	17	18.9
501,000-1,000,000	18	20

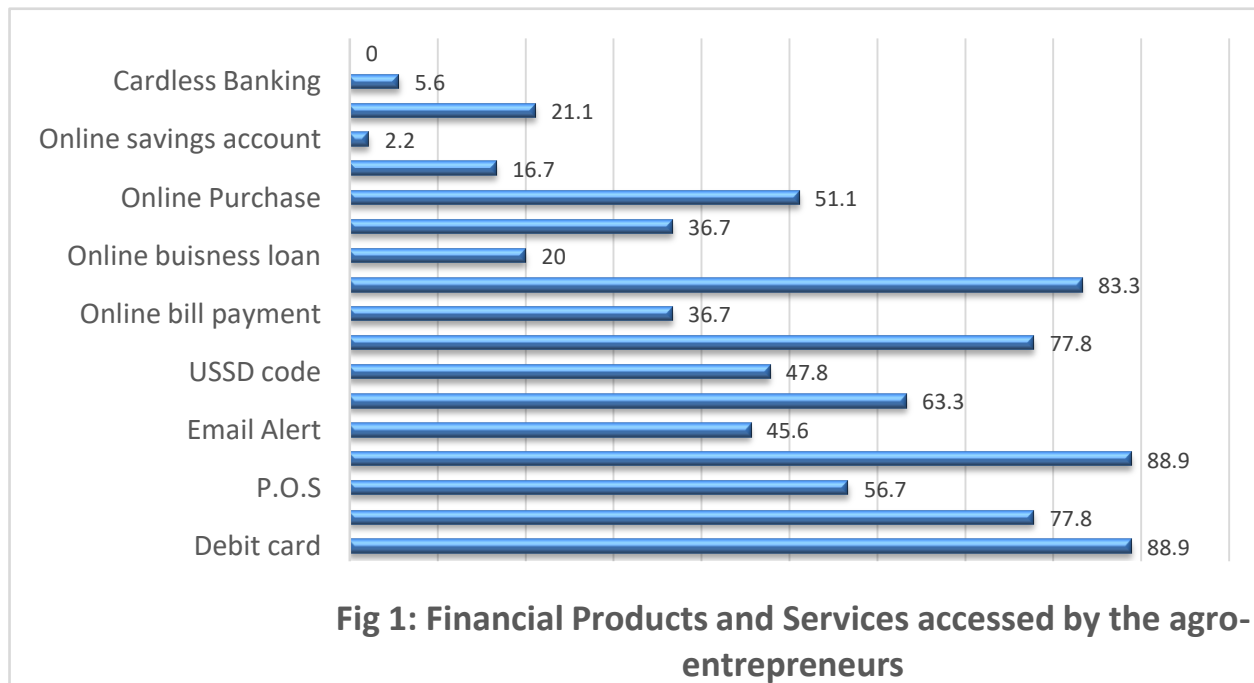
Source: Field survey (2019)

Various financial products and services used by agro entrepreneurs

Figure 1 shows the responses of agro-entrepreneurs on access to digital financial products. Majority (88.9%) of the respondents indicated accessing ATM/Debit cards, this agrees with the report of EFINA, (2016) who stated that 76.2% of banked population in Nigeria have ATM/Debit cards. SMS Alert services (88.9%) were also highly accessed by the respondents. Majority of the agro-entrepreneurs also indicated to be using Automated Teller Machine (77.8%), POS (56.7%), Balance inquiry (88.3%) and Online Fund Transfer (77.8%)

Analysis from the results also shows that the respondents moderately accessed these digital financial products; Email alert (45.6.0%), Online Bill Payment (36.7%), E-Statement (49.8%) and Online Purchases (51.1%). The following are the least accessed products as indicated by the respondents; Remittances (21.0%), Online loan (20.0%), Online Deposit Account (20.9%), Online Savings Account (2.2%) and Micro-insurance (16.7%). This corroborates the findings of EFINA, (2016) who reported that Online Savings account and Insurance are least accessed by banked population in Nigeria.

Various financial products and services accessed by agro entrepreneurs



Risks experienced by agro-entrepreneurs in accessing electronic banking products and services

The risks faced by agro entrepreneurs is summarized in Table 2, with 75.6% of the respondent stating the difficulty and delays in completing transactions with the aid of the USSD-based mobile banking, as a result of this, farmers are left with no other option than going to the bank facility. This is followed closely by 66.7% who complained that they had received text messages requesting that they provide their bank details for an urgent solution and after giving out their details, money was withdrawn afterwards from their accounts. The rate of cyber-crime is growing on a high scale and it is being marked as one of the major source of financial instability in business and enterprises. Also in addition to this risk statement 55% complained about the unsuccessful transactions while using Point of Sales (POS).

About 16.7% of the respondent indicated that they were accosted by criminals immediately after withdrawal from automated teller machines (ATM), this is as a result of the fact that they go to the ATM at odd hours when it will be free to be used due to long queue thereby making them susceptible to hoodlums and criminals. Also about 53.3% of the agro entrepreneurs in the study area further said that they have fallen victim to text messages from criminals who claimed that their ATM card is expired or due for renewal, requesting for the sensitive security numbers on the card from which their money was withdrawn, while 21.1% of the respondents also agreed that they have suffered from failed transactions when using their banking application attributed to failed network where their accounts were wrongly debited. About 60% of the respondents indicated that their ATM cards were accessed by third party and it has been suggested that lack of security in protecting personal information is a problem in

using internet banking according to the research carried out by Yousafzai, Pallister, and Foxal, (2003). Furthermore, 61.1% suffered unsuccessful transactions while using POS, and their money was wrongly debited. About 47.8% claimed to have received calls from unknown persons claiming to be their account managers or bank representatives requesting for some sensitive details that lead to the compromising of their account, while about 75.6% agreed that the error messages they get when trying to access their bank short code is not encouraging and it delays transactions. About 23.3% of the respondents reported that similar email address with that of the bank emailed them requesting for their details in order to perform upgrades from which accounts were hacked.

Table2: Risks experienced by agro entrepreneurs in accessing cyber security practices

Risks	Frequency	Percentage (%)
I received an email that looks similar to that of my bank requesting for my bank account details, through a link embedded in the email, which I did and thereafter money was withdrawn from my account.	21	23.3
I received a text message requesting urgently for my bank account details, and after giving the account details, money was withdrawn from my account.	60	66.7
I visited a malicious website resulting to the Exposure of my bank account details, which allowed Criminals to withdraw money from my account.	33	36.7
My ATM card was used by someone close to me to withdraw money from my account secretly.	54	60
After withdrawing money from an ATM,I was accosted by criminals who carted away with my money	15	16.7
I received a text message stating that my ATM card has been de-activated, and that to re-activate it I should call someone through a phone number provided in the message, which I did, and after providing my card details to the person for re-activation, money was withdrawn from my account.	48	53.3
I was trying to transfer money via my mobile application the transaction didn't go through due to network issues, but the money was debited from my account	19	21.1
Every time I try to make use of my bank's USSD code, I always get an error message before the transaction goes through.	68	75.6
I attempted making payment on POINT OF SALES (POS), the transaction wasn't approved, yet the money was deducted from my account	55	61.1
I received a call from an unknown person claiming to be a customer service representative of my bank, telling me that my online banking account have been temporally locked due to suspected unauthorized request for password change from someone, and that I should provide my account login details so they	43	47.8

can unlock the account, which I did, and thereafter money was withdrawn from my account.		
--	--	--

Field survey, 2019

Cyber security measures adopted by agro-entrepreneurs

Findings from the study showed that majority (90%) of the respondents block, ignore and or deletes irregular email context messages that has to do with their bank details thereby preventing risk due to phishing, while 83.3% of the respondent said they no longer use lonely ATMs or go to the ATM during odd hours. About 60% indicated that they keep contact with their bank in relation to information gotten online or via SMS from their bank accounts.

Also about 48.9% of the respondents periodically check their bank account history and request for a statement of their transactions. This is to keep the agro-entrepreneur and the bank on acceptable confidence level. About 38.9% reported that they call their bank immediately to deactivate their ATM card when it is lost, while 48.9% indicated that they periodically check with the bank history and account to know if everything is okay with their accounts. Meanwhile 61.1% of the agro entrepreneurs agreed that they do not use birthdates, address and other words or numbers that would be easy for attackers to figure out their passwords

About 63.3% of the respondent indicated that they no longer click on links from suspicious looking emails, while 30% of the respondents agreed that they make sure that the bank website is legitimate before keying in their banking details.

Table 3: Cyber security measures adopted by agro-entrepreneurs

Cyber security measures	Frequency	Percentage (%)
I received an email that looks similar to that of my bank requesting for my bank account details, through a link embedded in the email, which I did and thereafter money was withdrawn from my account.	21	23.3
I received a text message requesting urgently for my bank account details, and after giving the account details, money was withdrawn from my account.	60	66.7
I visited a malicious website resulting to the exposure of my bank account details, which allowed criminals to withdraw money from my account.	33	36.7
My ATM card was used by someone close to me to withdraw money from my account secretly.	54	60
After withdrawing money from an ATM, I was accosted by criminals who carted away with my money	15	16.7
I received a text message stating that my ATM card has been de-activated, and that to re-activate it I should call someone through a phone number provided in the message, which I did, and after providing my card	48	53.3

details to the person for re-activation, money was withdrawn from my account.		
I was trying to transfer money via my mobile application the transaction didn't go through due to network issues, but the money was debited from my account	19	21.1
Every time I try to make use of my bank's USSD code, I always get an error message before the transaction goes through. was deducted from my account	68	75.6
I attempted making payment on POINT OF SALES (POS), the transaction wasn't approved, yet the money	55	61.1
I received a call from an unknown person claiming to be a customer service representative of my bank, telling me that my online banking account have been temporarily locked due to suspected unauthorized request for password change from someone, and that I should provide my account login details so they can unlock the account, which I did, and thereafter money was withdrawn from my account.	43	47.8
I take special care whenever I want to login to my online banking platform	47	52.2
I ignore and delete emails/text messages that tells me to provide my online banking details through any channel.	81	90
I no longer click on links embedded in suspicious looking emails.	57	63.3
I contact my bank to crosscheck any information I receive online or via text messages concerning my online account.	54	60
I periodically check my account history and balance.	44	48.9
I no longer use birthdates, addresses and other words or numbers that would be easier for attackers to figure out my password	47	52.2
I don't use the same passwords for all my bank accounts	55	61.1
I don't use lonely ATM or go to the ATM during late hours	75	83.3
I now use two-factor authentication (PIN and OTP) process for my mobile banking	37	41.1
I call my bank immediately I lose or misplace my ATM card to block my account	35	38.9
I installed antivirus software to prevent viruses, keyloggers and other malicious programs from compromising my computer.	40	44.4
I don't use unsecured private wireless networks or Public Wi-Fi for my online transactions	25	27.8
I download apps only from approved app stores	56	62.2
I contact my bank immediately I see unauthorized debit alerts	53	58.9
I always request for my account statement regularly	45	50
I only use PREPAID CARD for my online transactions	6	6.7
I disallow web browsers from storing my online banking login credentials.	64	71.1

I make sure my bank website is legitimate before I enter my login details.	27	30
--	----	----

Field survey,2019

Socio-economic factors that influence rate of adoption of cyber security measures

Results of regression analysis for the socio economic characteristics for all the four functional forms are presented in Table 4. Linear form was chosen as the lead equation based on the highest value of R², more significant coefficients, highest F- value and conformity to theoretical expectations of the regression coefficients. The coefficient of multiple determination (R²) value of 0.69 indicates that about 69% of the variation in the dependent variation was explained by the independent variable (predictors) included in the regression while the remaining 31% was due to other factors not specified in the model; F-ratio with 1.876 value in the regression result, is significant at 1%. It implies that all the variables have significant or joint effect on the dependent variables. From the table independent variables such as education status (years), household size, business experience (years), farming status, internet access, annual income and extension services have positive coefficients, meaning that the more of these variables the more likely the adoption of cybersecurity measures.

Farming status (X₅) was significant at 1% and has positive coefficient. This implies that being part-time farmer increases the chances of adopting more cybersecurity measures. This may be due to part-time agro-entrepreneurs getting income from other sources and increasing their chances of having more resources that will enable them to adapt to more cybersecurity measures. This corroborates with the findings of Ugwuja and Onowvie (2019) who reported that being a full time farmer reduces the chances of adopting more of risk management strategies in electronic banking in Ughelli Local Government Area. The coefficient of cooperative membership(X₆) is positive and statistically significant at 5%. This shows that cooperative members are more likely to be aware of cyber security measures due to constant training of members for skill enhancement.

Internet access (X₈) was significant at 5% and related positively to the level of adoption of cyber security measures. This shows that the more access an agro-entrepreneur has to internet access, the more likely the adoption of more cyber security measures. Annual income(X₉) was significant at 10%, implying that those with higher annual income are more likely to adopt more cyber security measures

Table 4: Regression results on the level of adoption of cyber security measures by agro-entrepreneurs

Variables	Linear	Exponential	Double-log	Semi-log
constant	75.686	78.615	4.589	4.422
	(5.377)	(2.012)	(5.609)	(14.828)

Age(X ₁)	-0.741	-0.454	-0.400	-0.678
	(-0.033)	(-0.753)	(-0.846)	(-0.417)
H.holdsizes (X ₂)	0.859	0.688	0.667	0.853
	(0.178)	(0.403)	(0.432)	(0.185)
Edustatus (X ₃)	0.460	0.765	0.690	0.432
	(0.738)	(0.300)	(0.400)	(0.789)
Maritalstatus(X ₄)	-0.112	-0.04	-0.081	-0.203
	(-1.609)	(-1.998)**	(-1.770)	(-1.285)
Farming Status(X ₅)	0.023	0.329	0.384	0.030
	(2.321)***	(0.983)	(0.875)	(2.205)***
Cooperative Membership (X ₆)	0.054	0.623	0.663	0.058
	(1.953)**	(0.493)	(0.437)	(1.925)*
Business Exp(X ₇)	0.550	0.130	0.095	0.506
	(0.600)	(1.529)	(1.691)	(0.668)
Internet Access(X ₈)	0.012	0.031	0.440	0.020
	(2.559)***	(2.202)***	(2.046)***	(2.373)***
Annual Income(X ₉)	0.074	0.787	0.800	0.102
	(1.810)	(0.271)	(0.225)	(1.652)
Ext.services(X ₁₀)	0.219	0.290	0.158	0.242
	(1.329)	(1.065)	(1.427)	(1.178)
R ²	0.692	0.649	0.650	0.674
F-Ratio	1.876	1.382	1.395	1.662

Source: Field Survey, 2019 *** Significant at 1% level** Significant at 5% level*Significant at 10% level. Values in parenthesis are the t- values.

V. CONCLUSION AND RECOMMENDATIONS

Electronic banking has brought so much convenience in carrying out financial transactions, but the associated risks should be carefully managed. Findings from the study showed that the agro-entrepreneurs mostly accessed USSD-based mobile banking, SMS alert, ATM, Debit card and online banking for funds transfer. Risks faced by agro entrepreneur in accessing electronic banking services are the cases of

having a fraudster in the guise of a bank agent requesting for account details, receiving SMS and email alerts requesting for an immediate details of one’s account in which they gave out their bank details and money was deducted from their accounts, ATM card was used by someone close to them, and unsuccessful transactions through POS. Cyber security measures mostly used by agro-entrepreneurs are ignoring and deleting emails/text messages that tells me to provide my online banking details through any channel, and not using lonely ATMS or going to the ATM during late hours. Factors that influenced the adoption of cyber security measures were farming status, internet access, annual income and cooperative membership. The study recommends that the Central Bank of Nigeria should enforce banks with the responsibility of educating customers deeply, not only superficially, on the risk involved in digital finance, and what methods can be used to combat these risks. Banks should provide financial products and services that will expose customers to mild risks.

REFERENCES

- [1] Agboola, A. (2007). Information and communication technology (ICT) in banking operations in Nigeria- An evaluation of recent experiences. *African Journal of Public Administration and Management*, 18(1), 1-102.
- [2] Avgerou, C. (2003). The link between ICT and economic growth in the discourse of development. In Proceedings of the International Federation of Information Processing, IFIP 9, 373-386.
- [3] Consultative Group to Assist the Poor (CGAP), 2018. Cyber Security in Emerging Financial Markets, available at www.cgap/nodes/
- [4] Enhancing Financial Innovation and Access (EFInA) 2014. Access to Financial Services in Nigeria 2014 Survey. Retrieval from <http://www.efina.org.ng/media-centre/news>. (Accessed 4 June 2018)
- [5] Enhancing Financial Innovation and Access (EFInA) ,2016. Access to Financial Services in Nigeria 2016 Survey. Retrieval from <http://www.efina.org.ng/media-centre/news>(Accessed 16 June 2018)
- [6] Gujun, Y(2013). Risk types and risk amplification of online finance. *Information and Technology Journal*,12(3), 494-497
- [7] Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 11(4), 541-562.
- [8] Liao, Z., &Cheung, M.T. (2002). Internet-based e-banking and consumer attitudes: an empirical study. *Information & Management*, 39(4), 283-295.
- [9] Mgbenka, R.N., Mbah E.N. and. Ezeano C.I (2015). A Review of Small holder Farming in Nigeria: Need for Transformation. *Agricultural Engineering Research Journal* 5(2): 19-26.
- [10] Milis, K., &Mercken, R. (2002). Success factors regarding the implementation of ICT investment projects. *International Journal of Production Economics*, 80(1), 105-117.
- [11] Pilat, D.D., Lee, F., &VanArk, B. (2003).Production and use of ICT: A sectoral perspective on productivity growth in the OECD area. OECD Publishing.
- [12] Reynolds, D., Treharne, D., & Tripp, H. (2003).ICT—The hopes and the reality. *British journal of educational technology*,34(2), 151-167.
- [13] Schaeffer, B. S.. (2009): Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors.
- [14] Ugwuja V.C& Onavwie O. (2019). Determinants of Adoption of Risk Management Strategies in Electronic Banking Among Agro Entrepreneurs in Ughelli North Local Government Area of Delta State, Nigeria.*J ournal of Tropical Agriculture, Food, Environment and Extension*,18 (3) :19-24

[15] Yousafzai, S., Pallister, J., & Foxall, G. (2003). A proposed model of e-trust for electronic banking. *Technovation*, 23(11), 847-860.

[16] Zuppo, C. M. (2012). Defining ICT in a boundary less world: The development of a working hierarchy. *International Journal of Managing Information Technology*, 4(3), 13.