Cyber Risks in Electronic Banking: Exposures and Cybersecurity Preparedness of Women Agro-entrepreneurs in South- South Region of Nigeria

V. C. Ugwuja
University of Port of Harcourt

P. A. Ekunwe
University of Port of Harcourt

A. Henri-Ukoha
University of Port of Harcourt

This paper examines cyber risks exposures and cybersecurity preparedness of women agro-entrepreneurs. Women were exposed to risks of unsuccessful transaction through mobile apps and POS in which their accounts were debited, they were also exposed to social engineering threats such as smishing and vishing. With respect to cybersecurity preparedness, the women adopted few measures such as avoiding lonely ATM and ignoring text messages and email that request for banking details. Household size, cooperative membership, educational level and internet access were significant factors in accessing digital financial products and services. These findings call for interventions through policies that will enhance customer education to reduce vulnerabilities especially among women.

Keywords: electronic banking, cyber risks, cybersecurity, women agro-entrepreneurs, Nigeria

INTRODUCTION

The rise of financial technology has provided a wealth of opportunities for financial institutions to enhance services to customers through new channels. These have helped to save time, money and effort from an operational perspective. Banks have realized that digital finance has come to be recognized as the best means of financially empowering the poor, and making them to be more financially included, especially women. Access to finance is the central issue necessary for empowerment of women. (Enhancing Financial Innovation and Access, EFINA, 2018) reported that 40.9 percent of Nigerian women have no bank account compared to 32.5 percent of men. Women have customarily been excluded from the domain of external information, both deliberately and because of factors working to their disadvantage such as lack of freedom of movement or low levels of education. Digital finance opens up a direct window for women to the outside world. Information flows to them without any distortion or censoring (Suman, n.d). Digital finance through the use of ICT allows for greater financial inclusion, and the financial service sector is a primary driver of communications and network technology. There are many digital financial service offered by Deposit Money Banks and Mobile Money Operators. These include; fund transfers, mobile finance systems for payments, micro-lending platforms, notification systems for clients, savings, client enrollment through SMS, micro insurance products, including life and weather index insurance, claims payment through mobile phones and analysis of loans in the field using smartphones or tablets (World Bank, 2013).

Digital financial products and services are mostly electronic(internet) banking. The characteristics of electronic banking is such that factors that cause risks and the impact of risks are not exactly the same with traditional financial sector. Because risks in electronic 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 of internet banking, the risk control and management procedures must be strengthened. Otherwise, the existence and further development of internet finance will be severely threatened. As banks increasingly depend on information technology and the internet to operate their business and interact with the markets, their awareness and recognition of the magnitude and intensification of cyber risks should be more perceptive and discerning. Cyber risk refers to any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cyber-attacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information, be it related to individuals, companies, or governments (Financial Services Sector Coordinating Council, 2016).

Such risks as experience in electronic banking are classified into several clusters such as security risks, legal and ethical risks, reputational risks, operational risks, money laundering risk, strategic risks, cross border risks and traditional risks (Virender, 2012). Both the financial institutions and their customers face these risks dimensions in various aspects. There are various aspects of risk dimensions that give rise to the extent of consumers' perceived risk about using online banking services. Such risks as perceived by customers are; (a) social risk which refers to the utility or approval individuals receive by consuming products or services recognized within their own social group(s); (b) Financial risk is one of the underlying dimensions of the perceived risk which refers to riskiness associated with potential monetary loss expected in the form of erroneous money transfer and incomplete knowledge about transaction costs. (c) The functional dimension of risk refers to the core benefit and basic utilities of a good or service. It includes aspects such as the quality, the uniqueness, the usability, the reliability, and durability of the product (Sääksjärvi & Lampinen, 2005) as cited in (Nadine *et al* .2010. Individual risk expresses how 'risk -averse' people tend to be or try to avoid any form of risk, and how 'risk-friendly'people enjoy or expectantly tolerate the associated thrill or uncertainty (Slovic, 2003) as cited in (Nadine *et al*. 2010). (d)Security risk is associated with hacking of customers' account.

Cyber-attacks are both common and costly to consumers and banks alike, cybercriminals are finding new ways to exploit weaknesses and working to develop ever more sophisticated methods of attack. Cyber threats are becoming more sophisticated with the blending of once distinct types of attack into more damaging forms. Increased variety and volume of attacks are inevitable given the desire of financially and criminally-motivated actors to obtain personal and confidential information. Today customer expectations, technological capabilities, regulatory requirements, demographics and economics are together creating a crucial change. This leads to the need for banking institutions to get ahead of these challenges and adopt a proactive approach to security (BDO Network, 2017).

Achieving strong cyber security preparedness requires good technology, the right organizational structures, enhanced customer education, strong cooperation, legal support and investment. Statistical Analytical System, SAS (2013) reported that the weakest link within banks relates to a lack of internal resources devoted to cyber security. Their findings show that only 24 percent of survey respondents say they are "highly prepared" in this area, followed by 32 percent who cite external cooperation. In both instances, you can see limited preparedness or a lack of preparedness. As the nature and severity of cyber risks increase, what does this all mean for customers in terms of how they prepare and respond to cyber-attacks in Nigeria, bearing in mind that Nigeria is still developing in terms of digital technology? There are shortages of research information that dwell on this. Hence, the essence of this study.

Objectives of the Study

The specific objectives of the study were to:

i) identify digital financial products and services accessed by women agro-entrepreneurs in the South- South region of Nigeria.

ii) identify cyber risks experienced by women agro-entrepreneurs in South-South Nigeria.

iii) asses the degree of preparedness of the respondents towards cyber security in the study area.

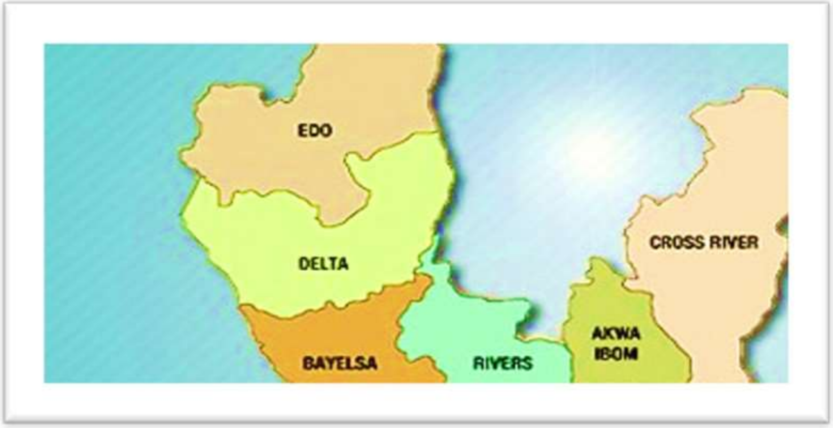
iv) determine the socio-economic factors and perceived security risks that influence access to digital financial products and services in the study area.

METHODOLOGY

Area of the Study

The South-South region of Nigeria comprises of six states which are Akwa Ibom, Bayelsa, Cross River, Delta, Edo and Rivers. Though a relatively small stretch of land, South-South region of Nigeria provides the economic mainstay of the economy which is oil. In addition to oil and gas, the region equally contributes other key resources, with potential huge investment opportunities in tourism and agriculture. Figure 1 shows the Map of South-South region of Nigeria.

FIGURE1
MAP OF SOUTH-SOUTH REGION OF NIGERIA



Sampling Procedure

The design for the study was the survey method. Multistage sampling procedure was employed in the selection of the respondents for this study. The first stage was random selection of two states out of the six states that make up South–South region of Nigeria. These states were Bayelsa and Rivers State. Stage two was a purposive selection of two Local Government Area (LGAs) from each State, based on high concentration of economic activities which are agro- based and availability of financial institutions, making it a total four LGAS for the study. In Bayelsa, the LGAs were Yenagoa and Sagbama and in Rivers, the LGAs were Eleme and Khana. Furthermore, two communities were randomly selected and that made it eight communities for the entire study, then in each community, there was a purposive selection of 10 women agro-entrepreneurs that access digital financial products, and 10 that do not access digital financial products. That made it a total of 80 of them that access digital financial products, and another 80 that do not access financial products. Making it total of 160 women agro-entrepreneurs for the entire study.

Data Collection

Primary data were collected using structured questionnaire and oral interview. Two sets of questionnaires were used for the study, the first set was for the women agro-entrepreneurs that are accessing digital financial products. The second set of questionnaire was for women agro-entrepreneurs that are not accessing digital financial products.

Data Analysis

Generally, data were analyzed using these approaches namely; descriptive statistics and inferential statistics such as binary logistic regression.

Model Specification for Binary Logit

Binomial logistic regression model is being used given that the dependent variable is dichotomous: 0 when a woman agro-entrepreneur is having no access to digital financial products and 1 when having access to digital financial products. Predictor variables are a set of socio-economic and demographic indicators of the women agro-entrepreneurs. They contain both dichotomous and continuous variables. Let Pj denote the probability that the j-th woman agro-entrepreneur is having access to digital financial product. We assume that Pj is a Bernoulli variable and its distribution depends on the vector of predictors X, so that:

$$P_j\,(X) = \frac{e^{\alpha+\beta X}}{1+e^{\alpha+Bx}} \qquad (1)$$

The logit function to be estimated is then written as:

$$\ln\{P_j/(1\text{-}P_j)\} = \alpha + \textstyle\sum_I \beta_i X_{ij} \qquad (2)$$

The logit variable ln{Pj/(1-Pj)}is the natural log of the odds in favour of a woman agro-entrepreneur having access to digital financial products. The coefficient estimates of β gives the change in the log-odds (logarithm of relative probabilities) of the outcome—here = 1—, for a one unit increase in the independent variable, holding all other independent variables constant. Logit regressions are estimated using Maximum Likelihood (ML) rather than OLS. ML calculates coefficient estimates that maximize the likelihood of the sample data set being observed.

The binary logit model to be estimated is specified as follows:

$$C_{ij} = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \beta_5X_5 + \beta_6X_6 + \beta_7X_7 + \beta_8X_8 + \beta_9X_9 + \beta_{10}X_{10} + u \qquad (3)$$

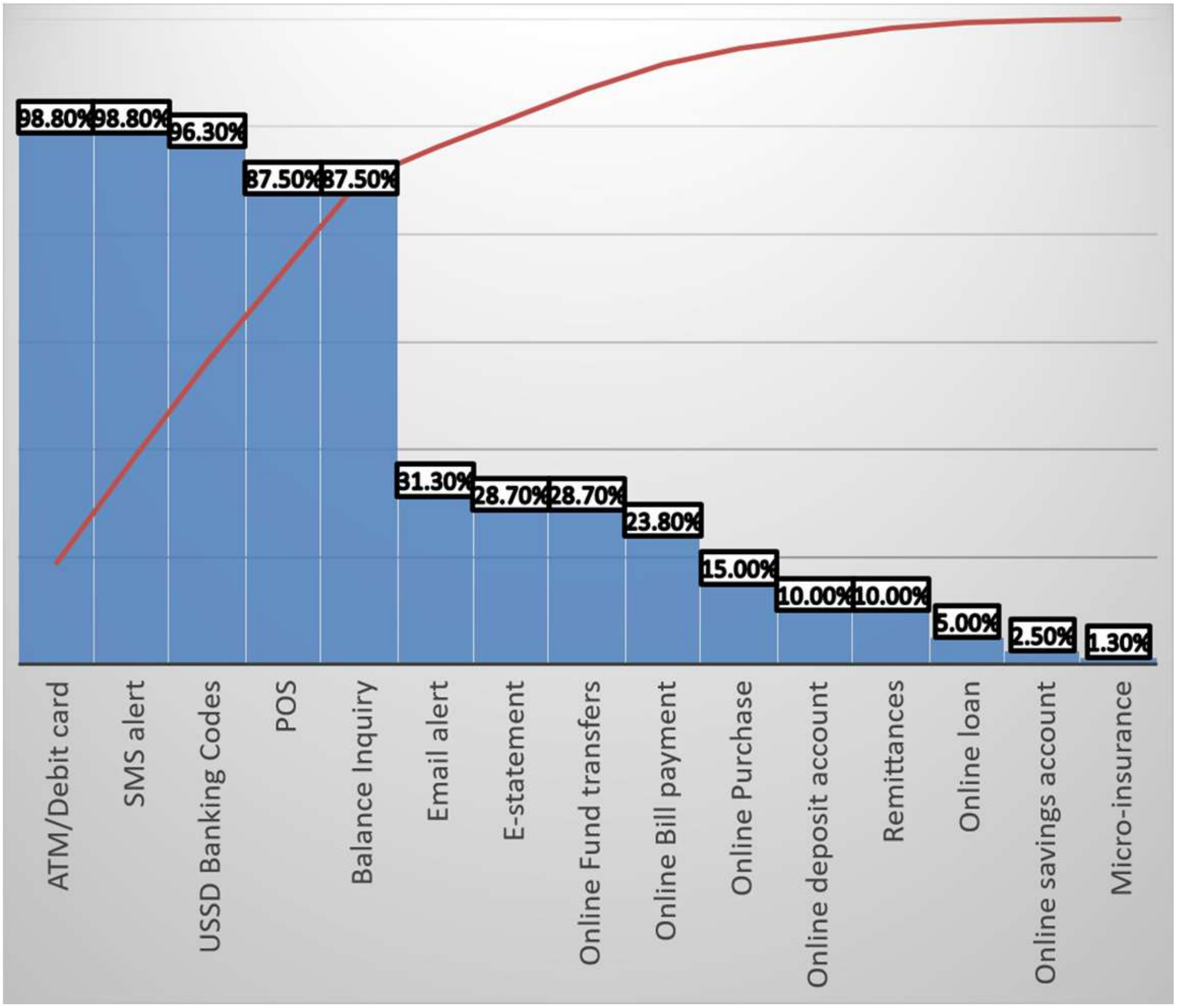
C_{ij}, = Dummy = 1 if the woman agro-entrepreneur is accessing digital financial products, and 0 otherwise.
X_1 = Age (Years)
X_2 = Household Size (Number)
X_3 = Educational Status (Years)
X_4 = Farming status (Full-time= 1, Part-time= 0)
X_5 = Cooperative Membership (Dummy; Yes =1, No=0)
X_6 = Business experience (Years)
X_7 = Internet access (Dummy; Yes= 1, No= 0)
X_8 = Owns ICT device (Dummy; Yes= 1, No= 0)
X_9 = Annual income (Naira)
X_{10} = Perceived security risk (Dummy; Yes= 1, No= 0)
u = stochastic error term.

RESULTS AND DISCUSSION

Digital Financial Products Accessed by Women Agro-entrepreneurs in South- South Region of Nigeria

The response of digital financial products accessed by women agro-entrepreneurs is presented in Figure 2. Majority (98.8%) of the respondents indicated accessing ATM/Debit cards, this agrees with the report of (EFINA, 2014) who stated that 76.2% of banked population in Nigeria have ATM/Debit cards. SMS Alert services (98.8%) were also highly accessed by the respondents. Majority of the women agro-entrepreneurs indicated to be accessing USSD Banking Codes (96.3%), POS (87.5%), and Balance inquiry (87.5%). Results from Figure 2 also showed that the respondents moderately access these digital financial products; Email alert (31.3%), E-statement (28.7%), Online Fund Transfer (28.7%) and Online Bill Payment (23.8%). These are the least accessed products as indicated by the respondents; Online Purchase (15%), Online deposit account (10%), Remittances (10%), Online Loan (5%), Online Savings Account (2.5%) and Micro-insurance been the least accessed with only 1.3% indicating having access to this product. This corroborates the findings of EFINA, (2016) who reported that Online Savings account and Insurance are least accessed by banked population in Nigeria.

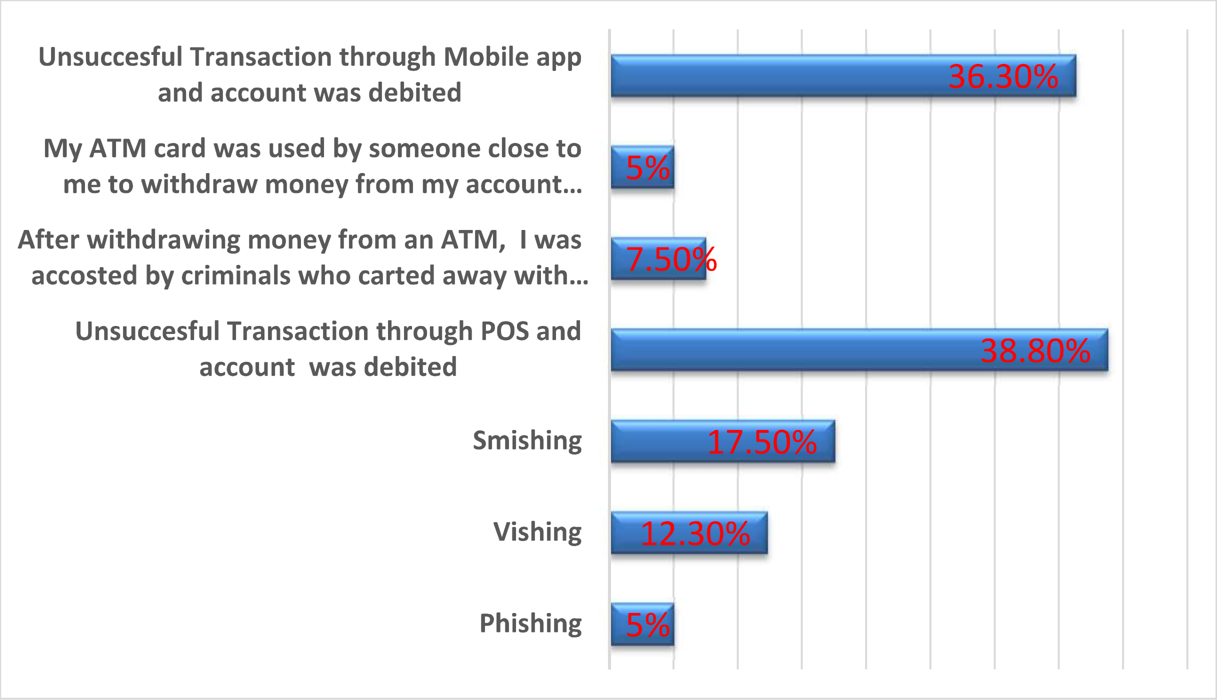
FIGURE 2
DIGITAL FINANCIAL PRODUCTS ACCESSED BY WOMEN AGRO-ENTREPRENEURS



CYBER RISKS EXPERIENCED BY WOMEN AGRO-ENTREPRENEURS

Results of the analysis on the cyber risks experienced by women agro-entrepreneurs in South-South region of Nigeria are presented in Figure 2. Findings from the results showed that about 36.3% of the respondents indicated unsuccessful transactions through mobile apps and their accounts were debited. Only 5% agreed that their ATM cards were used by someone close to them to withdraw money from their accounts without their knowledge. About 7.5% revealed that after withdrawing money from an ATM, they were accosted by criminals who carted away with their money. About 38.8% indicated that they made payment through POINT OF SALES (POS) terminal, the transaction wasn't approved, yet money was deducted from their accounts, most of the women experienced this type of cyber risks. The implies that many customers that pay through POS experience this risk. About 17.5% agreed that they have experienced smishing which indicated that they received a text message (SMS) requesting that they urgently provide their bank account details, and after giving the account details, money was withdrawn from their account. This conforms with the findings of Omodunbi et al (2016) who reported that most of their respondent suffered cyber-attack by giving away their banking details through text messages. About 12.3% of the respondents have experienced receiving a call from an unknown person claiming to be customer representative of their banks, and requesting for bank account details, which was provided thereafter and money was withdrawn from their accounts. This act is called Vishing. This finding is supported by National Cyber Security Centre (2016) who reported that common cyber-attacks are mostly caused by users divulging information to fraudsters. Only 5% of the respondents agreed they have experienced phishing implying that they received an email that looks similar to that of their banks requesting that they urgently provide their bank account details through a link embedded in the email, which they did and thereafter money was withdrawn from their accounts.

FIGURE 3
CYBER RISKS EXPERIENCED BY WOMEN AGRO-ENTREPRENEURS



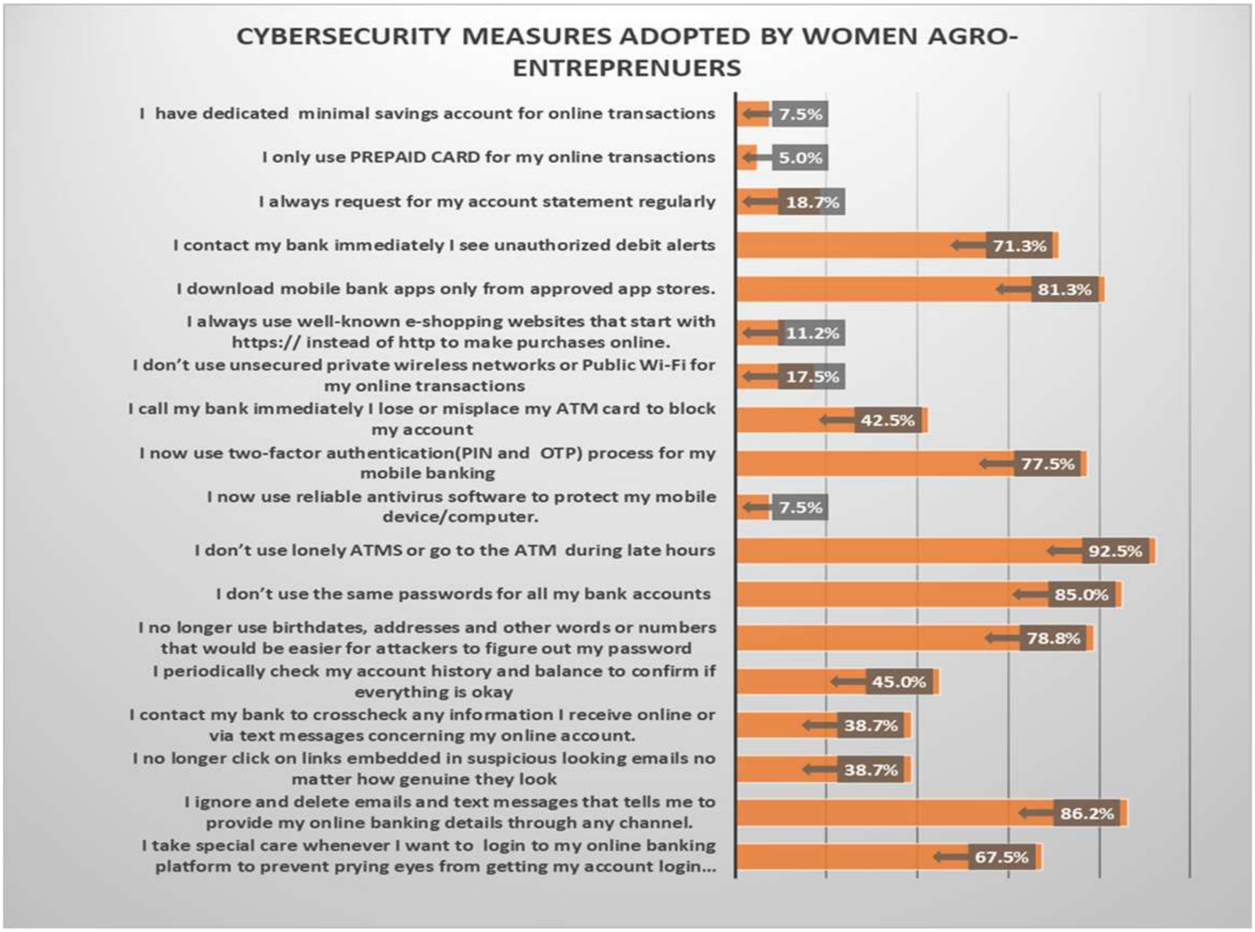
CYBERSECURITY MEASURES ADOPTED BY WOMEN AGRO-ENTREPRENEURS

With respect to cybersecurity measures adopted by the women agro entrepreneurs, the following measures were highly adopted as shown in Figure 4: (1) I don't use lonely ATMS or go to the ATM during late hours (92.5%); (2) I ignore and delete emails and text messages that tells me to provide my online banking details through any channel (86.2%); (3) I don't use the same passwords for all my bank accounts (85.0%); (4) I download apps only from approved app stores (81.3%); I no longer use birthdates, addresses and other words or numbers that would be easier for attackers to figure out my password (78.8%); I now use two-factor authentication(PIN and OTP) process for my mobile banking(77.5%); I contact my bank immediately I see unauthorized debit alerts (71.3%).

Women agro-entrepreneurs moderately adopted the following cybersecurity measures; (1) I periodically check my account history and balance to confirm if everything is okay (45.0%); (2) I call my bank immediately I lose or misplace my ATM card to block my account (42.5%); I no longer click on links embedded in suspicious looking emails no matter how genuine they look (38.7%); (3) I contact my bank to crosscheck any information I receive online or via text messages concerning my online account (38.7%).

The following cybersecurity measures were the least adopted by the women. They include the following; (1) I use PREPAID CARD for my online transactions (5%); (2) I have dedicated minimal savings account for online transactions (7.5%); (3) I now use reliable antivirus software to protect my mobile device/computer (7.5%); (4) I always use well-known e-shopping websites that start with https:// instead of http// to make purchases online (11.2%); (5) I don't use unsecured private wireless networks or Public Wi-Fi for my online transactions (17.5%); (6) I always request for my account statement regularly (18.7%).

FIGURE 4
CYBERSECURITY MEASURES ADOPTED BY WOMEN AGRO-ENTREPRENEURS



DETERMINANTS OF ACCESS TO DIGITAL FINANCIAL PRODUCTS BY WOMEN AGRO-ENTREPRENEURS IN THE SOUTH-SOUTH REGION OF NIGERIA.

Results of the analysis on the major determinants of access to digital financial products by women agro-entrepreneurs in the region are presented in Table 1. The result of the analysis indicates that the overall model with a log likelihood chi square ratio of 81.568 is significant at 1% suggesting the model has a strong explanatory power. Out of the ten examined explanatory variables in the model, four factors, household size, educational status, cooperative membership and internet access were statistically significant in accessing digital financial products.

The coefficient of household size is positive and significant at 10% level of probability. This implies that a unit increase in household size increases the chance of accessing digital financial products by 19%. The coefficient of educational status is also positive and significant at 5% level of probability. This indicates that women agro-entrepreneur's access to digital financial products is positively influenced by educational status. Cooperative membership impacts positively on access to digital financial products. Women agro-entrepreneurs who are members of cooperative societies are more likely to access digital financial products, this is shown in the results as the coefficient of cooperative membership is significant at 5% level of probability. Internet access is a strong determinant of access to digital financial products. The study reveals that not having access to internet reduces the probability of having access to digital financial products. This conforms with the findings of Vijay (2011) who stated that internet access is a major determinant of internet banking adoption in India.

TABLE 1
RESULTS OF DETERMINANTS OF ACCESS TO DIGITAL FINANCIAL PRODUCTS

Variables	Coeff	Std. Error	T-ratio	P-Values
Age (X_1)	-0.040	0.075	0.5333	.592
Household Size (X_2)	0.191	0.111	1.721*	0.085
Educational Status (X_3)	0.225	0.087	2.586**	0.010
Farming Status (X_4)	35.926	5329.220	0.007	0.995
Cooperative Membership (X_5)	1.096	0.690	2.332**	0.021
Business Experience (X_6)	0.019	0.050	0.3800	0.706
Internet access (X_7)	-2.369	1.188	-1.994**	0.046
Owns ICT device (X_8)	-18.613	3602.298	-0.0052	0.996
Annual Income (X_9)	0.000	0.000	0.000	0.692
Perceived Security Risks (X_{10})	0.198	0.282	.7021	0.483
Constant	-36.655	5329.221	0.0067	0.995
Log likelihood	81.568***			
Chi	0.000			
Article I. Pseudo R^2	0.584			

***Significant at 1% level, ** Significant at 5% level, *Significant at 10% level

CONCLUSION AND POLICY RECOMMENDATIONS

The study generated relevant and reliable information on cyber risk exposures and preventions of women agro-entrepreneurs that are accessing electronic banking products. We found out that women are exposed to risks of unsuccessful transaction through mobile apps and POS in which their accounts were debited. They were also exposed to smishing which involves receiving a text message (SMS) requesting that they urgently provide their bank account details, and after giving the account details, money was withdrawn from their accounts. With respect to cybersecurity preparedness, the respondents are prepared only in few cybersecurity measures such as avoiding lonely ATM or visiting ATM during late hours, using different passwords for different accounts and downloading mobile apps only from official app stores. Household size, cooperative membership, educational status and internet access were significant factors for accessing digital financial products and services. The findings suggest different policy instruments to combat cyber risks especially for women who are financially excluded more than men. Policies that will enhance customer education which will have pronounced effect on adoption of adequate cybersecurity measures. Regulators should therefore flex their regulatory power to address the issue of education of consumer customers about cyber risk. Also policy interventions through financial institutions providing suitable digital financial products and services tailored towards reducing exposures to cybercrime for women.

ACKNOWLEDGEMENT

This work is made possible by the support of AXA Research Fund, an AXA Group's Science Philanthropy Initiative in Paris, France. The project recognizes the support of the host University, University of Port Harcourt. Special thanks go to Prof O.M Adesope and Dr P.A. Ekunwe, the project supervisors for their mentorship and assistance.

REFERENCES

BDO Network. (2017). *Cyber Security in Banking Industry*. Retrieved October 12, 2018, from www.bdo.in

Enhancing Financial Innovation and Access (EFInA). (2014*). Access to Financial Services in Nigeria 2014 Survey*. Retrieved June 4, 2018, from http://www.efina.org.ng/media-centre/news

Enhancing Financial Innovation and Access (EFInA). (2016). *Access to Financial Services in Nigeria 2016 Survey*. Retrieved June 16, 2018, from http://www.efina.org.ng/media-centre/news

Enhancing Financial Innovation and Access (EFInA). (2018). *Access to Financial Services in Nigeria 2018 Survey*. Retrieved February 2, 2019, from http://www.efina.org.ng/media-centre/news

Financial Services Sector Coordinating Council. (2016). *Purchasers' Guide to Cyber Insurance Products*. Retrieved June 10, 2017, from www.fsscc.org

Gujun, Y. (2013). Risk types and risk amplification of online finance. *Information and Technology Journal*, 12(3), 494-497.

Nadine H., Klaus-Peter W., Barbara S., Lars P., & Martin K. (2010). The influence of consumers' risk attitudes and behavior on the adoption of online banking services. *Journal of Marketing Trends*, (1), 7-16.

National Cybersecurity Center (NCC). (2016). *Common Cyber attacks: Reducing the Impact*. Retrieved January 18, 2018, from https://cyber-center.org

Omodunbi, B.A., Odiase, P.O., Olaniyan, O.M., & Esan, A.O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. *Journal of Engineering and Technology*, 1(1), 27-42.

Sääksjärvi, M., & Lampinen. M. (2005). Consumer perceived risk in successive product generations. *European Journal of Innovation Management*, 8(2), 145-156.

Slovic, P. (2003, February 13-14). *Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality*. Paper presented at the National Cancer Institute workshop on Conceptualizing and Measuring Risk Perceptions, Washington, D.C.

Statistical Analysis System (SAS). (2013). *Cyber risk in banking: A review of the key industry threats and responses ahead*. Retrieved October 10, 2018, from https://www.kroll.com/media/

Suman, J. (n.d). *ICTs And Women's Empowerment: Some Case Studies from India*. A publication of the Department of Economics, LakshmiBai College, Delhi University. Retrieved from unpan1.un.org/intradoc/groups/public/documents/apcity

Vijay, M.K. (2011). Determinants of Internet Banking Adoption: An Empirical Evidences from Indian Banking. *Indian Journal of Commerce and Management Studies*, 2(1), 4-25.

Virender, S.S. (2012). Risks in E-Banking and Their Management. *International Journal of Marketing, Financial Services & Management Research*, 1(9), 164-178.

World Bank. (2013). *ICT enabling rural financial services and micro-insurance for smallholders*. World Bank's ICT in Agriculture e-Sourcebook discussion paper, e-Forum No. 6. Retrieved October 2, 2016, from http://www.ictinagriculture.org/sourcebook