The Seybold Report

ISSN 1533-9211

DOI: 10.5281/zenodo.10934838

DIGITAL FINANCIAL LITERACY AND CYBERCRIMES: MEASURING THE ROLE OF SUDANESE BANKS ENHANCING THEIR USERS' CONFIDENCE

WALEED E. KHALID [1], MOHAMMED MAQSOOD ALI [2], RADHOUAN ABDELMAJID GARBAA [3] and MUKKARAM ALI MOHAMMED [4]

[1,2,3,4] Applied College, Jazan University, KSA.

Abstract

Technological transformation has become the most prominent feature that greatly transitioning banking operations from traditional to digital. The Digital Financial Literacy and Cybercrimes are the challenges that customers are facing in using banking technology. The banks are neglecting its role to enhance user confidence towards digital financial literacy and cybercrimes. This study measures the relationships between digital financial literacy (attitude, awareness) and cybercrime (attitude, awareness) and examining the banks' roles in boosting user confidence towards digital financial literacy and cybercrimes. Using convenient sampling technique, a structured questionnaire was sent to the customers of private Sudanese banks' through WhatsApp groups and Facebook accounts. A total of 447 completed questionnaire were received. The Smart-PLS 4.0 was used to analyze the data. The results revealed that attitudes and awareness towards digital financial literary and cybercrimes are strongly influenced perceptions of banks' role in boosting user confidence. The implication of this study suggests that digital financial literacy and cybercrimes are crucial to both the customers and banks and therefore banks need to focus on policies towards enriching the education of digital financial literacy and cybercrimes in boosting user confidence.

Keywords: Digital Financial Literacy and Cybercrimes.

INTRODUCTION

Technological transformation has become the most prominent feature that greatly transitioning banking operations from traditional to digital. Digital banking operations involves various services such as the setting up of an account (current and savings), transferring funds, making withdrawals and deposits, applying for loans and investments, making bills payments and generating bank statements easily, quickly, anywhere and anytime. Digital banking has emerged in 1980s and the bank of Scotland is the first to provide its online banking services to its consumers in 1985. Many banks initiated their digital banking operations and implemented their digital banking strategies to use their digital channels for banking operations. The focus has now shifted from a product-centric approach to a customer-centric one, intending to deliver the best customer experience. But in terms of security, customers face financial literacy and cybersecurity challenges that advances with banking technology.

Globally, the use of financial technology (fintech) has elevated digital financial literary (DFL) to an important topic for customers as the most significant literacy (Golder and Cordie, 2022). DFL was first introduced in the late 1990s (Gilster, 1997). The Alliance for Financial Inclusion (AFI, 2021) network defines Digital Financial Literacy as "acquiring the knowledge, skills,

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

confidence and competencies to safely use digitally delivered financial products and services, to make informed financial decisions and act in one's best financial interest per individual's economic and social circumstance." On the other hand, the notion DFL is the integration of digital literacy and financial literacy. The former deals with how to access and use digital products and services through Tablets, Mobile phones, SMS, Internet and Web Browsers while later deals with how to carry out financial services such as transferring funds, making deposits and withdrawals, borrowings, savings and repaying. The concept of DFL encompasses: i) Awareness/and knowledge of DFS and the competency to use relevant DFS independently; ii) Awareness/ knowledge of relevant DFS-related risks and the competency to prevent these risks when using DFS; and iii) Awareness/knowledge of related consumer protection and redress mechanisms, and the competency to seek the same when needed. In addition, it is a significant requirement for the effective usage of digital financial services (DFS) (Ravikumar et al. 2022). It implies access and use of financial services through the digital platform at any time (Pazarbasioglu et al., 2020). Moreover, it is necessary to establish the DFL that help customers to avoid financial risks control, wrong decision-making and so on. Furthermore, DFL plays a crucial role in sustainable development and the minimizing of inequality and poverty in the world.

Cyber threats and attacks are challenging due to the rapid change in technologies. These challenges are not only concern for the banks but also to the consumers who are expose to cyber threats through their online digital channels such as smartphones, tablets, labtops, web browsers. Cybersecurity is a process designed to defend the computers, servers, networks, and digital data from unauthorized access and destruction or attack in cyberspace (Al-Alawi et al., 2019). Banks need to protect their clients by providing knowledge of cybersecurity and digital financial services in order to sustain development.

However, Sudanese Central Bank always seeks to achieve stability and sustainable development, so it sought and adopted expanding the base of financial inclusion and reducing the rates of deprivation and financial literacy, but the conditions that Sudan is going through, from fluctuations in the geopolitical, economic and security conditions,(Khalid, W.E, et, al., 2023), which greatly affected the implementation of strategies for financial and banking coverage and financial literacy despite the efforts made by the Central Bank towards it (CBOS, 59th Annual Report, 2019).

Sudan is one of the countries with low levels of financial inclusion, implying high levels of financial illiteracy between 2011 and 2017, according to the World Bank's Financial Inclusion Index, as the percentage of people with bank accounts does not exceed 25%. Despite the fact that the Fintech sector has created a revolution in the field of global and Arab financial systems in recent years, as it has come to meet many needs and services related to various financial operations in advanced ways that greatly compete with traditional financial services in terms of speed and cost, which would expand the Financial Inclusion Base (Union of Arab Banks, 2020). With the steady expansion of the base of banking digital services in the Sudanese banking sector, another challenge has emerged to the challenges that Sudan's economic situation is facing, which is cyber-crimes on the financial and banking sector, as well as the

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

absence of an effective role for the relevant institutions to carry out their duty to address and raise awareness of the dangers of these cybercrimes. It played the most prominent role in increasing the frequency of these threats and attacks, so the study aims to address digital financial illiteracy toward cyber-crimes, which has become a major threat to the world of financial technical services.

Digital financial literacy has become very imperative nowadays as we know that most financial services and products are now available in digital form, and the country's concern now is the economic transformation based on digital currency trading instead of traditional trading in physical currencies. This is coupled with the rapid developments in the digital payment system, allowing those who do not have bank accounts today to benefit from services that were previously out of reach or were not available to them. The researcher was also unable to obtain any indicators or figures related of the study from the official authorities or any statistics, so this study attempts to fill this gap by identifying the banking role, which can contribute to providing some data that can be used as an indicator to identify the reality in this sector both from the perspective of customers and bankers.

This study measures the role of Sudanese banks towards digital financial literacy and cybercrimes and determine the extent to which the banking sector contributes to educating customers about the risk of cyber-crimes and threats associated with technological development. This paper follows five sections. Section one discusses the statement of problems, concepts of Digital Financial Literary and Cybercrime. Literature is reviewed in section 2. Section 3 explains the process of research methodology. Section 4 analyses the results of the study and Section 5 includes the discussions and conclusions.

LITERATURE REVIEW

Many studies have addressed the issue of electronic crimes and threats facing the financial sectors. These studies have called for the need to raise awareness of the dangers of these crimes in light of the tremendous technological progress in the field of information technology, which has been reflected in banking and financial technology, and this in turn has led to a change in some concepts. Concepts and terminology, as the concept has become synonymous with financial culture, which is digital financial culture. Many studies have been conducted in this field, and in accordance with the objectives of our study, the focus will be on reviewing the literature related to dealing with electronic crimes in the banking sector, which goes through introducing the concepts of digital financial literacy and raising awareness of its use.

Previous studies are reviewed according to two main variables, which are Digital Financial Literacy and Cybercrimes. Each variable is dealt with through three dimensions, and to achieve the objectives of the study, they are dealt with as follows:

1.1 Awareness of Digital Finance Literacy (DFL)

The researchers found many definitions of digital financial literacy and in a number of studies related to addressing it through knowledge and awareness, and the most prominent of these definitions was "financial operations using digital technology, including electronic money,

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

mobile financial services, online financial services, i-teller, and branchless banking, whether through a bank or non-bank institutions" (OECD, 2017), while The AFI network (2017) has defines it as "acquiring the knowledge, skills, confidence and competencies to safely use digitally delivered financial products and services, to make informed financial decisions and act in one's best financial interest per individual's economic and social circumstance."

As Morgan et al (2019) pointed out, digital financial literacy is a multifaceted concept. Understanding of digital financial products and services, awareness of digital financial threats, knowledge of digital financial risk, and knowledge of consumer rights. Also (Rubble and Bailey, 2007) mentioned to Digital literacy is as an individual's capacity to use technology to handle and access information. While Prasad et al., (2018) demonstrated Digital financial literacy is the direct relationship or awareness of online systems of money management via various ways of making payments through the internet and banking system. Therefore, digital financial literacy (DFL) can be said as knowledge and awareness of the use of technology in all financial operations and how to gain it to help make informed decisions when managing money online.

1.2 Attitude of Digital Finance Literacy (DFL)

Regarding the behavior and attitudes of users of digital financial services, Morgan et al (2019) stressed the importance of knowledge digital financial products, as well as users' behavior around it, understanding and attitudes about their hazards. Park (2013) also emphasized the significance of attitudes about digital financial literacy, and he investigated the impact of each level of familiarity with technical components of the Internet. Awareness of common institutional practices and comprehension of current privacy policies in order to investigate the impact of these aspects on the behavior and attitudes of financial product users, as well as the impact on digital financial literacy. While Finau et al. (2016) discovered that consumers with attitudes toward digital financial services prefer to spend the money they receive through mobile money totally, they do not utilize their mobile phones to save.

Regarding improving basic skills to enhance attitudes and capabilities for digital financial literacy, Belshaw (2012), mentioned to eight fundamental components of digital literacy, and anyone looking for to optimize their digital literacy skills should develop skills, attitudes, and aptitudes in the eight areas he identified: cultural, cognitive, constructive, communicative, confidence, creative, critical, and civic. Garcia and Weiss (2017) also referred to aspects of digital literacy aspects as the set of digital abilities, attitudes, knowledge, and understanding necessary for interaction and using the internet skills and survivability and efficiency in the age of digitization.

1.3 The role of the bank to Enhance user confidence towards DFL

As for the roles that the banking and financial sectors should play to help increase awareness, eradicate digital financial literacy, and increase the confidence of users of these services, it has been (Bin Mohd ISA, 2021) indicated that in generally, must banks aggressively promote the development of e-banking (digital banking) to deliver fast and efficient banking services to all customers. While Prasad et al., (2018) emphasized, more rules must be implemented in the

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

cash-oriented economy to encourage the use of digital financial products and services currency while simultaneously reducing the use of cash. The governments and concerned sectors should also create user-simple applications that are accessible and usable by people with limited literacy. In order to achieve the reduction of digital financial literacy and awareness of its use and to move towards the digital economy, Also (Ali, 2019) pointed out to consider all measures that can help raise people's awareness of security while also ensuring a stable financial business environment, it consecrated one of the most important issues that the banking industry must address, and that in order to provide a safe online banking environment.

2.1 Awareness of cybercrimes:

As for the concepts of cybercrime, we found that there are many definitions of cybercrime, and the most prominent of these definitions came from the workshop on crimes related to the computer networks (2000), where cybercrime is defined as any illegal behavior directed by electronic means toward the security of systems. It contains information and data. Also, (Bin Mohd ISA, 2021) stated in his study that cybercrime is the illegal and criminal activities that involve a computer and network from anywhere in the world. It is on the rise as cybercriminals take advantage of technological advancements. It can be used as a medium for activities or as a target. Cybercriminals can target anyone who has a working computer and access to a network or the internet. It can affect any office online user, banks, business operators, government departments, schools, universities, and individuals.

Elradi et al (2020) investigated the level of cyber security knowledge of 200 students and 100 faculty members at a one of a Sudanese college using three crucial security parameters: trust, passwords, and defensive attitude. The study found that all participants had a relatively low level of security awareness, which was uneven between faculty members and students, and their defensive attitude is significantly weak. The study recommended educating users, developing policies and regulations that govern the use of information and devices in a simple and easy-to-understand manner. Basic cyber security awareness should be included in the first year of college or in early education levels at schools.

According to Stefan, I. (2011), cyber-crime can be referred to as crimes toward IT systems, which include any crimes that can be perpetrated using the internet and IT systems. Regarding the impact of cybercrime activities on economic growth, (Ali, L. 2019), stated that all steps that can help increase people's awareness of security while also ensuring a healthy financial business environment should be considered, as well as how to avoid the effect of this crime activities on the banking sectors in the GCC region.

2.2 Attitude of cybercrimes

And the expansion of hackers' activities (Gupta, 2012) indicated in his study that there are various types of cybercrimes. Some of the more common types of cybercrime are DDOS Attacks, Botnet, and Identity Theft. Others are Web browser fraud, identity theft (where personal data is hacked and used), theft of monetary or card financial data, theft and selling of company data, cyber extortion (demanding money to avoid a threatened attack) and cyber criminals are some other forms of cybercrimes (that are types of cyber extortion). Some of the

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

most dangerous cyber hazards and strongest forms of malware attacks are Ransomware, Trojan Horse Programs, Computer Viruses and Worms, File Infections, System Infections, Logic Bombs, Worms and Droppers.

These types and methods are developing very rapidly in a way that is synonymous with development in the field of cyber security, and these methods used have affected the banking sector, causing very large losses, as mentioned Saravade (2018) Indian banks have been witnessing persistent attacks from possible state and non-state actors, organized criminals and hacktivists. The case of cyber-attack on Canara Bank in the year 2016 explains this better, where bank's e payments were attempted to be blocked by vandalizing its site through the insertion of malicious software by a hacker from Pakistan [6]. Union Bank of India also fell prey to an attack in July 2017, where close to USD 170 million was looted from its Nostro account. According to reports the offender's gained entry by using spear phishing. In a survey conducted by KPMG in 2017 on cybercrime, it has been pre-supposed that initially banks were not well equipped with adequate cyber security mechanism, because of which they were succumbed to rampant cyber threats. Also, (Ali, L. 2019), mention to the term "Cyber Crime" refers to a variety of crimes that are committed virtually using any source of technology and digital tool. This includes distributing virus programs, hacking and cracking, sending spam emails, phishing, and gaining unauthorized access to other computers in order to steal financial data.

As a result, cybercrime can be defined as an unethical activity aimed at obtaining financial gain through illegal activities that seek to fraudulently financial in various electronic ways and threaten the integrity of banking services for individuals and institutions by attempting to steal data from consumers regarding online banking accounts, credit card or other bank account details. In addition to that, Cybercrime knows no bounds and evolves at the same rate as new technologies. Cybercrime's tremendous growth and disastrous consequences pose a significant threat to banking and financial institutions. So, it should be creating a thriving security readiness among financial institutions, including banks.

2.3 The role of the bank to Enhance user confidence towards Cybercrimes

Elradi et al (2020) investigated the level of cyber security knowledge of 200 students and 100 faculty members at a one of a Sudanese college using three crucial security parameters: trust, passwords, and defensive attitude. The study found that all participants had a relatively low level of security awareness, which was uneven between faculty members and students, and their defensive attitude is significantly weak. The study recommended educating users, developing policies and regulations that govern the use of information and devices in a simple and easy-to-understand manner. Basic cyber security awareness should be included in the first year of college or in early education levels at schools.

As Ali (2019) indicated to the cybercrime is one of the most important issues that the banking industry must address, and that in order to provide a safe online banking environment, it is necessary to understand the effects of cybercrime and take appropriate countermeasures. And should consider all measures that can help raise people's awareness of security while also

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

ensuring a stable financial business environment. Therefore, the banking sector had to know its role in reducing digital financial literacy and raising awareness of the dangers of cyber-crime banking , as well as working to enhance the confidence of customers by protecting them from cyber threats, hence the importance of this study to Measuring evaluation the impact of Digital Financial Literacy towards cybercrimes in the banking sector and identify the role of the Sudanese banking sector in reducing digital financial literacy and awareness of the risk of cyber-attacks, in this vital sector, which suffers, like other economic sectors, from many of the complications that we referred to earlier, as well as the absence of an effective role for institutions and bodies concerned with this role, as the researcher was unable to obtain sufficient information about the rate of electronic attacks or protocols that work to protect them, or to identify the features that these institutions can carry out to raise awareness of these electronic dangers or the mechanism for dealing with them.

Dashora, K. (2011) also emphasized the roles that responsible bodies, such as governments, police departments, intelligence units financial sectors around the world, should play in making and implementing ongoing modifications to information technology laws in order to make them more effective in combating constantly evolving cybercrimes.

This study attempts to shed light on the role that the Sudanese private banking sector can play towards eradicating digital financial illiteracy, in light of the low level of financial inclusion, as well as what roles these sectors must play to restore the confidence of customers and users of digital financial services after the development of electronic attacks on Banking and financial systems. Most of the studies reviewed by the researcher were focused on examining the level of digital financial illiteracy on a categorical level among users, while the researcher in this study attempts to combine the role of the banking sector in increasing awareness of digital financial illiteracy regarding electronic crimes.

RESEARCH METHODOLOGY

An exploratory research was designed to attain the key purpose of the study. Five (5) private Sudanese banks were selected based on their branches, mobile banking applications usage, advanced online services, largest e-commerce platforms and easy access to target groups. Using convenience sampling technique, a structured questionnaire was sent through private Sudanese banks' WhatsApp groups and Facebook accounts. A total of 447 completed questionnaires were received.

The questionnaire first includes the questions regarding the usage of banking technology and do they exposed to steal/hack the banking data electronically. Respondents who were using banking technology and exposed to hack their banking data are then asked to rate the constructs on 5-point Likert's scales using strongly disagree (1) to strongly agree (5). The multi-item scales were empirically tested and validated by previous research scholars. The researchers adapted six items of digital financial literacy awareness from Ravikumar et al., 2022. Seven items of digital financial literacy attitude and six items of role of digital banks for building user confidence are adapted from Ali et al., 2017. In addition, seven items of cyber security awareness (Mokha, 2017), seven items of cyber security attitude (Elradi, 2022; Alzubaidi,

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

2021) and seven items of role of digital banks for building user confidence towards cyber security (Alzubaidi, 2021; ISA et al., 2021; Acharya, S. and Joshi, S., 2020; Kshetri, N., 2019) were adapted.

The constructs' composite validity and reliability were tested (see table no.2) using SMART-PLS 4.0 to attain the key objectives of this study. The Cronbach's Alpha values for all the constructs are ranges from 0.65 to 0.87 that are considered good for measurement model. The discriminant validity for all the constructs are ranges from 68 percent to 86 percent except the role of banks construct (52 percent) which is very low (see table no 3). The results of discriminant validity supports for structural equation model.

DATA ANALYSIS

This study used SMART-PLS 4.0 to measure the constructs and demographic data (see table 1) for 447 respondents. Among the respondents, there were 67% male and 33% female. Their ages are between 18-24 years (4%), between 25-34 years (18%), between 35-44 years (65%) and remaining (13%) were 45 and above. The education among users, 32% doctorate, 10% masters, 36% bachelors, 14% diploma and 8% high schools. The employment status of banking service users were as follows: 25% users working in public sector, 29% users are working in private sectors and 46% are others (students, retired and unemployed) users.

Table 1: Respondents demographic data

Gender	***Numbers***	***Percentages***
Male	300	67
Female	147	33
	447	**100**
Age		
18-24	**18**	4
25- 34	**82**	18
35-44	**290**	65
45 and more	**57**	13
	447	**100**
Education		
High school or equivalent	36	8
Diploma	62	14
Bachelor	161	36
Masters	47	10
Doctorate	141	32
	447	**100**
Employment status		
Public sector	111	25
Private sector	131	29
Others (Students/Retired/Unemployed)	205	46
	447	**100**

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

Measurement Model

Statistical methods, especially SEM and confirmatory factor analysis, depend on the measurement model as shown in Figure 1. It analyses links between what is reflected in the model concept that goes with it to determine how accurate and dependable figures are. Researchers use this strategy to examine latent constructs and mental models of larger ideas. Finding factor loadings is a straightforward technique to compare measures to basic pieces. Validity and dependability are the most crucial aspects of a measuring model to evaluate. Cronbach's alpha, composite reliability and average variance extracted are examples. The empirical study gains legitimacy and rigor from a good measurement technique, which also serves as a foundation for future investigations (Aguirre-Urreta & Rönkkö, 2018).

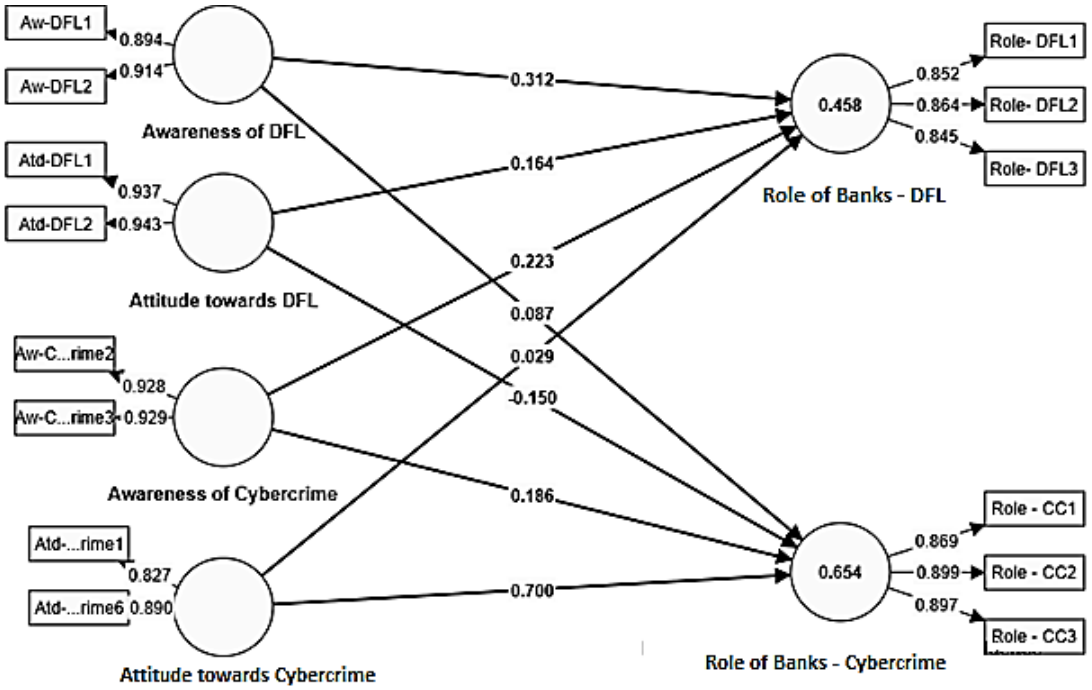

Figure 1: Measurement Model

Table 2: Construct Reliability & Validity

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Attitude towards Cybercrime	0.648	0.667	0.849	0.738
Attitude towards DFL	0.869	0.871	0.939	0.884
Awareness of Cybercrime	0.84	0.84	0.926	0.862
Awareness of DFL	0.777	0.782	0.899	0.817
Role of the bank Enhancing user confidence	0.867	0.872	0.918	0.789
Role of Banks-DFL	0.818	0.848	0.889	0.728

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

Cronbach's alpha, composite reliability (rho_a and rho_c), and average variance extracted (AVE) evaluate survey response reliability and validity. For reliability measures like Cronbach's Alpha and composite reliability (rho_a and rho_c) (Gill, 2020), a value above 0.6 indicates that section items consistently measure what they should. The concept explains a considerable portion of observed variable variability if AVE is 0.5 or higher. However, construct complexity may warrant smaller numbers. This threshold value helps researchers evaluate survey data dependability and validity for relevant conclusions. This section's questions measure cybercrime attitudes pretty consistently because the "Attitude towards Cyber Crime" construct has reasonable dependability. A greater composite reliability (rho_a and rho_c) indicates stronger item internal consistency. The construct explains much of the observed variance, as the average variance extracted (AVE) is substantial. The "Attitude towards DFL" construct exhibits high reliability and item internal consistency. Validity and reliability are indicated by high composite reliability and AVE. These constructs, "Awareness of Cybercrime" and "Awareness of DFL," have strong reliability and internal consistency. High composite reliability and AVE values imply construct validity. For "Role of the Bank to Enhance User Confidence" and "Role of Banks -DFL," dependability measures are adequate but very low. This suggests multiple responses to objects inside these categories. AVE and composite dependability remain satisfactory, indicating reliability and validity. Since our constructs measure what they should and are consistent, these reliability and validity measurements support our survey findings.

Table 3: Discriminant Validity - Fornell-Larcker criterion

	Attitude towards Cybercrime	Attitude towards DFL	Awareness of Cybercrime	Awareness of DFL	Role of the bank to Enhance user confidence	Role of Banks-DFL
Attitude towards Cybercrime	0.859					
Attitude towards DFL	0.682	0.94				
Awareness of Cybercrime	0.738	0.777	0.928			
Awareness of DFL	0.704	0.771	0.84	0.904		
Role of Banks-Cybercrime	0.797	0.539	0.659	0.621	0.888	
Role of Banks-DFL	0.526	0.598	0.635	0.647	0.523	0.854

In structural equation modeling (SEM), discriminant validity is crucial, especially when applying the Fornell-Larcker criterion as shown in Table 3. Discriminant validity determines whether the study's constructs are distinct. We use the Fornell-Larcker criterion to compare the square root of the average variance extracted (AVE) for each construct to the correlations between that construct and all other model components. It's like making sure each construct in your study is unique and not a copy. If the square root of the AVE for each construct is higher than its correlations with other constructs, the constructs are separate and discriminant. From your correlation matrix, we would calculate the square root of the AVE for each construct (which reflects how much variance it explains) and compare it to the correlations between that

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

construct and the others. When the square root of the AVE exceeds the correlation values, the Fornell-Larcker criterion is met, showing concept discriminant validity. This means each construct measures something distinct, not merely overlap.

Table 4: Collinearity Statistics – Outer Model

	VIF
Attitude -Cybercrime1	1.298
Attitude -Cybercrime6	1.298
Attitude -DFL1	2.443
Attitude -DFL2	2.443
Awareness-Cybercrime2	2.099
Awareness -Cybercrime3	2.099
Awareness -DFL1	1.676
Awareness -DFL2	1.676
Role of Banks - Cybercrime1	2.135
Role of Banks - Cybercrime2	2.290
Role of Banks - Cybercrime3	2.364
Role of Banks-DFL1	2.178
Role of Banks-DFL2	1.594
Role of Banks-DFL3	1.983

Collinearity statistics as shown in Table 4, in the outer model of a structural equation model (SEM) show if latent construct indicators are multicollinear. When two or more variables are highly linked, multicollinearity makes it hard to evaluate their influence on the latent construct. VIF values are provided for each pair of indicators inside the same latent construct in present data. Above 5 or 10 VIF values imply strong multicollinearity, whereas close to 1 implies low. For instance, in the construct "Attitude towards Cybercrime," “Attitude-Cyber Crime1" and “Attitude -Cyber Crime6" have a VIF of 1.298, indicating low multicollinearity. In "Role of Banks-DFL," "Role of Banks -DFL1" and "Role of Banks -DFL2" have a VIF of 1.594, showing low multicollinearity. The construct "Attitude-DFL," where the indicators “Attitude -DFL1" and” Attitude -DFL2" have 2.443 VIF values, has higher VIF values. While this is not high, it shows multicollinearity amongst various markers, which may need to be considered when interpreting results. Overall, collinearity statistics assist researchers discover potential multicollinearity issues across observed variables inside each latent construct in the SEM, which is essential for model reliability and validity (Rigdon & Gefen, 2011).

Table 5: Model Fit

	Saturated model	Estimated model
SRMR	0.088	0.089
d_ULS	0.820	0.837
d_G	0.734	0.7420
Chi-square	2387.433	2398.423
NFI	0.641	0.640

MFIs show how well the proposed structural equation model (SEM) matches the observed data as shown in table 5. Saturated and estimated models had Standardized Root Mean Square

ISSN 1533-9211

DOI: 10.5281/zenodo.10934838

Residual (SRMR) values around 0.09, indicating good fit. D_ULS and d_G indicate no change between the models, suggesting similar fit. Model fit may be improved due to significant chi-square values and poor Normed Fit Index (NFI) values around 0.64. Further model adjustments or fit indices may improve model goodness of fit (Dash & Paul, 2021).

Structural Model

Structural models visualize SEM construction as shown in figure 2. Observing the integration of the study's basic model components provides knowledge. We can test hypotheses about theoretical constructs, their observed indicators, and each other using a structural model. It allows construct-specific use of numerous indicator variables. Path factors show these events' magnitude and direction. Academics can validate concepts and assure organization with this method. This study's structural model explored numerous factors' linkages and effects on digital financial literacy (DFL) and user confidence. According to statistical analysis, attitudes about cybercrime strongly affect perceptions of banks' involvement in boosting user confidence, demonstrating a strong correlation between security and financial institution trust. Attitudes toward digital financial literacy also affected bank and individual DFL promotion. Awareness of cybercrime and digital financial literacy also shaped digital financial services attitudes and actions. These findings show the complicated relationship between attitudes, awareness, and perceptions in digital financial transactions, emphasizing the necessity for tailored initiatives to build trust, literacy, and user confidence (Sarstedt et al., 2020).

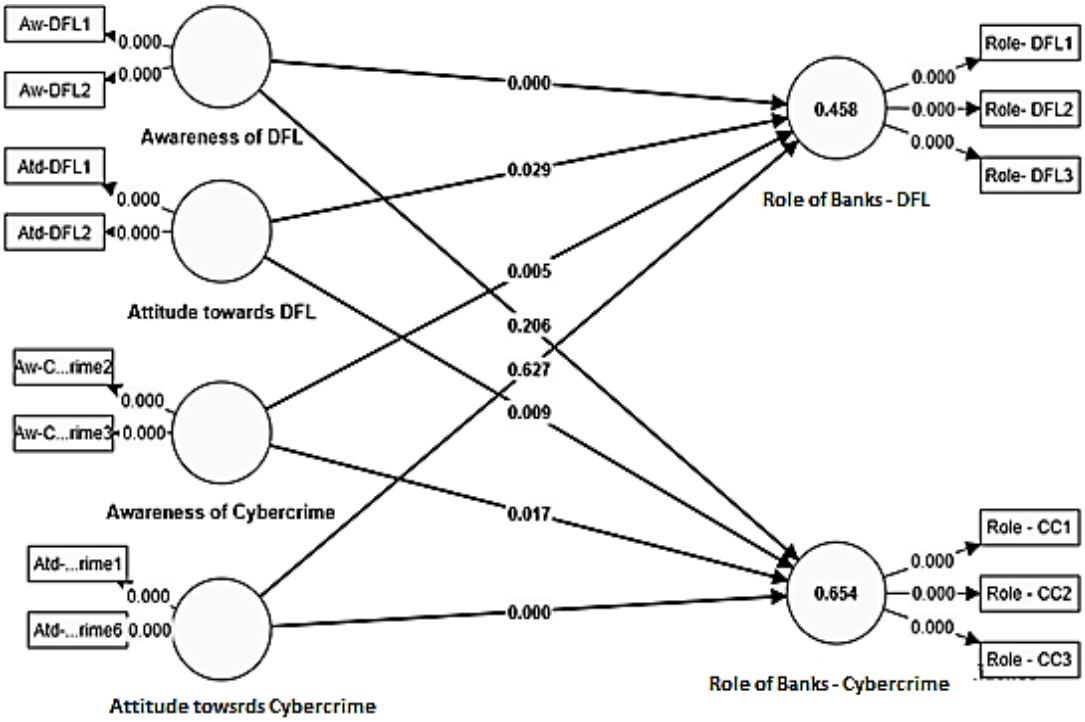

Figure 2: Structural Model

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

Table 6: Model Robustness

f - square matrix	Attitude towards Cybercrime	Attitude towards DFL	Awareness of Cybercrime	Awareness of DFL	Role of bank to Enhancing user confidence	Role of Banks-DFL	R - Square	R-square adjusted
Attitude towards Cybercrime					0.59	0.001		
Attitude towards DFL					0.02	0.017		
Awareness of Cybercrime					0.02	0.021		
Awareness of DFL					0.01	0.045		
Role of the bank-Cybercrimes							0.654	0.651
Role of Banks-DFL							0.458	0.454

The f-square values (Mustafa et al., 2020) show how each construct affects the model's outcome variables ("Role of the bank to Enhance user confidence" and "Role of Banks -DFL"). The predictor "Awareness of DFL" had the greatest influence size (f-square = 0.045) on both "Role of the bank to Enhance user confidence" and "Role of Banks -DFL," indicating that digital financial literacy has a greater impact on these outcomes than other predictions. Following that, "Attitude towards DFL" also has a significant influence (f-square = 0.022) on firms' role in boosting user confidence, demonstrating that digital financial literacy attitudes shape bank confidence. Compared to digital financial literacy knowledge and attitude, "Attitude towards Cybercrime" and "Awareness of Cybercrime" have less effect on both outcomes. These findings highlight the importance of digital financial literacy awareness and attitude in shaping bank assessments of user confidence and digital financial literacy.

R-square values show how much variance in the outcome variables ("Role of the bank to Enhance user confidence" and "Role of Banks -DFL") corresponds to model predictors. As for the "Role of the bank to Enhance user confidence," the model explains 65.4% of the variance (R-square = 0.654). This shows that the model's predictors—attitudes and awareness—explain a lot of the variation in perceptions of banks' role in user confidence. The model explains 45.8% of the variance in "Role of Banks -DFL," too (R-square = 0.458). This suggests that the model's predictors explain differences in perceptions of people's role in digital financial literacy. Due to the model's number of predictors, the corrected R-square values are significantly lower but still show strong explanatory power for both outcome variables.

These results show that attitudes and knowledge shape perceptions of banks and people's responsibilities in boosting user confidence and digital financial literacy. They can inform banking confidence and digital financial literacy programs by revealing the elements that shape these attitudes as shown in table 6.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

Table 7: Hypothesis Testing

		Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values	
H1	Attitude towards Cybercrime -> Role of the Bank to Enhance User Confidence	**0.700**	**0.700**	**0.045**	**15.433**	**0.000**	**Supported**
H2	Attitude towards Cybercrime -> Role of Banks-DFL	**0.029**	**0.034**	**0.060**	**0.486**	**0.627**	**Not Supported**
H3	Attitude towards DFL -> Role of bank to Enhancing user confidence	**-0.150**	**-0.151**	**0.058**	**2.600**	**0.009**	**Supported**
H4	Attitude towards DFL -> Role of Banks-DFL	**0.164**	**0.161**	**0.075**	**2.181**	**0.029**	**Supported**
H5	Awareness of Cybercrime -> Role of bank to Enhancing user confidence	**0.186**	**0.187**	**0.078**	**2.392**	**0.017**	**Supported**
H6	Awareness of Cybercrime -> Role of Banks-DFL	**0.223**	**0.223**	**0.080**	**2.790**	**0.005**	**Supported**
H7	Awareness of DFL -> Role of the bank to Enhance user confidence	**0.087**	**0.088**	**0.069**	**1.265**	**0.206**	**Not Supported**
H8	Awareness of DFL -> Role of Banks-DFL	**0.312**	**0.311**	**0.075**	**4.145**	**0.000**	**Supported**

In the present study, several hypotheses have been examined to determine the relationships between cybercrime, digital financial literacy (DFL), awareness, and perceptions of banks and individuals' roles in boosting user confidence and DFL as shown in table 7. Results were significant with hypothesis-specific values. Attitudes towards cybercrime strongly influenced perceptions of banks' role in boosting user confidence (H1, $p = 0.000$, $T = 15.433$), but not of individuals' role in promoting digital financial literacy (H2, $p = 0.627$, $T = 0.486$). In contrast, attitudes toward digital financial literacy significantly impacted perceptions of banks' role in boosting user confidence (H3, $p = 0.009$, $T = 2.600$) and people's role in promoting it (H4, $p = 0.029$, $T = 2.181$). Cybercrime awareness was also connected with opinions of banks' role in boosting user confidence (H5, $p = 0.017$, $T = 2.392$) and individuals' role in fostering digital financial literacy (H6, $p = 0.005$, $T = 2.790$). Digital financial literacy awareness strongly influenced perceptions of individuals' role in promoting digital financial literacy (H8, $p = 0.000$, $T = 4.145$) but not banks' role in boosting user confidence (H7, $p = 0.206$, $T = 1.265$). These exact values demonstrate how digital financial services and literacy models and views relate.

Table 8: Importance Performance Map

	Role of Banks-DFL	
	Importance	**Performance**
Attitude towards Cybercrime	0.029	50.901
Attitude towards DFL	0.164	50.586
Awareness of Cybercrime	0.223	50.936
Awareness of DFL	0.312	51.976

ISSN 1533-9211

DOI: 10.5281/zenodo.10934838

The Importance Performance Map (Ringle & Sarstedt, 2016) explains how context affects the importance and performance of different aspects or constructs as shown in table 8. Here, we're assessing "Role of Banks -DFL" elements' importance and performance. The data shows that "Awareness of DFL" is the most critical factor at 0.312. Its performance score is 51.976, slightly higher than other criteria but not significantly different. "Attitude towards Cybercrime" has the lowest relevance score of 0.029, indicating it's less relevant than the other elements. Its 50.901 performance score is comparable to other criteria. "Awareness of DFL" is the most significant component on the Importance Performance Map, and while its performance is slightly better than others, there's not much difference. While digital financial literacy understanding is recognized, these variables may still be improved in terms of performance or efficacy as shown in figure 3.

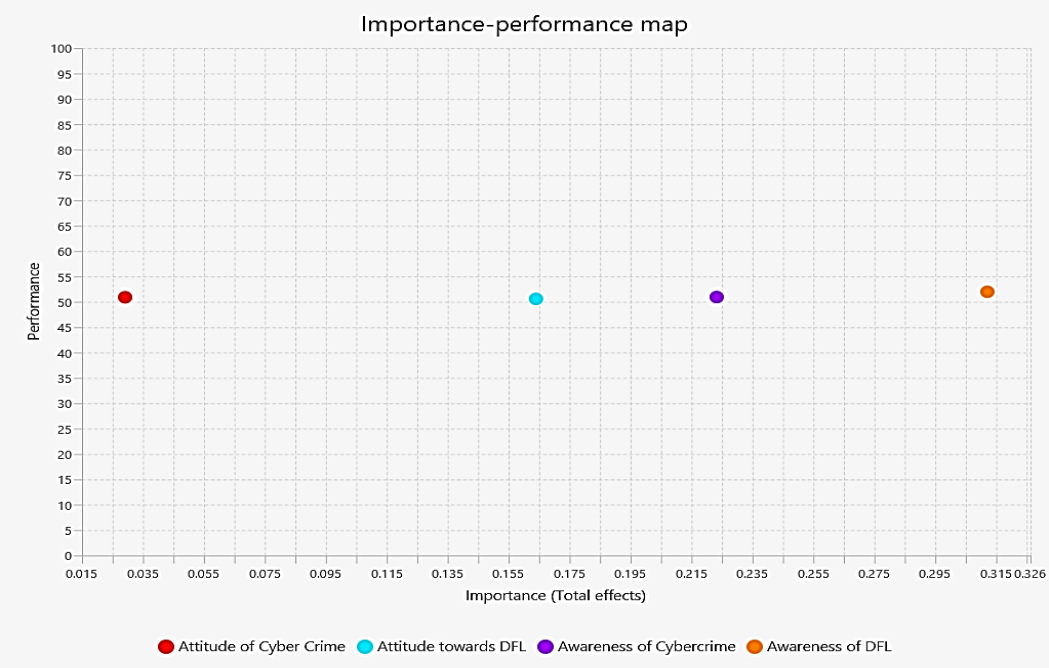

Figure 3: Importance – Performance Map

Table 9: Importance of Performance Map

Importance Performance Map	Role of Banks-DFL	
	Importance	MV performance
Attitude-Cyber Crime1	0.015	52.852
Attitude -Cyber Crime6	0.019	49.105
Attitude -DFL1	0.085	50.615
Attitude -DFL2	0.090	50.559
Awareness-Cybercrime2	0.120	53.132
Awareness -Cybercrime3	0.121	48.49
Awareness -DFL1	0.164	51.119
Awareness -DFL2	0.181	52.74

ISSN 1533-9211

DOI: 10.5281/zenodo.10934838

The "Role of Banks-DFL" (Role of banks towards Digital Financial Literacy) relevance Performance Map evaluates aspects based on their relevance as shown in figure 3 and figure 4. "Awareness of Cybercrime" and "Awareness of Digital Financial Literacy" (DFL) rank high in importance, ranging from 0.120 to 0.181. Even though awareness variables are crucial, their performance varies. For example, "Awareness of Cybercrime" has a great MV performance (53.132) but "Awareness of DFL" has a somewhat lower (51.119). This shows different levels of awareness-to-action efficacy. MV performance is reasonable for attitudes like "Attitude towards Cyber Crime" and "Attitude towards DFL," though less important. This map shows how awareness and attitudes affect digital financial literacy perceptions and behaviors, emphasizing the need for focused interventions to improve performance and correspond with perceived relevance.

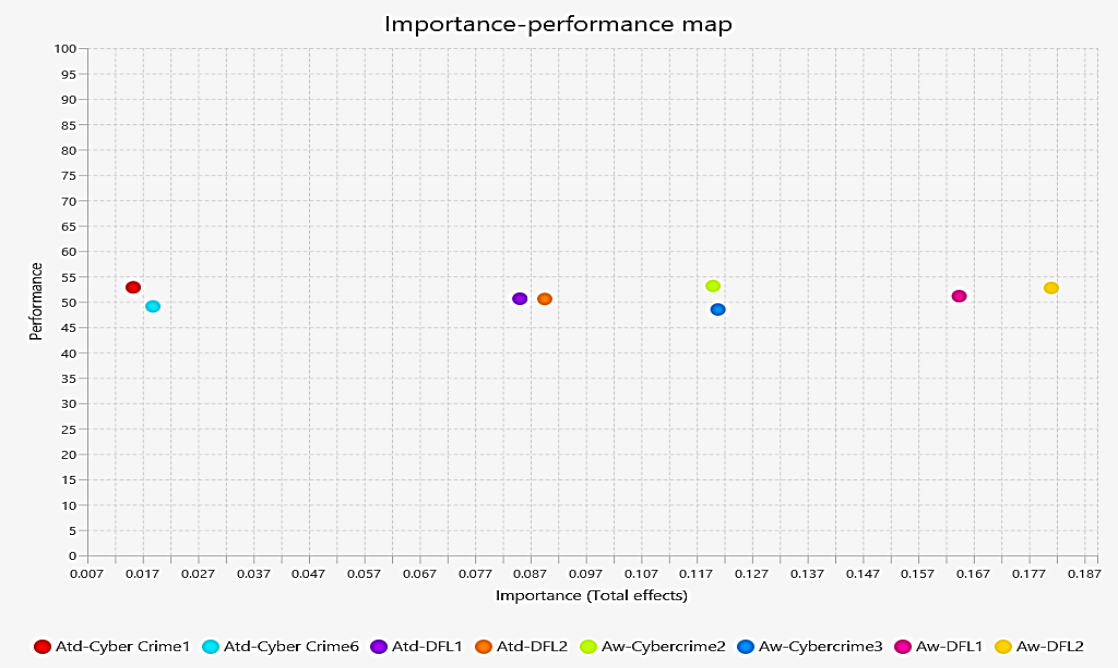

Figure 3: Importance – Performance Map

DISCUSSIONS AND CONCLUSIONS

The paper's aim is to measure the role of banks towards digital financial literacy (DFL) and cybercrime enhancing confidence among Sudanese banks' customers/users. Further examines the relationships between cybercrime, digital financial literacy (DFL), awareness, attitudes and role of banks in boosting user confidence. To obtain these objectives, a structured questionnaire was sent through WhatsApp and Facebook groups of private Sudanese banks. A total of 447 completed questionnaires received from the respondents. SMART-PLS 4.0 was used to analyze the collected data. To answer research objectives determining the roles of banks towards digital financial literacy (DFL) and cybercrime enhancing confidence among Sudanese banks' customers. Findings showed that DFL and cybercrime awareness have the greatest influence on both the role of banks enhancing user confidence towards the cybercrime and DFL. These

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

indicates the importance of DFL and cybercrime awareness in shaping bank assessment of user confidence and digital literacy. In addition, attitude towards DFL also has significant influence on banks' role in boosting user confidence but attitude and awareness towards cybercrime have less effect. Cybercrime is one of the most important issues that the banks must provide a safe online banking environment and also take appropriate countermeasures (Ali, 2019). The study demonstrated the several hypotheses that determines the relationships between cybercrime, awareness, attitudes and role of banks in boosting user confidence. The results depicted that attitudes towards cybercrime strongly influenced banks' role in boosting user confidence but not in promoting digital financial literacy. Further, users feel well protected from cybercrimes. Banks provide channels for reporting the security threats and information about the cybersecurity practices and hence protect the users from cyber frauds or crimes. Digital financial literacy (DFL) is also one of the important issues that cannot be neglected because lack of awareness may lower user confidence in using digital banking services. Scholars emphasized the importance of DFL that consumers must have the knowledge and ability to detect fraud attempts and employ best practices to avoid being victimized (Aziz and Naima, 2021; Morgan et al., 2019). The results demonstrated that attitude towards digital financial literacy (DFL) significantly impacted banks' role in boosting user confidence. Many previous studies have indicated these elements. Lack of DFL is a constraint for the rational and effective usage of digital financial banking services. Thus, DFL is a prerequisite to use Digital Financial Services (Ravi Kumar et al., 2022). In addition, DFL is an important component of education in this digital age (Morgan et al., 2019).

The distinctiveness of this study is to measure the relationships between DFL attitude, awareness, cybercrime attitude and awareness and the banks' role in boosting the user confidence. The findings provide the contributions to the policyholders either banking sectors or government organisations that increase the knowledge and awareness of digital financial literacy to avoid cyber threats through banks' online digital channels and defend banking system from unauthorized access and attack in cyberspace (Al-Alawi et al., 2019). Previous studies focused on digital financial services and cybercrimes dimensions but not focused the role of banks in boosting banking services users' confidence. No research has paid distinct scrutiny in boosting user confidence towards digital financial literary and cybercrimes. This study supplement past studies in the field of research.

This study cannot escape from the limitations as it was designed as a quantitative research rather than qualitative and mixed study whereby the dimensions of DFL and Cybercrime could be identified in more scientific ways. The other limitations include sampling because data was collected from few private Sudanese banks and hence generalization of results with private banks may be limited. The data in this study were collected from Private Banks' WhatsApp and Facebook groups, which may represent concern for quality of responses even though addressed validity threats. Limited access to banking information may also biased the results of the study. Future research should continue to identify the factors of digital financial literacy and cybercrimes that may reveal new findings. Future research may consider the impact of DFL and Cybercrime on the banks' role in boosting user confidence with different personality traits.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

References

1) Golden, W., & Cordie, L. (2022). Digital Financial Literacy. Adult Literacy Education, 4(3), 20-26.

2) Gilster, P., & Glister, P. (1997). Digital literacy (p. 1). New York: Wiley Computer Pub.

3) Alliance for Financial Inclusion (AFI), Digital Financial Literacy Toolkit, 2021, pp. 1-25. {Retrieved from https://www.afi-global.org/wp-content/uploads/2021/07/AFI_DFS_Literacy_Toolkit_V5_29July.pdf}.

4) Ravi kumar, T., Suresha, B., Prakash, N., Vazirani, K., & Krishna, T. A. (2022). Digital financial literacy among adults in India: measurement and validation. Cogent Economics & Finance, 10(1), 2132631.

5) Pazarbasioglu, C., Mora, A. G., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital financial services. World Bank, 54.

6) Al-Alawi, Adel Ismail and Sara Abdulrahman Al-Bassam (2019) Assessing the Factors of Cybersecurity Awareness in the Banking Sector, AGJSR 37 (4), pp. 17-31.

7) Khalid, W. E., Soussi, M. M., & Abdelmajid, R. (2023), The role of the investment actuary in managing financial market risks in light of the repercussions of geopolitical fluctuations. The Seybold report, 18(2).

8) CBOS, Central Bank of Sudan. 59th Annual Report, 2022. Retrieved from http://www.cbos.gov.sd.

9) Union of Arab Banks - The reality of financial inclusion and the role of financial technology in promoting it -Journal of Studies and Research - Issue 458, retrieved June 2022

10) OECD. (2017). G20/OECD INFE core competencies framework on financial literacy for adults. Available at https://www.oecd.org/finance/CoreCompetencies-Framework-Adults.pdf.

11) Morgan, P J., Bihong Huang, and Long Q. Trinh, (2019), The Need to Promote Digital Financial Literacy for the Digital Age, The Future of Work and Education for the Digital Age, T20 Japan March 31, 2019.

12) Rubble, M., Bailey, G. (2007). Digital Citizenship in Schools. Eugene, OR: ISTE, 21.

13) Prasad, H., Meghwal, D., & Dayama, V. (2018). Digital financial literacy: A study of households of Udaipur. Journal of Business and Management, 5, 23-32.

14) Park, Y. J. (2013). Digital literacy and privacy behavior online. Communication research, 40(2), 215-236.

15) Finau, G., Rika, N., Samuwai, J., & Mcgoon, J. (2016). Perceptions of Digital Financial Services in Rural Fiji. Information Technologies & International Development, 12(4), 11-21.

16) Belshaw, D. (2012). What is 'Digital Literacy'? [online] Available at: neverendingthesis.com/dougbelshaw-edd-thesis-final.pdf (accessed 21 November 2020).

17) Garcia, E., and Weiss, E. (2017). Education Inequalities at the School Starting Gate: Gaps, trends and Strategies to Address them. Report, Economic Policy Institute. Available at: epi.org/132500.

18) Mohd Yaziz Bin Mohd ISA, (2021), Wan Nora Binti Wan IBRAHIM, Zulkifflee Mohamed, The Relationship Between Financial Literacy and Public Awareness on Combating the Threat of Cybercrime in Malaysia Journal of Industrial Distribution & Business Vol 12 No 12 1-10

19) Ali, L. (2019). Cyber Crimes-A Constant Threat for The Business Sectors and Its Growth (A Study of the Online Banking Sectors in GCC). *The Journal of Developing Areas 53*(1), doi:10.1353/jda.2019.0016.

20) Elradi, Mohammed Daffalla * Altigani Abd alraheem Altigani Osman Idriss Abaker (2020), Cyber Security Awareness among Students and Faculty Members in a Sudanese College, Electrical Science & Engineering journal | Volume 02 | Issue 02 | October 2020

21) Ştefan, I. (2011). Cybercrime. Juridical Current, 14(3), 115-120.

22) Gupta, S. (2012). Buffer overflow attack. IOSR Journal of Computer Engineering, 1(1), 10-23

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10934838

23) Saravade, N; Bhalla, "Emerging trends and challenges in cyber security _ Reserve Bank Information Technology Private Limited (ReBIT)." 2018, [Online]. Available: https://rebit.org.in/whitepaper/emergingtrends-and-challenges-cyber-security

24) Dashora, K. (2011). Cybercrime in the society: Problems and preventions. Journal of Alternative Perspectives in the social sciences, 3(1), 240-259.

25) Mokha, A.K., 2017. A study on awareness of Cyber Crime and security. Research Journal of Humanities and Social Sciences, 8(4), pp.459-464.

26) Alzubaidi, A., 2021. Cybercrime awareness among Saudi nationals: dataset. Data in Brief, 36, p.106965.

27) Acharya, S. and Joshi, S., 2020. Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures. PalArch's Journal of Archaeology of Egypt/Egyptology, 17(6), pp.4656-4670.

28) Kshetri, N., 2019. Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), pp.77-81.

29) Aguirre-Urreta, M. I., & Rönkkö, M. (2018). Statistical inference with PLSc using bootstrap confidence intervals1. MIS Quarterly: Management Information Systems, 42(3). https://doi.org/10.25300/MISQ/2018/13587

30) Dash, G., & Paul, J. (2021). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. Technological Forecasting and Social Change, 173. https://doi.org/10.1016/j.techfore.2021.121092

31) Gill, S. L. (2020). Qualitative Sampling Methods. Journal of Human Lactation, 36(4). https://doi.org/10.1177/0890334420949218

32) Mustafa, N., Mohamed, Z., & Ubaidullah, N. H. (2020). Modeling of statistical reasoning and students' academic performance relationship through partial least squares-structural equation model (PLS-SEM). Universal Journal of Educational Research, 8(8). https://doi.org/10.13189/ujer.2020.080827

33) Rigdon, E. E., & Gefen, D. (2011). Questioning Some Claims Associated with PLS Path Modelling. American Marketing Association.

34) Ringle, C. M., & Sarstedt, M. (2016). Gain more insight from your PLS-SEM results the importance-performance map analysis. In Industrial Management and Data Systems (Vol. 116, Issue 9). https://doi.org/10.1108/IMDS-10-2015-0449

35) Sarstedt, M., Ringle, C. M., Cheah, J. H., Ting, H., Moisescu, O. I., & Radomir, L. (2020). Structural model robustness checks in PLS-SEM. Tourism Economics, 26(4). https://doi.org/10.1177/135

36) Aziz, A., & Naima, U. (2021). Rethinking digital financial inclusion: Evidence from Bangladesh. Technology in Society, 64, 101509.