Hindawi
Human Behavior and Emerging Technologies
Volume 2023, Article ID 2103442, 10 pages
https://doi.org/10.1155/2023/2103442

Research Article

Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation

Amar Johri[1] **and Shailendra Kumar**[2]

[1]*College of Administrative and Financial Sciences, Saudi Electronic University, Riyadh, Saudi Arabia*
[2]*Department of Management Studies, Indian Institute of Information Technology, Allahabad, Uttar Pradesh, India*

Correspondence should be addressed to Amar Johri; a.johri@seu.edu.sa

Received 24 August 2022; Revised 26 November 2022; Accepted 22 December 2022; Published 12 January 2023

Academic Editor: Zheng Yan

The annual rate of cybersecurity breaches has risen in the last few years, exposing millions of records in some cases. The average data breach cost in 2021 was a massive $4.24 million. This study examines customer awareness and satisfaction with cybersecurity in the context of the digital transformation of banking in Saudi Arabia. The study is empirical and based on the data collected from 355 banking customers in Saudi Arabia. Three significant aspects of cybersecurity, including cyberattacks, phishing, and hacking, have been analyzed through various dimensions. Customer satisfaction with bank cybersecurity assistance and their expectations of technical support and services on cybersecurity has also been studied. ANOVA and bivariate regression analysis are used to study the impact of cyberattack, phishing, hacking, cybersecurity assistance, and expectations on cybersecurity's technical awareness on customer satisfaction. The results show that digital transformation has boosted the banking sector, and users benefit from online services. However, an increase in the awareness level of customers on cyberattack, phishing, and hacking activities will influence customers' satisfaction with digital transactions. The results also revealed that customers need more satisfaction on security level aspects from the bank's side, and banks should provide regular training programs to safeguard customers from cyberattacks. If banks prepare more secure cybersecurity management, their long-term sustainability goals could be easily achieved.

1. Introduction

Digital transformation in the banking sector can be viewed as a great opportunity but brings multiple challenges also. Mobile banking and Internet banking are straightforward approaches in doing multiple financial transactions in banking digital transformation. While customers benefit from such services, the threat and possibility of cyberattacks also become a significant challenge for these digital services. Cyberattacks, banking fraud, hacking, phishing, and security awareness are significant challenges resulting from digital transformation in the banking sector. Generally, customers' awareness of cybersecurity could be more questionable in various aspects. They need to know how to use technology safely while using the banks' digital platforms. Customers are usually victims of cyberattacks, phishing, and hacking, leading to digital/cyber literacy among the bank's customers. A significant challenge for the banking sector is the advancement and innovation of digital technology. It has been considered an opportunity for growth and development in the present business model of the bank and a threat to the sustainability of the bank's business existence [1, 2]. Information technology also plays an essential role in such a kind of digital transformation. It provides operation support on various technical aspects and offers a platform for significant innovation in digital services [3]. There is a significant discussion required on monitoring the bank's cybersecurity. In the digital transformation, banks are now proceeding to digitize all banking services, including customers' confidential data, stored and flowing from one place to another over

a network. Several cyberattacks occur on these services because mobile banking and Internet banking users are less aware. Banks must strengthen their cybersecurity policies to safeguard against such attacks and increase customer satisfaction. Active awareness is also required towards ATM skimming among banking customers so that they can safeguard themselves against such types of fraud. The widespread problem of ATM skimming requires targeted action. It is called ATM skimming when skimming devices, like the rain cover and fake keypad, are installed on ATM machines. Card skimming is a significant contributor to the financial sector's already widespread card fraud problem.

Cybersecurity awareness has become a critical parameter to safeguard our mobile banking apps and Internet banking-related activities in the digital transformation of banking activities. The study covers three essential types of cybersecurity such as cyberattacks, hacking, and phishing. It is essential to explore and understand the awareness level of mobile banking apps and Internet baking users regarding their cybersecurity to protect them from cyberattacks. The present study will help customers understand various general and technological aspects of their cybersecurity. It will also help banks understand the present satisfaction level of customers on bank's security, cybersecurity assistance offered by the bank, and their expectations on technological support cybersecurity services.

2. Literature Review

Several studies have been conducted to determine the importance of cybersecurity, digital transformation adoption, and digital transformation in the financial sector, particularly in the banking sector. According to a prior study, traditional banks become more exposed to cyberattacks after cooperating with fintech companies [4, 5]. Skinner [6] has illustrated the impact of social networks on digitization in various industries. The study also looked at how digital disruption is affecting conventional social interactions. The growing usage of mobile devices is another important factor that has benefited the digital transformation process. The use of mobile banking apps climbed 19 percentage points between 2013 and 2014, according to a Bain & Company survey of digital clients from 22 countries, while the use of computer-based banking services remained virtually steady [7]. The term "digitalization" was initially created in 2000, and it has since become a significant driver of digital transformation, enabling a wide range of business models and organizations [8]. Acts that potentially harm an organization's assets are classified as threats. Cyberattacks wreak havoc on software, hardware, and data in particular. Microsoft created STRIDE, a standard threat classification system [9].

Digital transformation is described by Stolterman and Fors [10] as "the changes that digital technology entails or effects on all facets of human life." Digitization was initially described as converting text and images into binary digits. This makes it possible to manage, copy, and distribute data at a cheap cost on a large scale at an affordable price [11]. Digital systems and platforms evolve, resulting in new products, services, business models, and behaviours, as well as new working approaches and more efficient business process development opportunities, all of which impact society [11]. Customer satisfaction, experiences, awareness, and expectations are all elements to examine when evaluating recent digital transformation developments. Mbama and Ezepue believe that a positive customer experience is associated with higher customer satisfaction and loyalty (2016, p.250). Customers' experiences with digital banking are influenced by various elements, including the quality of their contacts with staff, the quality of their services, perceived usability, perceived risk, and observed value ([12], p.250).

Improved client experience can be achieved by providing high levels of security, increasing the quality of service provided, and providing value-added services. As the number of people who use digital banking to access bank services grows, more resources should be allocated to mobile banking services, which are becoming increasingly popular ([12], p.250). To provide a pleasant customer experience, banks must first understand the needs of their customers. Therefore, financial institutions recommend constant communication with consumers ([12], p.250). According to Jamal and Naser [13], consumer satisfaction is defined as the feeling or attitude a client has toward a product or service after using or receiving it. Customer satisfaction is a critical marketing approach since it connects multiple stages of a consumer's buying transaction in a single transaction ([13], p.147). Electronic financial services are driven by several factors, including technology, globalization, regulation, entrepreneurship, money, and competition ([14], p.367). Therefore, a new reality will form the future of digital banking, where e-money can be easily moved without needing a financial institution to facilitate the transfer of funds ([14], p.391).

Due to the vulnerability of the digital banking industry to a range of cyberattacks, security has become a priority. Banks are expected to maintain and upgrade security measures such as virus controls, password protection, intrusion detection, and technical system updates regularly, according to federal regulations ([14], p.392). Banks' expanded digital offerings necessitate developing more comprehensive technology solutions that are safe, secure, and dependable. Additionally, this technical design must connect the bank's legacy systems to a common thread across them ([14], p.392).

According to Mukherjee and Nath [15], the banking industry also suffers from trust due to digitalization. One of the study's key findings was a model of trust for online relationship banking, which indicated that trust is crucial for customers' commitment to online banking [15]. Banks must adapt to their client's changing needs as they migrate to the Internet, but the issue is that most banks still need to prepare [16].

The findings of Fiserv's research measuring the value of digital interaction show that digital banking results in the enhanced generation of revenue, enlarged product holdings and customer retention, decreased customer attrition, and more activities of the transaction [17].

To produce profit for their shareholders, banks must change how they communicate with their customers, and

technology plays an increasingly important role. However, rather than being only a transaction processor, this needs a change to long-term business partnerships with consumers and suppliers ([14], p.366). Banks are already aware of their future route, according to Lebo [18], and are seeking to minimize worries by bringing in digital expertise, becoming more customer-centric, and delivering requested services.

Al-Alawi et al. [19] stated that it might be more challenging to identify and prioritize risks and decide which protocols to address threats because banks' cyber responsibilities are spread across numerous divisions. Cawley [20] suggests that the banking sector needs help keeping up with high-tech innovation trends, particularly laws regulating banking system operations. Two-factor authentication, according to Cawley, is a security measure used to defend client bank accounts against online intrusions.

According to Kuepper [21], due to their prompt reporting of stolen funds to the bank, clients experience minimal losses due to banking cyberattacks. In order to minimize each of these threats, significant expenditures in technology and training are necessary ([22], p. 10). Additionally, customers must cooperate, be aware of the numerous cyber dangers, and respect privacy regarding security measures.

Claessens et al. [23] report that a range of frauds or cybercrimes, such as ATM fraud, cyber money laundering, and credit card fraud, has been seen in the banking industry. Because the banking industry's defensive mechanism has several flaws, Florêncio and Herley [24] contend that strategies to increase awareness of the actions that may be taken to combat cybercrime in the banking sector are needed. Lallie et al. [25] concentrated on cyberattacks and epidemic-related cybercrime. This study's findings can raise people's knowledge of other institutions, such as the government, the media, and other organizations. The study's findings can be used to educate the general public on the procedures that should be done to prevent cyberattacks and other crimes [25].

Information security is dependent on three main pillars: people, processes, and technology, according to a study on cybersecurity through employee hacking [26]. The empirical results of surveys and in-depth interviews with information security managers and users indicate a digital divide between these groups regarding their perspectives and experiences with information security practices [27]. Da Veiga and Eloff [28] proposed a framework to cultivate an organization's information security culture and provide examples of its use. The research highlighted the significance of establishing an information security culture that institutionalizes information security throughout the organization to address behavioural issues. A well-established culture of information security can help reduce the dangers posed by staff members' careless handling of data.

However, this importance depends on users' capacity to make important information security decisions. Information security risks must be explained to all users and their responsibilities for the security process [29]. The cyberbreach of fintech firms increases traditional banks' risk and fraud exposure [30]. As a result, fintech firms must ensure that they follow the cybersecurity rules of the countries where they do business.

According to Lewis and Baker [31], the rise in cybercrime has correlated with the financial inclusion of fintech companies. According to studies, hackers are increasingly targeting fintech organizations and the businesses of their partners [32]. The banking industry's most serious issue is the need for more technological adoption. One source of danger for Internet banking customers is their behaviour regarding online banking [33]. If an Internet banking security risk exists, monetary losses may occur. Security breaches are becoming more widespread in the banking and finance industries [34].

The existing literature primarily focused on customers' preferences, contentment, and experiences with cybersecurity. However, researchers did not find any significant studies focusing on customer awareness of cybersecurity factors and their impact on their satisfaction with banking services. Researchers also discovered a significant research gap in customers' satisfaction with current cybersecurity help provided by banks and their expectations for technical support and cybersecurity awareness programs from banks. The current research is aimed at filling this gap.

3. Objectives of the Study

This study has been done keeping in view the following objectives:

(1) To analyze the customer's cybersecurity awareness, including cyberattacks, phishing attacks, and hacking

(2) To determine the customer's satisfaction with the bank's monitoring and cybersecurity services

(3) To find out the customer's expectations from banks to make them aware of cybersecurity

4. The Research Model and Hypotheses

Based on the analysis of the literature review and the advice of the expert in cybersecurity, the study identified five independent variables: cyberattacks, phishing attacks, hacking, cybersecurity services and assistance offered by banks, and technical support and training and development on cybersecurity by banks. To understand the impact of these variables, the study identified two dependent variables: customer awareness of cybersecurity and customer satisfaction with cybersecurity. To measure the study's objectives, these variables were used to create the proposed hypothesis and became the background of the proposed research model.

The following hypotheses are being tested following the study's stated goals and proposed model:

H1. Customer's awareness of cyberattack will influence the customer's awareness of cybersecurity

H2. Customer's awareness of phishing attacks will influence the customer's awareness of cybersecurity

H3. Customer's awareness of hacking of mobile apps and Internet banking activities will influence the customer's awareness of cybersecurity

H4. Customers' satisfaction will be influenced by robust cybersecurity services and assistance offered by banks

H5. Customers' satisfaction will be influenced by technical support and training and development on cybersecurity by banks

The conceptual framework used in this study is shown in Figure 1.

5. Methodology

5.1. Data Collection and Sampling. The research method used in this study is descriptive and quantitative. The study incorporated both primary and secondary data. Primary sources include a structured questionnaire. The secondary sources include research articles, journals, business magazines, and published literature.

A structured questionnaire, constructed with the help of available literature, was utilized to collect the data from the respondents. The questionnaire contained 29 questions related to awareness of cyberattacks, hacking, and phishing activities, by which users are generally affected and become victims of such attacks. To formulate the survey questions, an extensive literature review was conducted. The previously published papers were studied and thoroughly examined to explore the possible literature related to the present study. The literature was used to create the statement-based questions which became part of our questionnaire. We also referred to the YouTube video of the cybersecurity experts and explored their comments in designing the questions for the questionnaire. The 29 questions used in the survey questionnaire result from this process.

We also pretested the questionnaire with 55 respondents, and after successful testing of the questionnaire, the final questionnaire was sent for data collection. Convenience random sampling, a nonprobability sampling, was used to collect the data. Questions related to customers' satisfaction with cybersecurity assistance provided by the banks and their expectations of the technical support were also included in the questionnaire. The responses were measured using a five-point Likert scale, where 5 = strongly agree and 1 = strongly disagree. The data was gathered by the convenience sample method. Three hundred and fifty-five people responded to the questionnaire and submitted their responses.

5.2. Data Analysis. The data gathered in this study were analyzed using a statistical package for social sciences (SPSS). Appropriate statistical tools were used to examine the collected data. A descriptive statistic was employed to describe the frequencies and percentages of the respondents' demographic profiles. The relationship between the variables was examined using correlation analysis. The hypotheses were tested using analysis of variance (ANOVA) and regression analysis.

The study's analysis is divided into two sections. The customer's awareness of cyberattacks, phishing, and hacking was investigated in the first section. The second section examined the customer's satisfaction with cybersecurity awareness assistance by the bank and technological support, training, and development on cybersecurity awareness.

5.2.1. Respondent's Demographic Profile. Table 1 summarizes the respondents' demographic characteristics. 292 (82.82%) of the 355 responders were men, while 61 (17.18%) were women. 14 (3.94%) respondents were under the age of 20, 200 (56.34%) respondents were between the ages of 20 and 40, 89 (25.07%) respondents were between the ages of 40 and 50, 44 (12.39%) respondents were between the ages of 50 and 60, and 8 (2.25%) respondents were over the age of 60. 35 (9.86%) respondents had a diploma, 145 (40.85%) had a bachelor's degree, 140 (39.44%) had a master's degree, and 35 (9.86%) had a Ph.D. A total of 188 respondents (52.96%) were self-employed, 137 (38.59%) worked for the government, and 30 (8.45%) had their enterprises. 347 (97.75%) of the participants had bank accounts, while 8 (2.25%) did not have bank accounts. For their financial transactions, many respondents chose mobile banking and Internet banking on laptops and desktops, which is a good indicator for analysis. The descriptive statistics in Table 2 are based on the mean, standard deviation, and minimum and maximum values.

5.2.2. Descriptive Statistics. Table 2 represents the descriptive statistics of independent variables. By observing the mean, standard deviation, and minimum and maximum values indicated in Table 2, it could be summarized that all three variables have a significant role in the customer's awareness of cybersecurity. However, the impact of hacking has a high impact as compared to phishing and cyberattacks.

We have also analyzed the individual score of each activity, and based on mean values, it was found that the customers are aware of cyberattacks, phishing, and hacking. However, there are a few activities of which they need more awareness. Customers need to gain more knowledge about getting secured against all types of cyberattacks and how to protect mobile banking apps and Internet banking from cyberattacks, phishing, and hacking while using them on smartphones and laptops/desktops. Customers also do not use a separate smartphone and laptop/desktop for online banking services; however, it is strongly recommended. Customers' knowledge is also less in case of awareness on identifying suspicious phone calls, e-mails, and SMS causing phishing attacks. Most customers also do not use a firewall program to safeguard laptops/desktops from unauthorized access. Customers generally do not give preference awareness about the safety features of the Internet while using banking activities on smartphones and laptops/desktops and use the on-screen virtual keyboard for providing the password for mobile banking apps and Internet banking because it decreases the chance of password theft.

5.2.3. Reliability Test. The reliability analysis (Cronbach's alpha) was used to analyze the internal consistency of the constructs. SPSS was used to examine the reliability of each construct. Reporting Cronbach's alpha coefficient for measuring the internal consistency reliability is essential for the scales if Likert-type scales have been used in a research

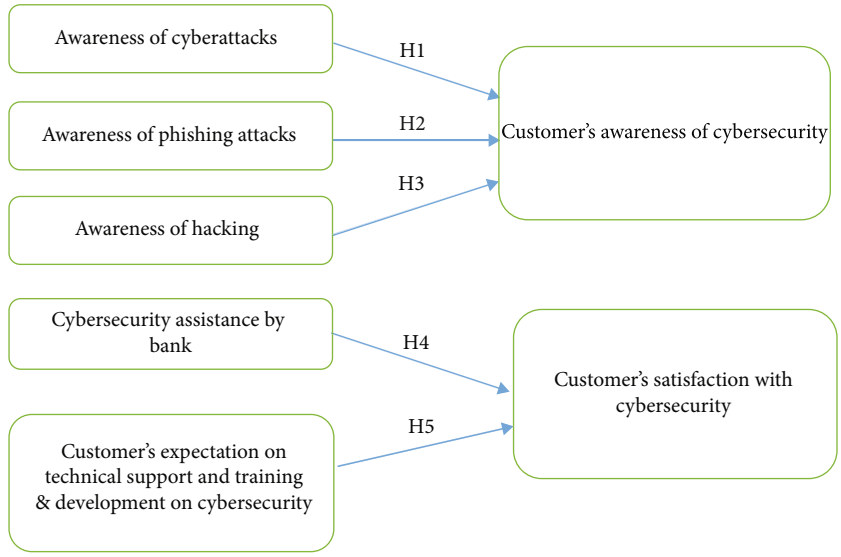

Figure 1: Conceptual framework on customer's awareness of cybersecurity and conceptual framework on customer's satisfaction with cybersecurity.

Table 1: Demographic profile of the respondents.

Variable	Category	Frequency	Percentage
Age	Less than 20	14	3.94
	20-30	74	20.85
	30-40	126	35.49
	40-50	89	25.07
	50-60	44	12.39
	Above 60	8	2.25
Gender	Male	294	82.82
	Female	61	17.18
Educational level	Diploma	35	9.86
	Bachelor's degree	145	40.85
	Master's degree	140	39.44
	Ph.D.	35	9.86
Profession	Government employee	137	38.59
	Private employee	188	52.96
	Business	30	8.45
Bank account	Yes	347	97.75
	No	8	2.25
Use of M-banking and I-banking	Yes	329	92.68
	No	26	7.32
Usage tenure	1-5 years	164	46.20
	6-10 years	128	36.06
	10-15 years	46	12.96
	More than 15 years	17	4.79
Prefer mode of financial transactions	Mobile banking	95	26.76
	Internet banking on laptop/desktop	56	15.52
	Both	204	57.76

Table 2: Descriptive statistics of the variables.

	N	Minimum	Maximum	Mean	Std. deviation
Cyberattacks	355	1.33	5	3.531	0.735
Phishing	355	1.33	5	3.362	0.590
Hacking	355	1.57	5	3.789	0.688

Table 3: Reliability of measurements.

Constructs	N	Number of items	Cronbach's alpha	Internal consistency
Customer's satisfaction	355	5	0.812	Excellent
Cyberattacks	355	6	0.823	Excellent
Phishing	355	5	0.855	Excellent
Hacking	355	5	0.901	Excellent
CSAAB	355	4	0.790	Excellent
TS T&D	355	4	0.840	Excellent

method [35]. Table 3 summarizes the constructions' reliability as well as their interpretations. Cronbach's alpha ranged from 0.812 to 0.901, indicating that the internal consistency of the data acquired was of good level and reliable. This demonstrates that the scale used to collect data was trustworthy and sufficient for the inquiry.

5.2.4. Correlation Analysis. Table 4 shows the relationship between the dependent variables and independent variables. Typically, the test results are contrasted using Pearson's correlation coefficient [36]. According to Litwin [37], a correlation coefficient value of less than 0.7 is considered good. There was a significant association among awareness of cyberattacks ($r\,(355) = 0.35$, $p < 0.05$), awareness of phishing attacks ($r\,(355) = 0.13$, $p < 0.05$), awareness of hacking ($r\,(355) = 0.51$, $p < 0.05$), and customer's awareness of cybersecurity.

5.2.5. Regression Analysis. Bivariate regression analysis was utilized to test the study's hypotheses. The ANOVA of the three regression predictor model is shown in Table 5. The findings of the regression analysis are summarized in Table 6, and the coefficients of the regression models are shown in Table 7. At the 0.05 level of significance, all three predictors significantly impacted the customer's awareness of cybersecurity.

A strong collective impact between awareness of cyberattacks, phishing, and hacking and customers' cyber security awareness was found in the regression results ($R^2 = 0.272$, $F(3, 351) = 43.908$, $p = 0.01$). To examine the association between the dependent and independent variables, individual predictors were examined. According to the results of the regression model, "awareness of cyberattacks" ($R^2 = 0.123$, $F(1, 353) = 16.042$, $p = 0.01$) was found to be a significant predictor, so this supports acceptance of Hypothesis 1. In addition, "awareness of phishing" ($R^2 = 0.019$, $F(1, 353) = 2.278$, $p = 0.133$) was determined to be an insignificant predictor; as a result, Hypothesis 2 was deemed rejected; however, "awareness of hacking" ($R^2 = 0.265$, $F(1, 353) = 41.127$, $p = 0.01$) was found to be a significant predictor; as a result, Hypothesis 3 was accepted.

Referring to Table 7, the third predictor has the most significant impact on the customer's awareness of cybersecurity ($\beta = 0.500$, $t = 6.413$, $p < 0.05$). The impact of the first predictor ($\beta = 0.319$, $t = 4.005$, $p < 0.05$) is after the third predictor. However, the impact of the second predictor was not found to be significant in the model ($\beta = 0.158$, $t =$ 6.1.509, $p > 0.05$).

5.2.6. Descriptive Statistics. Table 8 represents the descriptive statistics of independent variables. Table 8 shows that cybersecurity awareness assistance by the bank to their existing customers is appropriate, and they have significant awareness of these types of assistance. However, as per the mean value, it is revealed that customers need more technological support, training, and development on their cybersecurity.

5.2.7. Correlation Analysis. Table 9 shows the correlation between the dependent and independent variables. There was a strong correlation between cybersecurity awareness assistance by the bank ($r\,(355) = 0.40$, $p < 0.05$), technological support, training and development on cybersecurity awareness ($r\,(355) = 0.44$, $p < 0.05$), and customer's satisfaction with cybersecurity.

5.2.8. Regression Analysis. The ANOVA for the two regression predictor models is depicted in Table 10. Table 11 presents a summary of the regression analysis results, whereas Table 12 presents the coefficients of the regression models. At the 0.05 level of significance, it was proven that both predictors were statistically significant and that they had a statistically significant effect on the customer's satisfaction with cybersecurity.

Individual predictors were examined to examine the association between the dependent and independent variables. Because "bank assistance with cybersecurity awareness" ($R^2 = 0.166$, $F(1, 353) = 22.828$, $p = 0.01$) was shown to be a significant predictor in the model, Hypothesis 4 was accepted. Additionally, "technical assistance, training, and development on cybersecurity awareness" ($R^2 = 0.198$, $F(1, 353) = 28.313$, $p = 0.01$) were identified as a significant predictor in the model, indicating that Hypothesis 5 was accepted.

According to the values of Table 12, the first predictor has the most significant impact on the customer's satisfaction with cybersecurity ($\beta = 0.465$, $t = 4.777$, $p < 0.05$). The impact of the second predictor ($\beta = 0.366$, $t = 5.321$, $p <$ 0.05) is after the first predictor. Both predictors were found to be significant in the model.

6. Results and Discussion

The main objective of this research is to investigate and explore the customer's awareness of cybersecurity in mobile banking apps and Internet banking. The study explores the customer's awareness of cyberattacks, phishing, and hacking. The study is also aimed at assessing the customer's

Table 4: Correlation analysis of the variables.

	Cyber attack	Phishing	Hacking	Customer's satisfaction	p value
Cyberattack	1				0.01
Phishing	0.427266007	1			0.01
Hacking	0.81506966	0.466915388	1		0.01
Customer's awareness	0.351234394	0.139973141	0.514897904	1	0.01

Table 5: Variation analysis of the variables (ANOVA).

ANOVA[a]						
Model		Sum of squares	Df	Mean square	F	Sig.
1	Regression	6.362	1	6.362	16.042	0.000[b]
	Residual	45.214	353	0.396		
	Total	51.577	354			
2	Regression	1.010	1	1.010	2.278	0.133[c]
	Residual	50.567	353	0.443		
	Total	51.577	354			
3	Regression	13.674	1	13.674	41.127	0.000[d]
	Residual	37.903	353	0.332		
	Total	51.577	354			

[a]Dependent variable: customer's awareness of cybersecurity. [b]Predictors: (constant) and awareness of cyberattacks. [c]Predictors: (constant) and awareness of phishing attacks. [d]Predictors: (constant) and awareness of hacking.

Table 6: Regression model summary[b].

Model	R	R^2	Adjusted R^2	Std. error of the estimate	F change	Significance F
1	0.351[a]	0.123	0.115	0.629	16.042	0.000
2	0.139[a]	0.019	0.010	0.666	2.278	0.133
3	0.514[a]	0.265	0.258	0.576	41.127	0.000

[a]Predictors: (constant), awareness of cyberattacks, awareness of phishing attacks, and awareness of hacking. [b]Dependent variable: customer's awareness of cybersecurity.

Table 7: Coefficient regression models 1, 2, and 3.

Coefficients[a]					
Model	Unstandardized coefficients		Standardized coefficients	t	Sig.
	B	Std. error	Beta		
(Constant)	2.327	0.352		6.595	0.000
Awareness of cyberattacks	-0.170	0.125	0.319	4.005	0.000
Awareness of phishing	-0.132	0.102	0.158	1.509	0.133
Awareness of hacking	0.995	0.137	0.500	6.413	0.000

[a]Dependent variable: customer's awareness of cybersecurity.

Table 8: Descriptive statistics of the variables.

	N	Minimum	Maximum	Mean	Std. deviation
CSAAB	355	2.5	5	4.318	0.587
TS T&D	355	1.33	5	4.114	0.814

Table 9: Correlation analysis of the variables.

	CSABB	TS T&D	Customer's satisfaction	p value
CSABB	1			0.01
TS T&D	0.749724306	1		0.01
Customer's satisfaction	0.408460874	0.44604154	1	0.01

Table 10: Variation analysis of the variables (ANOVA).

Model		ANOVA[a] Sum of squares	Df	Mean square	F	Sig.
1	Regression	8.605	1	8.605	22.828	0.000[b]
	Residual	42.972	353	0.376		
	Total	51.577	354			
2	Regression	10.261	1	10.261	28.313	0.000[c]
	Residual	41.316	353	0.362		
	Total	51.577	354			

[a]Dependent variable: customer's satisfaction with cybersecurity. [b]Predictors: (constant) and cybersecurity awareness assistance by the bank. [c]Predictors: (constant), technological support, training, and development on cybersecurity awareness.

Table 11: Regression model summary[b].

Model	R	R^2	Adjusted R^2	Std. error of the estimate	F change	Significance F
1	0.408[a]	0.166	0.159	0.613	22.828	0.000
2	0.446[a]	0.198	0.191	0.602	28.313	0.000

[a]Predictors: (constant), cybersecurity awareness assistance by the bank, technological support, training, and development on cybersecurity awareness. [b]Dependent variable: customer's satisfaction with cybersecurity.

Table 12: Coefficient regression models 1 and 2.

Model	Coefficients[a] Unstandardized coefficients		Standardized coefficients	t	Sig.
	B	Std. error	Beta		
(Constant)	2.026	0.416		4.862	0.000
Cyber security awareness assistance by bank	0.192	0.143	0.465	4.777	0.000
Technological support, training, and development	0.262	0.103	0.366	5.321	0.000

[a]Dependent variable: customer's satisfaction with cybersecurity.

satisfaction with cybersecurity services offered by the banks and their expectation of technical support and cybersecurity awareness program provided by banks. The study is divided into two parts. In the first part, the customer's awareness of cybersecurity was analyzed, focusing on cyberattacks, phishing, and hacking. In the second part of the study, the customer's satisfaction with the cybersecurity assistance and customer's expectations from the bank related to cybersecurity was studied.

It is highly suggested to raise the awareness of banking sector cybercrime prevention techniques due to the banking industry's flawed defense mechanism [24]. The results of the ANOVA indicated that customers are aware of cyberattacks, phishing attacks, and hacking, but the level of awareness is not the same in all three types of attacks. Awareness level is more in cyberattacks and hacking but less in phishing attacks.

The first independent variable, cyberattack, is significant in customer satisfaction, indicating that customer satisfaction with cyberattack awareness is satisfactory. If banks increase customer awareness of cyberattacks, their satisfaction with digital services will increase. The second independent variable, phishing, is found insignificant in customer satisfaction, indicating that customer satisfaction with phishing awareness could be more satisfactory. This insignificance is due to the customers' awareness of the identification of such e-mails, phone calls, and SMS, which cause phishing attacks, which is significantly less. We did not find any evidence from sample data about phishing attacks; however, the data shows that customers are aware of this attack.

The third independent variable, hacking, is significant in customer satisfaction, indicating that customer satisfaction with hacking awareness is satisfactory. This signifies that customers will be more satisfied with the banks' digital services when they increase their awareness of hacking-related information.

In the second part of the analysis, the bank's first independent variable, cybersecurity assistance, is found to be significant in customer satisfaction, indicating that customers require more cybersecurity features from banks to safeguard them against all types of cyberattacks. The second independent variable, the customer's expectation of technical support and training and development on cybersecurity, is also significant in customer satisfaction. This indicates that customers need a technical support facility where their smartphone or laptop/desktop on which they frequently use mobile banking apps and Internet banking should be checked by banks regularly. Customers also require regular training by banks in using mobile banking applications and Internet banking to increase their awareness of cybersecurity.

According to employee hacking research, information security depends on people, processes, and technology [26]. The results drawn from this study will be helpful for customers to understand the importance of types of cybersecurity, and they will understand which activity is labelled as cyberattack, phishing, and hacking. Users' information security decision-making abilities determine this importance. Users must understand information security threats and their security duties [29]. The study will help them to understand the significance of cybersecurity awareness so that the chance of such attacks could be decreased. Device management and updating are essential to cybersecurity [38]. The customers will be required to increase their awareness level on various technical and user interface-related aspects by which they can reduce the chance of getting cyber victims. The study suggests that banks understand the role of cybersecurity awareness on customer satisfaction and make solid efforts to increase the cybersecurity awareness of their customers. The results also suggest that the Saudi Arabian Monetary Authority, the regulator of the banking sector in Saudi Arabia, should motivate banks to organize cybersecurity awareness camps and regular training and development on technical assistance to use mobile banking apps and Internet banking services for their customers from safeguarding them from possible cyberattacks.

7. Conclusions and Implications

The present study provides a better platform and a greater understanding of various issues related to cybersecurity awareness among customers and its influence on their satisfaction level. There has been an enormous increase in mobile banking and Internet banking in the digital transformation era. This facility provides multiple benefits such as easy online money transfer up to a specific limit, payment of utility bills, recharge, and many more. Some important implications could be drawn based on the study's findings and analysis. According to the results, customers are aware of cybersecurity, and their level of awareness influences their satisfaction with digital banking services. Cybersecurity indicators, cyberattacks, and hacking are significant predictors, and one indicator, phishing, is an insignificant predictor for the dependent variable, customer satisfaction. The descriptive statistics analysis shows that customers know about cyberattacks, phishing, and hacking. To increase their satisfaction with cybersecurity, they need technical assistance from the bank and regular training and development. ANOVA results indicated a difference in the awareness level of customers' satisfaction with cyberattack, phishing, and hacking. The correlation between dependent and independent variables is also found to be significant.

The correlation between cyberattack and hacking is more significant than phishing on customer satisfaction. Further, a significant correlation is found between cybersecurity assistance by the bank and technical support on customer satisfaction.

It can be concluded that irrespective of customers' present awareness of their cybersecurity, they will be more satisfied if banks get them educated on cyberattacks, phishing attacks, and hacking. If a bank organizes regular cybersecurity awareness camps and provides necessary training and development on technical support to their customers, their satisfaction level with banking digital services will increase.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia, for funding this research work through the project number 8034.

References

[1] J. Dermine, "Digital Banking and Market Disruption: A Sense of Dejà Vu?," in *Financial Stability Review*, pp. 17–24, Banque de France, 2016.

[2] M. Marinč, "Banks and information technology: marketability vs. relationships," *Electronic Commerce Research*, vol. 13, no. 1, pp. 71–101, 2013.

[3] I. M. Sebastian, J. W. Ross, C. Beath, M. Mocker, K. G. Moloney, and N. O. Fonstad, "How big old companies navigate digital transformation," in *MIS Quarterly Executive*, vol. 16, no. 3pp. 197–213, Routledge, 2017.

[4] Y. Creado and V. Ramteke, "Active cyber defence strategies and techniques for banks and financial institutions," *Journal of Financial Crime*, vol. 27, no. 3, pp. 771–780, 2020.

[5] A. Mok and R. Saha, "Strategic risk management in banking," *Deloitte Inside Magazine*, vol. 1, no. 1, pp. 1–16, 2017.

[6] C. Skinner, *Digital Bank: Strategies to Launch or Become a Digital Bank*, Marshall Cavendish International (Asia) Pte, Singapore, 2014.

[7] Bain & Company, "Customer loyalty in retail banking: Global edition 2014," 2014, http://www.bain.com/Images/DIGEST_Customer_loyalty_in_retail_banking_2014_.pdf.

[8] K. Patel and M. P. McCarthy, *Digital transformation: the essentials of E-business leadership 1st*, McGraw-Hill Professional, 2000.

[9] M. Muckin and S. C. Fitch, *A Threat-Driven Approach to Cyber Security, s. l.*, Lockheed Martin Corporation, 2019.

[10] E. Stolterman and A. C. Fors, "Information technology and the good life," in *Information Systems Research. IFIP International Federation for Information Processing, vol 143*, B. Kaplan, D. P. Truex, D. Wastell, A. T. Wood-Harper, and J. I. DeGross, Eds., Springer, Boston, MA, 2004.

[11] C. Lindholm, "Digitalisering - Uppslagsverk-NE.se," 2019, May 2019, https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/digitalisering.

[12] C. I. Mbama and P. O. Ezepue, "Digital banking, customer experience and bank, financial performance," *International Journal of Bank Marketing*, vol. 36, no. 2, pp. 230–255, 2018.

[13] A. Jamal and K. Naser, "Customer satisfaction and retail banking: an assessment of some of the key antecedents of customer satisfaction in retail banking," *International Journal of Bank Marketing*, vol. 20, no. 4, pp. 146–160, 2002.

[14] M. Shahrokhi, "E-finance: status, innovations, resources and future challenges," *Managerial Finance*, vol. 34, no. 6, pp. 365–398, 2008.

[15] A. Mukherjee and P. Nath, "A model of trust in online relationship banking," *International Journal of Bank Marketing*, vol. 21, no. 1, pp. 5–15, 2003.

[16] T. Olanrewaju, *The rise of the digital bank*, McKinsey, 2013, April 2019, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-rise-of-the-digital-bank.

[17] Fiserv, "Study from Bank of the West and Fiserv Quantifies the Value of Digital Banking," 2019, April 2019, https://www.fiserv.com/blog/the-point/study-bank-west-fiserv-quantifies-value-digitalbanking-blog.aspx.

[18] H. Lebo, "The Future of Money and Banking," *Center for the Digital Future*, 2018, May 2019, https://www.digitalcenter.org/wp-content/uploads/2019/03/Future-of-Money-and-Banking-Report-Center-for-the-Digital-Future-April-2018.pdf.

[19] A. I. Al-Alawi, S. A. Al-Bassam, and A. A. Mehrotra, "Critical cybersecurity threats: frontline issues faced by Bahraini organizations," in *Implementing Computational Intelligence Techniques for Security Systems Design*, pp. 210–229, IGI Global, 2020.

[20] J. Cawley, "The impact of cyber attacks on the banking system," 2017, December 2017, https://wall-street.com/impact-cyber-attacks-banking-industry/.

[21] J. Kuepper, *Cyber Attacks and Bank Failures: Risks You Should Know, 21-01-2017 available at: Countering Terrorist Activities in Cyberspace, Z. Minchev & M. Bangladesh (eds)*, Z. Minchev and M. Bangladesh, Eds., 2017.

[22] VanBankers, "Cybersecurity in Banking," 2016, April 2017, http://www.vabankers.org/LiteratureRetrieve.aspx?ID=155390.

[23] J. Claessens, V. Dem, D. De Cock, B. Preneel, and J. Vandewalle, "On the security of today s online electronic banking systems," *Computers & Security*, vol. 21, no. 3, pp. 253–265, 2002.

[24] D. Florêncio and C. Herley, "Where do all the attacks go?," in *Economics of Information Security and Privacy III*, pp. 13–33, Springer, New York, 2013.

[25] H. S. Lallie, L. A. Shepherd, J. R. Nurse et al., "Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, article 102248, 2021.

[26] Z. L. Svehla, I. Sedinic, and L. Pauk, "Going white hat: security check by hacking employees using social engineering techniques," in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1419–1422, Opatija, Croatia, 2016.

[27] E. Albrechtsen and J. Hovden, "The information security digital divide between information security managers and users," *Computers & Security*, vol. 28, no. 6, pp. 476–490, 2009.

[28] A. Da Veiga and J. H. Eloff, "A framework and assessment instrument for information security culture," *Computers & Security*, vol. 29, no. 2, pp. 196–207, 2010.

[29] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Information security awareness in educational institution: an analysis of students' individual factors," in *Proc. 13th IEEE Int. Symp. Parallel and Distributed Processing with Applications (ISPA'15)*, vol. 1, pp. 352–359, Helsinki, Finland, August 2015.

[30] B. K. B. Kwok, "Accounting Irregularities in Financial Statements: A Definitive Guide for Litigators," in *Auditors and Fraud Investigators*, Routledge, 2017.

[31] J. Lewis and S. Baker, *The economic impact of cybercrime and cyber espionage*, McAfee, 2013.

[32] J. Austin and J. Bloggs, "Big Data Outsourcing and Identity Verification in Fintech Credit Assessment: A Case Study of a Microloans Platform in China," in *Australasian Conference on Information Systems*, Sydney, Australia, 2018.

[33] C. Martins, T. Oliveira, and A. Popovič, "Understanding the Internet banking adoption: a unified theory of acceptance and use of technology and perceived risk application," *International Journal of Information Management*, vol. 34, no. 1, pp. 1–13, 2014.

[34] I. Ivan, C. Ciurea, M. Doinea, and A. Avramiea, "Collaborative management of risks and complexity in banking systems," *Informatica Economica*, vol. 16, no. 2, pp. 128–141, 2012.

[35] J. A. Gliem and R. R. Gliem, "Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales," in *2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education*, pp. 82–88, Columbus, 2003.

[36] C. Beanland and Z. Schneider, *Nursing Research: Methods, Critical Appraisal and Utilization*, Mosby, Sydney, 1999.

[37] M. Litwin, *How to Measure Survey Reliability and Validity*, Sage Publications, Thousand Oaks, CA, 1995.

[38] K. Arlitsch and A. Edelman, "Staying safe: cyber security for people and organizations," *Journal of Library Administration*, vol. 54, no. 1, pp. 46–56, 2014.