Journal of Education and Finance Review (JEFR)
ISSN (Online): 3006-9211
RESEARCH ARTICLE

Cybersecurity Problem Impacting Online Banking in FR Peshawar

Tayyeb Khan [1]

Volume 1, **Issue** 1 (2022) **Pages:** 43–54 **DOI:** 10.62843/jefr/2022.3477305

Abstract: *This study examines cyber security vulnerabilities that affect Pakistani internet banking. This research aims to do this. The banking industry's weaknesses and risks must be examined now more than ever. This tendency is due to the rapid rise of digital technologies and Internet banking. This report examines Pakistan's online banking industry's cyber security. Prospective dangers and mitigation strategies are also considered to improve online banking platform security. The latest research shows that online banking in Pakistan is harmful. Seventy college and university students completed an online questionnaire. The survey was online. SPSS 21 was used to analyse the data. SPSS calculates ANOVA and coefficients. The study found that phishing, identity theft, and hacking affect Internet banking, but other factors also affect it.*

Keywords: Cybersecurity, FR Peshawar, Banking System, Threat

Introduction

In this digital age, online banking is an important part of modern banks and is known for being both convenient and cutting-edge. Cyber threats have made people worry about how safe and reliable virtual banking systems are. Because Peshawar is in the Federally Administered Tribal Areas (FR), the unique mix of technological progress and socio-economic factors makes it more vulnerable to hacking risks. This makes the issue even more important in this area. As the digital economy grows, so do the risks that come with it. FR Because Peshawar is at the intersection of technology and tradition, it faces risks in cybersecurity that are complicated and multifaceted, especially when it comes to Internet banking. The region's move from traditional banking methods to digital platforms has caused a big change in how money is handled. Because of this change, things are easier than ever before, but it has also made people and businesses more exposed to new threats. The study looks at the complicated web of security problems that Internet banking in the Federal Region of Peshawar is currently facing. There are a lot of threats that financial institutions need to improve their digital defences against like advanced malware getting into banking systems and phishing attacks that target customers who don't know what's going on. Another thing that makes the problem more difficult is the social and political situation in FR Peshawar. There is a unique risk environment because of how historical and regional factors affect modern cybersecurity problems.

It is very important to fully understand the complex security issues that come up with online banking. This article will look at the complexity of these problems by looking at their causes and effects and the many ways to make them better or avoid them. We want to bring attention to the problems with Internet banking in FR Peshawar so that people are more aware of them and can talk about them more easily. This will make it easier for everyone to work together to strengthen the area's safety. To protect the trustworthiness and integrity of online banking in FR Peshawar from constantly evolving cyber threats, we need a comprehensive plan that includes new technologies,

[1] M.Com, Branch Manager, Allied Bank Limited, Islamic Banking Branch Village Lund Khawar, District Mardan, Khyber Pakhtunkhwa, Pakistan.

Correspondence to Tayyeb Khan, M.Com, Branch Manager, Allied Bank Limited, Islamic Banking Branch Village Lund Khawar, District Mardan, Khyber Pakhtunkhwa, Pakistan.Email: tayyeb.khan@abl.com

Cite this Article as Khan, T. (2022). Cybersecurity Problem Impacting Online Banking in FR Peshawar. *Journal of Education and Finance Review, 1*(1), 43-54. https://doi.org/10.62843/jefr/2022.3477305

stronger rules, and more community input. By going beyond the digital line, we can protect everyone from cyber threats and make sure that the financial environment is safe and strong for everyone. Using information and working together can help make this happen.

Problem Statement

Before online banking, people/customers physically go to the bank to collect the money or transfer the money. After increasing in population and advancement in technology occur. The online banking (E-Banking) concept occurs when the customer leaves the traditional method and adopts the online banking system. Every technology is made for the purpose of the comfort of humans. Every technology has its advantages and disadvantages. Online banking has a lot of advantages, but the disadvantage is hacking cyber-attacks.

Research Gaps

The purpose of selecting this particular study is to recognize the cyber security issue in online banking. However, Pakistanis are not aware of the concept of cyber security/cyberattacks in online banking. The researcher analyses the barriers and identifies cyber-attacks.

Research Objectives

- To identify cyber security issues in online banking in Pakistan.
- To identify how to secure your online transaction.
- To identify how to secure your privacy.

Methodology

There were 70 people who answered an online survey as part of this quantitative study, which is how the researcher got the original data. Also, the people in the study are French people who use online banking. The city of Peshawar.

Research Design

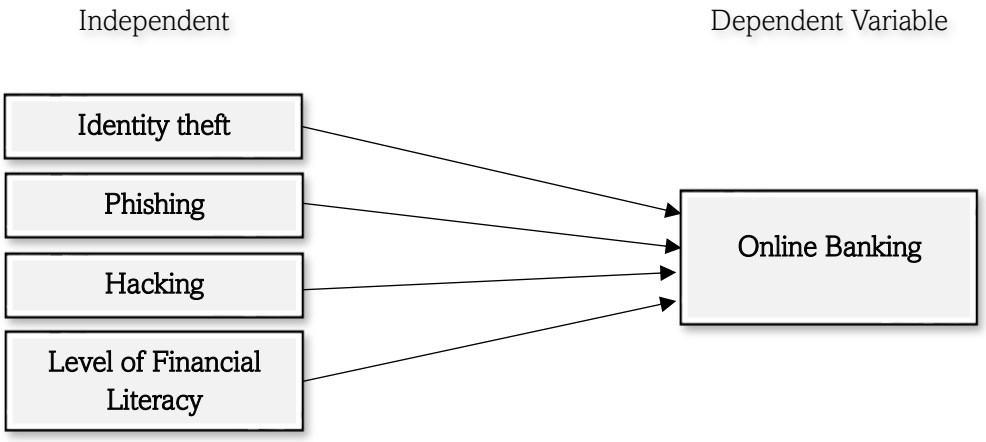
The researcher used a quantitative research design in this study because the researcher will collect data in numerical form using a Likert scale survey question. Quantitative research is utilized to quantify a big issue by producing numerical data that can be transformed into numerical data (Jones et al., 2018).

Data and Sample

Population and Sample Size

This study focuses on how cyber security impacts online behaviour. Peshawar is a student at FATA University and uses online banking. The researcher must gather data from a suitable demographic to enhance the data's effectiveness for the study. Seoane-Mato et al. (2019) stated that it is uncommon to have statistics for the entire population. With fewer resources, they could make precise measurements of the population. We employ a random sample strategy in the investigation. The sample size used for this investigation is 70. They recognise a specific number of participants selected from the general community as the sample size, assuming they accurately represent the entire population for the study in question (Shirazi et al., 2017).

Theoretical Framework



Hypotheses Development:

Main hypotheses: H* cyber security affects online banking

Roy et al. (2017) found that IB has become one of the most effective e-commerce applications. It elaborates on the unique rewards of the International Baccalaureate (IB) programme that lead to a perceived advantage. The results showed that the inclination to use IB is mainly hindered by security risk, with some financial risk involved, and is predominantly motivated by perceived advantage, attitude, and utility.

Khedmatgozar and Shahnazi (2018) examined the main factors influencing the adoption of International Business (IB) that are significant for both organisations and consumers. However, there is a lack of understanding regarding the risk perception and obligations of users while implementing IB. The author collected 247 pertinent examples from Portugal to assess the theoretical framework. The results validated some interactions related to the adoption of IT technology, including expected performance, expected effort, and social power, along with the incorporation of risk in achieving system suitability. The primary focus of using IB is crucial in elucidating IB usage patterns.

Marafon et al. (2018) found that trust and danger were not significant factors influencing the adoption behaviour of business-to-consumer e-commerce. The questionnaire was distributed shortly after through online advertisements on the above websites. The author collected 250 survey replies. This study discovered that the level of trust in both the electronic channel and the bank influenced the adoption of Internet banking. To better understand the effects of inconsistent adoption, they should separate the outcomes related to trust from those associated with potential concerns.

H1: phishing attacks affect online banking.
H2: hacking affects online banking.
H3: identity theft affects online banking.

Literature Review

Cyber Security in the Digital Banking Sector

IT now serves as the foundation of the digital banking system. It provides top-notch assistance for digital banking. Cyber crimes like phishing, hacking, forgery, and cheating are currently occurring in the digital banking industry. To prevent cybercrime, utilise authentication, identity, and verification techniques. Cybersecurity is a crucial instrument

in digital banking and serves as a defence against cybercrime. The rise of digitization in banking has increased the risk of cyber attacks by criminals, highlighting the need for implementing cyber security knowledge and techniques. Modern online technology has been enhanced for optimal efficiency and is extensively utilised by all users in the twenty-first century. The Digital Banking Sector, which is in the top five, frequently utilises online technologies like NEFT, Google Pay, and PhonePe. Cybercrime in the banking sector has been growing despite the rise in online banking usage. Reports indicate that 50% of cybercrime is associated with ATMs, debit cards, and internet banking. The banking sector is more susceptible to cyber-attacks than other industries. This study investigates cyber-attacks inside the banking industry and strategies for mitigating such attacks. Cyber threats are deliberate and harmful efforts to disrupt or damage data within a computer network or system. Cyber dangers originate from various sources, such as websites and computer systems. Cyber-attacks aim to obtain sensitive information from different businesses through internet methods. Cyber threats are impacting various industries, such as digital banking. A cyber threat is any malicious activity aimed at gaining unauthorised access to a Digital Banking account. A security breach has occurred, resulting in the unauthorised withdrawal of funds from consumers' accounts at a major bank. In 2021, hackers targeted banks globally. The main objective of cybersecurity in digital banking is to protect the user's digital financial accounts, including debit cards and credit cards, during transactions.

Banking Information Resource Cyber Security System

We aim to provide a comprehensive understanding of performance by offering insights into individual components and their interactions inside applications, operating systems, servers, data stores, and various other systems. The infrastructure condition monitoring tool enables users to track resource utilisation (CPU, RAM, and HDD), analyse data access and production activity performance, and evaluate risk and impact. Current situations can cause firm objectives to conflict with the increasing pressure of rising cyber risks. The pandemic lockdowns shifted the safety boundary of financial institutions to customers' homes, leading to the expansion and reinforcement of information security legislation. The regulator will offer banks methodological guidance, specifically focusing on improving the security of online banking, online card transactions, mobile applications, and chatbots on messaging platforms. Financial institutions need to efficiently recognise cyber-attack dangers and successfully fight against them rather than only having a theoretical understanding. Implementing global best practices, refining company processes, fostering teamwork, and adopting modern technologies can help achieve this goal. This decreases the chances of unauthorised access to the bank or payment system, enabling intruders to be intercepted, preventing harmful actions, and quickly resuming financial services. Cognitive models have been created to evaluate the security of computer networks, information security systems, and financial institutions. The proposed models facilitate the identification of the most significant hazards and the analysis of the relative change in the safety level of the systems being studied. The fuzzy cognitive maps have been analysed structurally and topologically, revealing their adequate density, complexity, and balance. The most structurally significant concepts have been identified, and scenario modelling has been conducted. It has been determined that these concepts will increase the safety level of computer network security by 65%, information security systems by 32%, and banks by 2%. This study's findings allow for the prediction of the state of bank cyber security, aiding in the implementation of essential measures to prevent, safeguard, and control access at appropriate levels of network infrastructure.

Barriers Faced by Consumers in the Adoption of Internet Banking

The study shows that participants consider the absence of personalised service and direct interaction with a banker, the lower perceived value of Internet banking compared to traditional banking, and concerns about security, including the risk of hackers and data breaches, as significant barriers to adopting internet banking Owais, (2021).

Contrary to other research, concerns about flawed transactions and significant financial risks are seen as important impediments, with a moderate level of comprehension being a key factor. The report recommended that organisations recognise consumer data requirements and establish suitable communication channels to engage with the benefits and advantages of IB services in order to cultivate enduring partnerships. Jibril, Kwarteng, Botchway, Bode, & Chovancova. (2020). Studies on e-banking transactions have, up until recently, been more concerned with the motivational aspects that set off the desire to accept and utilize the e-banking transaction than with the de-motivating variables that drive the action. The research on the issues connected to the former, however, is still in its infancy in emerging nations like the Sub-Saharan economies. The study, which is based on the Technology Threat Avoidance Theory (TTAT), aims to investigate how online identity theft affects consumers' desire to conduct e-banking transactions in Ghana.

To explain online banking in Pakistan

This study confirmed that the Internet is essential in the financial system and has been crucial in modernising the banking sector. Customers can use the IB system to enter their balance sheets and access transactions and resources from bank websites without needing physical documents. The service provides consumer banking features such as balance monitoring, multi-account transfer, and fund transfer without requiring consumers to provide documentation or signatures, streamlining the process for them. Masrek et al. (2018) emphasised that Internet banking (IB) is a vital component of electronic banking in Pakistan and has played a significant role in its expansion. It is advantageous for both clients and financial institutions, serving as a means to save time and money. Users continually show high degrees of adaptability and openness to resources, as demonstrated by the study's findings. IB is a network that disseminates self-service and digital banking technology. Customers can control and supervise their financial and banking transactions utilising IB. Consumers can easily get IB services using digital technologies.

Seemma, Nandhini, and Sowmiya (2018). Cybersecurity involves strategies detailed in published papers that are designed to safeguard the digital space of an individual or entity. It supervises the various techniques used to safeguard the integrity of networks, software, and data from unauthorised access. It refers to the assortment of technologies and protocols involved in protecting information, commonly referred to as information technology security. The topic is gaining significance due to the growing reliance on computer systems, including smartphones, televisions, and many devices that constitute the Internet of Things.

To identify the relationship between barriers faced by consumers and the adoption of online banking

This study revealed a correlation between obstacles and the approval of IB, as individuals disagreed with the implementation of IB. Most people in Pakistan were uninformed about IB due to a lack of knowledge on how to utilise it, as indicated by the research conducted by Liat et al. (2017). Moreover, there is a prevailing poor reputation around digital banking, where individuals tend to trust and accept criticisms without verifying the information from alternative sources. Moreover, individuals distrust banking sectors because they think that investment banking necessitates bank management to pay taxes. Nevertheless, there is a correlation between barriers encountered by customers and the adoption of IB.

Schatz, Bashroush, & Wall,. (2017). 'Cyber Security' has become a well-known word in recent years because of its growing use by both professionals and politicians. However, much like other trendy jargon, there doesn't seem to be much comprehension of what the phrase actually means. When the phrase is used informally, this might not be a problem, but when it comes to organizational strategy, corporate goals, or international agreements, it could pose serious issues. In this work, we examine the current literature to determine the key meanings of the word "Cyber Security" as offered by reliable sources. Then, using a variety of lexical and semantic analysis tools, we seek to

comprehend the range and significance of these meanings. Finally, using the same lexical and semantic analysis methodologies, we suggest a new, improved definition based on the analysis that was done, and we then show that it is a more representative definition.

Boateng et al. (2016) assert that in light of this innovation and the urgent requirement for current, straightforward, and precise information, information methods have gained considerable organisational significance. In light of this, a significant correlation is forming between the achievements of the businesses and their information technology infrastructure. The theory investigated how the utilisation of technology may expose users to potential hazards and proposed efficacious approaches to mitigate such risks. In the current era, organisations will capitalise on the advent of digital technologies and adapt to changing modes of consumer communication. The banking industry utilises the information system not only to facilitate internal business processes and product sales but also to deliver essential services to their customers. In addition, the sector confronts a critical challenge in the securitization of consumer relationships, which necessitates improved utilisation of the numerous new information systems that are commercially available. Adapting to this issue would enable the client to satisfy nearly all of their financial requirements with minimal human intervention. According to Khamitkhan et al. (2018), IB is defined as the utilisation of the Internet or a computer system to access information. This enables government agencies to benefit from a broader range of advantages due to the increased accessibility and user-friendliness of the innovation. By utilising the bank's IB platform, customers were able to perform a diverse range of tasks remotely. These tasks included writing checks, paying expenses, exchanging currency, publishing receipts, and inquiring about current accounts. On the contrary, IB exerts a substantial impact on electronic payments by serving as a forum for the operation of numerous e-commerce platforms, including online purchasing, online auctioning, and online trading (Afshan et al., 2018). Although IB gained popularity, its primary function was to furnish the bank with data required to sell its products and services online. However, as secure Internet transactions became more advanced, an increasing number of banks adopted IB as a transaction-based mechanism. Although Internet banks have expanded their market presence to encompass the European continent and implemented supplementary channels like contact centres, their impact on the banking sector as a whole has been limited.

Szopiński, (2016). The expansion of e-business and e-society relies heavily on electronic banking, particularly online banking. The essay aims to identify the factors influencing Poland's adoption of Internet banking. The University of Finance and Management in Warsaw's Board of Social Monitoring undertook a "Social Diagnosis" research project, providing empirical data for the current article. The linear regression study revealed that Internet usage, utilisation of alternative financial services, and trust in commercial banks are the primary determinants influencing employment. Mortgages and credit cards are the primary financial instruments that influence the frequency of online banking usage.

Goutam, (2015). Various entities collect, analyse, and retain significant amounts of confidential information on computers, including governments, the military, organisations, financial institutions, colleges, and other businesses. Subsequently, this data is transmitted across networks to other computers. Urgent measures are required to protect vital corporate and personal data and ensure national security in response to the increasing frequency and complexity of cyber-attacks. The essay outlines the features of cyberspace and illustrates the internet's vulnerability in transmitting sensitive financial and personal information. We explored several methods employed in cyber attacks in India and globally to demonstrate the growing prevalence and harmful impact of hacking on the worldwide economy and security.

Craigen, Diakun-Thibault, & Purse (2014). The interpretations of the commonly used term "cybersecurity" differ significantly, can be subjective, and might lack practical value. Technology and scientific progress are hindered

by the absence of a concise, universally acknowledged definition that fully encompasses the complex aspects of cybersecurity. This is because it promotes a technical perspective on cybersecurity and creates divisions among disciplines that should collaborate to tackle intricate cybersecurity issues. We engaged in numerous discussions on cybersecurity with a diverse set of professionals, scholars, and postgraduate students, alongside an in-depth review of the literature to explore different perspectives on the components of a cybersecurity definition. This article presents a revised definition of cybersecurity: "Cybersecurity involves the arrangement and gathering of resources, procedures, and frameworks designed to safeguard cyberspace and the systems capable of functioning within it from conflicts arising between de jure and de facto property rights." An interdisciplinary approach to cybersecurity will be achieved by clearly defining a concise, comprehensive, significant, and cohesive definition. This will influence how academics, business, government, and non-governmental organisations address cybersecurity concerns.

Schoenmaker, & Peek,. (2014). This essay examines the status of the European banking industry. The empirical evidence suggests that, overall, the Baltic States, Cyprus, Greece, and Ireland are particularly affected by a sharp fall in lending during the financial crisis. The fundamental reason for this deleveraging is a decrease in the availability of credit available across borders. Using stock market data from November 2013, we also assess the capital status of the European banking sector. For the top 60 banks, additional capital of EUR 84 billion would be required in the simplest scenario to bring capital back to a market-based leverage ratio of 3%. At the bank level, lending is still being done by the top tertile of well-capitalized banks (with a market-based leverage ratio considerably over 4%). In contrast, lending has significantly decreased for the second tertile of medium-capitalized banks (between 3 and 4%) and the third tertile of weakly capitalized banks (far below 3%), respectively. Additionally, these banks have a market-to-book ratio that is less than one. As a result, the market values these banks less.

Luiijf, Besseling, and De Graaf (2013). Several countries have publicly released their national cyber security strategies (NCSS). Significant discrepancies exist among the national focal points and approaches, even if each of these NCSS aims to address the same cyber security challenges. This study analyses and compares 19 National Statistical Offices (NSOs) from different countries: Canada, Estonia, South Africa, Australia, Czech Republic, France, Germany, India, Japan, Lithuania, Luxembourg, Romania, The Netherlands, New Zealand, Spain, Uganda, UK (2009 and 2011), and the United States. This work demonstrates similar tactics and weaknesses through analysis and comparisons. The conclusions and recommendations, which propose a framework for a National Cybersecurity Strategy (NCSS) and content ideas, could assist governments in constructing an NCSS.

Haneef, Riaz, Ramzan, Rana, Ishaq, and Karim (2012). This study aims to analyse the impact of risk management on non-performing loans and the profitability of the banking industry in Pakistan. The entire dataset was of secondary origin and was collected from five banks. The report shows that Pakistan's banking sector does not have an adequate risk management framework. The study concluded that non-performing loans are increasing due to inadequate risk management, posing a threat to bank profitability. This paper suggests that the banking industry could decrease its nonperforming loans by implementing the techniques advised by the State Bank of Pakistan.

Bowra, Sharif, Saeed, & Niazi, (2012). This study's primary goal is to investigate the nature of the link between employee perceptions of their performance and human resource (HR) procedures (pay, performance assessment, and promotion policies) in Pakistan's banking industry. A survey of 235 banking workers was undertaken using a personally administered questionnaire to find out how HR policies affected how well the employees were regarded to be doing. By using Spearman's correlation matrix and multiple regression analysis, the connection and its nature are computed. The results of Spearman's correlation show a strong and positive link between employee

perceptions of their performance and HR procedures. According to the regression results, the two HR practices of performance assessment and promotion are significant, while the practices of remuneration are not. Additionally, this study aids top banking sector management in developing or revising their HR policies and processes to achieve high employee performance.

Mohsan, Nawaz, Khan, Shaukat,& Aslam, (2011). The wants and demands of its clients are something that top-performing financial institutions constantly consider in order to thrive and compete in today's fast-paced business climate. The significance of customer happiness, loyalty, and retention has, therefore, been consistently stressed by organizational scholars from all over the world. The goal of the current study is to determine how customer satisfaction affects customer loyalty and switching intentions. One hundred twenty consumers who visited the bank counters and had an account with a Pakistani bank provided the data. After gathering the data, SPSS 16 and Microsoft Excel were used to evaluate it. According to the study's findings, customer happiness was inversely connected to consumer intent to switch and positively related to customer loyalty.

Mohsan, Nawaz, Khan, Shaukat, & Aslam, (2011). Top-performing financial institutions always consider their clients' wants and requests in order to thrive and compete successfully in today's changing business climate. That is why organizational studies all across the world have consistently stressed the significance of customer happiness, loyalty, and retention. The current study seeks to determine the influence of customer satisfaction on customer loyalty and switching intentions. The information was gathered from 120 people who visited bank counters and had an account with a bank in Pakistan. The data was then analyzed using Microsoft Excel and SPSS 16. According to the study's findings, customer happiness was favourably associated with customer loyalty and adversely related to consumer intent to switch.

Raza, Farhan, & Akram, (2011). The main drivers of a nation's economic growth are investment banks. They have a significant influence on a nation's credit and financial markets. This study compares financial performance for the years 2006 to 2009 using financial ratios and indicators from Pakistani investment banks. Three basic categories and measurements, including two indicators, are used to categorize financial ratios. Nine investment institutions were chosen; however, only seven will be analyzed for comparison. This study comes to the conclusion that the performance of investment banks differs depending on the efficiency ratio compared to the liquidity ratio, capital or leverage ratio, and financial metrics. The findings are produced from the data of seven banks because the data of the other two banks were unavailable.

Yap, Wong, Loh, & Bak, (2010). Client confidence in the e-banking service is increased by traditional service excellence. It was discovered that the consumer might receive structural confidence from the bank due to its size and reputation, but not in the absence of conventional service quality. Significant situational signals for situational normalcy are website elements that inspire client confidence.

Statistical Technique

Statistical Tools for Data Analysis

The following statistical equation is used for the research:

$Y=\alpha + \beta X1 + \beta X2 + \beta X3 + \beta x4 - - - - - ei$ ---------- (1)

Y= Adoption of online-banking

P X1= Phishing

ET X2= Identity theft

CI X3= Hacking

LL X4= Level of financial literacy/level of understanding
Reporting and interpretation of the results with the relevant analysis tables

Reliability

The Cronbach's alpha shows how internally consistent a set of things is or how closely they fit together as a category. It is used to measure how reliable a scale is. It's not always true that a "strong" alpha number means the test only looks at one thing. Cronbach's Alpha must be between 0.7 and 0.9. It is required that the Cronbach alpha number for this test be 789, which it is.

Table 1
Reliability statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.794	.813	25

Model summary

The pattern is described in detail in table 3. Because the R-square value is 0.814, it is possible to assert that 81% of the data is genuine and dependable. The benchmark of reliability and validity is found within the best condition.

Table 2

Model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.814[a]	.81	.812	.50200

a. Predictors: (Constant), Level of Literacy, Phishing, Identity Theft

ANOVA
The statistical means variances are measured using the ANOVA interpretation. The model fulfils the necessary criterion of 3.14, as evidenced by the Statistics value of 9.709.

Table 3

ANOVA[a]

Model	Sum of Squares	df	Mean Square	F	Sig	
1	Regression	2.949	3	.983	9.709	.000[b]
	Residual	6.682	66	.101		
	Total	9.631	69			

a. Dependent Variable: Online Banking
b. Predictors: (Constant), Level of Literacy, Phishing, Identity Theft

Coefficients

Model: The variable or factor that the regression model is taking into account is shown in this column. While "Identity Theft," "Phishing," and "Level of Literacy" are the independent variables being examined, the "Constant" stands in for the intercept of the regression equation.

Unstandardized Coefficients (B): independent variable on the dependent variable (online banking). The unstandardized coefficient, for instance, is 0.486 for "identity theft," which means that when all other variables are kept constant, a rise in "identity theft" is correlated with an increase in "online banking" by 0.486 units. When all other factors are held constant, these coefficients show the estimated impact of each.

Standards Coefficients (Beta): The standardized impact of each independent variable on the dependent variable is represented by these coefficients. They make it possible to compare the relative weights of each independent variable. As an illustration, "Phishing" has a larger Beta value (0.399) than "Identity Theft" (0.275), indicating that it may have a greater influence on Banking.

T value: The importance of each coefficient is gauged by the t-value. The coefficient is more statistically significant when the t-value is larger. The fact that all of the t-values in this table have related p-values (Significance) that are less than 0.05 (5%) shows that "Identity Theft" and "Phishing" are statistically significant predictors of "Online Banking," but "Level of Literacy" is not statistically significant.

Significance (Sig.): The p-value for each coefficient is shown in the significance column. A low p-value (usually under 0.05) denotes a statistically significant coefficient, which has a substantial effect on the dependent variable.
In order to evaluate the relevance and potency of each predictor, this table offers useful information about the relationship between the independent variables and the dependent variable in the regression model.

Table 4

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.352	.306		10.961	.000
	Identity Theft	.486	.198	.275	2.454	.017
	Phishing	.582	.158	.399	3.683	.000
	Level of Literacy	.002	.061	.003	.027	.978

a. Dependent Variable: Online Banking

Conclusion

In conclusion, the field that encompasses both online banking and cyber security is dynamic and always undergoing change. As technology continues to progress, the strategies that hackers utilise will also continue to evolve. An approach to cyber security that is both proactive and adaptable is absolutely necessary in order to guarantee the availability, integrity, and confidentiality of financial services in the world of digital technology. By remaining vigilant, inventive, and cooperative, the financial sector will be able to overcome these challenges and continue to provide individuals and businesses all over the world with secure and dependable online banking services.

References

Amini, M. T., Ahmadinejad, M., & Azizi, M. J. (2011). Adoption of Internet banking by Iranian customer: An empirical investigation. *The International Journal of Management Science and Information Technology (IJMSIT)*, (1-(Jul-Sep)), 27–44. Retrieved from http://hdl.handle.net/10419/97860

Arif, I., Aslam, W., & Hwang, Y. (2020). Barriers in adoption of internet banking: A structural equation modeling - Neural network approach. *Technology in Society*, *61*, 101231. https://doi.org/10.1016/j.techsoc.2020.101231

Bashir, U., & Ramay, M. I. (2010). Impact of stress on employees job performance a study on banking sector of Pakistan. *International Journal of Marketing Studies*, *2*(1). https://doi.org/10.5539/ijms.v2n1p122

Bhat, M. A., & Tariq, S. (2020). Factors affecting adoption of internet banking: A study of Jammu and Kashmir with special reference to J & K bank. *MUDRA : Journal of Finance and Accounting*, *7*(1), 111. https://doi.org/10.17492/mudra.v7i1.195697

Bowra, Z. A., Sharif, B., Saeed, A., & Niazi, M. K. (2012). Impact of human resource practices on employee perceived performance in banking sector of Pakistan. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, *6*(1). https://doi.org/10.5897/ajbm11.2312

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, *31*(5), 583-603. https://doi.org/10.1108/14684520710832315

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21. https://doi.org/10.22215/timreview835

De Jonghe, O. (2010). Back to the basics in banking? A micro-analysis of banking system stability. *Journal of Financial Intermediation*, *19*(3), 387-417. https://doi.org/10.1016/j.jfi.2009.04.001

Doyon-Martin, J. (2015). Cybercrime in West Africa as a result of Transboundary E-waste. *Journal of Applied Security Research*, *10*(2), 207-220. https://doi.org/10.1080/19361610.2015.1004511

Ghelani, D., Hua, T. K., & Koduru, S. K. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. https://doi.org/10.22541/au.166385206.63311335/v1

Ghillani, D., & Gillani, D. H. (2022). A perspective study on malware detection and protection, a review. https://doi.org/10.22541/au.166308976.63086986/v1

Goutam, R. K. (2015). Importance of cyber security. *International Journal of Computer Applications*, *111*(7), 14-17. https://doi.org/10.5120/19550-1250

Hernández-Murillo, R., Llobet, G., & Fuentes, R. (2010). Strategic online banking adoption. *Journal of Banking & Finance*, *34*(7), 1650-1663. https://doi.org/10.1016/j.jbankfin.2010.03.011

Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, *7*(1), 1832825. https://doi.org/10.1080/23311975.2020.1832825

Kamalul Ariffin, S., Mohan, T., & Goh, Y. (2018). Influence of consumers' perceived risk on consumers' online purchase intention. *Journal of Research in Interactive Marketing*, *12*(3), 309-327. https://doi.org/10.1108/jrim-11-2017-0100

Khurshid, A., Rizwan, M., & Tasneem, E. (2014). Factors contributing towards adoption of e-banking in Pakistan. *International Journal of Accounting and Financial Reporting*, *1*(1), 437. https://doi.org/10.5296/ijafr.v4i2.6584

Loonam, M., & O'Loughlin, D. (2008). Exploring E-sErvicE quality: A study of Irish online banking. *Marketing Intelligence & Planning*, *26*(7), 759-780. https://doi.org/10.1108/02634500810916708

Luiijf, E., Besseling, K., & Graaf, P. D. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, *9*(1/2), 3. https://doi.org/10.1504/ijcis.2013.051608

Mohsan, F., Nawaz, M. M., Khan, M. S., Shaukat, Z., & Aslam, N. (2011). Impact of customer satisfaction on customer loyalty and intentions to switch: Evidence from banking sector of Pakistan. *International journal of business and social science*, *2*(16), 263-270.

Nasri, W. (2011). Factors influencing the adoption of internet banking in Tunisia. *International Journal of Business and Management*, *6*(8). https://doi.org/10.5539/ijbm.v6n8p143

Raza, S. A., & Hanif, N. (2013). Factors affecting internet banking adoption among internal and external customers: A case of Pakistan. *International Journal of Electronic Finance*, *7*(1), 82. https://doi.org/10.1504/ijef.2013.051746

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2017.1476

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, *7*(11), 125-128. https://doi.org/10.17148/ijarcce.2018.71127

Szopiński, T. S. (2016). Factors affecting the adoption of online banking in Poland. *Journal of Business Research*, *69*(11), 4763-4768. https://doi.org/10.1016/j.jbusres.2016.04.027

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415

Waseem, N., Frooghi, R., Sharif, A., & Afshan, S. (2018). Internet banking in Pakistan: An extended technology acceptance perspective. *International Journal of Business Information Systems*, *27*(3), 383. https://doi.org/10.1504/ijbis.2018.10010588

Wasiq, S., Othman, M., & Abdullah, Z. S. (2022). Factors affecting customers' adoption of internet banking in Afghanistan. *2022 10th International Conference on Cyber and IT Service Management (CITSM)*. https://doi.org/10.1109/citsm56380.2022.9935999

Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010). Offline and online banking – where to draw the line when building trust in E-banking? *International Journal of Bank Marketing*, *28*(1), 27-46. https://doi.org/10.1108/02652321011013571

Yildiz Durak, H. (2019). Human factors and cybersecurity in online game addiction: An analysis of the relationship between high school students' online game addiction and the state of providing personal cybersecurity and representing cyber human values in online games. *Social Science Quarterly*, *100*(6), 1984-1998. https://doi.org/10.1111/ssqu.12693