International Journal of Aquatic Science
ISSN: 2008-8019
Vol 13, Issue 01, 2022

Cybercrime Techniques in Online Banking

Md Rokibul Hasan

MBA Business Analytics, Gannon University, Erie, Pennsylvania

Email: buppy_du@yahoo.com

Acknowledgment: I would like to thank Dr. Barbara A. Manko, Assistant Professor, Graduate Business Studies, Gannon University, Erie, Pennsylvania for her valuable and constructive suggestions during the planning and development of this research paper. Her advice and guidance got me through every stage of writing my paper.
My family members have been more crucial to me than anyone else in the pursuit of this mission. I'd like to express my gratitude to my father and mother, who have always supported and guided me in my endeavors. They are the epitome of positive role models.
Most notably, I want to express my gratitude to Farhana Latif Sumi, my loving and supporting wife, and Raonaf Hasan Inni, my inspirational daughter.

Abstract: Cybercrime is a threat that spans a wide range of online criminal activity in a broad range of settings. In the twenty-first century, financial institutions were most concerned about the rapid rise of cybercrime. The outcomes of attacks on financial institutions were compared throughout the year. When it comes to cybercrime, companies need to be aware of its impact to adopt suitable measurements. The best method to keep financial institutions safe is to implement comprehensive internal and cyber security analyses and cyber defense training. As a result, the present study looked at the influence of cybercrime tactics on online banking use and the potential benefits of big data. Based on quantitative cross-sectional surveys, the researchers concluded that the financial system is negatively impacted by cybercrime approaches. Financial institutions (24.90%) are the most vulnerable to cybercrime, followed by social media (23.60%). When it comes to cybercrime, webmail accounts for 19.60% of the attacks; e-commerce accounts for 8.50%; logistics accounts for 5.80%; cryptocurrencies account for a total of 8%. The negative effect was caused by security vulnerabilities in some cybercrime tactics, which might lead to the theft of customer data. For example, consumer trust and performance were negatively affected by vishing schemes that robbed banks of their security credentials.

Keywords: Cybercrimes, E-banking, Online Banking, Bigdata

1. INTRODUCTION

Background History

The cyber-crime danger exists in a variety of scenarios and encompasses a wide spectrum of online criminal activities, ranging from simple scamming to sophisticated attacks on financial institutions as well as other huge organizations. The majority of people were aware of phishing emails as well as the dangers of clicking on a link and files that may infect your computer or mobile device with malware. Most people also were aware that unless you pay a ransom, this

software may steal your Passwords, bank accounts, and credit card information, or lock up your files and databases (Camillo, 2017).

Cybercrime is illegal conduct that is carried out primarily via the use of a computer. In American law, there is no concept of cybercrime. Even in the USA, the Information Technology Act of 2000 lacks a definition of cybercrime.

The fast increase in cybercrimes was the key worry by financial institutions throughout the 21st century as well as the necessity to defend cyberspace has become more vital than ever before. Cybercrime is one of the major challenges in today's Internet banking business around the globe. Cybercrime according to Douglas and Loader (2000) may be characterized by computer-mediated acts undertaken across worldwide electronic networks which are either unlawful or regarded illegitimate by certain parties. The effect of cybercrime must be understood by organizations before appropriate measurements can be established (Ezeoha & Commerce, 1970). There are various steps that financial organizations may take to ensure the safety of their customers and to maintain a stable economic business environment on the Internet. The financial integrity of financial institutions as well as other enterprises cannot be overestimated by cybercrime. Companies need to understand the effect of cybercrimes to implement appropriate metrics (Usman, Shah, & Commerce, 1970).

When dealing with ever-increasing data volumes, businesses turn towards big data analytics. A potential benefit to the battle against cybercrime is that it might help. Financial institutions were targeted by hackers in 2018, and the results of such assaults were compared. Directly and indirectly, losses were found to be the most common kinds of damage caused by cyberattacks. Direct costs include money and data loss, but indirect costs include dissatisfied customers and tarnished brand reputations. However, the researchers found that strong internal security or cyber security analysis as well as cyber defense training, and a cyber security audit are all effective ways to keep financial institutions secure from cyberattacks (Dzomira, Markets, & Institutions, 2014).

1.1. Problem statement

The problem that might be addressed in this study is that there have been security breaches inside the online banking system, which is causing a decrease in total clients as a result of cybercrime. The study needs to explore the different cyber-attack techniques that might help to reduce these cyber threats to the banking system.

1.2. Research Objectives

The objective of the research is to examine cybercrime strategies and how they might be mitigated in the online banking sector utilizing big data technologies. In that regard, the following research questions are answered in the current research.

RQ1 What is the impact of cybercrimes techniques on the usage of online banking by consumers?

RQ2 How does big data help combat the cybercrimes in online banking?

1.3. Scope

The findings had a wide range of consequences for policymakers and responsible authorities in terms of taking real action against cybercrime and reducing it through the use of big data applications. The study would help to reduce the cybercrime attacks on the banking system. The study might p to bankers avoid cybercrime attacks on their systems.

1.4. Significance of the study

This new study would be extremely beneficial to cybercrime prevention in the online banking sector. Stakeholders and decision-makers must take immediate action in this area.

Literature Review

E-banking fraud and other electronic fraud as well as security literature are examined in the study's literature review. In a literature review, all relevant research is identified, evaluated, and interpreted to answer a specific research question, subject, or phenomenon. As a result, a methodical strategy is used to ensure full coverage of relevant material. Rather than employing predefined linear search tactics as proposed by Usman et al. (1970), an iterative search approach was used as the review progressed.

The strategic, operational, legal, and reputational risks connected with e-Banking are the most significant. The most important operational risk in e-Banking is security. According to Sokolov (2007), A security breach that allows unauthorized access to customer information might be classified as risk management, but still the bank is also exposed to legal and reputational risk as a result. Customers should be educated about security threats, procedures, and the use of intelligent technologies to protect themselves and their reputations. Many Romanian banks that are involved in e-Banking operations have provided prospective customers with advice on how to increase their security while doing business online (Ahmad, Iqbal, & Shahzad Jamil, 2021). According to Azhar, Shahi, and Chhapola (2020), the goal of E-Banking is to "provide consumers access to their bank accounts through a website and enable them to conduct specific activities on their account, subject to strict security checks." The words "PC banking," "online banking," "Internet banking," "telephone banking," and "mobile banking," according to Vrîncianu and Popa (2010), clients may reach the banks in several ways without actually visiting a bank facility. Customers may perceive risks while making purchases online, particularly if they are paying with their hard-earned cash. According to several polls, customers are concerned about security threats.

According to Ige (2015), Computerized financial services are often seen to be riskier than their manual counterparts. e-Banking security is deemed vital since it directly impacts the activities of its users. Consider how one of the most major obstacles to the expansion of electronic services has been customer views about online transaction security. Bakare and Commerce (2015) A survey is being conducted to find out how consumers feel about online banking today and in the future. He concluded there were universal views about online banking that was unaffected by demographic, geographical, or psychological characteristics. Internet banking security and lack of knowledge are two of the main "non-adoption" areas, according to him. e-Banking is characterized by a high degree of automation. Aribake and Finance (2015) defined 17 service quality aspects, with security being among them.

Banks are not as frequently looted in modern times since money is no longer housed only in bank vaults. A bunch of cash exists within cyberspace thanks to contemporary computer technology and data networks. Banks must adapt to contemporary trends of conducting business online (Akinbowale, Klingelhöfer, & Zerihun, 2020) while also protecting themselves from cyber-crime. The first "cybercrime" was committed in the year 1820! Abacus, which is a computer, has been utilized in India, Japan, and China since at least 3500 BC.

In contrast, it was Charles Babbage's analytical engine that ushered in the modern era of computers. Almost all of Zimbabwe's banks have implemented some type of electronic banking or cyberbanking. The United States' first outward sign of electronic innovation, according to

Saini, Rao, Panda, and Applications (2012) occurred in the Automatic teller machines (ATMs) were first deployed in the early 1990s by Standard Chartered Bank and the Central African Building Society (CABS) (ATMs). E-banking has grown significantly in recent years. According to Goel (2016), at least 15 financial institutions have partnered with cell carriers to provide mobile banking services, as well as the lot of banks joining the sector is increasing. The amount of internet transactions and mobile money transactions has grown dramatically during the last several years. According to Kamal, Chowdhury, Haque, Chowdhury, and Islam (2012), as more consumers and businesses move their money to the internet, possibilities for 21st-century tech-savvy burglars grow. While US financial institutions grapple with global technological advancements, cyber fraudsters are on the prowl.
E-banking fraud is a global problem that continues to cost both banks as well as customers money. According to Arrawatia (2019), there have been millions of dollars in financial transactions across network connections due to eCommerce, online banking, as well as associated technologies. However, as banks extend their online services to customers, the danger of internet computer fraud (ICF) increases, and the risk landscape alters. E-banking services are gaining in popularity throughout the globe and are likely to take over during the near future, leading to a rise in high-profile financial-motivated attacks. To reduce the risk of a significant security breach, several factors have been identified and need to be addressed. (Wang, Nnaji, Jung, & Justice, 2020).

A bank may indeed give customers and companies electronic banking services via the use of electronic techniques like a fixed and mobile phone or the Internet. Modern e-banking services are much different from their predecessors because of the tremendous advancements in internet technology over the years. There are several types of E-Banking services accessible today, including online banking, automated teller machines (ATM), electronic payments, electronic check conversion, and money transfer, including web ATM services. These services have several security problems, and so this article will analyze relevant studies to identify elements that may be essential in preventing fraud in the e-banking sector (Vrîncianu & Popa, 2010).

Financial services may be delivered more cheaply and conveniently via online banking when an account has been set up. Because of this, banks all around the globe are moving toward electronic banking. There are a few known elements that contribute to the enormous security problem that must be addressed with the rise in popularity and predicted dominance of e-expanding banking. This research emphasizes and synthesizes several variables that may be crucial in reducing e-banking fraud, including an increase in money supply, change management, rapid access to information, and strict internal controls. Such features may assist bank regulators and management teams in identifying areas in need of more focus and improvement (Akinbowale et al., 2020).

Techniques of Cyber Crime in Online Banking

Following are some different types of cybercrime techniques that are influencing the banking system:

Phishing Personal information, such as credit card or debit card numbers, online banking login credentials, and account numbers, may be obtained by using this kind of fraud. Email phishing is a misleading method of stealing personal data. It's very uncommon to get phishing emails pretending to be from a well-known organization and asking for personal information like your

credit or debit card number, PIN code, expiry date and CVV code, mobile phone number, and other login credentials to online banking. Sites, services, and companies with someone you have no connection with may be the source of phishing attempts. In phishing emails, the user is instructed to click on a link that directs them to a website that requests personal information. An email from a legitimate company asking for this information would never be sent to you (L. J. T. J. o. D. A. Ali, 2019).

Vishing is criminal conduct that involves utilizing the telephone network to gather sensitive personal and financial information from the general public, most often via the use of Voice over Internet Protocol (VoIP) as well as mobile phones. Portmanteau's words "voice phishing" are used to describe a kind of scam that uses the words "phishing" and "voice". As part of Vishing, scam artists call innocent bank customers/consumers pretending to be from a bank or a merchant and inform them that they have issues with their bank accounts/online shopping but that they need to verify their account, KYC, or online order but also request the victim's payment credentials because once they commit fraud. Today, virtually all financial cybercrimes are committed using a method known as phishing, a kind of social engineering attack (L. J. T. J. o. D. A. Ali, 2019).

Data Diddling It seems that fraudsters illegally modify raw data before entering but rather processing into a computer system, and instead change it back to its original form before processing it so the data alteration cannot be readily discovered. It's a kind of cyber-crime (More, Nalawade, & Paper, 2015).

Cyber Squatting (Domain Squatting*)* When someone registers, traffics or uses a web address in bad faith, they are committing the act of "cyber-squatting," which is a kind of trademark infringement. For this reason, the cyber-squatter sells the domain at a higher price to a trademark holder (More et al., 2015).

Cyber Bullying As the term implies, cyberbullying is the act of someone intentionally and repeatedly harassing, mistreating, and making fun of another person online, via mobile phones, or other electronic methods. Using mobile phones, instant messaging, e-mails, chat rooms, and social networking sites like Facebook or Twitter, someone might be harassed, threatened, or intimidated (More et al., 2015).

Impact of Cybercrimes Techniques on the Usage of Online Banking:
The rise of mobile devices having internet access has led to an increase in cybercrime instances. Several online activities can be carried out on smartphones these days, including internet banking and e-commerce. Criminals are always looking for ways to get their hands on personal information from these devices. Revenge, extortion, and political objectives have all been cited as reasons for conducting cybercrime in the past, but the financial gain has remained the clear leader for many years. Unfortunately, basic phishing assaults have a rate of success of 45 percent since people aren't aware of the typical protections to protect themselves from clever cyber thieves(Raghavan, Parthiban, & Review, 2014).
The scope of cybercrime in 2020 may be extrapolated from the NTRO and CERT-In estimates of 3855 financial gain cybercrimes and 534 phishing occurrences. From January through June of this year, there were 27,482 incidents of cybercrime recorded. Only occurrences that have

been reported are included in this list, which excludes instances that have gone unreported or disregarded (Rathore, 2016).

Bigdata helps combat the Cybercrimes in Online Banking:
There were two hurdles to combating cybercrime in internet banking before big data analytics: The volume of data is expanding, as is the variety of threats. Because there are numerous assaults, ranging from compromising online banking information to credit card theft, cybercrime doesn't follow a single discernible pattern or approach (at least on the surface). Combating these instances, which are becoming increasingly common, has become practically difficult.

The rising volume of data is the second cause. With petabytes of data being collected by online banking, finding appropriate measures for data protection becomes even more challenging. Employees must wade through massive data quantities without data analytics, pushing them to hunt for a needle in the haystack. Because of these factors, cybercrime has proven to be hard to tackle, at least using traditional means (Hassani, Huang, Silva, & Computing, 2018).

What role does big data analytics play in the solution?
Because it is designed to manage expanding amounts of large data, big data analytics is a viable answer. Data analytics is more than capable of dealing with the massive amounts of data that businesses collect (Barbara A. Manko, 2021). The advanced data algorithms that make up a data analytics framework are the reason for this capability. Large amounts of data can be processed, managed, and secured with the help of big data analytics (Apurva, Ranakoti, Yadav, Tomer, & Roy, 2017).

Secondly, big data analytics frameworks might break down and discriminate between distinct cybercrime attacks, such as hacking as well as online fraud. Since analytics can break down attack data and uncover similarities by analyzing patterns utilizing pattern recognition technology, even while the assault technique varies, this is the case (Apurva et al., 2017).

Instruct analysts on how to proceed
The capacity to identify abnormalities is one of the most powerful features of big data analytics. Analytics can identify unusual behavior in the network as well as on devices, which can then be highlighted for further examination. Because big data analytics can analyze data on a huge scale to uncover connections and patterns, it may detect abnormalities. As a result, if something is out of the ordinary, analytics will notice it right away as well as a flag for further examination. It's a fantastic tool to have since it can steer network analysts in the proper direction, focusing attention their time and effort on the most likely sources of an attack (Amrollahi, Dehghantanha, & Parizi, 2020).

The use of big data analytics could help to identify criminal activity
With the use of big data analytics, it is possible to anticipate assaults in the future. It is possible to make predictions by studying data and drawing inferences from it. When artificial intelligence (AI) systems are implemented into an analytics platform, this is especially the case. This is one of the best strategies to fight cybercrime since financial systems can safeguard their

data more efficiently and establish an effective network that guards the information (Amrollahi et al., 2020).

Theoretical Framework

Wada and Odulaja (2012) examined cybercrime policy challenges and provided insight into how cybercrime affects E-banking. To guide policymakers on behavioral aspects that should be addressed while establishing regulations to combat Cybercriminals' activities in the United States, social theories were employed to explain causality. The current research applies technological theory, including that the application of computer security theories to create and evolve solutions that enable authentication, confirmation, non-repudiation, and validation is fundamental to the response of technology to cybercrime challenges. These models and theories use cryptography, steganalysis, internet protocol, and software development process/models to create systems that secure users and the infrastructure provider. Cybercrime flourishes on the internet today because the internet's protocols did not include a feature that enables a host to selectively deny communications from the start. In the current research on cybercrime, techniques are independent variables while the dependent variable is online banking usage. Besides the independent and dependent variables, big data relies on a mediating variable in the current research.

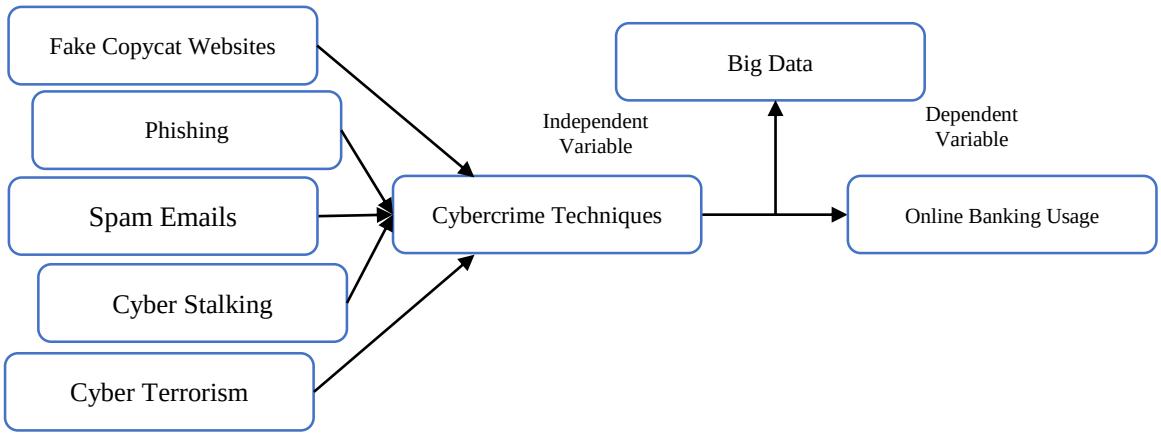

Figure: Conceptual Framework

2. METHODOLOGY

Design

After establishing the research problem, designing the research, or research design, is perhaps the most critical step. Researchers can take action on research subjects like what, when, where, how, and by what methods, for example, because of the study's design. Exploratory and conclusive research designs are the two most common types. Experimentation is often qualitative, whereas finalization is typically quantitative in this context. Descriptive and causal research designs are two of the most common forms of conclusive research designs. We took a cross-sectional strategy to our study. The current study uses a cross-sectional design and a

quantitative technique. The current study obtained numerical data that may be examined statistically (Goddard & Melville, 2004).

Deductive approach

Acceptance and refining of a subject matter hypothesis into the more precise, testable hypotheses are the first steps in the deductive process. After data has been gathered and examined, theoretical misunderstandings might be addressed by additional filtering. Therefore, the researcher may check the basic assumptions of the study by looking at the data. Saunders, Lewis, and Thornhill (2009) deductively demonstrate how an existing theory may be used to generate a new method.

Participants

Only IT professionals working in small and medium-sized enterprises (SMEs) from the United States were included in the study's target audience. We made sure that all participants knew about the consent process and that the information we were gathering would only be used for academic purposes. The study's scope was widened by reaching out to the general technical community. The intended audience consisted of both sexes, i.e., men and women (Goddard & Melville, 2004).

Materials

The data was collected using a five-point Likert scale questionnaire **(Appendix A)**, which was based on the three sections of the questionnaire. The first half focused on demographics, such as gender, age, and social class, whereas the second section examined the study's main variable, hostile insider threats, and operational practices. Those variables are made up of the answers to the 21 questions that made up that portion of the test (Noor, 2008).

Procedure

For this study, the respondents were asked to rate their demographics, cybercrime threats in online banking, and banking processes on a one to five scales. As a result of the questionnaire being published on Google Forms, participants were personally contacted and given direct links to fill out the form. The respondents were informed that the information they provided would be used only for academic purposes by asking a consent-related question at the beginning of the survey.

Analytical Procedures

The present study work used SPSS v26.0 on Windows to do the statistical analysis. For this purpose, descriptive statistics were used. Cronbach's Alpha values and factor analysis were used to examine the scale data's believability. Following this, Pearson correlations and multiple regressions were employed to examine the influence of independent factors on dependent variables, respectively.

RESULTS

Demographics

Table 1 lists the demographics of the survey participants. Gender, marital status, age, educational attainment, and work experience are all represented in the percentages in the following table. There are 56% male and 44% female respondents; 53.1 percent and 47.9

percent of the total populous answer are single and married, respectively, which indicates that most of the respondents are unmarried. The remainder of the category distribution is shown in the table.

Table 1. Percentage Distribution

		Table N %
Gender of the respondents	Male	56.0%
	Female	44.0%
Marital status of the respondents	Single	53.1%
	Married	47.9%
Age of the respondents	18-25 years	30.8%
	25-35 years	53.4%
	35-50 years	15.8%
	Above 50	0.0%
Qualification of the respondents	Graduation	30.2%
	Master	49.9%
	PhD	5.5%
	Other	14.4%
Experience of the respondents	Less than 1 year	8.2%
	1-5 years	51.6%
	6-10 years	30.4%
	Above 10 years	5.9%

Descriptive Analysis

Summary statistics, such as frequencies, measurement items, means, and standard deviations, are used to summarize data using descriptive statistics. The descriptive statistics show the mean values of 4.6 for cybercrime techniques with a standard deviation of .43 while the mean values for big data are 3.03 and the mean values for online banking users can be seen as 2.3 which is considerably low.

Table 2 Descriptive Statistics

	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
Cybercrime Techniques	100	1.00	5.00	4.6505	.43810
Bigdata	100	1.00	5.00	3.0357	.44326
Online Banking Usage	100	1.00	5.00	2.3456	.46356
Valid N (listwise)	100				

Reliability Analysis

It is used to determine whether or not the data is reliable enough to be utilized in future statistical analyses. If Cronbach's alpha value is closer to 0.7 or above, it is considered credible data and may be utilized for correlation and regression. Among the 21 entries in Table 4, Cronbach's Alpha is 0.71, which is quite dependable. Using the current Cronbach's Alpha values, regression and correlation analysis may be applied to the data.

Table 3 Case Processing Summary

		N	%
Cases	Valid	100	99.1
	Excluded	1	.9
	Total	106	100.0
a. Listwise deletion based on all variables in the procedure.			

Table 4 Reliability Statistics

Cronbach's Alpha	**N of Items**
.710	21

Factor Analysis

If a factor supports the variables and has sufficient coherence to maintain the variables, it is studied using factor analysis. Coherence of factors is shown in their extraction values, which range from 0.6 to 0.7 for CCT (Cybercrime Techniques) and BD (Online Banking Usage), respectively, which is sufficient to maintain the variables. Also, the value range of 0.7-0.8 is ideal for supporting OBU in the factor analysis.

Table 5 Factor Analysis

	Initial	Extraction
CCT1	1.000	.874
CCT2	1.000	.698
CCT3	1.000	.843
CCT4	1.000	.831
CCT5	1.000	.754
CCT6	1.000	.794
CCT7	1.000	.776
BD1	1.000	.721
BD2	1.000	.783
BD3	1.000	.795
BD4	1.000	.668
BD5	1.000	.769
BD6	1.000	.799
OBU1	1.000	.751
OBU2	1.000	.793
OBU3	1.000	.851
OBU4	1.000	.718
OBU5	1.000	.811
OBU6	1.000	.741
OBU7	1.000	.700
Extraction Method: Principal Component Analysis.		

Correlation Analysis

Correlation analysis is used to investigate the relationship between the variables, which is significantly negative suggesting that higher the cybercrimes and higher techniques such as phishing of data, spam, and emails are in the online market, there would be low usage of online banking. The relationship between both the variables is negative which is significant at p=0.000.

Table 6 Correlations

		Cybercrime Techniques	**Online Banking Usage**
Cybercrime Techniques	Pearson Correlation	1	-.548**
	Sig. (2-tailed)		.000
	N	100	100
Online Banking Usage	Pearson Correlation	-.438**	1
	Sig. (2-tailed)	.000	
	N	105	
****. Correlation is significant at the 0.01 level (2-tailed).**			

Regression Analysis

Regression illustrates the impact of the independent variable on the dependent one, in the current study the independent variable is Cybercrime Techniques while the dependent variable in the current research is Online Banking Usage. The regression illustrates the negative impact of Cybercrime Techniques on Online Banking Usage. Meanwhile, the Bigdata solutions mediated the relationship between both variables.

Table 7 Model Summary

Model	**R**	**R Square**	**Adjusted R Square**	**Std. The error in the Estimate**
1	-.563[a]	.163	.224	.04278249
a. Predictors: (Constant), Cybercrime Techniques				
b. Dependent Variable: Online Banking Usage				

The individual impact of the independent variable on the dependent one is seen in table 8 which is B=0.445 with a significance of p=0.000.

Table 8 Coefficients

Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	Std. Error	Beta		
1	(Constant)	.000	.089		.003	.997
	Cybercrime Techniques	-.660	.032	.448	3.440	.001
	Bigdata	0.393	.038	0.445	3.422	0.000
a. Dependent Variable: Online Banking Usage						

International Journal of Aquatic Science
ISSN: 2008-8019
Vol 13, Issue 01, 2022

Cybercrime Current Scenario in the USA

The cybercrime scenario in the USA is evolving constantly and with new and innovative technologies emerging, it's hard to keep track of all the latest trends. In this research, we have taken a closer look at the cybercrime landscape in the USA.

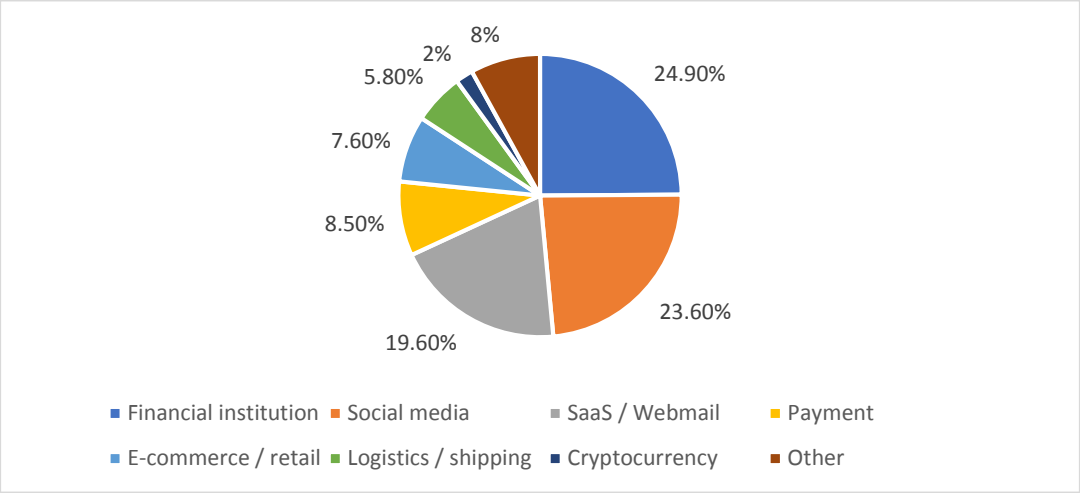

Figure 1.1 Most Cybercrime Targeted Industry in USA 2021

The above assessment revealed that the most exposed industry to cybercrime is financial institutes (24.90%) while social media comes at second place with 23.60%. meanwhile SaaS/Webmail is 19.60% target with cybercrime, likewise, payment, e-commerce, logistics, cryptocurrency and others are 8.50%, 7.60%, 5.80%, 2% and 8% respectively.

Year-wise cybercrimes are increasing with greater intensity while looking at the typology of crimes it can be in the below figure 1.2 that fraud stays at the top, identity theft at second while others are at third place.

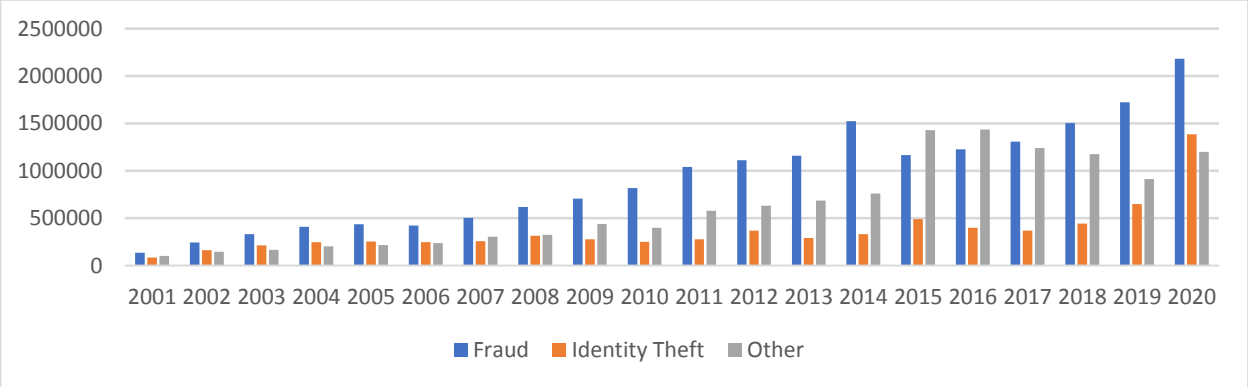

Figure 1.2 Category (Fraud, Identity Theft, and Other) Wise Cybercrime in the USA

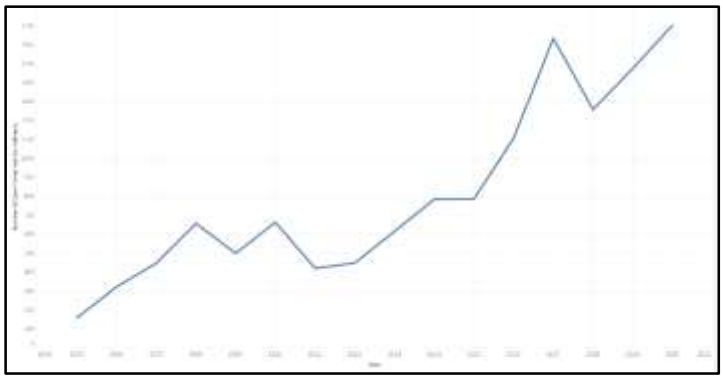

Figure 1.3 Year Wise Cybercrime in the USA

Year-wise cybercrime in the USA trend line is given in figure 1.3, where exponential growth in the increasing cybercrimes can be seen.

Figure 1.4 Cybercrime losses in USA in 2020

Figure 1.5 Cybercrime victims per 100k population in USA in 2020

In the end, the cybercrime victims per 100k population and cybercrime losses state-wise are given in figures 1.4 and 1.5 where the higher tracked target states were colored in dark blue and red revealing that Nevada was the most target for the victims while California and New York were the most targets for losses.

3. DISCUSSIONS

To acquire the financial information of end-users, computer fraudsters utilize a variety of tactics and procedures, including computer hacking, phishing, vishing, identity theft, and more. For this reason, clients of internet banking should be aware of the tactics and strategies used by cybercriminals. However, only 31% of the survey participants said that they were aware of all of the hazards listed in this study. This demonstrates that over 70% of internet consumers have minimal or no knowledge of the hazards posed to individuals and the banking business. This is a major problem. To add to the problem, this further allows computer crooks and fraudsters to obtain unlawful client information and use it for their nefarious purposes (Ataya & Ali, 2019).

The study finds a negative impact of cybercrime techniques on online banking as various studies find the same impact. Several authors L. Ali, Ali, Surendran, Thomas, and e-Learning (2017) find the same negative impact of cybercrime on the banking system. Aribake and Finance (2015) also find a negative impact of cybercrime threats on the banking system in the US. Akinbowale et al. (2020) find some kind of different results from the previous studies. But this study finds(Akinbowale et al., 2020) the same results as the previous studies mentioned.

4. CONCLUSIONS

The study can't overlook the reality that Competitive Intelligence programs try to use divergent information sources to boost an institution's competitiveness while degrading its competitors'. This data is typically obtained legally or illegally via economic espionage. The next stage in e-Banking security has been discussed for many years. It's hard to tell when the market will gain momentum and adopt innovative new technology. Banks have a difficult option in the e-Banking environment. A rise in the number of cyberattacks on established e-banking systems may be seen across all markets (Hussain, 2016). Unfortunately, today's authentication solutions share the same drawbacks. They do not stop today's most common online man-in-the-middle attacks. There are many solutions available that aim to provide a further layer of protection for the consumer by requiring them to physically validate certain transactions. In conclusion, no one method can cover all the threats to the result, multi-layered security is the ideal choice for an e-banking platform.

According to the results, the study concludes that there is a negative impact of cybercrime techniques on the banking system. The reason for the negative impact was that certain cybercrime techniques had some security breaches through which consumer data might be lost. For example, the vishing techniques lost bank credentials for which their performance was lost, and consumer trust was also lost. After the loss of consumer trust, the usage of online banking was also lost, so the performance of online banking would be decreased. So, in this way, the study finds the negative impact of cybercrime techniques on online banking (Ataya & Ali, 2019).

Recommendation

Based on the facts as well as the discussion above, this study recommended the following:

The usage of secure software applications must be enhanced or adapted to further enhance online banking security. More advanced and powerful methods are needed to monitor computer fraudsters as well as hackers to prevent unauthorized access to online banking consumers'

financial information. This will also assist safeguard commercial transactions. People who utilize internet banking need to be informed on the processes and approaches that are used to build trust.

As a result, the banking industry must take major measures to ensure that online bank users are aware of possible online dangers. Online bankers must use strong passwords but also unique usernames for each site and account. Customers should be informed of the necessity of safe internet banking and users must also avoid security dangers.

Appendix A (Questionnaire)

Cybercrime Techniques

How confident, if at all, do you feel that you know how to keep your personal devices and online accounts secure?

Strongly Disagree				Strongly Agree
1	2	3	4	5

Is the password for your email account being used for any other online accounts?

Strongly Disagree				Strongly Agree
1	2	3	4	5

Are you currently using your web browser or a password manager app to save or create passwords?

Strongly Disagree				Strongly Agree
1	2	3	4	5

Have you enabled Two-factor authentication (2FA) for any of your online accounts?

Strongly Disagree				Strongly Agree
1	2	3	4	5

Do you regularly backup your devices? E.g. Phones, laptops, tablets?

Strongly Disagree				Strongly Agree
1	2	3	4	5

Do you install software updates on your devices when they become available?

Strongly Disagree				Strongly Agree
1	2	3	4	5

Were you aware that victims of fraud and cybercrime should report it to Action Fraud?

Strongly Disagree				Strongly Agree
1	2	3	4	5

Were you aware that you can report a suspicious email by forwarding it to: report@phishing.gov?

Strongly Disagree				Strongly Agree
1	2	3	4	5

Were you aware that you can report a suspicious text message (SMS) by forwarding it?

Strongly Disagree				Strongly Agree
1	2	3	4	5

Usage of Online Banking

Indicate the level of usage of online banking?

Strongly Disagree		Strongly Agree

1	2	3	4	5

How long do you use e-banking for the transactions?

Strongly Disagree			Strongly Agree	
1	2	3	4	5

How long do you use ATM and electronic banking systems?

Strongly Disagree			Strongly Agree	
1	2	3	4	5

Bigdata

Do you think big data can solve cybercrime in the online banking system?

Strongly Disagree			Strongly Agree	
1	2	3	4	5

Do you think machine learning is the best approach to minimizing the cybercrimes in the online banking system?

Strongly Disagree			Strongly Agree	
1	2	3	4	5

Can augmented reality replace human resources in electronic banking?

Strongly Disagree			Strongly Agree	
1	2	3	4	5

5. REFERENCES

[1] Ahmad, I., Iqbal, S., & Shahzad Jamil, M. K. J. L. A. (2021). A Systematic Literature Review of E-Banking Frauds: Current Scenario and Security Techniques. 3509–3517-3509–3517.

[2] Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. J. J. o. F. C. (2020). Analysis of cyber-crime effects on the banking sector using the balanced scorecard: a survey of the literature.

[3] Ali, L., Ali, F., Surendran, P., Thomas, B. J. I. J. o. e.-E., e-Business, e-Management, & e-Learning. (2017). The effects of cyber threats on customer's behaviour in e-Banking services. *7*(1), 70-78.

[4] Ali, L. J. T. J. o. D. A. (2019). Cyber crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC). *53*(1).

[5] Amrollahi, M., Dehghantanha, A., & Parizi, R. M. (2020). A survey on application of big data in fin tech banking security and privacy. In *Handbook of Big Data Privacy* (pp. 319-342): Springer.

[6] Apurva, A., Ranakoti, P., Yadav, S., Tomer, S., & Roy, N. R. (2017). *Redefining cyber security with big data analytics.* Paper presented at the 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN).

[7] Aribake, F. O. J. I. J. o. T., Economics, & Finance. (2015). Impact of ICT tools for combating cyber crime in Nigeria online banking: a conceptual review. *6*(5), 272.

[8] Arrawatia, M. A. (2019). A Comparative Study of E banking Services Provided by Public and Private Sector Banks in India.

[9] Ataya, M. A. M., & Ali, M. A. (2019). *Acceptance of Website Security on E-banking. A-Review.* Paper presented at the 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC).

[10] Azhar, S., Shahi, M., & Chhapola, V. (2020). E-Banking Frauds: The Current Scenario and Security Techniques. In Encyclopedia of Criminal Activities and the Deep Web (pp. 905-918): IGI Global.
[11] Bakare, S. J. T. J. o. I. B., & Commerce. (2015). Varying impacts of electronic banking on the banking industry. 20(2).
[12] Barbara A. Manko. (2021). Big data: The effect of analytics on marketing and business.
[13] Dr. Ritika Malik, Dr. Aarushi Kataria and Dr. Naveen Nandal, Analysis of Digital Wallets for Sustainability: A Comparative Analysis between Retailers and Customers, International Journal of Management, 11(7), 2020, pp. 358-370.
[14] Camillo, M. J. J. o. R. M. i. F. I. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *10*(2), 196-200.
[15] Dzomira, S. J. R. G., Markets, C. F., & Institutions. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *4*(2), 16-26.
[16] Ezeoha, A. E. J. T. J. o. I. B., & Commerce. (1970). Regulating internet banking in Nigeria: Some success prescriptions-Part 2. *11*(1), 1-12.
[17] Goddard, W., & Melville, S. (2004). *Research methodology: An introduction*: Juta and Company Ltd.
[18] Goel, S. (2016). *Cyber-Crime: A growing threat to Indian banking sector*. Paper presented at the 3rd Int. Conf. Recent Innov. Sci. Technol. Manag. Environ.
[19] Hassani, H., Huang, X., Silva, E. J. B. D., & Computing, C. (2018). Digitalisation and big data mining in banking. *2*(3), 18.
[20] Hussain, R. J. I. o. b. a., Karachi, Pakistan. (2016). Cyber-crimes and e-banking: An empirical study.
[21] Ige, M. S. (2015). *The impact of computerised accounting information system on the performance of the banking industry in Nigeria.* Thesis (MSc), University of Lagos, Social Science Research Network [Online …,
[22] Kamal, M. M., Chowdhury, I. A., Haque, N., Chowdhury, M. I., & Islam, M. N. J. A. S. S. (2012). Nature of cyber crime and its impacts on young people: A case from Bangladesh. *8*(15), 171.
[23] More, D. M. M., Nalawade, M. J. I. J. o. A. R. i. C. S., & Paper, S. E. R. (2015). Online banking and cyber-attacks: the current scenario.
[24] Noor, K. B. M. J. A. j. o. a. s. (2008). Case study: A strategic research methodology. *5*(11), 1602-1604.
[25] Raghavan, A., Parthiban, L. J. I. J. o. C. R., & Review, A. (2014). The effect of cybercrime on a Bank's finances. *2*(2), 173-178.
[26] Rathore, N. K. J. J. o. I. T. (2016). Ethical hacking & security against cyber crime. *5*(1), 7-11.
[27] Saini, H., Rao, Y. S., Panda, T. C. J. I. J. o. E. R., & Applications. (2012). Cyber-crimes and their impacts: A review. *2*(2), 202-209.
[28] Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. doi:https://doi.org/10.1108/et.2007.49.4.336.2
[29] Usman, A. K., Shah, M. H. J. T. J. o. I. B., & Commerce. (1970). Critical success factors for preventing e-banking fraud. 18(2), 1-14.
[30] Vrîncianu, M., & Popa, L. A. J. T. A. E. J. (2010). Considerations regarding the security and protection of e-banking services consumers' interests. 12(28), 388-403.

[31] Veeranki S. R, Varshney M. (2022). Intelligent Techniques and Comparative Performance Analysis of Liver Disease Prediction, International Journal of Mechanical Engineering, 7(1), 489-503. https://kalaharijournals.com/ijme-vol7-issue-jan2022part2.php,
[32] Wada, F., & Odulaja, G. (2012). Assessing cyber crime and its impact on e-banking in Nigeria using social theories. *African Journal of Computing & ICT*, *5*(1), 69-82.
[33] Wang, V., Nnaji, H., Jung, J. J. I. J. o. L., Crime, & Justice. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *62*, 100415.