SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

"A PRIMARY STUDY ON USER PERCEPTION OF PHISHING IN BANKING SECTOR"

Ayesha Warda*, Jhumur Samaddar**

Abstract

Phishing is the malicious act of retrieving sensitive information from users disguising oneself as trust worthy entities. In banking, phishing is the retrieval of privileged information such as username, passwords, ATM pin and other account related intelligence from users by enacting as their banking representative. The objectives of the study: To determine the level of awareness of the term phishing among bank users, to analyze the satisfaction level of the users towards the awareness methods implemented by the banks and to discover the most commonly used media for phishing attack from the point of view of the users.The study made use of both primary data and secondary data. Primary data wascollected using well-framed questionnaires on Google Forms. Non-discriminative snowball sampling was used for sample selection and included 385 samples. The studyfound out that most users were aware of the term phishing, were dissatisfied by the way banks provided awareness, and the most commonly used medium for phishing attack was SMSs.

Key words: Phishing, Cybercrime, Bank users, Malicious, Sensitive Information

**Research Scholar, "VISTA", Opp. MES School, Ambilad, Kuthuparamba, Kannur, Kerala*
ayshawardah97@gmail.com
***Assistant Professor, St Joseph's College Of Commerce, Bengaluru Bengaluru,*
Email :anjhu09@gmail.com

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

Introduction

Banks are financial institutions which are popularly involved in transactions that encompass money. Banks' primary function is to accept deposits from public who are willing to give, and use this deposit to lend money to public who are in dire need of the same. They act as a source of borrowing and saving for the public. This way, banking sector is considered to be the backbone of any economy as it accelerates the flow of money.

Phishing is the malicious act of retrieving sensitive information from users disguising oneself as trust worthy entities. In banking, phishing is the retrieval of privileged information such as username, passwords, ATM pin and other account related intelligence from users by enacting as their banking representative.

Scope of the study

The study is conducted in the vicinity of Bengaluru City. The study took a time period of six months to complete. The population is people living in Bengaluru City from the age of 15 years and above. The study shall be useful for banks to understand the level of awareness of phishing among their customers, the efficiency of their awareness methods and their consequent satisfaction level among their customers, and find out the most commonly used medium/media for phishing attacks and be able to work further on tackling the issue.

Review of Literature and theoretical background

Phishing is an activity on the internet in the form of identity theft. This scam uses believable spoofing methods to retrieve social information of its victims(Aburrous et al., 2010). It is the most dangerous of cybercrime as it causes paramount loss to users and banking institutions and is one of the most widely used methods of cybercrimes in banking sector by tech savvy fraudsters. It is also the fastest growing cybercrimes. (Singh, 2007). The issue of fraudulent activities online has turned into an epidemic. Such malicious acts are more prominent in areas where people have switched to e-commerce, which in turn leads to, an increased usage of online modes of financial affair (Alanezi, 2016).

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

Such scams do not have one measure or solution to curb because the fraudsters use psychological move to trick the users (Aburrous et al., 2010). The fraudsters who are behind such acts are able to put into use kindred methods of attaching mala fide links which consist of bogus news, viral videos and so on which can easily attract victims (Frauenstein et al., 2020).

Trojan horse is the latest application in phishing. This application finds a way to enter into the user's system through emails. Once inside the system, it acts as a guide for the users to log on to website that look similar to the user's bank's website. When the user logs in, his/her password and other sensitive information is retrieved(Singh, 2007).Bulk and unwanted emails or "spam" as they are called is a major threat globallybecause these emails act as vectors to attack the personal system of people all around the world in the form of MALWARE attacks (Broadhurt et al., 2017).Phishing attacks have evolved from email to Social Networking Sites (SNS). Since SNS is huge, the market for fraudsters is ipso facto large, with plenty of chances to defraud users. The main focus of fraudsters is using the vulnerabilities of behaviour among users on SNS (Frauenstein et al., 2020).

Traditional indicators of phishing are futile. Intelligent indicators are the need of the hour (Aburrous et al., 2010). Assessment of vulnerability to phishing concluded that users who could identify bogus messages could not give an apt reason for their decision (Karakasiliotis et al., 2007). Users in general spend very less time on looking at the potential yardstick to pinpoint illegitimate websites. Additionally, the technical know-how of users was not related to the ability to pinpoint illegitimate and malicious gauge of websites (Alsharnouby et al., 2015).

Phishing targets customers of financial service or consultancy enterprises. Therefore, employees and customers should be aware of the various dangers that this can cause, and must be cautious (Kumudha et al., 2018).Apparently, the vulnerability of employees falling for such malicious acts are high irrespective of whether or not they are educated regarding the same (Williams et al., 2018).

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

As per Information Technology Act (2000), news reports and National Crime Record Bureau (NCRB), phishing attack was one of the important cybercrimes in India, and they were usually targeting Nationalised Banks (Nalawade et al., 2015). The rise in cases of phishing attack and its consequent identity theft along with poor initiatives of banks in the rural and semi-urban areas can be an alarming threat to the future of banking in India (Vijaya Geeta, 2011).

The major catalyst for the success of such online fraud in the banking sector is the lack of education, and the aim is to get the attention of thecustomers. Emails sent to the customers of the banks have been the most effective mode of education (Swann,2006).Phishing is a huge threat not just to individuals but also to the organizations involved mainly due to the big amounts lost yearly, security breaches, loss of data, breach of privacy and many more.

The solution or suggestion is that there ought to be a proper implementation of spreading awareness among customers which shall educate them aptly, and periodical review of sensitive information of the customers should be followed (Singh, 2007).Therefore, organisations along with customers have to undertake training efforts to protect themselves (Wright et al., 2014).

Measures to fight or prevent phishing include personalisation of email and web pages, using protective software, two-factor authentication and finally focussing on spreading awareness to customers (Bilgrami, 2017). People do not understand the magnitude of preventive measures as they are not properly skilled to implement these measures against phishing (Jansen et al., 2016).

The countermeasures available and put to use are highly inadequate and inefficient and that these measures might have failed because of the vulnerability of the organizational and environmental circumstances (Alanezi, 2016).The efficiency of anti-phishing awareness can be increased if the pedagogy used is altered according to the motivational

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

level of the trainees. This along with proper integration of available technology can bring out greater results (Jerry Chih-Yuan Sun et al., 2016).

Researchers are of the belief that empirical research is one of the best ways to reach a conclusion for the predicament (Aburrous et al., 2010). Also, there is a need for international cooperation against phishing which can lead to developments of new protection techniques. Amulti-level involvement from government, law and private sector is imperative because phishing has an adverse effect on all three entities. (Casim, 2014).

However, the technology and geography in these cybercrimes are vast and complex, which creates disharmony among the laws created by different nations to fight this common evil(Dupont et al., 2018).Fighting or curbing or preventing online frauds become relatively easier and effective when people are well educated and trained regarding the adverse effects and the measures to combat online frauds (Alanezi, 2016). Banking administration has to be efficient and effective to form a method to foresee any undesirable events before they actually happen and the most important way to curb frauds is by educating customers on how to understand a potential scam. Banks should also be more cautious with their business model and risk management programs. These two factors ought to be flexible enough to accept any change in regulation. There has to be cooperation and synergy between banks and their customers (Jeyanthi et al., 2020).

Research Gap

There have been multiple studies and articles on phishing attacks but a study on the same topic from the point of view of users is few, especially with reference to Bengaluru.Since there is no turning back in the way internet banking functions, it is imperative to carry out a study to acknowledge the immediate need to tackle phishing attacks from the user's point of view to facilitate banks to understand where they stand in terms of spreading awareness and formulate better plans and policies to do the same.

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

Research Design/Methodology

Research Problem

Internet banking is the present and the future of the banking industry. There will be only a forward move from this point in e-banking. However, Phishing has become a common issue in the online world. This billion-dollar industry targets users. The loss suffered by users and subsequently by banks are enormous.

Research Objectives

The primary objective of the paper is to study the user perception of phishing in banking sector.

Consequently, the study also possesses the following objectives:

- To determine the level of awareness of the term phishing among bank users.
- To analyze the satisfaction level of the users towards the awareness methods implemented by the banks.
- To discover the most commonly used media/medium for phishing attack from the point of view of the users.

Hypotheses

1. H0 – There is no association between awareness of the concept of phishing and likelihood of falling prey to phishing with such awareness.
   H-There is association between awareness of the concept of phishing and likelihood of falling prey to phishing with such awareness.
2. H0 – There is no association between satisfaction in banking system and satisfaction level on awareness methods
   H1-There is association between satisfaction in banking system and satisfaction level on awareness methods

Conceptual and operational definitions of Variables

1. Independent variables:

- **User awareness:** As per various literature on phishing, it is understood that lack of awareness among common public or particularly among bank users is one of the most significant reasons for the success of phishing attacks.

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

- *Initiatives of banks:* For as long as users are not given proper awareness on the very existence of phishing attacks, it will continue to be on a rise.
- *Media:* Media play a pivotal role in facilitating a smooth and successful fraud. Media such as phone calls, SMSs, emails and believable links on various socialmedia are the biggest facilitators of phishing attacks.

2. Dependent variable:

- **Phishing:** It is depended on the level of awareness of bank users, the efficiency of awareness methods implemented by banks and their subsequent satisfaction from the users and the media through which phishing attacks usually take place.

Sample and Sampling

The sample for the study is any banking user residing in Bengaluru. The age group selected is 15 years and above. Gender of sample includes female, male and others. Taking a confidence level of 95% and a Margin of Error at 5% for population of 10,391,294., the study had 385 samples. The sampling technique used for the study is snowball sampling. Under snowball sampling, the study exercised exponential non-discriminative snowball sampling, which means one sample provides referral to multiple other samples who will further provide referrals to other samples until the desired count is achieved.

Data analysis technique

The collected data was downloaded to a Microsoft Excel sheet and coded. The coded data was imported to IBM SPSS Statistics 21 version for accurate data processing and analysis.

The objectives were analyzed on the basis of Descriptive Statistics focusing mainly on mean. The respective hypotheses were tested using Linear Regression Analysis to form an equation using beta coefficients of the dependent, independent and constant variables, checked for the fitness of the model on the basis of adjusted R square and used p value to accept or reject null hypothesis.

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

Source of Data Collection

A Primary Study on User Perception of Phishing in Banking Sector is an empirical study. The study made use of both primary data and secondary data. The source of primary data is the questionnaire which was sent out and collected. Well-framed questionnaires were prepared on Google Forms. The URL link was shortened and sent to people through various social media apps like Instagram and WhatsApp. Secondary data was collected from various online sources of journals like jstor, research gate, emerald, science direct, blogs on phishing, newspaper articles, Wikipedia, slide share, UN world population prospects and so on.

Limitations of the study

- The analysis, interpretation and conclusion of the study is limited to the city of Bengaluru. Hence, the conclusion cannot be completely generalized throughout the state and/or the country.
- There was difficulty in collecting data from the samples. The difficulty included locating the samples, convincing them to fill the questionnaire and even persuading the samples to send the questionnaire to other samples.
- The lack of time was an added limitation to the study

Analysis and Interpretation of Results

Table-1

Level of awareness of the concept of phishing among bank users

Descriptive Statistics

	Mean	Std. Deviation	N
Fall prey with awareness	1.90	.950	385
Aware of concept of phishing	**3.56**	**1.257**	**385**
Aware of education on phishing by banks	3.18	1.237	385

Source: Primary data

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

Interpretation: In the above table, it is evidently given that the mean value for the level of awareness of the term or concept of phishing is 3.56, which is closer to 4 in a 5-point Likert scale. 4 in the scale given for the study is "AWARE". Therefore, it can be inferred that users are aware of the concept of phishing existing in banking sector.

Table-2

The satisfaction level of users towards awareness methods implemented by banks

Descriptive Statistics

	Mean	Std. Deviation	N
Satisfaction on banking system	3.31	.887	385
Satisfaction level on awareness methods	**3.01**	**.928**	**385**

Source: Primary data

Interpretation: In the above descriptive statistics table, it is evident that the mean value for satisfaction level on awareness methods is 3.01, which is the closest to 3 in the 5-point Likert scale. 3 in the scale given for the study is "NEUTRAL". Therefore, it can be inferred that users are not satisfied with the methods used by banks to spread awareness on phishing.

Table-3

Media used for phishing attack

Descriptive Statistics

	Mean	Std. Deviation	N
Phone calls	3.84	1.171	385
SMS	**3.88**	**1.150**	**385**
Emails	3.64	1.135	385
Links on social media	3.79	1.181	385

Source: Primary data

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

Interpretation: It is seen that SMS has the highest mean of 3.88 when compared to other media used for phishing attack like phone calls (3.84), emails (3.64) and links on social media (3.79). SMS stands first in mean ranking between phone calls, SMSs, emails and links on social media. Therefore, it can be inferred that the most commonly used medium for phishing attacks by fraudsters are SMSs.

Hypothesis testing

1.H0 – There is no association between awareness of the concept of phishing and likelihood of falling prey to phishing with such awareness.

H1 -There is association between awareness of the concept of phishing and likelihood of falling prey to phishing with such awareness.

Linear regression equation:

$$Y = a + b_1X_1 + b_2X_2$$

$$Y = 2.279 + -.112X_1 + .007X_2$$

where;

y = Falling prey to phishing with awareness

x_1 = Awareness of the concept of phishing

x_2 = Awareness of the education provided by banks on phishing to users

Table-4.1

Coefficient of awareness of the concept of phishing and likelihood of falling prey to phishing with awareness

Model	Unstandardized Coefficients		Standardized Coefficient	t
	B	Std. Error	Beta	
(Constant)	2.279	.155		14.708
Aware of concept of phishing	-.112	.046	-.148	-2.413
Aware of education on phishing by banks	.007	.047	.009	.140

Dependent variable: Fall prey with awareness

Predictors: (Constant), Aware of education on phishing by banks, Aware of concept of phishing

Source: Primary data

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

Table-4.1.1

Coefficient of awareness of the concept of phishing and likelihood of falling prey to phishing with awareness

Model	Sig	95% Confidence Interval for B	
		Lower Bound	Upper Bound
(Constant)	.000	1.974	2.584
Aware of concept of phishing	.016	-.203	-.021
Aware of education on phishing by banks	.888	-.086	.099

Dependent variable: Fall prey with awareness

Predictors: (Constant), Aware of education on phishing by banks, Aware of concept of phishing

Source: Primary data

Interpretation: Since the p value of awareness of the concept of phishing is .016, which is less than .050, there is sufficient evidence to reject null hypothesis and accept alternative hypothesis. Therefore, it is inferred that there is association between awareness of the concept of phishing and likelihood of falling prey to phishing with such awareness. Awareness of concept of phishing exerts significant influence on the likelihood of falling prey to phishing with such awareness. This means that the more users are aware of phishing, chances are less that they may fall prey to phishing and vice-versa.

Table-4.2

Model summary of linear regression between awareness of the concept of phishing and likelihood of falling prey to phishing with such awareness

R	R Square	Adjusted R	Std. Error of	Change Statistics	
		Square	estimate		
				R Square Change	F Change
.144	.021	.016	.942	.021	4.025

Dependent variable: Fall prey with awareness

Source: Primary data

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

Interpretation: Since Adjusted R square is .016, dependent variable is explained by independent variable to the extent of 1.6%. Therefore, the model is not a good fit.

H0 – There is no association between satisfaction in banking system and satisfaction level on awareness methods

H1 - There is association between satisfaction in banking system and satisfaction level on awareness methods

Linear Regression Equation

$$Y = a + b_1X_1$$

$$Y = 2.039 + .421X_1$$

Where;

Y = Satisfaction towards banking system

X_1 = Satisfaction towards awareness methods

Table-5.1

Coefficientsof satisfaction on banking system and satisfaction level on awareness methods provided by banks

Model	Unstandardized Coefficients		Standardized Coefficient	t
	B	Std. Error	Beta	
(Constant)	2.039	.138		14.762
Satisfaction level on awareness methods	.421	.044	.441	9.615

Dependent variable: Satisfaction on banking system

Predictors: (Constant), Satisfaction level on awareness methods

Source: Primary data

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

Table-5.1.1
Coefficients of satisfaction on banking system and satisfaction level on awareness methods provided by banks

Model	Sig.	95% Confidence Interval For B	
		Lower Bound	Upper Bound
(Constant)	.000	1.768	2.311
Satisfaction level on awareness methods	.000	.335	.508

Dependent variable: Satisfaction on banking system
Predictors: (Constant), Satisfaction level on awareness methods
Source: Primary data

Interpretation: Since the p value of satisfaction level on awareness methods is .000, which is less than .050, there is sufficient evidence to reject null hypothesis and accept alternative hypothesis. Therefore, it is inferred that there is association between satisfaction in banking system and satisfaction level on awareness methods. Satisfaction level on awareness methods exerts significant influence on the satisfaction in banking system. This indicates that if the methods implemented by banks to spread awareness on phishing are not satisfactory, then it will affect the satisfaction level of users towards the entire banking system.

Tab-3
Hods provided by banks

R	R Square	Adjusted R Square	Std. Error of Estimate	Change Statistics	
				R Square Change	F Change
.441	.194	.192	.797	.194	92.450

Dependent Variable: Satisfaction on banking system
Source: Primary data

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

*Interpretation:*Since adjusted R square = .192, the dependent variable is explained by the independent variables to the extent of 19.2%. Therefore, this model is not a good fit.

Results and Findings

Demographic details of the respondents

Majority of the respondents are female (57.1%) followed by male (41%) and others (1.8%).Majority of the respondents belong to the age group of 20-30 years (63.4%) followed by 15-19 (14.5%), 31-40 (11.9%), above 50 (6.2%) and finally 41-50 (3.9%).The educational qualification of majority of the respondents is undergraduate degree (48.6%) followed by postgraduate degree (36.4%), higher secondary 8.6%), doctorate (4.2%) and up to high school (2.3%) in that order.A major chunk of respondents are students (51.2%) followed by private sector employees (18.2%), professionals (11.9%), self-employed (7.5%), home-maker (4.7%), business (4.2%) and public sector employees (2.3%) in this order.Public sector bank stands top (42.9%) in the type of bank used by the respondents, closely followed by Indian private sector bank (42.6%), international private sector bank (7.8%) and finally co-operative bank (6.8%) in that order.Majority of the respondents held only one bank account (46.2%) followed by users holding two bank accounts (32.3%), three bank accounts (14.8%) and more than three bank accounts (6.8%) in that order.

Discussion

Most of the respondents are "aware" of the term and concept of phishing. Consequently, there is a significant association between being aware of phishing and falling prey to it with this awareness. Awareness of phishing definitely exerts influence on the likelihood of falling prey to it. As far as the satisfaction level on the methods of awareness implemented by banks is concerned, respondents are not satisfied with the methods as they seem to be neutral towards it. Leading to an association between satisfaction on the banking system and satisfaction derived from the awareness methods implemented by banks. Satisfaction for awareness methods exerts influence on the overall satisfaction level of the respondents towards the entire banking system. SMSs are discovered to be

SJCC Management Research Review
Print ISSN-2249-4359
Vol - 12 (1) June 2022. Page No. 59-79
DOI : 10.35737/sjccmrr/v12/i1/2022/155

the most commonly used medium for phishing attack according to the respondents because they are personal yet distant and difficult to identify as a bait for phishing.

Conclusion

A Primary Study on User Perception of Phishing in Banking Sector was able to showcase the understanding of phishing among users. The study found out that most users were aware of the term phishing and its conceptual knowledge. This awareness about the concept of phishing has a direct impact on whether or not the users fall prey to phishing.

The study brought out the truth about methods used for educating users on phishing implemented by banks through SMS, email, posters in branch, newsletters, alerts on official websites etc. These methods were clearly inefficient. Therefore, users are dissatisfied with the kind of educative methods currently used for spreading awareness to them. The most commonly used or seen medium for phishing attack according to the users was SMS. The less is the awareness level of users, the more prone they are to fall prey to phishing via SMS.

In conclusion, banks and banking system have a long way to go in order to protect their customers from phishing and retain them. The study was able to convey that the basic awareness on phishing provided by banks to educate their customers is utterly inefficient. As the first aid to phishing comes from customers, it is important to educate them with precision and update them with innovations which arise in phishing.

Suggestions

Phishing has become one of the most commonly seen types of cybercrime. The chances of falling prey to it is high if proper awareness on the same is not given. It is suggested that banks spend a considerable amount on hoardings on roads and streets to reach every kind of audience.Even broadcasting creative and strong advertisements on television will definitely help reach mass audience and can bring an impact in the minds of the watchers. The advertisement can include narration of real-life incidents, short documentaries etc. to sow the seed of seriousness among people.

Customers can be educated over the counter when they open an account with a bank or visit the branch for any service. An awareness drive can be initiated by banks especially in rural and semi-urban areas. This way people who miss out on information published by banks regarding phishing can also be included. Educating employees is a strong factor that can curb and minimize the loss associated with phishing.

Introducing new methods may take time to be executed and accepted. It is also preferrable to improve the existing methodslike sending warning messages via SMSs, emails, alerts on websites and so on.

Practical/ Managerial/ Social implications

Banks and banking system are the backbone of any economy as they facilitate in accelerating the movement of money in the economy. As a result, people should have immense faith and trust in the system which they presume will protect their money. When that trust breaks, then everything will go downhill. Phishing is a cybercrime relevant in the recent days and have impacted many people. If banks do not take preventive and curative measures to curb this issue, then people will continue to suffer. As the paper found out that, people are not satisfied with the ways awareness is spread on phishing. It is imperative for banks to find innovative and creative ways of doing the needful.

References

1. Casim, F. (2014). Addressing the Specter of Phishing: Are adequate Measures in Place to Protect Victims of Phishing? *The Comparative and International Law Journal of Southern Africa, 47*(3). 401-428. https://www.jstor.org/stable/43894816

2. Broadhurst, R., &Alazab, M. (2017). Spam and Crime. In DRAHOS P. (Ed.). *Regulatory Theory: Foundations and Applications.* (517-532). Anu Press. http://www.jstor.org/stable/j.ctt1q1crtm.41

3. Dupont, B., & MacLellan, S. (2018). *Governing Cyber Security in Canada, Australia and the United States* (23-28, Rep.) (Leuprecht C., Ed.). Centre for International Governance Innovation. http://www.jstor.org/stable/resrep17311.10

4. Wright, R., Jensen, M., Thatcher, A.B. et al. (2014). Research Note: Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research*, *25*(2). 385-400. https://www.jstor.org/stable/24700179

5. Jerry Chih-Yuan Sun., &Kuan-Hsien Lee. (2016). Which Teaching Strategy is Better for Enhancing Anti-Phishing Learning Motivation and Achievement: The Concept Maps on Tablet PCs or Worksheets*? Journal of Educational Technology & Society*, *19*(4). 87-99. https://www.jstor.org/stable/jeductechsoci.19.4.87

6. Swann, J. (2006). Phishing and Pharming for Fraud. *Community Banker, 15*(12). 64-64. 1/3p.

7. Kumudha, S., &Rajan, A. (2018). A Critical Analysis of Cyber phishing and its Impact on Banking Sector. *International Journal of Pure and Applied Mathematics,119*(17). 1557-1569.

8. Singh, N.P. (2007). Online Frauds in Banks with Phishing. *Journal of Internet Banking and Commerce,12*(2).1-27.

9. Jansen, J., &Leukfeldt, R. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91. https://doi.org/10.5281/zenodo.58523

10. Williams, E. J., Hinds, J., &Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. International Journal of Human-Computer Studies, 120, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

11. Aburrous, M., Hossain, M. A., Dahal, K., &Thabtah, F. (2010). Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies. Cognitive Computation, 2(3), 242–253. https://doi.org/10.1007/s12559-010-9042-7

12. Jeyanthi, P. M., Mansurali, A., Harish, V., &Krishnaveni, V. D. (2020). SIGNIFICANCE OF FRAUD ANALYTICS IN INDIAN BANKING SECTORS. Journal of Critical Reviews, 7(04). https://doi.org/10.31838/jcr.07.04.38

13. Alanezi, F. (2016). Perceptions of online fraud and the impact on the countermeasures for the control of online fraud in Saudi Arabian financial institutions. Brunel University London

14. Online banking fraud rises fast. (2006, November 7). News.Bbc.co.uk. Retrieved from http://news.bbc.co.uk/2/hi/business/6122116.stm

15. Phishing through VoIP: How scammers do it. (2019). In Techadvisory.org. Retrieved from https://www.techadvisory.org/2019/01/phishing-through-voip-how-scammers-do-it/

16. Phishing is a billion-dollar global industry, consumers are the main target. (2019, July 26). Retrieved from Help Net Security website: https://www.helpnetsecurity.com/2019/07/26/phishing-economic-impact/

17. Wikipedia Contributors. (2019, June 29). Banking in India. Retrieved from Wikipedia website: https://en.wikipedia.org/wiki/Banking_in_India

18. Editors, H. com. (2018,). Renaissance. Retrieved from HISTORY website: https://www.history.com/topics/renaissance/renaissance#:~:text=The%20Renaissance%20was%20a%20fervent

19. Talha Ali. (2017,). Origin, history and types of banking system. Retrieved from slideshare website:https://www.slideshare.net/talharao679/origin-history-and-types-of- banking-system

20. Andrews, E. (2018,). Who Invented the Internet? Retrieved from HISTORY website:https://www.history.com/news/who-invented-theinternet#:~:text=ARPANET%20 adopted%20TCP%2FIP%20on

21. The Internet turns 25 in India. A timeline - The 1980s. (2020,).Retrieved from The Economic Times website: https://economictimes.indiatimes.com/tech/internet/the-internet-turns-25-in-india-a-timeline/the-2010s/slideshow/77589523.cms

22. Bangalore Population (2020).Retrieved from www.populationu.com website: http://www.populationu.com/cities/bangalore-populationhttps://www.history.com/topics/renaissance/renaissance#:~:text=The%20Renaisance%20was%20a%20fervent

23. Samarati, M. (2019,).Phishing attacks: 6 reasons why we keep taking the bait. Retrieved from IT Governance UK Blog website: https://www.itgovernance.co.uk/blog/6-reasons-phishing-is-so-popular-and-so-successful

24. Karakasiliotis, A., Furnell, S., &Papadaki, M. (2007). An assessment of end-user vulnerability to phishing attacks. Journal of Information Warfare, 6(1), 17-28. https://www.jstor.org/stable/26503466

25. Frauenstein, E. D., &Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. Computers & Security, 94, 101862. https://doi.org/10.1016/j.cose.2020.101862

26. Vijaya Geeta, D. (2011). Online identity theft – an Indian perspective. Journal of Financial Crime, 18(3), 235–246. https://doi.org/10.1108/13590791111147451

27. M.More, M., P. Jadhav, M., &Nalawade, K. M. (2015). Online banking and cyber-attacks: The current scenario. International Journal of Advanced Research in Computer Science and Software Engineering, 5(12), 743–749. https://www.researchgate.net/profile/Dr_Manisha_More/publication/290325373_Online_Banking_and_Cyber_Attacks_The_Current_Scenario/links/56962a8308ae425c6898fe70/Online-Banking-and-Cyber-Attacks-The-Current-Scenario.pdf

28. Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

29. O. Alsayed, A., & L. Bilgrami, A. (2017). E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities. International Journal of Emerging Technology and Advanced Engineering, 7(1), 109–115. https://www.researchgate.net/profile/Alhuseen_Alsayed/publication/31539938_E Banking_Security_Internet_Hacking_Phishing_Attacks_Analysis_and_Prevention_of_Fraudulent_Activities/links/58cfbf14aca27270b4acaeb5/E-Banking-Security-Internet-Hacking-Phishing-Attacks-Analysis-and-Prevention-of-Fraudulent-Activities.pdf

30. Irwin, L. (2019, July 9). The 5 most common types of phishing attack - IT Governance Blog En. Retrieved from IT Governance Blog En website: https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack

31. Review, L. S. P. (2020, October 7). Phishing - Examining Stakeholders' Liability and Awareness in India. https://lawschoolpolicyreview.com/2020/10/07/phishing-examiningstakeholders-liability-and-awareness-in-india/