INTERNATIONAL RESEARCH JOURNAL OF HUMANITIES AND INTERDISCIPLINARY STUDIES
(Peer-reviewed, Refereed, Indexed & Open Access Journal)
DOI : 03.2021-11278686 ISSN : 2582-8568 IMPACT FACTOR : 5.828 (SJIF 2022)

Review of Rising Cyber Crimes in Banking Sector and its impact on Individual's Economic Welfare

Niyatee Bhalgat[1] Tuba Vasgare[2] Rozmin Tasbi[3] Rujuta Joshi[4]

[1,2,3]*Student, F.Y.B. Com., Dapoli Urban Bank Senior Science college, Dapoli (Maharashtra, India)*
[4]*Assistant Professor, Dapoli Urban Bank Senior Science college, Dapoli (Maharashtra, India)*

DOI No. 03.2021-11278686 **DOI Link ::** https://doi-ds.org/doilink/03.2022-74684761/IRJHISIC2203036

ABSTRACT:

Internet banking or online banking was revolutionized the integral activity of our early twenty first century within the era of globalization. Man has built various means of contact that is of great importance to him as a social being for exchanging information, thoughts, and knowledge. The advancement of e-banking the technology makes the work very simple; with a click, banking transactions are in no time Internet banking and mobile banking make banking fast and convenient daily. An online and mobile banking, however, isn't one hundred pc secure. This study paper seeks to research the foremost current scenario of online banking and the cyber-attack. We specialize in cyber-crimes connected to online banking during this paper and new methods employed by hackers. This paper also identifies the emerging online banking-related the cybercrime from various journals and news articles. The report largely focuses on information available from the secondary source of knowledge. When handling online financial systems, this paper thoroughly analyses and explores the results of cyber attacks. The study concludes that there is a requirement to boost consciousness among consumers about the presence of the cybercrime within the handling of online banking and confidential financial data and how to defend themselves against these external challenges.

Keywords: *Cyber-crimes, cyber-attacks, hacking, mobile banking, online banking.*

Introduction:

Banking has been one among the foremost basic institutions in any country and thus the protection of the purchasers of banks is consummate for the well-functioning of the country. Banks have been subject to numerous pitfalls. The development of computers has made a great impact in the banking sector still along with it grew the different ways people would fall prey to different attacks. The spectacular growth in cybercrime is the main problem for economic institutions in the 21st century. Culprits sometimes committed crimes via telephone lines at the launch of the 1970s.

The suspects were called Phreakers and located that, counting on those sounds, the phone system in America worked. These tones were getting to be imitated by them to form free calls. Before the 1980s, there was still no real cybercrime. One reality has addressed the pc of another person to detect, copy, or exploit particular data and knowledge. Ian Murphy, also recognized as Captain Zap, was the primary person to be plant shamefaced of cybercrime, and it passed within the time 1981 to regulate the inner timepiece, he had compromised the American telephone pot So that guests at peak hours could still make free calls. Hackers, still, have persisted in distinct ways over time. While telecommunications providers were the very first target, it soon followed banks, online stores, and indeed private individualizes. Online banking is extremely popular moment, and it offers a serious occasion as well. Hackers can, for case, dupe log-in codes and addresses or recover credit card and bank account watchwords. The effect is that one can either empty accounts or make payments online from someone others account (Soni, 2019). Cybercrime is one of the world's most prominent and utmost involved forms of crime. The internet is after all, available to everyone and that of course includes pitfalls. It's unsafe to commit a felonious offense using a machine or other system linked to the web and the identity of the suspect is hard to figure out. From phishing and investment fraud to ID theft and gouging, cybercrime can take several forms. To date, since the walkout began, further than 5 m has been lost to coronavirus- related swindles and 16 m has been lost to online retail fraud. The bulk of coronavirus- related fraud includes online deals of particular defensive outfit, similar as face masks, that no way arrives. To convert the stoner to open links or attachments to prompt them to partake particular or fiscal details, malefactors have indeed submitted phishing emails and textbooks pretending to be from the army, HMRC, and health bodies.

Literature review:

Mostly all the fraudulent attacks have revolved around ATM, concealment, a master card fraud. The most aim of those attacks is to require over the user's bank accounts and funds in such how the attacker occupies the funds without proper knowledge of the user. A number of the ways to require a control of the users' account are explained within the next section. In some situations, to enter banks and steal an outsized amount of cash, cybercriminals use banking passwords like a pin, a password, certificates, etc. while in other circumstances, they'll attempt to steal all the cash and transfer the funds into mule accounts. Cyber attackers often aim to a wreck the bank's reputation then blocks bank servers in order that consumers are unable to access their accounts (Claessens, et. al., 2002). Online crimes mostly occur from the nuisance caused by amateur hackers. This paper also looks at the data of online crime and many problems. Issues that banks and police forces face in controlling traditional enforcement (Ali L, et. al., 2017). Significant improvements are possible within the way of handling an online fraud and to review online crime to suggest that to understand

its economic perspective (Moore, et. al., 2009). He made an overview of cyber legislation formulated to address cybercrime in the United States of America, The United Kingdom, Australia, India, The gulf Countries and South Africa. The study reveals that the incapability of public laws to address the challenges posed by cybercrime has led to the preface of technical cyber legislation. It has supported those countries should introduce new cyber laws to respond to the rapid-fire change in technology and cybercrime. There should be nonstop exploration and training of IT security help, fiscal service sector help, police officers, prosecutors and the bar to keep them abreast of the evolving technology (Cassim, 2009). The issue of cyber security isn't new but rather has developed further than a half century. The arrest of an East German asset in IBM's German by West Germany's police in 1968 was conceded as the first case of cyber spying (Warner, 2012). 'The thing of cyber security is to enable operations in cyberspace free from the threat of physical or digital detriment' (p. 18). How country perceive the accumulation of interplay within securitization rudiments in cyber security issue and the criterion problem makes their cyber security strategy and policy are different each other. Dewar (2014) uses triptych term to explain three paradigms of cyber security defense, which are Active Cyber Defense (ACD) that focuses on relating and negativing pitfalls and trouble agents both inside and outside the protector's network, Fortified Cyber Defense (FCD) that builds a defensive terrain', and Resilience Cyber Defense (RCD) that focuses on icing system durability'. Study and dissect the loopholes being in the Indian Banking Sector in order to check the fraudulent conditioning and to be suitable to take corrective conduct, thereby enhancing the security measures of this sector (Simran, et.al., 2018). Cybercrime has high eventuality and therefore creates high impact when it's done. It's easy to commit without any physical actuality needed as it's global in nature due to this it has come a challenge and threat to the crime fighter and vice versa (Poonia, 2014).

In 1983, high academy pupil that were inspired by War Games movie and called their characters as 414s had successfully got inside the unclassified military networks (Ibid, p. 787). Ten years ago," the first real war in cyberspace" attacked Estonia and put the country into" a public security situation". Unless the bushwhackers declare they're responsible for the trouble, like Al Qaida in9/11 tragedy, they will remain unknown, as in the case of Estonia (Hansen and Niessenbaum, 2010). People now live in a cyber-world where all data and information would be stored digitally whether it's for business, education, virtually everything that focus on cyber security is constantly on trying to characterize the problem and determine the genuine trouble position. Cyber security is critical to the advancement technology and Internet services. Cyber-attacks will be on the rise in 2021-22 (Perwej, 2017). They examined the different types of cybercrime which persecute the banking sector and the motives of the cyber culprits behind similar acts (Raghavan and Parthiban,

2014). The model is extended with fresh variables, making it suitable for the Internet banking environment. The managing perspective, which is central to the Protection Motivation (Jansen, 2015). The effect of cyber pitfalls in Internet banking services and had strengthened client mindfulness when dealing with Internet banking services (Ali, 2017). Internet banking is getting is decreasingly getting popular because of both convenience and inflexibility (Singhal and Padhmanabhan, 2008).

Currently, the cyber security has been a diurnal issue that can be a plant anywhere, from the news that reports a spam, swindles, frauds, and an identity theft, to academic papers that bandy cyber warfare, a cyber spying, and a cyber defense (Dunn-Cavelty, 2010). The study simply concentrated on the cybercrime and a plant that the cybercrime conditioning will be rising in the forthcoming days and there's no full stop for that (Lakshman, 2019). An exploration composition on Cybercrime in Banking sector suggests that cyber-attacks should be averted by clinging strict compliance of a law (Baksh, 2019). The study stressed the fact that India stands third among top 20 cybercrime victims. In this script, the experimenter attempts to study the cybercrime which has a major impact on a banking sector. The study was made from the standpoint of the Directors and Officers of Banks (Rao, 2019). A study revealed that the main causes or the reasons of cyber-crimes in a banking sector were 1) a capacity to store information in nearly little space 2) Easy to pierce 3) complex 4) the negligence 5) the loss of evidence (Rao, 2019).

There are some major causes of cyber-crimes one must be apprehensive of. According to the study the main causes which lead to cyber-crimes at similar stunning rates are Easy Access to System, Storing Data in a Small Space, Complex Coding, a negligence or an ignorance and a loss of a substantiation (Jyotsana, 2020). The loophole in a banking system which paved the way for a shipbuilder's $ 3 billion dereliction. A study revealed that a lack of regulation, defective lending programs, and a hamstrung fraud monitoring medium are among the factors that have constantly led to cases of a fraud and a rise in nonperforming means (Verma, 2022). An overview of a cyber legislation formulated to address the cybercrime in the United States of America, The United Kingdom, Australia, India, The gulf Countries and South Africa. The study reveals that the incapability of public laws to address the challenges posed by the cybercrime has led to the preface of a technical cyber legislation. It is supported that the countries should introduce new cyber laws to respond to the rapid-fire change in a technology and the cybercrime. There should be a nonstop exploration and training of IT security help, a fiscal service sector help, police officers, prosecutors and the bar to keep them abreast of the evolving a technology (Cassim F., 2009).

Recommendation:

- User data and information must be regularly secured and should be safe backed up.

- Every employee of company should have a separate user account with a policy that stipulates the changing of passwords every month.
- Administrators and bankers must prohibit employees from downloading and installing unauthorized pirated software.
- Bank policies must also set appropriate approval protocols.
- Employees working in a bank's call center must always verify the details of a vendor or a customer who has requested any changes to be made to the billing account.
- Ensure that an advanced level of authentication is required to secure financial transactions.
- Customers must be provided with guidelines for checking the authenticity of any sources that are asking for account details.
- Risk management plans need to be continuously updated by conducting risk assessments and identifying new risks.

Conclusion:

The rapid-fire growth of a technology requires banks to review their programs and make their system stronger. Banks can be apprehensive guests through their websites about banking frauds and what measures should be taken to help these crimes. Banks ought to have a review a premonitory group to regulate the false and a fraud conditioning in banks. They should take sufficient measures to combat these crimes and hire workers with a strong IT background with proper training, a skill and streamlined knowledge. Together, banks and guests win the race for a better hereafter.

References:

1. Ajeet Singh Poonia (2014), Cybercrime, challenges and its classification, International journal of Emerging Trends and Technology in Computer Science, 3(6).120-127.
2. Ali, L., Ali, F., Surendran, P. and Thomas, B., 2017. The effects of cyber threats on customer's behaviour in e-Banking services. International Journal of e-Education, e-Business, e-Management and e-Learning, 7 (1), 70-78.
3. A.R. Raghavan and Latha Parthiban (2014), The effect of cybercrime on a Bank's finances, 2 (2), 173-178.
4. Cassim F. (2009) In the article "Formulating specialized legislation to address the growing specter of cybercrime: A comparative study".
5. Claessens, J., Dem, V., De Cock, D., Preneel, B. and Vandewalle, J., 2002. On the Security of Today's Online Electronic Banking Systems. Computers & Security, 21 (3), Moore, T., Clayton, R. and Anderson, R., 2009. The Economics of Online Crime. Journal of Economic Perspectives, 23 (3), 3-20.
6. Dewar, R. 2014. 'the Triptych of Cyber Security: A Classification of Active Cyber Defense'.

6th International Conference on Cyber Security.

7. Divya Singhal and V. Padhmanabhan (2008), A Study on Customer Perception towards Internet Banking: Identifying Major Contributing Factor, 5 (1).
8. Dunn-Cavelty, M. 2010. 'Cyber Security' in A. Collins, Contemporary Security Studies. Oxford: OUP. Dunn-Cavelty, M. 2013. From Cyber-Bombs to Political fallout: threat representations with an impact in Cyber-Security Discourse. International Studies Review, 15, pp. 105-122.
9. Hansen, L. and Niessanbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, pp. 1155-1175.
10. Jansson, K. & VonSolms, R. (2013), Phishing for phishing awareness. Behavior & Information Technology, 32(6), 584–593.
11. Liaqat Ali, Faisal Ali, Priyanka Surendran, Bindhya Thomas (2017), The effects of cyber threats on consumer behavior and e-banking services,7(5), 70-76. [2].
12. Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru, (2018), Cybercrime: A Growing threats to Indian banking sector, 5 (1), 926-933. [4] Siaw I, Yu A (2004).
13. Warner, M. 2012. Cybersecurity: A Pre-history. Intelligence and National Security, 27 (5), pp. 781-799.
14. Yusuf Perwej, "An Experiential Study of the Big Data", International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Science and Education Publishing, Volume 4, No. 1, Pages 14-25, 2017.