PHISHING AND VISHING ATTACKS: AN EMERGING PITFALL OF FINTECH WORLD

Arkajit Debnath, Research Scholar, ICFAI University Tripura

Dr. Raghunath Chakraborty, Assistant Professor, ICFAI University Tripura

ABSTRACT

The technological advancement within financial sectors boosts the digital economy through launching various apps. Government of India acts as an additional actor by virtue of the accessibility of government schemes digitally. Everything seems polished until phishing and vishing attacks ruin the very purpose of technological benefits. This paper will articulate the growing phishing and vishing attacks in India and its prominent impact on the financial ecosystem. This Paper also highlights the major incidents of phishing and vishing attacks along with the relevant reports to unfold it further. Lastly the paper will suggest some welfare steps that can be taken in this regard.

Keywords: Phishing, Vishing, Fintech, Financial Ecosystem, Bank Sectors

Introduction

Technology serves as a tool to emancipate the efficacy and convenience of an individual. The technological advancements are gaining its dominance and transcends in various facets of daily life. Financial dependency is not an exception of it because of the fact that the financial technology has revolutionized the way Financial Services are delivered and accessed all over the globe providing convenience and efficiency to users worldwide. [1]The accessibility of such efficient modes of technology also introduced new avenues for cyber threats and attacks within the financial ecosystem[2]. Fintech refers to the technological advancements which are directly being channelized in the form of software or applications playing a key role in the financial management of either a customer or even a bank. The Fintech Scenario is widespread in India to such an extent that the giant fintech apps like Google Pay; Phonepe amongst other has already targeted the small scale vendors like vegetable sellers, fruit sellers, fish sellers and even the street vendors. Fin-tech is growing to become the new norm and has almost integrated all modes of Financial Transaction and services. The vital factor behind this magnanimous growth of fintech giants are the accessibility and convenience of its users but the convergence of technological tools into a serious menace takes place when the innocent users lose their valuable money because of phishing and vishing. The Phishing and Vishing techniques are used to obtain the valuable information of the customer and once they obtain the information they use it gain unauthorized access to bank accounts or identity of anyone else.[3] These techniques have certain level of sophistication with regard to posing and targeting significant challenges to the security of financial institutions and their customers. [4] The modus-operandi of the attack is crafted with such finesse that the identification of deceit is rarely feasible. The APWG Report, quarter 3 of 2023 pivots the fact that Phishing is gradually grasping its roots and the financial institutions are most attacked victims among all other heads. The rising number of phishing and vishing attacks in India when read with the APWG report can be assessed that Indian Financial Ecosystem has a grievous threat owing to the growing Phishing

[1] Arner,D.W.,Barberis, J.N.,& Buckley, R.P.(2015). The Evolution of Fintech: A New Post Crisi Paradigm? Georgetown Journal of International Law, 47(4), 1271-1319.
[2] Choo, K.K.R. (2011). Cybercrime and Cyberterrorism: Current Issues. Hershey, PA: Information Science and Reference
[3] Barman, S., Pal, U., Sarfaraj, M A., Biswas, B., Mahata, A., & Mandal, P. (2016, January 1). A complete literature review on financial fraud detection applying data mining techniques. https://doi.org/10.1504/ijtmcc.2016.084561
[4] Yar,M. (2013) . Cybercrime and Society. London, UK: SAGE Publications.

and Vishing attacks in India.

Interplay of phishing and Vishing mechanism: Targeting Bank Consumers

Phishing Attacks in Financial Sector include Deceptive communication in a professional manner to access the unauthorized information of an individual. The communication is executed using deceptive e-mails, websites, links, tricks which induce the individual in such manner leading to unauthorized access to restricted information with sophistication. The traps are well tailored creating a persona of the legitimate banking or financial institution building a sense of trust among the individuals and urgency to act promptly. Vishing attacks on the other hand are differentiated with Phishing on the basis of their Modus-Operandi. The Vishing attacks are executed using voice calls or video calls which escalate the fraud to a step further making a direct communication with the consumers enticing them using social engineering methodologies convincing their authenticity and to ultimately extort or fraud the consumer. Phishing and Vishing have turned out to be a large scale organized crime which functions in a systematic manner in order to target and commence the fraud. The phishing and Vishing groups are so well organized that they maintain hi-tech organized offices from where they function under the radar of the authorities in the name of call centers or technical support services. The digitization of the financial sector in India starting with Pradhan Mantri Jana Dhan Yojana, promoting the proper utilization of the wealth of the citizen by channeling through a Bank account and co-relating the same with the Digital India Initiative, whereby all the citizens were encouraged to use digital payments established the fact that the financial economy has driven towards the digital economy till such depth, that a minor error in the handling of a PIN code can be lethal to an individual's life earned assets. The financial ecosystem in India is growing internationally, and the recent advancements in digital infrastructure are leading to a digitally reliant economic structure. In order to protect the banking sector from the threats of phishing and vishing, it is crucial to establish a proactive cyber security mechanism.

Phishing and Vishing attacks in the Financial Ecosystem

The Financial Ecosystem refers to the flow of money and other financial instruments via mediums like banks, investors, financial markets and other technology providers. The banking sector faces numerous attacks compromising the online banking security most of which

comprise of Phishing and Vishing attacks.[5] The major reason for the drastic growth in the magnitude of the offence lies within the modus-operandi, the use of manipulation techniques in phishing attacks is particularly concerning for the consumers in the banking sector. The cybercriminals use elements like fear, urgency, curiosity and lack of awareness in order to assess the psychological trigger of the consumer and accordingly engineer the attack. Phishing and Vishing attacks not only result in cash losses but also raise concerns about trust within the cash Ecosystem.[6] The presence of such a virus within the body of Finance is affects the overall stability of the system at a large scale. The modern financial system is totally dependent on the data of the various sectors involved, it will not be wrong if stated that data is the most valued commodity in the present time and the attacks are taking place with a core reason of data misappropriation. The exponential growth in the Digital transactions and the proliferation of the online financial services have fundamentally altered the landscape of financial activities in such a manner that, the digitization has increased the convenience for the customers meanwhile, the interconnected nature of the digital financial markets has made them more susceptible to sophisticated exploitation.[7] The APWG report for the 3rd quarter of 2022 clearly states that phishing attacks are at an All-Time High and the Financial Sectors are most vulnerable to this growth since the rise in technology within the ecosystem is creating more room for the cyber criminals to act with versatility.[8]

Major Incidents depicting the Modus Operandi of Phishing and Vishing

Phishing and Vishing are particularly insidious forms of cybercrime which have significant impact on the Fintech and Banking Sector. Phishing is the fraudulent attempt to obtain sensitive data such as usernames, passwords and credit card details by masquerading as a trustworthy entity in the digital communication, whereas vishing is a similar form of cybercrime that uses voice communication to deceive individuals into revealing personal and financial information. Research conducted by the Data Security Council of India revealed a significant surge of around 72% in phishing attempts targeting the Indian Banking Sector. The profound impact of

[5] Tawar, K. (2020, November 30). Laws Relating to Phishing Scams (IT Act 2000): A Socio-Legal Analysis
[6] Before calling customer care numbers think twice - The Hindu. (2020, September 4). https://www.thehindu.com/news/national/tamil-nadu/before-calling-customer-care-numbers-think-twice/article32523140.ece
[7] Barman, S., Pal, U., Sarfaraj, M A., Biswas, B., Mahata, A., & Mandal, P. (2016, January 1). A complete literature review on financial fraud detection applying data mining techniques. https://doi.org/10.1504/ijtmcc.2016.084561
[8] APWG World Phishing Report 2022, 4th quarter 2022.

these attacks on the banking industry may be further elucidated by examining the challenges that the sector has encountered in recent years.

In 2020 citibank experienced a phishing attack where the criminals posed as legitimate representatives of the bank and sent a fraudulent mail to the customers requesting sensitive information using social engineering techniques stating that some data might be lost and the customers were requested to verify their cards by clicking on a link.[9] In 2021, a phishing incident targeted the Wells Fargo customers by faking their website making the customers believe that they were interacting with the legitimate financial institution, later the bank took action to shut the website down and comprehensive action to improve security. [10] The threat of Phishing and Vishing is more active in India, in 2019, the cyber criminals forged SBI Webpages' to trick customers divulging their details which led to financial loss of several customers. This incident contributed in the extensive awareness campaigns by the banks.[11] A similar incident happened in 2020 with one of the largest private bank of India i.e. ICICI bank creating counterfeit websites resembling the original one taking credentials of several customers.[12] These incidents when analyzed with a common filter deduces the fact that the phishing attacks are at a rise not only in India but also at a global level and such a growth could be catastrophic if not mitigated through proper means.[13]

Phishing and vishing are using social engineering methodologies which directly play with the vulnerabilities of the customers in the form of fear, curiosity etc. it is being observed that the vulnerability of the customers are contributing to the vulnerability of the institutions at large. The institutions are trying to change the ratio of vulnerability through awareness. The awareness campaigns are mandatory but simultaneously the reach of such campaigns are also a matter of question. The Financial Ecosystem is at a risk and the only remedy to such risk is the proactive approach of the institutions along with the state in order to mitigate the threat permanently because this evil is in the form of a hydra, where severance of a head is the birth of a new.

[9] Cybersecurity News, "Major Phishing Attack Targets Citibank Customers," April 2020
[10] Banking Security Journal, "Wells Fargo Customers Beware: Phishing Scam Alert," July 2021
[11] "SBI Reports Phishing Scam: Customers Warned Against Unauthorized Emails," October 2019
[12] Business Standard, "ICICI Bank Customers Targeted in Sophisticated Phishing Fraud," February 2020
[13] Bose, I., & Leung, A C M. (2007, January 1). Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities. https://doi.org/10.17705/1cais.01924

Concluding Remarks:

The Financial Institutions must stay in synchronization with the advancements in cyber security to effectively combat phishing and vishing. The escalating threat to the banking sector is a matter of grave concern for the financial economy at large since the digitization of the banks has resulted in a global cashless trading scenario.[14] The recent attacks on the banking sector establishes the fact that the functioning cyber security mechanism is not adequate enough to protect the digital consumer-base completely and thus a robust mitigation technique is the hourly need for a full proof financial ecosystem.

The financial institutions need to invest in advanced email facilities that can accurately detect and flag phishing spam mails and also monitor the internet for potential harmful sites[15] which would regularly update the database with suspicious activities in order to assess further threats. The Financial Institutions should also foster the culture for cyber education among the customers as well as the employees in order to provide a secure environment for the financial flow. The fintech companies must collaborate and aim for adopting a multi-layered approach which encompasses robust technology, ongoing education and proactive response plans in order to fight a common evil.[16] The cross-industry collaboration would aid in the collective information sharing against financial frauds in the digital realm. The integration of cutting-edge technological advancements like block-chain technology and the bio-metric authentication holds a lot of potential in order to fortify the financial ecosystem from within.[17] The banks and the fintech companies need to assess the human resources in order to implement a separate wing for the combat of phishing and vishing attacks within the company to ensure swift reaction against the offence. The absence of synchronization between the financial institutions and the technical advancements within the cyber crime scenario is directly affecting the financial ecosystem at large bringing a sense of distrust and incompetency for then institutions among the consumers. The recent attacks in the banking sector and several scams

[14] Canfield, C., Fischhoff, B., & Davis, A. (2016, September 27). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. Human Factors, 58(8), 1158-1172. https://doi.org/https://doi.org/10.1177/0018720816665025

[15] Gupta, B B., Tewari, A., Jain, A K., & Agrawal, D P. (2016, March 17). Fighting against phishing attacks: state of the art and future challenges. https://doi.org/10.1007/s00521-016-2275-y

[16] Jeyanthi, P., Mansurali, A., Harish, V., & Krishnaveni, V. (2020, February 1). SIGNIFICANCE OF FRAUD ANALYTICS IN INDIAN BANKING SECTORS. Journal of critical reviews, 7(04). https://doi.org/10.31838/jcr.07.04.38

[17] V.S, A., & Sreelakshmi, D. (2020, November 1). A DESCRIPTIVE STUDY ON THE FINANCIAL FRAUD MANAGEMENT AND RISING FINANCIAL FLOWS IN INDIA. https://doi.org/10.33564/ijeast.2020.v05i07.023

which come across the cyberspace relating to QR code scans and ATM skimming, vishing are all facets of a rooted crime called phishing which has disrupted the flow of financial sector globally as well as in India.