International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No.42, December 2023 – www.ijais.org

Safeguarding FinTech: Elevating Employee Cybersecurity Awareness in Financial Sector

Sivaraju Kuraku, PhD
University of the Cumberlands
School of Computer and Information Sciences
Williamsburg, KY, USA

Dinesh Kalla
Colorado Technical University
Department of Computer Science and Doctoral Studies
Colorado Springs, CO, USA

Nathan Smith
Colorado Technical University
Department of Computer Science and Doctoral Studies
Colorado Springs, CO, USA

Fnu Samaah
Harrisburg University
Department of Science and Technology
Harrisburg, PA, USA

ABSTRACT
The financial sector faces a significant threat from phishing attacks that strike them and result in financial loss, illegal access to customers' sensitive information, and damage to the financial institution's reputation. Hackers utilize phishing attacks to lure employees in financial institutions into giving sensitive financial information and customer data so that they can breach the institution's security. While financial institutions have built safety protocols both in their customer-facing and internal banking apps and websites, employees' human element fails to identify phishers scams, thus resulting in the theft of financial information, customer data, and small and large sums of money. This study focuses on addressing the importance of raising employees' levels of cybersecurity awareness to detect and stop phishing attacks. The study also sheds light on how financial institutions can reinforce their entire security posture as well as mitigate financial losses and risks resulting from data breaches by enhancing employees understanding and knowledge of phishing countermeasures, simulation, indicators, and techniques.

General Terms
Cybersecurity Awareness, Phishing Attacks, Data Security, Cyber Threats, Spear-Phishing and Financial Industry

Keywords
Financial sector, phishing attacks, financial loss, sensitive information, financial institutions, reputation, cybersecurity awareness, security posture, data breaches, phishing simulation.

1. INTRODUCTION
In the current digital age, the advancement of technology has digitally transformed the financial sector, providing accessibility, efficiency, and convenience to customers throughout the world. Nonetheless, the revolution has also brought new challenges, mainly the increasing cybercrime threats and attacks, with the most predominant and damaging ones facing financial institutions being phishing and spear-phishing attacks. Financial institutions in this study entail traditional banks offering savings and checking accounts, credit cards like MasterCard and Visa, payment processing corporations such as Paypal, as well as web e-tailers like eBay, Apple, or Amazon. It is worth noting that phishing attacks entail the use of deceiving methods to trick people into revealing valuable sensitive information like financial data, personal details, or login credentials [1]. Spear-phishing involves precise and targeted endeavors to steal sensitive information like financial credentials or account credentials from a particular victim, mainly for malevolent reasons [2]. Employees in financial institutions play a vital role in protecting customers data and information and safeguarding their financial institution's integrity [3]. In regard to security, they play the role of being the first institution's defense against phishing attempts and attacks. Below figure shows the share of financial phishing attacks worldwide from year 2016 to 2022.

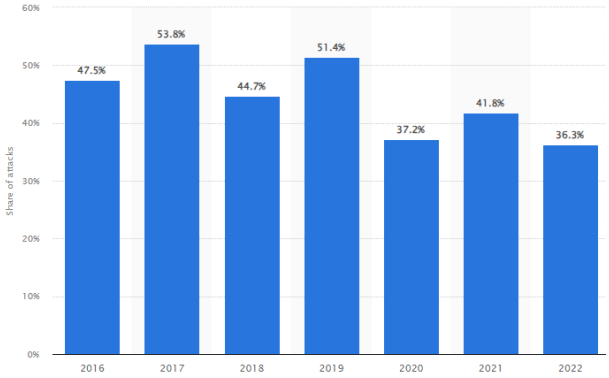

Fig 1: Share of Financial Sector Phishing Attacks from 2016 to 2022 (Statista 2023 Report)

Nonetheless, despite financial institutions deploying sophisticated cybersecurity safeguards, employees continue to face phishing attacks, repeatedly taking advantage of their human element. Research shows that the increasing number of phishing attacks occur because of workers' lack of cybersecurity awareness and readiness to recognize and stop them [4]. This research focuses on addressing the importance of raising employee's levels of cybersecurity awareness to detect and stop phishing attacks. Through enhancing employees understanding and knowledge of phishing countermeasures, indicators, and techniques, financial institutions can reinforce their entire security posture as well as mitigate financial losses and risks resulting from data breaches. Due to significant increase in phishing email organizations are using Machine Learning models to detect them and filter them [5].

2. BACKGROUND
Financial institutions have been faced with the significant cyber threat of phishing attacks that bring extensive risks, such as compromised security of personal data, financial losses, and

reputational damage, to customers, employees, and institutions themselves. Financial institutions have been prime targets of phishers for a long time because of the enormous amount of valuable data that they retain. Below figure shows financial sector is most targeted industry from the attackers

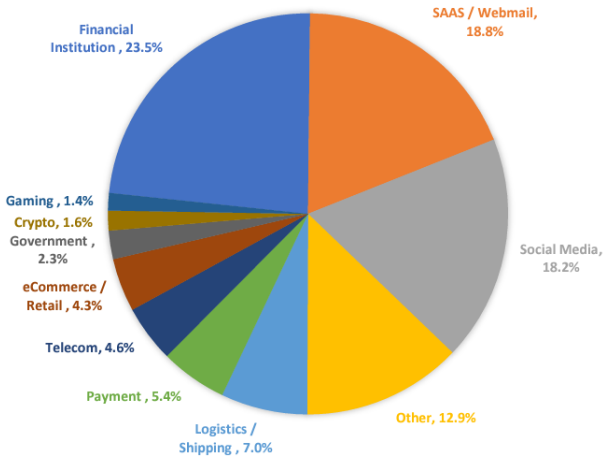

Fig 2: Phishing Attack Percentage vs Industry Targeted (APWG 2023 Report)

Attackers typically execute phishing attacks on financial institutions through malicious attachments, fake websites, or fraudulent emails that seem to appear genuine, leading victims to reveal their private information [6]. Once phishers obtain their targeted data, they exploit it to conduct financial fraud, illegal access to individuals accounts, and identity theft. Phishers continue to increasingly sophisticate their phishing attacks on financial institutions, employing advanced social engineering methods like spear-phishing to effectively reach their targeted victims and exploit susceptibilities in financial corporation's security systems [7]. Cybercriminals even go a step further and leverage existing events, like financial crises or data breaches, to invent a sense that the victims will feel urgent in order to manipulate them into taking hasty actions. Precisely, the collapse of Silicon Valley Bank necessitated depositors to rush and withdraw their deposits amounting to billions of dollars, thus bringing attention to the crisis to hackers who made numerous phishing campaigns impersonating the bank [8]. Fundamentally, various aspects contribute to employees in financial institutions falling victim to phishing attacks. The first one is that attackers keep evolving their phishing tactics and disguise them as genuine correspondence, thus making it difficult for employees to detect and prevent phishing and spear-phishing attacks. Equally, the fast-moving nature of financial operations makes staff overlook possible red flags, like unusual requests or distrustful email addresses. Additionally, cybercriminals take advantage of employee's human factors, like fear, urgency, or curiosity, to manipulate them into executing functions that compromise their entity's security. Research also states employees with more browsing hours are more prone to phishing attacks [9].

3. PROBLEM STATEMENT

The financial sector is a major target for hackers utilizing phishing attacks to lure employees in financial institutions into giving them sensitive financial information and customer data so that they can breach the institution's security. While financial institutions have built safety protocols both in their customer-facing and internal banking apps and websites, employees human element fails to identify phishers scams, thus resulting in the theft of financial information, customer data, and small and large sums of money. According to Kuraku et al. (2022), phishing attacks in financial institutions, which are executed by phishers through persuasive methods of enticing employees to click on phishing emails, result in huge losses. In 2021, the monetary costs of phishing attacks on US organizations increased to 14.8 million dollars from 3.8 million dollars that were recorded in 2015, with large US corporations losing 1500 dollars per worker and 14.8 million yearly. With the many phishing emails that phishers send every day, almost half impersonate or target financial institutions. Despite financial institutions using spam filters to detect almost 99 percent of phishing attacks, cleverer phishing iterations leverage the human element of financial institution workers, thus making them a weaker link between phishers and their institutions.

4. SIGNIFICANCE OF THE STUDY

The study on enhancing the level of cybersecurity awareness among financial institution employees can help them identify and stop phishing attacks because it offers wide-ranging training and education on detecting the suspicious activities of phishers and the techniques and signs used in spear-phishing attacks. By educating staff on phishing attacks, financial institutions can foster vigilance in identifying deceitful phone calls, fake websites, and phishing emails [10]. This increases the awareness of employees to report and promptly respond to cyber threats, thus preventing possible security breaches. Secondly, the study can help to cultivate a security culture in financial institutions as employees can swiftly adhere to security best practices and protocols by understanding the importance of being cautious and the impacts of their security actions, such as verifying the genuineness of inquiries involving sensitive information, downloading attachments, exercising caution while browsing sites and clicking links, and updating their passwords on a regular basis. Through cultivating a security-conscious culture and mindset, financial institutions can develop strong defense systems that safeguard their customer data and services from phishing attacks [11]. Thirdly, this study sheds lighter on human susceptibilities, like fear, urgency, curiosity, and social engineering manipulations that attackers employ on employees, thus educating them on these psychological methods and enabling financial institutions to empower their workers to not only recognize but also resist those manipulations. This study can help financial institutions devise novel ways of reinforcing workers knowledge of phishing attacks, like simulating spear-phishing exercises through training sessions, to enable them to be proactive towards cybersecurity.

5. LITERATURE REVIEW

Research posit that a lack of user education and first-hand phishing tests makes employees in the financial sector easily fall for phishing and spear-phishing attacks [12]. The financial sector, which is highly targeted by attackers, can be secured from phishing attacks through financial institutions using the transfer of cybersecurity knowledge and cyber drills to improve cybersecurity awareness among employees in the sector [12]. The transfer of cybersecurity knowledge described entails conducting frequent cybersecurity training to educate workers on numerous kinds of phishing attacks, their impacts on the business, the need to maintain good security practices, and offering real-life descriptions of phishing messages and emails and how to identify them.

Equally, the cyber drills described by the authors involve conducting simulated phishing exercises to gauge the ability of employees to recognize and report scams. Phishing simulations coupled with the transfer of cybersecurity knowledge can effectively raise the worker's level of cybersecurity awareness, thus reducing cyber threats and risks and enabling employees to report phishing attempts while timely responding to them.

The professional role of employees in the banking sector can highly determine the success or failure of phishers tailored campaigns [13]. Also research posit that employees lacking knowledge of an organization's internal processes can be taken advantage of by phishers to develop credible pretexts as well as get a foothold in the institution, such as by executing lateral spear-phishing attacks [13]. The authors stress that junior employees can be most susceptible to adequately tailored attacks impersonating institutional settings. Burda et al. (2020) further add that newly hired employees in senior proficient roles can be highly vulnerable to phishers tailored campaigns due to their unfamiliarity with their newly introduced roles. Therefore, specific cybersecurity training directed towards these vulnerable people, like detection of URL phishing, can help reduce their vulnerability to phishing attacks.

6. METHODOLOGY

The study obtained approval to utilize an online phishing IQ test from the President of PhishingBox. The Phishing IQ test is a tool designed to assess an individual's ability to identify and respond to phishing attempts effectively. The approval from PhishingBox's president signifies a collaboration or endorsement, indicating that the test aligns with the study's objectives and standards. Below flowchart shows different stages of the survey research from developing the survey to data analysis stages.

Fig 3: Survey Implementation and Methodology

The research study methodology employed PhishingBox's online phishing IQ test to evaluate individuals' capacity for detecting and preventing phishing attempts. The online phishing IQ test is accessible at https://www.phishingbox.com/phishing-iq-test.

The president of PhishingBox's approved the use of this test for research purposes. The study targeted professionals within the finance sector, recognizing the sector's unique susceptibility to phishing attacks. The study surveyed 100 individuals from the financial sector to participate in the phishing test. Participants taking the online test undergo fake phishing scenarios to assess their ability to identify and effectively respond to such attempts.

Participants received the phishing IQ test link to assess their ability to identify and effectively respond to fake phishing scenarios. Participants in the test went through ten simulated phishing situations over the course of about 15 minutes. At the end of the test, each individual got a score between 0 and 100 that showed how well they could spot phishing attempts. The goal was to assess and analyze participants' cognitive skills, with a specific focus on their ability to recognize and effectively respond to phishing attempts. Following the completion of the phishing test, the collected data underwent a rigorous analysis process.

The data obtained through this methodology provided valuable input on the susceptibility of the finance sector to phishing attacks. It helped identify areas where further staff training may be beneficial to improve the cybersecurity awareness and preparedness of the industry. The detailed analysis also informed recommendations on how to tailor awareness initiatives and training programs based on user demographics to enhance cybersecurity training and defense.

7. RESULTS

The data represents phishing identification scores for 100 individuals who were tested on their ability to recognize phishing emails. There are numbers in the whole range, from 20 to 100, showing that people in the group have a wide range of skill levels. Let's take a look at how the scores are spread out.

Examining the distribution of scores:

26 of the 100 people who took the test (26%) got a score in the bottom quartile, which is between 20 and 49. This shows that over a quarter of those tested had major knowledge gaps and had a hard time spotting common scams. A lot of people got scores between 20 and 29, which is an extremely low range. This means they don't know basic things that can help them spot malicious emails

46% of the people who took the test (46 people) got a score in the middle, between 50 and 79. A lot of people are pretty good at finding suspicious emails, but they could use some extra training to get closer to advanced levels. One strength that individuals can utilize is their ability to identify obvious signs, such as spelling mistakes. However, there are probably holes in the ability to spot more complex phishing schemes.

Of the 100 people who took the test, 28 (28%) got high scores, ranging from 80 to 100. Notable are the many instances of nearly perfect scores in the 90 to 100 range, which show examples of strong mastery in the tested group that could serve as models and help raise the rest. However, it's not clear if these top scores really show the highest levels of skill without knowing more about how hard the test was.

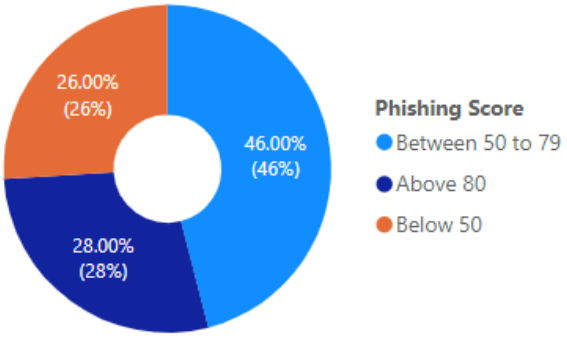

Fig 4: Phishing Score Vs Participant Percentage

Additional observations:

In addition. Low numbers, particularly those between 20 and 30, reveal weak spots that require immediate fixing. They might not be able to spot emails that are fraudulent because they aren't aware of them or haven't had enough training

"Significant variation" means that low and high scorers probably had very different experiences with the same phishing emails. In real life, this could mean that different people in the same company respond and report in very different ways.

People who regularly experience extreme highs and lows of 80+ or below 50 can see some signs of stability. This points to deeply rooted habits, both good and bad. Training that is specific to the level could help fill in gaps or make the most of skills.

In summary, a scary number of people are struggling very badly, while a fair middle group has average skills and a small but promising group is doing really well. Peer mentoring and targeted training, tailored to the level, could enhance general skills. However, addressing low scores promptly is crucial to preventing adverse consequences associated with phishing risks. Regular assessments and continuous training may help improve overall phishing identification skills across the group.

8. DISCUSSION

The study results highlight the importance of ongoing training and awareness programs to enhance people's ability to identify phishing emails. Individuals with lower scores could benefit from targeted education and simulations to improve their skills. The wide range of scores may reflect individual differences in factors such as cybersecurity knowledge, experience, and cognitive abilities. Customized training programs that consider individual strengths and weaknesses might be more effective. Given the dynamic nature of phishing techniques, continuous assessment and training are crucial to keep individuals up-to-date with the latest tactics employed by malicious actors. The variation in scores emphasizes the importance of continuous awareness programs to keep individuals updated on evolving phishing tactics. A holistic approach that includes both initial training and ongoing awareness initiatives is crucial to fostering a well-prepared community against phishing threats.

Financial institutions can effectively stop phishing attacks targeting their employees by training their staff on proper organizational security protocols to raise their security IQ through Phishing scam security education and awareness and phishing simulation. However, financial institutions can design their phishing tests in a manner that redirects unsuspecting employees who click on phishing test links to a secure web program that educates them on their mistakes. Financial institutions can customize various email templates for use to bait employees, such as emails that mimic security notices, personal messages, or corporate communications, and send them to raise cybersecurity awareness in the organizations on a regular basis.

9. CONCLUSION

The phishing identification scores indicate a varied level of proficiency among individuals. While some are adept at recognizing phishing emails, others may need additional support and training. A holistic approach to cybersecurity education, tailored to individual needs, is crucial for improving overall resilience against phishing attacks. Continuous assessment and adaptation of training programs are key to ensuring that individuals stay informed about evolving phishing tactics. Given the dynamic nature of cyber threats, regular assessments and updates to training are essential to ensure preparedness against new and evolving phishing techniques.In summary, the scores reveal a spectrum of phishing identification skills among individuals, highlighting the need for a multifaceted and adaptive approach to training and awareness for effective cybersecurity. In the financial Sector, raising employees' level of cybersecurity awareness is important for recognizing, detecting, and stopping spear-phishing and phishing attacks. Through equipping workers with the knowledge and understanding of phishing attacks and techniques, training them on the identification of social engineering attacks and tactics, building a security-focused mindset, and simulating phishing attacks to raise cybersecurity awareness, financial institutions can build a robust defense against social engineering attacks and cyber threats in general. It is important to note that investing in security education and raising cybersecurity awareness protects the reputation and assets of financial institutions and guarantees the security of the sensitive information of their customers. Therefore, vigilant and educated personnel are a valuable asset in safeguarding financial institutions from phishing attacks in this constantly developing digital landscape.

10. ACKNOWLEDGMENTS

We researchers would like to thank PhishingBox's president for providing tools to conduct extensive research related to phishing emails. We want to express our sincere appreciation University of the Cumberlands, Colorado Technical University and Harrisburg University faculty members for providing guidance in research and writing papers. We also thank the anonymous referee, reviewers, and editors for reviewing our paper. Finally, we sincerely thank the International Journal of Applied Information System for allowing us to publish the paper.

11. REFERENCES

[1] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

[2] Baig, M. S., Ahmed, F., & Memon, A. M. (2021). Spear-phishing campaigns: Link vulnerability leads to phishing attacks, spear-phishing electronic/UAV communication-scam targeted. *2021 4th International Conference on Computing & Information Sciences (ICCIS)*. https://doi.org/10.1109/iccis54243.2021.9676394

[3] Johan, S., & Ariawan, A. (2022). Correlation financial institutions, customers and employees per labour law. *Arena Hukum*, *15*(1), 38-58. https://doi.org/10.21776/ub.arenahukum.2022.01501.3

[4] Kuraku, S. (2022). Curiosity Clicks: The Need for Security Awareness (Doctoral dissertation, University of the Cumberlands).

[5] Kalla, D., Samaah, F., Kuraku, S. & Smith, N. Phishing Detection Implementation Using Databricks and Artificial Intelligence. SSRN Electronic Journal 185, doi: 10.2139/ssrn.4452780 (2023).

[6] Jain, A. K., & Gupta, B. (2021). A survey of phishing attack techniques, defense mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527-

565. https://doi.org/10.1080/17517575.2021.1896786

[7] Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, *128*,103158. https://doi.org/10.1016/j.cose.2023.103158

[8] Radanliev, P. (2023). Review and comparison of US, EU, and UK regulations on cyber risk/Security of the current blockchain technologies: Viewpoint from 2023. *The Review of Socionetwork Strategies*. https://doi.org/10.1007/s12626-023-00139-x

[9] Kuraku, S., & Kalla, D. (2023). Impact of phishing on users with different online browsing hours and spending habits. *International Journal of Advanced Research in Computer and Communication Engineering*, *12*(10), 34–41. https://doi.org/10.17148/IJARCCE.2023.121005.

[10] Alabdan, R. (2020). undefined. *Future Internet*, *12*(10), 168. https://doi.org/10.3390/fi12100168

[11] Anderson, R. (2020). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons.https://cdimage.debian.org/mirror/archive/ftp.sunet.se/pub/security/docs/crypt/Ross_Anderson/toc.pdf

[12] Chatchalermpun, S., & Daengsi, T. (2021). Improving cybersecurity awareness using phishing attack simulation. *IOP Conference Series: Materials Science and Engineering*, *1088*(1),012015. https://doi.org/10.1088/1757-899x/1088/1/012015.

[13] Burda, P., Chotza, T., Allodi, L., & Zannone, N. (2020). Testing the effectiveness of tailored phishing techniques in industry and academia. *Proceedings of the 15th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3407023.3409178