Volume 9, Issue 12, December – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14610632

The Psychology of Phishing: Why Users Fall Victim to Deceptive Emails

[1]Freyha A. Bahari; [2]Tadzmera A. Daud; [3]Mhesi D. Arabbi; [4]Noralyn I. Jalah; [5]Nuralyn O. Adjid; [6]Fatmahal Abah; [7]Sitti Aiman A. Amiddin; [8]Ayang A. Ibno; [9]Alsanoh S. Abduhail; [10]Masukud Ajijul; [11]Riza M. Sali; [12]Shernahar K. Tahil
[1] BSIT Student, College of Computer Studies, Mindanao State University – Sulu, Phillipines
[2]Faculty, College of Computer Studies, Mindanao State University – Sulu, Philippines

Abstract:- Phishing emails are type of Social Engineering attacks which are currently among the most widespread cybersecurity threat due to their impact on human psychology. These attacks aim to gain sensitive information from the user such as passwords, banking details, or personal information. This research aims at identifying the psychological factors that make users vulnerable to phishing including, manipulation of trust and credibility, cognitive biases and heuristics, emotional triggers, social proof, and scarcity. Through the evaluation of these factors, this paper offers information on how phishing schemes exploits authority, self-control bias, and scarcity. Based on the findings of the present research, it concerns the increased user awareness and the developing tools to prepare individuals to stand against any phishing attacks. This study contributes to the understanding on how and why phishing occurs, as well as it offers suggestions for addressing the problem.

Keywords:- *Susceptibility, Psychological Vulnerabilities, Phishing, Heuristics.*

I. INTRODUCTION

Phishing attacks refers to the deceptive effort to acquire confidential information by presenting oneself as a reliable source in online communication (Desolda et al., 2022). Phishing is a popular and most dangerous type of threat that the cybercriminals actively use on the internet platforms in which cyber criminals lure their targets into providing their details, possibly through the use of malware or tricking them into disclosing their requisite information (Gupta et al., 2017). Several studies have suggested that factors including age, gender, internet addiction, user stress, and many other determinants contribute to susceptibility to phishing (Alkhalil et al.,2021). In simplest form, phishing attacks refers to the deceptive efforts to acquire confidential information by presenting oneself as reliable source in online communication (Desolda et al., 2022). Despite how convincing phishing email by using latest technology to appear professional, cybercriminals will exploit humans' common psychological tendencies by targeting how people think, feel, and make decisions manipulating their psychological triggers based from trust, urgency, or feelings to fall victim to their deceptive scam.

This persuasive form of cybercrime that have been significantly changed from basic technical methods to advanced strategies that manipulate human psychology over time. Cybercriminals create deceptive emails that take advantage of human psychological vulnerabilities; therefore, it is essential to grasp the psychological factors that contribute to this susceptibility. Phishing e-mails is among the biggest dangers to cybersecurity (McAlaney & Hills, 2020). Phony e-mails or the phishing e-mails are emails that sent by cybercriminals who is determined to lure the recipients of the e-mail into providing certain information like passwords, banking details, credit card information, and other sensitive personal information. Such messages often look like they were sent by a familiar brand, such as bank or an internet shop; they lead to bogus website or a virus.

II. MANIPULATION OF TRUST AND CREDIBILITY

Scammers frequently take advantage of individuals' trust by masquerading as legitimate organizations, such as banks, government bodies, or well-known companies, in order to deceive people into accessing harmful content. This strategy referred to as manipulation of trust and credibility, leverages the inherent tendency of users to trust established and reputable sources.

A research study conducted by Butavicius et al. (2016) explored how social engineering tactics affect users' perceptions of the safety of clicking links in emails. The investigation centered on three principles: authority, scarcity, and social proof, which were applied to authentic phishing, and spear – phishing emails. The results indicated that utilizing authority was the most potent strategy in persuading users that a link in an email was trustworthy. Participants found it challenging to differentiate between genuine and spear – phishing emails, especially when authority indicators were included. Moreover, individuals who exhibited lower impulsivity in their decision – making were less prone to consider fraudulent emails as safe, implying that impulsivity influences vulnerability to authority – driven phishing schemes.

In similar research conducted by Diaz et al., (2018) examined the vulnerability of users to phishing attacks within a university context. The findings revealed that people frequently struggled to differentiate between authentic and spear – phishing emails, particularly when these messages included cues of authority. This struggle was linked to the persuasive nature phishing attempts that leverage authority, preying on users' tendency to comply

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14610632

with request from they perceive as authoritative figures.

The findings highlight the potential impact of phishing tactics that leverage authority and emphasize the difficulties uses face in recognizing phishing emails that masquerade as genuine business. Manipulating trust and credibility serves as effective strategy for phishers, and there is a strong need to enhance user education or training program geared towards building the ability to detect and withstand misleading schemes.

- *Cognitive Biases and Heuristics*

Cognitive biases can be defined as a situation where decision making or making a certain belief is carried out in a certain predetermined incorrect way due to a set of characteristics leading to subjective instead of objective ways of making decision. These biases originate with the brain's effort to make decision – making and information processing more efficient, and therefore, not entirely rational. For instance, the confirmation bias makes people accept only positive information regardless of other workable evidence that depicts otherwise (PositivePsychology.com, 2020).

Heuristics are decisions or principles that humans apply in arriving at certain conclusions in the least time possible. Even through these shortcuts are mostly useful, they can sometimes distort data or contain some sort of bias. For example, the named single – cause fallacy or the availability heuristics leads people to think that if they can easily recall instances about a phenomenon, then, probably the occurrence of that phenomenon is high;which is flawed notion (PositivePsychology.com, 2020).

Cognitive biases and heuristics greatly affect the likelihood of falling for phishing schemes in many ways. Alseadon (2014) discovered that people who score high on agreeableness and openness to experience are more vulnerable to phishing schemes. These individuals are generally more trusting and eager to engage in unfamiliar situations, making them more accessible targets for deceptive emails. Additionally, research revealed that individuals with greater impulsivity and extraversion, as well as those with lower levels of openness and agreeableness risk for phishing (Alseadon, 2014).

Cognitive biases, human factors that make use of the availability heuristic in the phenomenon of phishing, influence people make decisions based on incomplete information or rather positive outlook, and this result in underestimating the risks that are involved with questionable emails. Butavicius et al. (2016) observed that people do not recognize phishing as a threat mainly because they use heuristics to quicken their decision – making process instead of being cautious. Extraversion, characterized by sociability and assertiveness, has been associated with greater susceptibility to phishing. Extraverts are more inclined to stimuli, such as emails, without proper scrutiny, thus increasing the likelihood for falling for scams (Alseadon, 2014). Conversely, individuals who score high on conscientiousness, known for their meticulousness and caution, usually exhibit lower susceptibility to phishing attacks (Butavicius et al., 2016).

- *Emotional Triggers in Phishing*

Phishing schemes frequently take advantage of emotional triggers to elicit quick responses, exploiting human psychological weaknesses. A study conducted by Butavicius et al., (2016) revealed that emails posing as authoritative sources were more likely to be viewed as trustworthy, suggesting that emotional manipulation via perceived authority can heighten vulnerability. Additionally, studies also demonstrate that emotional triggers, such as fear or urgency negatively affect judgement through cognitive biases. Luo et al. (2013) found that phishing emails designed to provoke intense emotions, like panic or excitement, often disrupt logical reasoning, causing people to act rashly without thoroughly evaluating the situation. These insights highlight the necessity of comprehending the psychological strategies used in phishing attacks to formulate effective defenses.

Emotional triggers in phishing use psychological tactics that force the targeted user to perform actions such as clicking on the link, downloading the attachment, or asking you to provide the pin code of your credit card to the phisher. A common lure used by phishers is to used fear or threat actions such as account compromise or legal actions for user to panic. They also employ greed by posing as agencies that will offer fake prizes or sweet attractive deals; curiosity through sensational messages. The following are the common pressure tactics used by phishers; Urgency is the next method, making the receivers timeline tight hence, they do not have time to think and act without thinking critically. There are two primary coercion – one is to trust someone who sent a link, and thinking in terms of employer, a bank or a government agency for a fake letter authored by a friend in need, takes advantage of trust placed in it. Those emotional triggers exclude logic entirely hence, making victims susceptible to scams, highlighting the need for education and awareness to prevent phishing attacks.

- *Scarcity Bias*

Scarcity bias refers to the tendency of individuals to view an item or opportunity as more valuable because it is limited in availability. Phishing emails frequently exploit this bias by creating an artificial sense of urgency, encouraging users to act promptly before an offer ends or a danger arises.

As explained by Dr. Cialdini's seven principles of persuasion, effectively persuading others through the scarcity principles requires more than simply highlighting the benefits of your products and services. It's necessary to also emphasize what makes your offering unique and the potential losses if they disregard your proposal. The concept of scarcity suggest that people tend to value things that are or in limited supply. Consequently, individuals are more likely to respond to messages that claim an offer is accessible for only a short duration (Butavicius et al., 2016).

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14610632

Scarcity can be utilized to convey that only a few units of a coveted reward are available, urging a user to act swiftly to secure it. For example, an email might prompt a user to reply immediately or risk missing out on a desirable item, such as a complimentary gift.

- *Social Proof*

Also, from Dr. Cialdini's seven principles of persuasion, instead of relying solely on our own persuasive abilities, we can refer to what a large number of others are already doing, particularly similar individuals. Alseadon (2014) found that individuals who consulted other victims are equally victim because the victim cannot confirm that the action performed is legitimate email.

Social proof is a psychological phenomenon wherein people look to the behaviors or opinion of others to inform their actions, especially in uncertain circumstances. Phishing attackers take advantage of this bias by crafting emails that seem more trustworthy through fabricated reviews, testimonials, or assertions of widespread endorsement.

In the realm of phishing, emails that suggest an offer has already been taken advantage of by others are often more persuasive (Butavicius et al., 2016). Social proof leverages an individual's desire to belong to a group or community. For instance, an email might assert that the majority of individuals within a group are engaging in a specific behaivior.

III. CONCLUSION

Phishing attacks continue to harm and target individual's psychological vulnerabilities making it important to understand the factors why users fall victims to this cyberattack. This paper has examined the roles of manipulation of trust and credibility, cognitive biases and heuristics, emotional triggers in phishing, scarcity bias, and social proof as psychological factors that contribute to phihers tactic in deceiving users to fall victims to harmful phishing emails.

REFERENCES

[1]. Alseadon, A. (2014). The impact of personality traits on phishing susceptibility: The case of Saudi Arabia. International Journal of Computer Application.
[2]. Butavicius, M., Parsons, K., Pattison, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear phishing e – mails.
[3]. Diaz, A., Sherman, A. T., & Joshi, A. (2018). Phishing in an academic community: A study of user susceptibility and behaivior.
[4]. Luo, X., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the phishing heuristic – semantic model: A theoretical framework and an explanation. Computer & Security.
[5]. Robert Cialdini: "Dr. Robert Cialdini's seven principles of persuasion, IAW". Influence work retrieved 18 May 2022.
[6]. Desolda, G., Ferro, L. S., Marella, A., Catarci, T., & Costabile, M. F. (2020). Human factors in phishing attacks: A systematic literature review., AMC Computing surveys.
[7]. Jain. A. K., & Gupta, B. B. (2017). Phishing detection: Analysis of visual similarity – based approaches. Security and communication network.
[8]. Alkhalil., Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy.
[9]. Frontiers in computer science. 3.
[10]. McAlaney, J., & Hills, P. J. (2020). Understanding phishing email processing and perceived trustworthnes through eye tracking. Frontiers in psychology.
[11]. PositivePsychology.co. (2020, April 4). What is cognitive bias? 7 examples & resources (Incl. Codex).