Issues in Information Systems
Volume 24, Issue 2, pp. 71-83, 2023

DOI: https://doi.org/10.48009/2_iis_2023_107

Psychological tactics of phishing emails

Ping Wang, *Robert Morris University, wangp@rmu.edu*
Peyton Lutchkus, *Robert Morris University, pglst259@mail.rmu.edu*

Abstract

Phishing is a common form of social engineering attack that exploits human psychology and vulnerabilities to persuade victims to give away sensitive information. Phishing emails are an increasingly prevalent fraud and threat with various tactics to manipulate, influence, and victimize email users. Phishing is the primary starting point and success factor for cyber-attacks, and it is a significant research issue to understand the human psychological vulnerabilities to phishing victimization. This research reviews the research psychological factors targeted by the common tactics of phishing. Adopting Cialdini's psychological principles of influence as the research model, this research analyzes selected real-life phishing emails from the Berkeley Phish Tank database to illustrate and expose various categories of psychological tactics of phishing emails.

Keywords: phishing emails, social engineering, psychology, tactics, principles of influence

Introduction

Phishing is a common form of fraudulent attempt often used by cyber criminals to steal sensitive data such as login credentials and financial account information from users (Wang & Girma, 2020). Phishing has become a significant and challenging issue for cybersecurity practitioners. Statistically, 91% of all cyber-attacks begin with a phishing email to an unexpected or unsuspecting victim, and 32% of all successful cybersecurity breaches involve the use of phishing techniques (Deloitte PLT, 2020). In addition, 95% of all cyber-attacks on enterprise networks are the result of successful spear phishing masked as trusted sources, and 96% of phishing attacks are delivered via email (Swiss Cyber Institute, 2021). Phishing attacks have been fast growing. According to the latest report by Anti-Phishing Working Group (APWG), the number of phishing attacks has increased by more than 150% per year since 2019, reaching a quarterly total of 1,350,037 phishing attacks in the 4th quarter of 2022; and the BEC (Business Email Compromise) identity theft attacks, with an average attempt to steal $132,559, have caused total losses of billions of dollars at large and small companies (APWG, 2023).

Phishing in nature is a type of social engineering that exploits human vulnerabilities. Kevin Mitnick, who was once the world's most famous hacker, concluded that security vulnerabilities will continue to exist and worsen due to human gullibility, naivete, and ignorance because "the human factor is truly security's weakest link" (Mitnick & Simon, 2002, p.12). Given the continued growth and impact of phishing, it is important for the cybersecurity research community to identify the vulnerable human factors targeted and exploited by the common tactics of phishing so as to educate users to prevent or minimize phishing attacks. Recent empirical research on measuring cognitive vulnerability triggers in phishing emails indicates that cognitive assessment of the phishing email body could help to predict the degree of phishing success and improve the effectiveness of anti-phishing responses and remediations (van der Heijden & Allodi, 2019).

Social engineering attacks, which are commonly employed in phishing emails, are still unpredictable for unsuspected victims despite extensive prior research on prevention of social engineering attacks (Syafitri et al., 2022). Therefore, further research is still needed to discover and understand the human psychological traits exploited by social engineering tactics. In addition, technical approaches to phishing detection and prevention such as the comprehensive multi-dimensional model based on a machine learning algorithm have identified personality, cognitive processes, and computer knowledge as the most influencing factors of susceptibility in predicting phishing victims. However, such research is based on limited datasets and samples and further research is needed to address dynamic aspects such as why victims fail to recognize phishing attacks (Yang et al., 2022).

The goal of this research paper is to identify the key human cognitive and behavioral vulnerabilities targeted by common social engineering and psychological tactics in phishing emails to better understand the dynamics in recognizing phishing emails and to improve prevention of email phishing attacks. This study will contribute a mapping of comprehensive principles of influence to the psychological tactics of phishing emails. Selected cases of real-life phishing emails from the Berkeley Phish Tank database are used to illustrate the human vulnerabilities and psychological tactics of phishing. The following sections of the paper will review the relevant background research literature, explain the comprehensive model, describe the case study methodology, and present the findings, discussions, and conclusions.

Background

There has been growing research into the vulnerability factors that influence user judgement, susceptibility and response to online fraud and phishing emails. The research efforts range from common ploys and techniques of social engineering to more subtle psychological factors of human users including cognitive and behavioral variables that contribute to phishing susceptibility (Brody, Brizzee, & Cano, 2012; Yang et al., 2022). Table 1 below highlights and summarizes significant research efforts and progress in recent years on psychological tactics of phishing attacks.

Table 1: Summary of Recent Research on Psychological Tactics of Phishing

B	Authors	Psychological Tactics/Factors	Methodology	Key Findings/Conclusions
2022	Murtza, Pak, & Siddiqi	Authority Influence; Scarcity Influence; Social engineering tactics	Theoretical review	- People tend to comply with orders from someone believed to be an authority figure. - Attackers use symbols or logos to make them look like they are coming from an authentic source. - Attackers use a time pressure or scarcity tactic to influence the decision making of a target. - Targets may make harmful mistakes because of the pressure or urgent feeling.

B	Authors	Psychological Tactics/Factors	Methodology	Key Findings/Conclusions
2022	Yang, Zheng, Wu, Li, Wang, & Wang	Personality, Cognitive Processes, Security Behavior, Knowledge of computer security	Experimental; Machine learning approach	- Identifiable models can predict potential phishing victims more accurately. - Computer knowledge characteristics are highly correlated with phishing. - Knowledge of network security is one of the key factors influencing the phishing susceptibility
2021	Abroshan, Laermans, Poels, & Devos	Risk-taking, Decision-making, Demographics	Psychological tests; Phishing simulation	- A high level of general risk-taking can increase the possibility of clicking on a phishing link. - Women seem to be more prone to clicking on a phishing link. - Findings may vary across cultures and countries.
2021	Mark	Perceived susceptibility, Perceived threat, Avoidance motivation, Threat avoidance	Survey	- Perception of threat by an individual is the vital factor in influencing a person's avoidance behavior. - Motivation is a key driving force to a person's avoidance behavior of IT security threats. - Tactics using psychological manipulation are the most dangerous because they cannot be prevented by technology.
2020	Albladi, & Weir	Perceived risk, Competence, Trust, Motivation	Survey	- When individuals feel competent in their abilities to control information, they are less susceptible to phishing attacks. - People who are confident in their ability to protect themselves online and having high security awareness can be perceived as highly competent.

B	Authors	Psychological Tactics/Factors	Methodology	Key Findings/Conclusions
2020	George, Teunisse, & Case	Gullibility, Personality traits, Cognitive stimulus	Survey	- Those who are more gullible are more likely to find phishing emails trustworthy. - There is a strong correlation between gullible individuals and high emotionality (high levels of anxiety or fear) and low sense of self.
2019	Norris, Brookes, & Dowell	The range of psychological vulnerabilities to online fraud victimization linked to human factors	Systematic research review	- Messages appeal to specific psychological vulnerabilities, the most successful linking message with human factors. - The total number of studies able to identify specific psychological processes associated with increased susceptibility to online fraud victimization is still limited.
2019	Campbell	Behavioral trust, Cognitive response, Human deception	Qualitative Delphi design; Survey	- A balanced controls program is needed to support employee development in recognizing human deception. - A significant factor for social engineering victimization is ineffective or lack of organizational security practices and ongoing education and training of employees in social engineering.
2019	William, & Polage	Influence of message factors on trust and persuasiveness of emails; Loss and reward-based techniques; Authentic design cues; Reference to current events.	Online survey	- The use of loss-based influence techniques and the presence of authentic design cues was found to increase perceived trustworthiness and persuasiveness of emails. - The presence of authentic design cues and the type of influence technique used significantly impacted participant judgements.
2018	Rajivan, & Gonzalez	Adversarial behaviors; Persuasion strategies; Emotional strategies; Authoritative tone; Shared interest.	Experimental	- People may be more averse to accept failure and more willing to take actions on emails that involve possible losses. Phishing emails that use friendly- and authoritative tone may evoke more trust. - Phishing emails with persistent use of specific attack strategies are more successful.

B	Authors	Psychological Tactics/Factors	Methodology	Key Findings/Conclusions
2018	Kleitman, Law, & Kay	Cognitive and behavioral indicators of phishing susceptibility and false positives.	Experimental	- Human-centered variables account for the majority of variance in phishing susceptibility. - Perceptions of maliciousness, intelligence, knowledge of phishing, and on-task confidence are the most significant factors in phishing susceptibility.
2018	Hadlington	Personal attitude to security; Personality Traits of Targets.	Survey	- There is a significant negative correlation between attitudes towards cybersecurity and risky cyber security behaviors. - A more negative attitude towards cybersecurity is linked to higher levels of risky behaviors and falling for cyber attacks such as phishing.
2016	Conteh, & Schmick	Technical and psychological vulnerabilities to social engineering tactics	Research review	- Human psychological vulnerabilities always exist despite security technology. Exposing psychological vulnerabilities allows for a successful phishing attack. Alternate routes of persuasion attack a victim's emotions, such as fear or excitement, which may cause a harmful action.
2016	Harrison, Svetieva, & Vishwanath	Message factors; User knowledge and experience with phishing; User cognitive process of phishing emails.	Experimental	- Phishing susceptibility was predicted by a combination of both low attention to the e-mail elements and high elaboration of the phishing message. - The presence of a threat or reward-based phishing message did not affect phishing susceptibility. - Individual factors such as knowledge and experience with e-mail increased resilience to the phishing attack.

The research efforts presented in Table 1 above employ various methodologies including experiments and surveys with some important progress and empirical findings on various psychological factors for phishing susceptibility. Most of the studies have found correlations between some psychological vulnerabilities to social engineering tactics and risks of falling victims of phishing. However, the psychological factors addressed in the empirical studies are sporadic and lack a comprehensive map of common human factors targeted by corresponding social engineering tactics in specific phishing emails.

In addition, there are significant research limitations, needs, and opportunities for further research indicated by the existing research efforts. As existing research often focuses on limited types of phishing tactics, an important need for further research on human factors on phishing susceptibility is to address the impact of

more psychological and behavioral attributes and on more and other types of phishing (Abroshan et al., 2021; Albladi & Weir, 2020). With disparate research on different human attributes in phishing, there is a lack of consensus on the key factors and solutions for countering human deception in social engineering attacks (Campbell, 2019). Future research on persuasion strategies should include real world phishing data with more diverse background and subjects to study the impact of cultural and language differences on the strategies used to build phishing emails (Rajivan & Gonzalez, 2018). Further research on human vulnerabilities to phishing should also include larger size of sampling and address more dynamic aspects of human users such as attention to details of phishing emails (Yang et al., 2022).

Theoretical Model

Based on the review of existing research and limitations on human factors and social engineering tactics for phishing susceptibility, this research adopts Cialdini's six psychological principles of influence as the comprehensive model of major factors of cognitive, social, and behavioral psychology to analyze common email phishing tactics. Table 2 below presents this model of principles of influence from Cialdini and the definitions and interpretations of the principles (Cialdini, 2007; van der Heijden & Allodi, 2019).

Table 2: Cialdini's Principles of Influence and Definitions

Principles	Definitions and Interpretations
Reciprocation	"The Old Give and Take… and Take" (p. 13). To appeal to one's feeling of the obligation to return favors from others.
Consistency	"Commitment and Consistency" (p. 43). To appeal to one's behavioral consistency with prior commitments, decisions, and behaviors.
Social Proof	"Truths are Us" (p. 87). To appeal to people's tendency to follow the suit or use the majority behavior as benchmark or reference.
Liking	"The Friendly Thief … As a rule, we most prefer to say yes to the requests of someone we know and like" (p. 126).
Authority	"Directed Deference" (p. 157). To appeal to human and social tendency to obey people in authoritative positions with implied penalty for disobedience.
Scarcity	"The Rule of the Few" (p. 178). To appeal to one's feeling of more value to things and opportunities with limited availability, urgency, and possible loss for missing out.

Methodology

This research uses the case study methodology to analyze selected phishing cases from the Phish Tank database published by the information security office of University of California at Berkeley. The Phish Tank database collects and publishes examples of real-life phishing emails at the Berkeley campus dated from 2015 to 2023. Intended to educate campus email users about phishing, these phishing examples come

with analysis of detailed indicators of scams, forgery, impersonation and tips and information on how to spot and report such phishing attacks (Berkeley Information Security Office, 2023).
The selected cases of phishing are real-life phishing cases from the Berkeley Phish Tank involving different types of tactics or psychological principles to manipulate and persuade email users to become victims of phishing attacks. The 10 selected phishing emails for this study are of different years and include various subjects of potential interest to users, ranging from offers of paid work opportunities to urgent requests for compliance. The case study approach will use the adopted model of psychological principles of influence by Cialdini (2007) to analyze the phishing emails to identify the phishing tactics and map them to specific psychological principles. The following section presents the findings and discussions on the cases of phishing emails.

Findings and Discussions

Table 3 below presents the 10 selected phishing emails from the Berkeley Phish Tank, year of the email, and specific principles of influence mapped to the phishing tactics. The psychological tactics of each phishing email may involve multiple principles of influence for persuasion and victimization.

Table 3: Case Studies of Real-life Phishing Emails

Year	Content of Phishing Email	Principles of Influence
2023	The faculty/department of Computer Science urgently needs undergraduates to work virtually as research assistants at $350 per week. Note: Candidates should be proficient in Microsoft Office and have a solid understanding of its capabilities (Excel, Word, and PowerPoint). Your job will be done remotely, and you can accomplish all remote chores whenever it's convenient for you to do so. The position is open to all university undergraduates from all departments. Please text Prof. Murat Arcak at if you would (510) 216-7076 like to continue with the application process. Please provide your full name, email address, department, and year of study in order to get the job description and other application requirements. Best Regards, Prof. Murat Arcak Title: Professor, Department of Computer Science University of California, Berkeley P: (510) 216-7076	Liking, Authority, Social Proof
2022	Welcome Subscriber; Your Annual membership for NORTON 360 TOTAL PROTECTION has been renewed and updated successfully. The amount charged will be reflected within the next 24 to 48 hrs on your profile of account. INVOICE NO. @ GGH1644259106OV ITEM NAME @ NORTON 360 TOTAL PROTECTION START DATE @ 2022 Feb 07 END DATE @ 1 year from START DATE GRAND TOTAL @ $240.42 USD PAYMENT METHOD @ Debit from account	Reciprocation, Consistency

Year	Content of Phishing Email	Principles of Influence
2021	Our security system has detected some irregular activity connected to your account. you will be unable to send and receive emails until this issue has been resolved > CLICK HERE TO VALIDATE NOW To prevent further irregular activity we will restrict access to your account within 72 hours if you did not validate your account. *Note:* Mail Administrator will always keep you posted of security updates. Mail Admin	Reciprocation, Scarcity, Authority
2020	Each year, as an employee of University of California, Berkeley you are eligible to schedule a phone call, teleconference, or in-person meeting off campus with a representative for answers to your specific state, federal and individual retirement benefit questions. At your consultation you will be provided with information on what your expected income will be from UCRP when you retire, and how much longer you will have to work. Secure your spot by clicking on the link below or simply reply “yes” to this email.	Reciprocation, Consistency, Authority, Scarcity
2019	From: David Card <dvdmson @ gmail . com> To: RECIPIENT Date: Sat, Oct 19, 2019 at 2:22 PM Subject: ******Part time home work assistant needed****** Hello RECIPIENT I am urgently seeking for a Clerical/Administrative Assistant to work for me on campus at their own free time while I am away on my work and earn basic wage $250 weekly. This is a flexible job that requires little to no prior experience.Let me know you are interested and I will fill you in. Sincerely *Professor David Card* *Department of Economics* *530 Evans Hall #3880* *University of California Berkeley* *Berkeley, CA*	Reciprocation, Scarcity, Liking, Authority
2018	From: XXX.subdomain.berkeley.edu Subject: Quick question To: xxxxx@berkeley.edu(link sends e-mail) I'm in a meeting and need help getting some Amazon Gift Cards <Name Removed> University of California, Berkeley	Liking, Authority

Year	Content of Phishing Email	Principles of Influence
2017	Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account. For this purpose, click the web address below or copy and paste it into your web browser. A successful login will activate your account and you will be redirected to your library profile. https://auth.berkeley.edu/cas/login?service=https%3a%2f% If you are not able to login, please contact <Name Removed> at xxxxx@berkeley.edu(link sends e-mail) for immediate assistance. Sincerely, <Name Removed> University Library University of California Berkeley	Reciprocation, Authority, Scarcity
2016, Dec 14	Good Morning Berkeley Family, Please read attached for an important announcement from Chancellor Nicholas B. Dirks Thanks, Nicholas B. Dirks Chancellor 1 attachment: shared Document.pdf	Liking, Authority
2016, Oct 20	From: BankOfAmerica Subject: Irregular Activity Date: 10/20/2016 7:27 AM We have detected irregular activity on your account on the date 10/20/2016. For your protection, we have temporary limited your account. In order to regain full access to your account, you must verify this activity before you can continue using your account. We have sent you an attachment , open it and follow the steps to verify your account. Once completed, please allow up to 48h to update. Copyright © 2016 BankOfAmerica, All rights reserve IrregularActivityFile.html	Consistency, Reciprocation, Authority
2016, May 23	Hello, Please refer to the vital info I've shared with you using Google Drive. Click https://www.google.com/drive/docs/file0116 and sign in to view details.. Regard <sender's name removed> Readmission Representative Office of the Registrar	Authority

The phishing email of 2023 involves psychological tactics reflecting the principles of Liking, Authority, and Social Proof for influence and victimization. The tactic of using a named professor from the Department of Computer Science shows the principle of Liking to manipulate potential victims to say yes to someone known to the public. Using the official title, department, and the university in the signature reflects the principle of Authority to appeal to people's obedience or deference to authority. This phishing email also repeatedly emphasizes the convenient feature of working virtually or remotely for this job offer, which

reflects Cialdini's principle of Social Proof as people are increasingly receptive to and prefer working virtually for convenience and health concerns after just going through the Covid-19 pandemic.
The phishing email of 2022 shows the psychological tactics appealing to the principles of Reciprocation and Consistency. The emphasis on the successful renewal and update of the NORTON 360 TOTAL PROTECTION is to highlight the service provided. The charged amount and the invoice details indicate the logical obligation to pay for the service provided in the principle of the reciprocation. The emphasis on Annual membership appeals to the psychological principle of consistency for sticking to the regular behavior and commitment as a member.

The phishing email of 2021 demonstrates psychological tactics appealing to the principles of Reciprocation, Scarcity, and Authority. The Reciprocation principle is shown in the trade-off between the user's need to be able to send and receive emails as an essential daily function and the perceived obligation to click the link to validate the user account. The phishing tactic also appeals to the principle of Scarcity by imposing the urgent deadline of "within 72 hours" for validating the account and the penalty of losing account access if the deadline is not followed. The phishing mail also uses "Mail Admin" in the signature as an additional tactic to appeal to the user's trust and obedience to Authority.

The phishing email of 2020 reflects psychological tactics appealing to the principles of Reciprocation, Consistency, Authority, and Scarcity. Reciprocation is shown in the trade-off between the provided consultation service to answer your retirement benefit questions and your obligation to respond by clicking the link or reply to the email. The emphasis on the annual service "each year" is to appeal to Consistency for sticking to the regular commitment. The use of the well-known institution name of University of California, Berkeley is to appeal to Authority for credibility. The words "secure your spot by clicking the link below" are a tactic of Scarcity to suggest that the availability is limited and at risk and quick response is necessary to secure the opportunity for the service.

The phishing email of 2019 shows psychological tactics appealing to the principles of Reciprocation, Scarcity, Liking, and Authority. Reciprocation is the give and take between responding to the phishing email and getting the paid homework assistant position. Scarcity is shown in the urgent seeking for this position. The email's appeal to Liking is evident from the description of the position as "flexible" and "requires little to no prior experience" to be attractive to maximum number of people. The detailed signature block with a named Professor at the well-known institution appeals to Authority for credibility.

The short phishing email of 2018 reflects psychological tactics appealing to the principles of Liking and Authority. This phishing email creates the impression that it comes from someone familiar to the target to appeal to the Liking principle to get a positive response. The named sender (removed for publication) and the institution name in the signature block appeal to Authority for obedience.

The phishing email of 2017 demonstrates psychological tactics appealing to the principles of Reciprocation, Authority, and Scarcity. Reciprocation is the trade-off between getting continued access to your library account and the obligation to respond to this phishing email as directed. The contact name (removed for publication) and the institution name in the signature block appeal to Authority for credibility and obedience. The emphasis on your account "expiring soon" appeals to Scarcity for urgency with implied penalty for no response.

There are three phishing emails selected from the data collected for 2016 with different dates. All three emails include psychological tactics to appeal to Authority for credibility and obedience, including using the Chancellor position title, Bank of America, and Office of the Registrar in the signatures. In addition, the email of December 14, 2016 appeals to the principle of Liking as it emphasizes the specific individual

of Chancellor Nicholas B. Dirks who is known to everyone in the institution. The phishing email of October 20, 2016 also appeals to the principles of Consistency and Reciprocation. Appeal to Consistency is shown in the email's emphasis on irregular activity and temporary restriction versus the preferred regular and stable full access. Appeal to Reciprocation is the obligation to respond to this email in return for regaining full access to your account.

The selected cases of phishing emails indicate that attempts to appeal to the principles of Authority and Reciprocation are the most common psychological tactics. It should be noted that other factors may also be indicators to help spot phishing attacks, including errors in spelling, grammar, and punctuation as well as suspicious links.

Conclusion

This research focuses on the tactics of phishing emails to appeal to psychological factors for persuasion and victimization. This research adopts Cialdini's six principles of influence as the theoretical model for content analysis of phishing emails: Reciprocation, Consistency, Social Proof, Liking, Authority, and Scarcity. The case study method is used to analyze and discuss 10 real-life phishing emails in the last 8 years from the Berkeley Phish Tank database. The research on psychological tactics and principles of phishing with real-life phishing cases contributes significant theoretical perspectives and empirical data analysis to on-going research on phishing and to anti-phishing training and education solutions.

Theoretically, this research is focused on Cialdini's six principles of influence. Future research may explore additional theories and other possible psychological factors and attributes involved in phishing attacks. The phishing examples for the case study are limited to the Berkeley Phish Tank in a higher education setting. Future research may include more diverse phishing data for analysis. Future research on phishing may also include phishing attacks on mobile devices and text messages, which are increasingly targeted.

An emerging area of challenge for future research is the use of artificial intelligence (AI) in phishing. AI tools like ChatGPT can be weaponized to make common phishing tactics of social engineering and impersonation attempts highly credible (Chickowski, 2023). AI-enabled phishing presents increasing challenges for anti-phishing solutions as AI tools can be trained in all tactics of phishing datasets to generate very persuasive phishing emails with perfect English, which can also be delivered in large volume of attacks quickly (Benishti, 2023). Follow-up research on phishing may focus on assessing the effect and risks of AI-enabled phishing techniques and exploring effective solutions.

References

Abroshan, H., Laermans, E., Poels, G., & Devos, J. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. https://doi.org/10.1109/ACCESS.2021.3066383

Albladi, S. M., & Weir, G. R., S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity, 3*(1). https://doi.org/10.1186/s42400-020-00047-5

APWG (Anti-Phishing Working Group). (2023). Phishing activity trends report, 4th Quarter 2022. https://apwg.org/trendsreports/

Berkeley Information Security Office. (2023). The Phish Tank. Retrieved May 10, 2023 from https://security.berkeley.edu/resources/phish-tank

Benishti, E. (2023, March 3). Prepare for the AI phishing onslaught. *Forbes.* https://www.forbes.com/sites/forbestechcouncil/2023/03/03/prepare-for-the-ai-phishing-onslaught/?sh=61cf13341925

Brody, R. G., Brizzee, W. B., & Cano, L. (2012). Flying under the radar: Social engineering. *International Journal of Accounting and Information Management, 20*(4), 335-347. https://doi.org/10.1108/18347641211272731

Campbell, C. C. (2019). Solutions for counteracting human deception in social engineering attacks. *Information Technology & People, 32*(5), 1130-1152. https://doi.org/10.1108/ITP-12-2017-0422

Chickowski, E. (2023, April 27). SANS reveals top 5 most dangerous cyberattacks for 2023. https://www.darkreading.com/attacks-breaches/sans-lists-top-5-most-dangerous-cyberattacks-in-2023

Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. HarperCollins e-books.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23), 31-38. https://doi.org/10.19101/IJACR.2016.623006

Deloitte PLT. (2020). 91% of all cyber attacks begin with a phishing email to an unexpected victim. Retrieved May 12, 2023, from https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

George, M. S., Teunisse, A. K., & Case, T. I. (2020). Gotcha! Behavioral validation of the gullibility scale. *Personality and Individual Differences*, 162. https://doi.org/10.1016/j.paid.2020.110034

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviors: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269-281. DOI: 10.5281/zenodo.1467909

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. *Online Information Review, 40*(2), 265-281. https://doi.org/10.1108/OIR-04-2015-0106

Kleitman, S., Law, M. K. H., & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLoS One, 13*(10), 1-29. https://doi.org/10.1371/journal.pone.0205089

Mark, M. S. (2021). *An analysis of factors influencing phishing threat avoidance behavior: A quantitative study* (Order No. 28320611). Available from ProQuest Dissertations & Theses Global. (2506645080). Retrieved from https://reddog.rmu.edu/login?url=https://www.proquest.com/dissertations-theses/analysis-factors-influencing-phishing-threat/docview/2506645080/se-2

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security.* Wiley Publishing, Inc.

Murtaza, A. S., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences, 12*(12), 6042. https://doi.org/10.3390/app12126042

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of Internet fraud victimization: A systematic review. *Journal of Police and Criminal Psychology, (2019)* 34, 231–245.

Rajivan, P., & Gonzalez, C. (2018). Creative persuasion: A study on adversarial behaviors and strategies in phishing attacks. *Frontiers in Psychology, 9*(135), 1-14. doi: 10.3389/fpsyg.2018.00135

Swiss Cyber Institute. (2021). 27 Phishing Attack Statistics You Probably Didn't Know. Retrieved May 12, 2023, from https://swisscyberinstitute.com/blog/cybersecurity-facts-phishing-statistics/

Syafitri, W., Shukur, Z., Asma' Mokhtar, U., Sulaiman, R., & Ibrahim, M. (2022, March 28). Social engineering attacks prevention: A systematic literature review. *IEEE Access, 10*(2022), 39325-39343. DOI: 10.1109/ACCESS.2022.3162594

van der Heijden, A., & Allodi, L. (2019). Cognitive triaging of phishing attacks. *Proceedings of the 28th USENIX Security Symposium, August 14-16, 2019, Santa Clara, CA, USA.* 1309-1326.

Wang, P., & Girma, A. (2020). Online phishing and solutions. In M. Khosrow-Pour (Eds). *Encyclopedia of criminal activities and the deep web* (pp.837-850). Hershey, PA, USA: IGI Global. doi:10.4018/978-1-5225-9715-5

Williams, E., & Polage, D. (2018). How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. *Behavior & Information Technology, 38*(2), 184-197. https://doi.org/10.1080/0144929X.2018.1519599

Yang, R., Zheng, K., Wu, B., Li, D., Wang, Z., & Wang, X. (2022). Predicting user susceptibility to phishing based on multidimensional features. *Computational Intelligence and Neuroscience, 2022* (Article ID 7058972), 1-11. https://doi.org/10.1155/2022/7058972