"Slow Down and Frown" to improve Phish Detection

Patricia Nevin[1], Karen Renaud[2], George Finney[3]
[1]Stirling University, UK; [2]University of Strathclyde, UK; [3]Southern Methodist University, Texas
karen.renaud@strath.ac.uk (Corresponding Author)

Abstract
The move to 'digital first' has led to increasing dependence on online services, which increases susceptibility to security incidents.1 Human behaviours can compromise organisational information security, with myriad perpetrators willing to exploit the human propensity to trust in order to achieve such compromises.2 Phishing emails – which present recipients with an email containing a fraudulent link or a rogue attachment that can lead to the installation of malware or facilitate a ransomware attack – are a key attack vector. But encouraging users to slow down when processing emails can help combat this threat.

1. Introduction

The move to "digital-first" has led to increasing dependence on online services, which increases susceptibility to security incidents[9]. Human behaviours can compromise organisational information security, with myriad perpetrators willing to exploit the human propensity to trust to achieve such compromises[5].

Reducing cybercrime is a top priority for Government bodies[1]. Phishing emails are the key attack vector[5], which presents recipients with an email containing a fraudulent link or a rogue attachment that can lead to the installation of malware or facilitate a ransomware attack. Over 5.5 million phishing reports were made in 2021[22.] The email itself utilises *social engineering* techniques to persuade people to take an unwise action. They might make people fearful, or trigger a sense of urgency, for example. The sophistication of phishing tactics advances daily, as attackers innovate using ever more skilful deception techniques[12.] Phishers want the email recipient to click on a link, provide information or open a malicious attachment. Social engineering triggers emotions e.g., fear, curiosity, empathy, and greed[2]. A number of interventions have been proposed to help employees to spot Phishing attacks, but these have had limited success[21].

In this paper, we investigate a technique called '*Slow Down and Frown'* proposed by Finney[8]. This advice encourages email recipients to slow down when processing emails, and this admonition is delivered as and when people are reading their email messages. This ought to encourage more rational and reflective thought processes and thereby maximise the likelihood that email recipients will detect deceptive techniques[18]. Social engineering techniques try to persuade people to act quickly, so the idea behind "slow down and frown" is to make them pause to consider whether an email is genuine or not. The precautionary message also uses the motivational factor of 'frowning', the purpose of which is to impact neurological signalling to the brain to boost awareness and greater vigilance[14].

2. Related Research

Humans tend to prefer operating in a fast automatic way (System 1) rather than using slow rational processing (System 2)[11]. Kahneman's Dual Process Theory, presents System 1 as an intuitive system of thinking and System 2 as a more analytical approach[10]. This kind of duality is often referred to as the 'root cause' of problems within the security chain[17,20]. The human propensity to want to trust[13] and to miss important cues which signal untrustworthiness is also skilfully preyed upon by cyber criminals using social engineering tactics.

2.1 Phishing Interventions

Much current research focuses on counteracting biases and on shifting the Internet user to engage System 2 thinking and encourage a slower, rational, more controlled response. For example, TORPEDO deactivates links for a few seconds to encourage closer inspection of the email[19]. An additional factor that may affect the processing of information is when it is received, how the information is presented and the presence of other sensory information. People may know what the phishing red flags are but spotting them when the mind is concentrating on something else, such as reading an email, may affect their ability to identify the phishing techniques.

2.2 Proposed Intervention

An online survey displayed the "slow down and frown" image on top of ostensible emails, as shown in Figure 1 for an experimental group, to see whether this would improve Phish detection. They were shown 6 emails, with four of these using social engineering tactics. They were asked to decide whether the email should be acted upon, or not.

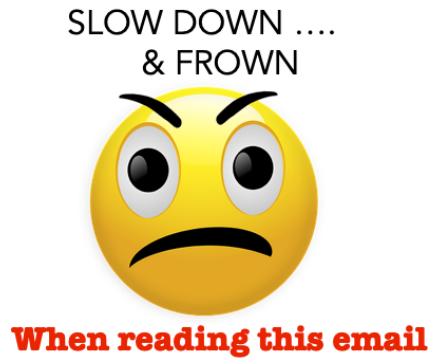

Figure 1. 'Slow down and Frown' Intervention.

3. "Slow Down and Frown" Intervention Study

Research Question: Does displaying the "Slow Down and Frown" image improve phish detection?

3.1 Recruiting

Four hundred and seven participants over the age of 18 were recruited via Prolific Academic and data collection took place on 14th July 2021. Respondents were informed that the survey would take 10 minutes to complete, and paid £1.25

for their time. Participants in the experimental group saw the "slow down and frown" image. Four hundred and seven responses were gathered through a randomisation sampling approach.

3.2 Parameters

After giving consent, participants were given a scenario where Sam and Jo are best friends. Jo has sent Sam an email. Jo's email address is jokerr@gmail.com. They were asked to judge six emails from Jo (screenshots) and asked whether or not they would advise Sam to:

a) Click on the link;
b) Click on the attachment;
c) Provide personal phone number;
d) Download macros.

Phish & Legitimate Emails: Four emails were Phish, while two were genuine. The order of the emails was randomised. The content of the phishing emails ranged between:

1. **Curiosity: easy to spot cues**. From email address was wrong: joekerr@gmail.com – as opposed to jokerr@gmail.com
2. **Greed: hard to spot cues**. URL had spelling mistake: 'Ticketmastr'.
3. **Urgency: almost impossible to spot**: embedded email zoom link was not legitimate – 'myzoom.com' was used.

Piloting: Twenty people, including friends and family, were asked to review and complete the survey to improve the clarity of the survey questions[7].

3.3 Ethics

Ethical approval was obtained from the University of Stirling Ethics Committee prior to data collection. To ensure anonymity, no identifiable information was collected from participants.

4. Results

After cleaning the dataset, 407 responses were retained to support analysis. STATA was used to analyse the data. The dependent variable for the study, phish detection score, was the number of correct answers, based on the six emails. To test the hypotheses, the regression model of fractional logistic regression was used[16] and Chi-square test was used to examine differences between the Treatment and Control group.

The findings suggest that Phish detection is not improved by the presence of the image (*chi2 [5] = 2.9713, p=0.704*). The findings indicate that we cannot reject that there is no association between phishing detection scores and Condition groups i.e. Control and Treatment as the test is not significant (*chi2 [5] = 2.9713, p=0.704*).

A further analysis, focusing on questions individually, using binary logistic regression estimates, reveals statistically significant results for participants in the experimental group. The results show significantly increased likelihood of spotting Phish emails eliciting greed or curiosity.

5. Conclusion

The research trialled the 'slow down and frown' intervention to improve Phish detection. The analysis revealed a positive relationship between the intervention 'slow down and frown' and phish detection rates when emails elicit *urgency* or *greed/curiosity*. It is important to keep trying to identify effective measures to help people to spot Phishing attacks. If organisations embed the "slow down and frown" message in emails that contain links or attachments, our findings suggest that Phish detection would improve for certain kinds of attacks.

References

1. ABC7 Chicago. (2017). Wired away: couple loses life savings during home purchase. 13 November. Available at: https://abc7chicago.com/realestate/wired-away-couple-loses-life-savings-during-home-purchase/2630496/ [accessed 7 August 2021].
2. Abraham, S. and Chengalur-Smith, I. (2010) An overview of social engineering malware: trends, tactics, and implications. *Technology in Society*, 32 (3), pp. 183-196.
3. ActionFraud – National Fraud and Cyber Crime Reporting Center. (2020). Coronavirus-related fraud reports increase by 400% in March. 20 March. Available at: https://www.action. fraud.police.uk/alert /corona virus-related fraud-reports-increase-by-400-in-march [accessed 16 July 2021].
4. Allen, M. (2006). Social Engineering: A Means to Violate a Computer System. Bethesda, MD: SANS Institute.
5. Arachchilage, N. A. G., & Cole, M. (2011). Design a mobile game for home computer users to prevent from "phishing attacks". *Information Society (i-Society*), 27-29 June 2011(p.p.485e489).http://ieeexplore.ieee.org/stamp/stamp/jsp?tp.&arnumber.5978543&isnumber.59784 [accessed 16 July 2021].
6. Arachchilage, N. A. G., Namiluko, C., & Martin, A. (2013). A taxonomy for securely sharing information among others in a trust domain. *Internet Technology and Secured Transactions (ICITST)* pp. 296e304.
7. Draugalis, J., Coons, S., Plaza, C., (2008). Best practices for survey research reports: A synopsis for authors and reviewers. *American Journal of Pharmaceutical Education*.https ://doi.org/10.5688/aj720 111.
8. Finney, G. (2018). *Slow Down and Frown Your Way to Cybersecurity*. Available: https://*www.securityroundtable.org/Frown-Way-Cybersecurity*
9. Furnell, S.M., Bryant, P. and Phippen, A.D. (2007) Assessing the security perceptions of personal Internet users. *Computers & Security*, 26 (5), pp. 410-417
10. Kahneman, D. & Frederick, S. (2002). Representativeness Revisited: Attribute substitution intuitive judgement. In: T. Gilovich, D. Griffin, & D. Kahneman (Eds.), *Heuristics and Biases: The Psychology of Intuitive Judgment*. Cambridge: Cambridge University Press. pp. 49-81.
11. Kahneman, D. (2011): Thinking, Fast and Slow: *Penguin. Statistical Papers,* 55 (3), pp. 915.
12. Kirlappos, I., & Sasse, M. A. (2012b). Security education against phishing: a modest proposal for a major rethink. *Security & Privacy*, IEEE, 10, 24e32. March-April. Available at: http://dx.doi.org/10.1109/MSP.2011.179 [accessed 25 June 2021].
13. Kirlappos, I., Sasse, M.A. and Harvey, N. (2012). Why Trust Seals Don't Work: A Study of User Perceptions and Behavior. In: S. Katzenbeisser, E. Weippl, L.J. Camp, M. Volkamer, M. Reiter and X. Zhang, (Eds). *Trust and Trustworthy Computing*. Springer Berlin: Heidelberg. pp. 308-324
14. Lang, P.J. and Bradley, M.M. (2010). Emotion and the motivational brain. *Biological Psychology*, 84 (3), pp. 437-450.

15. Luo, X., Brody, R., Seazzu, A. and Burd, S. (2011) Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal*, 24 (3), pp. 1-8.

16. Papke, L.E. and Wooldridge, J.M. (1996) Econometric methods for fractional response variables with an application to 401(k) plan participation rates. *Journal of Applied Econometrics*, 11 (6), pp. 619-632.
17. Russell C. (2002). Security awareness implementing an effective strategy. Available at: http://rr.sans.org/aware/sec_aware.php. [Accessed 14 July 2021].
18. Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51 (3), pp. 576-586.
19. Volkamer, M., Renaud, K., & Reinheimer, B. (2016, May). TORPEDO: tooltip-powered phishing email detection. In *IFIP International Conference on ICT Systems Security and Privacy Protection* (pp. 161-175). Springer, Cham.
20. Voss BD. (2001). The ultimate defence of depth: security awareness in your company. Available at: http://rr.sans.org/aware/ultimate.php. [accessed 21 August 2021].
21. Zimmerman, J.D., (2016). *How slow thinking and acting can help cyber security*. Available: https://itsecuritycentral.teramind.com
22. https://www.splunk.com/en_us/form/top-50-security-threats.html