An Analysis of Phishing Bait

Olga Zielinska, Patrick Lawson, Dr. Christopher B. Mayhorn

Introduction

Phishing is a social engineering tactic designed to trick users into divulging sensitive personal information, such as one's social security or bank account numbers, through impersonation of a trustworthy third party.

There are many persuasion strategies that can be used in phishing attempts. Cialdini identified six broad persuasion principles, four of which have been found to be increasing in volume among phishing emails. We will focus on these four:

Commitment/ consistency: Completing an action you previously initiated.

Liking: Trust due to a prior interaction or familiarity, such as for a largely recognizable brand.

Authority: An authority figure mandating an action, with consequences for failing to comply.

Scarcity: A short and specific time frame to complete an action.

Here we investigate the success of these persuasion principles across two diverse populations: NCSU undergraduates, and participants recruited through Amazon Mechanical Turk (mTurk).

The 'Big 5' personality traits (neuroticism, extroversion, openness, agreeableness, conscientiousness) were also measured. Their potential contribution to the observed difference in phishing efficacy between the two populations is discussed.

Methods

58 participants were recruited through mTurk (mean age=35.8, SD=10.0), and 53 were recruited through NCSU's Experimetrix (mean age=18.8, SD=1.1).

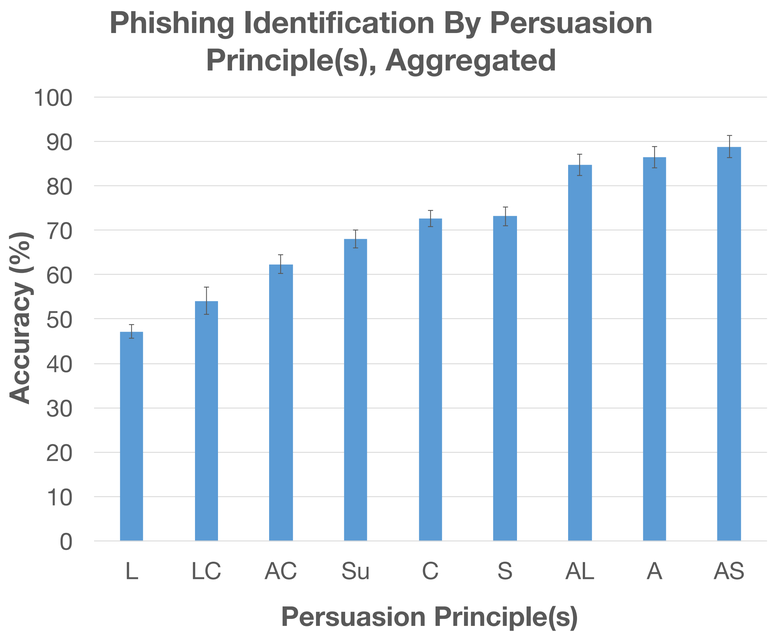
Participants performed an email identification task where they determined if 90 emails were legitimate or phishing attempts.

Participants also received a personality inventory (NEO-FFI-3) to assess the 'Big 5' personality traits. Impulse control was assessed by the impulse control subsection of the IPIP ABC5. Trusts was assessed by the trust subsection of the IPIP NEO PI-R.

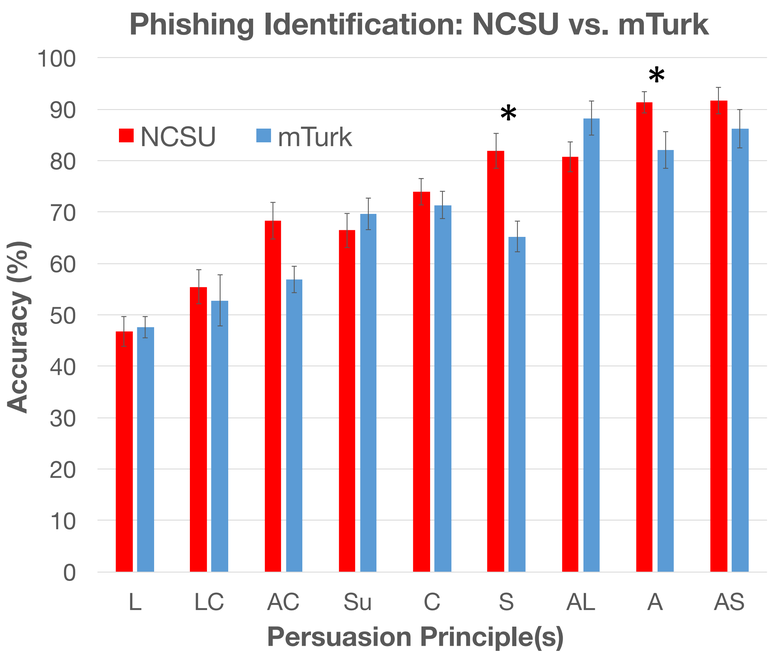
Results

Phishing Accuracy		Legitimate Accuracy *	
MTurk	NCSU	MTurk	NCSU
70.1%	73.0%	76.3%	63.9%

*Significant at p=.01



Key: L=Liking, C=Commitment/Consistency A=Authority S=Scarcity, Su=Super (3+ principles)



*Significant at p=.01

Variable	Higher Mean	p
Personality		
Impulse Control	mTurk	**.009***
Trust	mTurk	.146
Neuroticism	NCSU	**<.001***
Extroversion	NCSU	**<.001***
Openness	mTurk	**<.001***
Agreeableness	NCSU	**.002***
Conscientiousness	mTurk	**.001***
Demographics		
Age	mTurk	**<.001***

*Significant at p=.01

Discussion

Phishing emails using the Liking principle are especially effective. The Authority principle was most likely to be correctly labeled as a phishing attempt.

The NCSU population outperformed the mTurk population at identifying two types of phishing emails: Scarcity, and Authority. The NCSU population was not, however, significantly better at overall identification of phishing emails.

The mTurk population was significantly better at identifying legitimate emails than the NCSU population.

We found that the mTurk population was more likely to correctly identify legitimate emails than phishing emails- the reverse of the NCSU population. It is likely that the NCSU population's higher neuroticism contributed to this response pattern of erring on the side of safety. Similarly, higher impulse control likely contributed to the mTurk population's ability to resist the safety-conscious urge to flag legitimate emails as phishing attempts. Further analyses are underway to investigate these interactions.

These findings suggest that potential phishing interventions should account for population differences. For undergraduates, for instance, such an intervention might aim to diminish false positives. For older populations it would be wise to emphasize Scarcity and Authority principles, as this demographic appears especially susceptible to these persuasion principles.

References

- Cialdini, R. B. (1987). *Influence* (Vol. 3). A. Michel.
- Costa, P. T., & McCrae, R. R. (1992c). Neo PI-R professional manual.
- Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE.
- Zielinska, O. A., Welk, A. K., Mayhorn, C. B., & Murphy-Hill, E. (2016, September). A Temporal Analysis of Persuasion Principles in Phishing Emails. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 60, No. 1, pp. 765-769). SAGE Publications.