The roles of self-control, need for cognition, impulsivity and viewing time in deception detection using a realistic e-mail phishing task

Christina Rajagulasingam
School of Psychology
Western Sydney University
Sydney, Australia
christina.raj2@gmail.com

Jacqui Taylor
Department of Psychology
Bournemouth University
Poole, UK
jtaylor@bournemouth.ac.uk

***Abstract*— Phishing attacks manipulate people into giving away personal information, which can lead to detrimental consequences for individuals and organizations. This study aimed to understand how viewing time and traits relating to cognition influenced participant's ability to detect phishing e-mails. One hundred and twenty-two undergraduate students participated in an online survey which collected measures of impulsivity, need for cognition, self-control, time spent viewing e-mails and correct detection of phishing. There were no significant correlations between correct phishing detection and traits relating to cognition. However, viewing time was a significant factor where the more time individuals spent viewing e-mails the greater their accuracy in both perception of phishing e-mails and intention to correctly respond to phishing e-mails. The findings suggest that individual psychological differences have little influence on deception detection, supporting some of the previous research on the lack of effects relating to personality differences. In practical terms, individuals should be advised to spend more time viewing e-mails than they usually would, in order to increase their ability to detect phishing e-mails.**

Keywords—phishing, online deception, need for cognition, self-control, impulsivity, viewing time, persuasion

I. INTRODUCTION

One of the biggest cybersecurity challenges facing individuals and organisations is dealing with phishing attacks (1). Phishing involves impersonating a trustworthy source in order to convince individuals to give away personal information (2). Succumbing to phishing scams can lead to significant financial loss and affect internet user's confidence and wellbeing (3, 4). Therefore, being aware of the factors that influence an individual's susceptibility to online deception is useful for implementing cybersecurity training to counteract phishing attacks. Researchers have recently explored the impact of individual differences in personality on susceptibility to online deception. Usually, the Big Five Personality Measure (5) is employed and researchers have attempted to correlate deception susceptibility with each of the five personality factors (openness to experience, neuroticism, conscientiousness, extraversion and agreeableness). However, often there is mixed support or inconsistent results. For example, in one study (6) it was found that none of the personality factors significantly predicted whether there was an accurate response to a phishing attempt. While the factor 'openness to experience' was correlated positively with accuracy in detecting phishing e-mails in one study (3), but negatively in another (7). Modic et al. (8) found that only the 'neuroticism' factor was correlated with phishing detection; while the other four factors were not correlated at all. Our study aimed to explore whether cognitive factors may be a better predictor of phishing detection than personality factors, as cognitive factors are more clearly linked with the decision-making process. Drawing on theories of cognitive psychology, this study tested whether cognitive individual differences and viewing time influenced a person's susceptibility to phishing attacks.

A. Cognitive individual differences: need for cognition, self-control and level of impulsivity

The first objective of this study was to investigate if traits relating to cognition were correlated with or could be better predictors of phishing detection than personality factors. Our review of the literature identified three factors which affect decision-making: need for cognition, impulsivity, and self-control.

The construct of need for cognition is defined as the desire to seek an intellectual challenge (9). Leding & Antonio (10) found that higher need for cognition was associated with a higher ability to detect online deception. This may be due to an individual's desire to critically analyse e-mails and discern markers of phishing e-mails.

Self-control can be seen as the ability to regulate behaviour through systematic evaluation of the influences surrounding an individual (11). Self-control can help individuals be more aware of the strategies that the malicious user is using to try influence them. Modic and Lea (8) found a small effect of low self-control on increasing scam compliance. Similarly, Vishwanath (12) found a small effect for low self-control on increasing susceptibility to social media attacks. Reisig & Holtfreter (13) also found that low self-control led to higher victimization. It is therefore suggested that self-control will positively predict correct e-mail detection.

A somewhat opposite construct to self-control is impulsivity, which involves acting without thought (8). Survey-based studies of phishing have found a small to moderate negative effect for impulsivity on phishing detection (14, 2, 8). These were measured in the forms of sensation-seeking cognitive reflection, impulse control, urgency and premeditation. In a survey and field-based study by (15), they found that those individuals who were more impulsive were more likely to click on phishing e-mails. This suggests that impulsivity

978-1-6654-8029-1/21/$31.00 ©2021 IEEE

plays a role in phishing e-mail susceptibility with some e-mails being more appealing to certain individuals with higher impulsivity. Pattinson et al. (16) found that impulsivity marginally predicted incorrect detection of phishing and genuine e-mails when participants were uninformed in the field-based part of the study. However, they found a non-significant effect when they were informed in the survey and lab-based part of the study. Those high on impulsivity may also use more heuristic routes of processing information (11). Since a more intuitive approach can lead to more errors it is likely that impulsivity will impair an individual's decision-making skills, particularly in the ability to accurately perceive and respond to phishing. Thus, it seems that impulsivity has a negative effect on detection accuracy of e-mail detection.

B. Making decisions about the legitimacy of e-mails: time pressure

One of the main methods used in research investigating phishing susceptibility is to present individuals with target e-mails that are either real or phishing. To increase ecological validity, these e-mails are often explained as being in an individual's inbox which they must then sort through deciding which are real and which are phishing (17). In the real-world individuals are often busy and under time-pressure when dealing with e-mails. Therefore, the addition of time-pressure in these studies helps to replicate the cognitive load that individuals experience when they receive an email and need to make a quick decision as to whether to respond to it (11). The dual processing model posits that individuals will use heuristic, automatic and intuitive processing rather than rational thinking when under a greater cognitive load such as time-pressure (18; 9; 12). Using heuristic processing can lead to more errors in detection (18; 19). Since a more intuitive approach can lead to more errors it is likely that time-pressure will impair an individual's decision-making skills, particularly in the ability to accurately perceive and respond to phishing.

Scarcity has been proposed as a persuasion principle (20) and involves persuading individuals to behave or think in a certain way by suggesting that an item is limited in supply (2). Time-pressure is a particular form of scarcity and refers to the perception that the time available to complete a task is less than the time needed. In a study (21) evaluating the message content of real-world phishing e-mails, it was found that 57% included time restrictions. However, this percentage was less than the other persuasion principles proposed (20), such as authority, emotional appeals and rational appeals, in phishing e-mails. Jones et al. (14) found that individuals made fewer correct responses when there was time-pressure compared to when there was no time-pressure. Despite the importance of time-pressure, the research located so far does not record viewing time. Therefore, it is not known whether the accuracy in detecting deception is a function of time taken to view the target email. The only study located (22), which did collect this measure found that the more time spent viewing e-mails was correlated with greater accuracy in detecting phishing emails. Therefore, the recording of viewing time was included in this study.

C. Rationale

To address the two objectives of this research we investigated the correlations between e-mail viewing time, the traits of impulsivity, self-control and need for cognition and correct detection of deceptive e-mails. Ability to detect deception was measured using four measures: perception of phishing e-mails, perception of genuine e-mails, correct response to phishing e-mails and correct response to genuine e-mails. The following were hypothesised:

- H1 a, b, c, d: Need for cognition will be positively correlated to correct perception of phishing e-mails (a), correct perception of genuine e-mails (b), correct response to phishing e-mails (c), and correct response to genuine e-mails (d).
- H2 a, b, c, d: Self-control will be positively correlated to correct perception of phishing e-mails (a), correct perception of genuine e-mails (b), correct response to phishing e-mails (c), and correct response to genuine e-mails (d).
- H3 a, b, c, d: Impulsivity will be negatively correlated to correct perception of phishing e-mails (a), correct perception of genuine e-mails (b), correct response to phishing e-mails (c), and correct response to genuine e-mails (d).

  H4 a, b, c, d: Time spent viewing e-mails will be positively correlated to correct perception of phishing e-mails (a), correct perception of genuine e-mails (b), correct response to phishing e-mails (c), and correct response to genuine e-mails (d).

II. METHOD

A. Participants

One hundred and twenty two first-year psychology students with ages ranging from 18-50 years old (M = 20.97, SD = 4.34), were recruited from an Australian University; 122 were female (84%). Students participated for online course credit and gave consent online. Four cases were excluded as participants were under 18 years of age. Since the sample size was greater than 111 cases there was enough power to conduct correlation and regression analysis with four predictors (23). This strengthened the predictive power of the regression analysis on the population of interest (23). Using a priori G*Power analysis (24), this sample size was deemed acceptable (N > 85) to have adequate statistical power for hypothesis testing. Ethics approval was obtained from the University Human Research Ethics Committee.

B. Design

A correlational design was employed. Participants completed the online survey using the survey tool Qualtrics which collected measures of cognitive psychological differences and then presented a set of e-mail phishing detection tasks. The independent variables with their score range were: time spent viewing e-mails (1-14 seconds); need for cognition (0-72); self-control (13-65); and impulsivity (1-4). Two accuracy measures were collected from the phishing detection task developed in previous research (6), one

measuring cognitive perception and the other measuring behavioural response. To measure cognitive perception of e-mails, participants were asked to rate the likelihood of each e-mail being a phishing or genuine e-mail on a scale of 0-100 with 100% being definitely phishing and 0% being definitely not phishing. Average perceptions of whether an e-mail was phishing were computed for genuine e-mails and phishing e-mails. To measure their behaviour, after being presented the emails participants were asked what action they would take: trash e-mail, keep e-mail or seek more information. Correct response scores included the sum of the number of times an individual chose to trash or seek more information for phishing e-mails and the number of times they chose to keep or seek more information for genuine e-mails. Hence the dependent variables were Phishing Perception, Genuine Perception, Genuine Response and Phishing Response. Correct response scores included the sum of the number of times an individual chose to trash or seek more information for phishing e-mails and the number of times they chose to keep or seek more information for genuine e-mails. De-identified data were analysed using SPSS to conduct correlational and regression analysis.

C. Procedure

Participants were asked to sort through a student's university e-mail inbox. A total of 32 e-mails were used for the phishing detection task. Participants were randomly presented with 16 phishing e-mails and 16 genuine e-mails and answer two questions about each e-mail. Drawing from a previous study (21) it was found that 8 seconds for each e-mail was too short and 16 seconds was too long for viewing and responding to phishing e-mails. Thus all e-mails included a fixed time pressure variable and participants were told that they had a maximum of 14 seconds to view each e-mail but they were encouraged to move quickly through the task. Once participants completed the survey they were thanked for their time, debriefed and redirected to the SONA system to receive course credit. The entire survey took on average around 20 minutes.

D. Measures

Kleitman et al. (6) created a phishing detection task with a Cronbach's alpha of .80 which suggests good internal reliability. These e-mails were obtained and adapted from real experiences such as the authors own inbox or real examples from anti-phishing websites. While the original phishing detection task (6) consisted of 40 e-mails, 8 of these were excluded as participants in the pilot study noted that it was difficult to read the longer e-mails under time-pressure. Time was measured by recording the time elapsed between viewing the e-mail and clicking to go to the next section.

The 18-item Need for Cognition scale (25) has good internal reliability with a Cronbach's alpha greater than .85. The scale was used previously in an online deception study (10). The Brief Self-Control scale was developed by Holtfretter et al. (26). This measure was also used in a previous study of deception detection (8) which had moderate internal reliability with a Cronbach's alpha of of .70. The Brief Self-Control scale contains 13 items. To measure impulsivity, a subscale from the UPPS-P (Urgency, Premeditation, Perseverance, Sensation Seeking and Positive Urgency) Impulsive Behaviour scale was used (27). The 'lack of premeditation' subscale closely represents the definition of narrow impulsivity and was also used in a deception detection study (8). This scale has a Cronbach's alpha of .85, demonstrating reasonable internal reliability and contains four items.

III. RESULTS

The descriptive statistics for all measures are shown in Table I. The dependent variables are recorded in percentages and it can be seen that participants were slightly better at correctly responding to phishing e-mails (83%) than genuine e-mails (81%), while perception of genuine and phishing e-mails appear to be the same.

TABLE I. DESCRIPTIVE STATISTICS FOR EACH VARIABLE

	Minimum %	**Maximum %**	**Mean %**	**SD**
Need for cognition	18	59	34.76	7.35
Self-control	30	50	39.60	4.29
Impulsivity	1	3.25	1.89	0.52
Time spent viewing e-mails	1.57	14.00	7.43	3.13
Genuine e-mail response	25	100	81.14	17.27
Phishing e-mail response	0	100	83.32	17.12
Phishing e-mail perception	17.25	97.00	65.08	16.05
Genuine e-mail perception	16.8	97.06	65.69	16.50

For phishing e-mails, on average, participants responded by trashing the e-mail in 56% of the cases, keeping the e-mail for 16%, and seeking more information 25% of the time. For genuine e-mail items, the corresponding averages were 19%, 49%, and 32% respectively. Correlations between the predictors and dependent variables are shown in Table II. The positive correlation between viewing time was significant for all dependent variables, indicating that the more time spent deciding whether an e-mail was phishing or genuine the better the accuracy of that judgment. This provides support for the hypotheses H4 a, b, c and d that viewing time significantly relates to all levels of accuracy across the four measures. None of the cognitive traits were significant at the 5% level, therefore there is no support for the hypotheses H1, H2 or H3. However, the level of self-control approached significance in correlating with the correct response to phishing e-mails.

TABLE II. CORRELATIONS BETWEEN VARIABLES

	Phishing e-mail perception	**Genuine e-mail perception**	**Genuine e-mail correct response**	**Phishing e-mail correct response**
Need for cognition	-.126	-.145	-.092	-.106
Self-control	-.111	-.063	.028	**-.169***
Impulsivity	.021	-.067	-.097	-.010
View Time	**.284****	**.266****	**.289****	**.247****

[a.] *** p < .001, ** p < .05, * p < .1

Four regression analyses were conducted and the standardised regression coefficients (β) and the significance levels are displayed in Tables III and IV. From these tables, it

can be seen that across all four regression models, only viewing time significantly predicted the correct detection of genuine and phishing e-mails. This provides further support for the hypotheses H4 a, b, c and d that viewing time significantly predicts levels of accuracy across the four measures. The factor self-control approached significance in predicting phishing detection, however as it exceeded the alpha level set at 5% it will need further study to test the hypotheses.

TABLE III. HIERARCHICAL MULTIPLE REGRESSION OF ACCURACY IN PERCEPTION OF PHISHING AND GENUINE E-MAILS

	Phishing Perception			**Genuine Perception**		
	β	***t***	***p***	***β***	***t***	***p***
Need for cognition	-.095	-1.042	.300	-.128	-1.383	.169
Self-control	-.116	-1.280	.203	-.060	-.658	.512
Impulsivity	.062	.670	.504	.042	-.452	.652
View time	**.279**	**3.038**	**.003****	**.243**	**2.63**	**.010****

[b.] *** p < .001, ** p < .05, * p < .1

TABLE IV. HIERARCHICAL MULTIPLE REGRESSION OF ACCURACY IN DETECTION OF PHISHING AND GENUINE E-MAILS

	Phishing Detection			**Genuine Detection**		
	β	***t***	***p***	***β***	***t***	***p***
Need for cognition	-.088	-.960	.339	-.068	-.741	.460
Self-control	**-.172**	**-1.893**	**.061***	.039	.429	.669
Impulsivity	.031	.339	.735	-.071	-.760	.449
View time	**.236**	**2.568**	**.012****	**.273**	**2.955**	**.004*****

[c.] *** p < .001, ** p < .05, * p < .1

IV. DISCUSSION

The main aim of this study was to investigate the relationship between cognitive factors and viewing time on detecting phishing e-mails. To achieve this aim, the study had two objectives: to revise the methods used in previous research in an attempt to introduce more ecological validity, and to examine the cognitive dimensions of personality (rather than the five personality factors used in previous research).

The first objective was to design a more ecologically valid study by including an element of time pressure, something which is often present in the real world when deciding whether to act upon e-mails. This was achieved through partially replicating a previous study (6) with the addition of time-pressure. The results from this study provide support for hypotheses H4a, b, c and d, that the more time spent viewing e-mails predicted correct detection of phishing and genuine e-mails. Also, the more time spent viewing e-mails, the more accurate were individuals' perceptions of whether e-mails were genuine or phishing. Time spent viewing e-mails was a significant predictor in the regression analyses and appears to play an important role in decision-making and can be an indication of how individuals process information, as they may move away from intuitive decision-making to more rational decision-making (18; 9; 12). We suggest that incorporating time-pressure in future phishing tasks may help reflect an individual's real-life experiences when making decisions as to whether believe of not a potentially phishing e-mail, increasing the ecological validity of the findings.

The second objective was to investigate psychological factors, however instead of using the Big Five Factor Model of personality as used by other researchers (e.g. 6), our study collected measures of individual's need for cognition, impulsivity and self-control. This would test whether traits relating to cognition were correlated with or could be better predictors of deception detection, than personality factors. However, there were no significant correlations and a regression analysis revealed that no predictors reached significance. Our findings are similar to previous research (6), which found negligible relationships between individual psychological differences and accuracy in detection of phishing.

An understanding of the factors influencing human susceptibility to online deception is necessary to identify how we can reduce this susceptibility. Since individual psychological differences seem to play no significant role in online deception this could mean that education programs about online fraud will be equally effective in assisting individuals regardless of their personality type. Since time played an important role in phishing detection, training should highlight to users to spend more time viewing e-mails, even when under time-pressure. This is supported by Cialdini's (20) persuasion principle of scarcity which proposes that individuals may overvalue an item if it is perceived as scarce (20). Even when time seems scarce, it is important that individuals can take extra time to make better decisions.

The two main strengths of this study are that it attempted to be more ecologically valid than previous studies. The key limitations are that the composition of the sample was skewed towards young, educated females and further work is needed with a sample more representative of the general population. Further research also needs to measure accuracy as a function of time to help identify the optimal amount of time individuals should spend viewing e-mails to achieve the best accuracy in detecting deception. Finally, the statistical analysis showed that one of the variables (self-control) almost reached significance in relating to and predicting phishing detection. Therefore, self-control could be investigated in further research.

In conclusion, viewing time appears to be the most important factor when detecting phishing and psychological factors may play a negligible role in individual's susceptibility to phishing. This research highlights the need to develop studies which are more realistic of an individual's everyday experience of online deception, through the addition of time-pressure.

REFERENCES

[1] F. Salahdine, & N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, 11(4), pp. 89, 2019.

[2] P. Lawson, C. J. Pearson, A. Crowson, & C. B. Mayhorn, "E-mail phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy," *Applied Ergonomics*, 86, 103084, 2020.

[3] I. Alseadoon, M. F. I. Othman, & T. Chan, "What is the influence of users' characteristics on their ability to detect phishing e-mails?", *Proceedings of the 1st International Conference on Communication and Computer Engineering*; Malacca, Malaysia: Springer, 2015, pp. 949–62.

[4] M. Jakobsson, & S. Myers, (Eds.), *Phishing and Countermeasures: Understanding the increasing problem of electronic identity theft.* Chichester: John Wiley & Sons, 2006.

[5] O. P. John, & S. Srivastava, "The Big-Five trait taxonomy: History, measurement, and theoretical perspectives", in L. A. Pervin & O. P. John Eds., *Handbook of Personality: Theory and Research* (Vol. 2), New York: Guilford Press, 1999, pp. 102–138.

[6] S. Kleitman, M. K. H. Law & J. Kay, "It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling," *PloS ONE*, 13(10), e0205089, 2018. https://doi.org/10.1371/journal.pone.0205089

[7] T. Halevi, N. Memon, & O. Nov, (2015, January), "Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks," *Social Science Research Network (SSRN) Electronic Journal*. Available: http://dx.doi.org/10.2139/ssrn.2544742

[8] D. Modic, and S. E. G. Lea, (2012, September), "How Neurotic are Scam Victims, Really? The Big Five and Internet Scams," ," *Social Science Research Network (SSRN)*, Available: http://dx.doi.org/10.2139/ssrn.2448130

[9] R. E. Petty, & J. T. Cacioppo, "The elaboration likelihood model of persuasion," in L. Berkowitz (Ed.), *Advances in Experimental Social Psychology* (vol. 19), pp. 123-205. San Diego: Academic Press, 1986.

[10] J. K. Leding, & L. Antonio, "Need for cognition and discrepancy detection in the misinformation effect," *Journal of Cognitive Psychology*, 31(4), pp. 409-415, 2019.

[11] E. J. Williams, A. Beardmore, & A. N. Joinson, "Individual differences in susceptibility to online influence: A theoretical review," *Computers in Human Behavior*, 72(C), pp.412-421, 2017.

[12] A. Vishwanath, "Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack," *Journal of Computer Mediated Communication*, 20(5), pp.570-584, 2015.

[13] M. D. Reisig, & K. Holtfreter, "Shopping fraud victimization among the elderly," *Journal of Financial Crime*, 20(3), pp. 324–337, 2013.

[14] H.S. Jones, N. T. John, N. Race, & T. Harrison, "E-mail fraud: The search for psychological predictors of susceptibility," *PLoS ONE*, 14(1), e0209684, 2019. https://doi.org/10.1371/journal.pone.0209684

[15] G. D. Moody, D. F. Galletta, & K. D. Brian, "Which phish get caught? an exploratory study of individuals′ susceptibility to phishing," *European Journal of Information Systems*, 26(6), pp. 564-584, 2017.

[16] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, A., & M. Butavicius, "Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, 20(1), pp. 18-28, 2012.

[17] Y. Oh, & T. Obi, "Evaluation of field phishing study setup method," *International Journal of Information and Network Security*, 1(4), pp. 235, 2012.

[18] S. Goel, K. Williams, & E. Dincelli, "Got phished? internet security and human vulnerability," *Journal of the Association for Information Systems*, 18(1), pp. 22-44, 2017.

[19] Z. Xu, & W. Zhang, "Victimized by phishing: A heuristic-systematic perspective. *Journal of Internet Banking and Commerce*, 17(3), pp. 1-16, 2012.

[20] R. B. Cialdini, *Influence: The Psychology of Persuasion* (volume 3). Port Harcourt: A. Michel, 1987.

[21] D. Kim & J. H. Kim, "Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis," *Online Information Review*, 37(6), pp. 835-850, 2013.

[22] J. Wang, Y. Li, & H. R. Rao, "Overconfidence in phishing e-mail detection," *Journal of the Association for Information Systems*, 17(11), pp. 759-783, 2016.

[23] B. G. Tabachnick, & L. S. Fidell, L. S. *Using Multivariate Statistics* (6th ed.). Boston: Pearson, 2013.

[24] F. Faul, E. Erdfelder, A. G. Lang, & A. Buchner, "G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences," *Behavior Research Methods*, 39(2), pp. 175-191, 2007.

[25] J. T. Cacioppo, and R. E. Petty, "The need for cognition," *Journal of Personality and Social Psychology*, 42, pp. 116–131, 1982.

[26] K. Holtfreter, M. D. Reisig, N. Leeper Piquero, & A. R. Piquero, "Low self-control and fraud: offending, victimization and their overlap,"*Criminal Justice and Behavior*, 37(2), pp. 188-203, 2010.

[27] S. P. Whiteside, & D. R. Lynam, "The five factor model and impulsivity: Using a structural model of personality to understand impulsivity," *Personality and Individual Differences*, *30*(4), pp. 669-689, 2001.