Understanding Susceptibility to Phishing Emails: Assessing the Impact of Individual Differences and Culture

M. Butavicius[1], K. Parsons[1], M. Pattinson[2], A. McCormac[1], D. Calic[1] and M. Lillie[2]

[1]Defence Science and Technology Group, Edinburgh, South Australia
[2]University of Adelaide, South Australia
e-mail: {marcus.butavicius; kathryn.parsons; agata.mccormac
dragana.calic}@dst.defence.gov.au; {malcolm.pattinson@;
meredith.lillie@student.}adelaide.edu.au

Abstract

In a lab-based empirical study, we examined how individual differences and an aspect of national culture impacted on participants' responses to phishing and spear-phishing emails. Results showed that the strongest predictor of the participants' ability to detect these malicious emails was cultural orientation towards the needs of the individual rather than the needs of society. For both types of emails, there was also a positive association between self-reported information security awareness and detection ability. Impulsivity in decision making predicted poorer detection of phishing emails, but not spear-phishing emails, and different personality traits predicted detection ability for the two email types.

Keywords

Cyber Security, Phishing, Spear-phishing Empirical Study, Culture, Individual Differences

1. Introduction

Phishing email attacks use emails that appear to be from reputable sources with the intention of influencing the recipient's behaviour for malicious purposes. This involves persuading the user into replying to the email, clicking on a link or opening an attachment in order for the phisher to acquire either personal information or access to the recipients' computer or system for malicious purposes (Butavicius *et al.* 2015). It is estimated that in 2016 there were at least 255,065 unique phishing attacks (APWG Web Site, 2017) and 85% of organisations reported falling victim to at least one of these attacks (Wombat Web Site, 2017). There has also been an increase in the sophistication of these attacks towards a variant known as spear-phishing. In comparison with phishing emails, which are generic and sent en masse, spear-phishing emails are crafted to appear relevant to recipients through the inclusion of background information, and so are targeted towards a smaller number of users. There has been an estimated 22% increase in spear-phishing attacks from 2015 to 2016 (Wombat Web Site, 2017) and more recently, 84% of 300 companies surveyed reported falling victim to spear-phishing attacks (Cloudmark Web Site, 2017).

Given the risks posed by these cyber attacks, it is important to investigate why individuals fall victim to them in order to develop effective, validated strategies to protect sensitive personal or organisational information. These strategies may be implemented in control mechanisms such as training and awareness programs or enforced policy. In what follows, we provide a brief literature review of a selection of variables that have been linked to phishing susceptibility including personality traits, decision making styles, culture and Information Security Awareness (ISA). In summary, although there are significant findings in the literature with regards to these predictive variables, there are inconsistencies in the patterns of results between different studies and no previous study has attempted to examine the relative effects of these variables in a single design. We then present a multivariate study on how phishing detection performance relates to these variables.

1.1. Personality and gender

Our review of the literature found contradictory results regarding the relationship between the Big Five personality dimensions, gender and phishing email detection. Sheng *et al.* (2010), Halevi *et al.* (2013) and Jagatic *et al.* (2007) found that women were more susceptible to phishing emails than men. Halevi *et al.* (2013) found a positive correlation between levels of neuroticism and phishing susceptibility in only the women taking part in the experiment. Vishwanath (2015) also found an association between phishing susceptibility and neuroticism (albeit an indirect relationship via the intermediary variable of email habits). However, the effect was evident for both genders and they also found evidence for an association between phishing email susceptibility and conscientiousness. In contrast to their previous study, Halevi *et al.* (2015) found that phishing susceptibility was associated with higher levels of conscientiousness rather than neuroticism while Pattinson *et al.* (2012) found that the ability to correctly identify an email as phishing was positively linked to only the traits of openness and extraversion.

Based on an extensive literature review, Uebelacker and Quiel (2014) proposed a Social Engineering Personality Framework (SEPF) which posits that high levels of agreeableness are associated with greater susceptibility to the social engineering found in phishing emails because "the motivational system of agreeable persons consists of pursuing communal goals and seeking interpersonal harmony" (p.28). In a phishing email, the attacker presents requests to the recipient where the fulfilment of these requests allows these communal goals to be achieved and interpersonal harmony to be maintained. They argue that gender differences in phishing susceptibility may be due to the higher levels of agreeableness found in women (Costa Jr., *et al.* 2001). However, to date there is no direct empirical evidence to support this claim of the SEPF. In fact, Pattinson *et al.* (2012) found that participants with higher levels of agreeableness were more likely to incorrectly classify a genuine email as phishing. However, agreeableness was not found to affect classification of phishing emails. This suggests that people who score more highly on agreeableness may be more cautious (i.e., rule following) with emails, however this may not translate to better performance when detecting phishing.

1.2. Information Security Awareness (ISA)

Prior research has shown that higher levels of ISA are associated with better phishing detection (Parsons *et al.*, 2017). It may be that the somewhat counterintuitive role of agreeableness in phishing detection highlighted above may be due to its association with ISA. Pattinson *et al.* (2015) and McCormac *et al.* (2017) found that agreeableness was positively associated with ISA, measured using the Human Aspects of Information Security Questionnaire (HAIS-Q). While agreeableness is linked to cooperation, compliance and dependability, and therefore might be construed as implying greater compliance with requests in emails, these qualities might, on the other hand, mean greater compliance with an organisation's information security policies, rules and guidelines, and in turn, greater knowledge of, and effort to resist, phishing attacks (even when the email is genuine). This is consistent with Salgado *et al.'s* (2002) finding that low levels of agreeableness actually predict deviant workplace behaviour.

1.3. Cognitive impulsivity

Previous research has also examined the impact of cognitive impulsivity, as measured by the Cognitive Reflection Test (CRT: Frederick, 2005) on phishing email detection, again yielding contradictory results. The CRT measures an individual's tendency to overcome an intuitive, but incorrect, response to a problem and to engage in more analytic decision making. Parsons *et al.* (2013) and Butavicius *et al.* (2015) found that low CRT scores were associated with poorer performance in the detection of phishing emails. However, Kumaraguru *et al.* (2007) found that users with higher CRT scores were more susceptible to phishing emails when the email purports to come from a company with which the recipient does not have an existing account.

1.4. National Culture

Previous literature has suggested that cultural differences may impact an individual's susceptibility to requests such as those found in phishing emails. In these studies, the predominant framework for examining culture has been the six dimensions of national culture developed by Hofstede (1980) with particular focus on the Individualism dimension. Countries with high levels of Individualism are characterised as preferring loosely-knit social frameworks whereby an individual is more likely to focus on the needs of themselves and their immediate family members. Personal goals are given higher priority than group goals. In contrast, countries low on this dimension, have tightly-knit social frameworks whereby individuals are more focused on the needs of the wider group than their own personal needs (Hofstede, 1980). Individualism may predict how a user responds to certain email requests because someone with a focus on the group's needs may be more inclined to comply with a request in order to maintain interpersonal harmony.

In a study on intended compliance with a request to take part in a survey, Cialdini *et al.* (1999) found significant differences between participants from two different cultures - the United States and Poland - which are, respectively, high (91) and low (60) on the 100 point Individualism scale (Geert Hofstede Web Site, 2017). Flores *et al.* (2014) also found that certain predictors of phishing susceptibility differed between users from Sweden, USA and India. In particular, the correlation between receiving formal ISA training and resistance to phishing was strongest for the American and weakest for the Indian participants. The relative strengths of these correlations lines up with Individualism dimension values for the three countries with USA, at 91, highest on the scale and India, at 48, lowest. However, Tembe *et al.* (2014) found significant differences in self-reported phishing susceptibility and the perception of factors related to phishing attacks between American, Indian and Chinese samples that were not consistent with any of the Hofstede dimensions.

1.5. Our study

To examine these issues further, we conducted a lab-based study examining the role of individual differences (i.e., age, gender, personality traits, cognitive impulsivity, and ISA for emails) and culture (i.e., as measured by Hofstede's Individualism dimension) on phishing and spear-phishing email detection. The literature identifies several correlations between these dependent variables such as the relationship between age and ISA (Pattinson *et al.*, 2015), age, gender and race and cognitive impulsivity (Albaity *et al.*, 2013) and culture and personality (McCrae *et al.*, 2005). In light of these interdependencies, we used a linear multiple regression model to estimate the relative contribution of these variables to the detection of malicious emails. We investigated participants' ability to detect phishing emails as well as spear-phishing emails given the increase in the latter type of cyber attack (Wombat Web Site, 2017). In addition, rather than select cohorts from a small number of different countries as per the cross-national studies cited above, we used a sample of students from an Australian university enrolled in courses with a high proportion of international students from a larger number of different countries.

2. Methodology

2.1. Participants

We recruited 121 students via email from a large South Australian university. These students were enrolled in undergraduate and postgraduate courses including finance, international business, accounting, management, marketing and entrepreneurship. Most of the participants were female (68%), all were 18 years or older and the majority were between 20-29 years of age (62%). Participants came from a wide variety of cultural backgrounds and this is consistent with the high number of international students enrolled in the courses targeted. Approximately half of the participants (60) had undertaken most of their tertiary education in Australia. Only 34% of participants considered Australia to be their country of origin and in total there were 23 different countries represented in this field from Europe, the Middle East, the US, Asia, South America and Africa. Twenty six percent of the participants were born in non-English speaking countries and forty four percent of the participants primarily spoke a language other than English at home.

2.2. Emails

The stimuli consisted of 12 emails which were either phishing, spear-phishing or genuine. The four phishing emails were based on actual emails provided by IT security staff at the associated university that, based on user and system monitoring, were judged as successful phishing attacks. The four spear-phishing and four genuine emails were based on non-malicious emails received by students of the university with the only difference being the URL type – a legitimate address for the genuine emails but an illegitimate address (derived from some of the phishing emails collected) for the spear-phishing emails. The emails were modified such that the link in the email was a non-specific phrase that did not disclose the URL (e.g., "Click here") and hover functionality for displaying the underlying URL was enabled in the experiment. Accordingly, participants were advised of this hover functionality, both verbally and in writing, at the start of the experiment.

To control for the effects of social engineering, we balanced email type (spear-phishing, phishing, and genuine) across four types of social engineering strategies derived from Cialdini's (2007) social influence framework. This was done to ensure that what we were testing was not the influence of the social engineering strategies themselves (which occur naturally in all the email types we were examining), but rather the type of email (e.g., spear-phishing, phishing and genuine) and their inherent qualities. Such qualities include the degree and accuracy of background information present in the email, personalisation, appropriate logo use, consistency, grammar and spelling irregularities (Parsons *et al.*, 2015). For each email, we modified the text to implement one of three different types of social engineering strategies (Authority, Social Proof and Scarcity) and one control condition with no strategy.

2.3. Procedure

A maximum of 20 participants were allocated to separate lab-based sessions. Each student completed the experiment on Qualtrics^{TM} independently and simultaneously using an assigned desktop computer. Participants were not told explicitly that they were taking part on an experiment on phishing detection to avoid the priming effect that has been shown to artificially improve performance on a phishing task (Parsons *et al.*, 2013). Participants completed a set of demographic questions relating to age range, gender, language spoken at home, country of origin and the country most of their studies had been completed in. Participants were then shown each email individually and were asked to provide a 'Link Safety' judgement (i.e., 'It is okay to click on the link in this email') on a five point Likert scale (where "1" = strongly disagree and "5" = strongly agree). The emails were presented in a different, random order in each session. Participants then completed the Human Aspects of Information Security Questionnaire (HAIS-Q: Parsons *et al.*, 2017), the Ten-Item Personality Inventory (TIPI: Gosling *et al.*, 2003) and the Cognitive Reflection Test (CRT: Frederick, 2005).

3. Results

Cultural information for respondents was derived from the self-reported demographic data. We assigned an *Individualism* score to each participant based on the Hofstede data averages normalised to a 100 point scale for their nominated country of origin (Geert Hofstede Web Site, 2017). We also calculated a *HAIS-Q Email* score for each participant based only on responses to email focus area questions within the HAIS-Q.

We recoded the ‘Link Safety’ results into a binary variable for accuracy (i.e., correct or incorrect). For genuine emails, scores of 4 (‘agree’) and 5 (‘strongly agree’) were categorised as correct while all other responses were categorised as incorrect. For phishing and spear-phishing emails, scores of 1 (‘strongly disagree’) and 2 (‘disagree’) were categorised as correct and all other responses categorised as incorrect. We applied Signal Detection Theory (SDT) to calculate *A'* and *B''* which are non-parametric measures of *discrimination* and *bias*, respectively (Stanislaw & Todorov, 1999). We consider the ‘signal’ to be the malicious emails (i.e., phishing and spear-phishing) and the ‘noise’ to be the genuine emails (Swets, 1964). *Discrimination* measures how well a user can distinguish between a malicious email and a genuine email. A score of 1 for *A'* means that discrimination ability is perfect while a score of 0.5 means that fraudulent emails cannot be distinguished from genuine emails. *Bias* measures a user’s tendency to respond one way or the other, i.e., their bias towards saying an email is malicious or that it is genuine. *B''* scores can range from -1 (i.e., everything is classified as malicious) to 1 (i.e., everything is classified as genuine) while zero indicates no response bias.

We performed separate multiple regression analyses using the discrimination and bias scores as the dependent variables for the phishing and spear-phishing conditions. For all four analyses, we used the same independent variables: age range, gender, Extraversion, Agreeableness, Conscientiousness, Emotional Stability, Openness to Experience, CRT, HAIS-Q Email and Individualism (see *Appendix A* for descriptive statistics and correlations). In all multiple regressions, there were no signs of multicollinearity with Variance Inflation Factors (VIF) for all independent variables less than 2. In addition, there was no evidence of outliers skewing the data set with Cook’s distances below 1 for all independent variables.

None of the regression analyses with *B'* as the dependent variable were significant and the Adjusted R squared values (R^2_{adj}) were only .045 and .025 for phishing and spear-phishing bias, respectively. The regression models for *A'* accounted for 27% of the variation in phishing ($R^2_{adj} = .266$, F(10,100) = 4.619, $p < .001$) and 51% ($R^2_{adj} = .505$, F(10,80) = 9.151, $p < .001$) for spear-phishing discrimination, respectively. Further details on these regression analyses for A’ can be found in Table 1. For phishing emails, there were significant contributions from Individualism, HAIS-Q Email, CRT and Agreeableness. For spear-phishing emails, there were significant contributions from Individualism, HAIS-Q Email, and Emotional Stability.

	Variable	*B*	*SE B*	$\beta_{\text{Standardised}}$	*t*	*p*
Phishing	Age	-.002	.032	-.005	-.055	.956
	Gender	-.003	.054	-.006	-.060	.953
	Extraversion	-.006	.009	-.067	-.748	.456
	Agreeableness	**.030**	**.013**	**.229**	**2.339**	**.022**
	Conscientiousness	-.003	.011	-.030	-.304	.762
	Emotional Stability	.000	.009	-.005	-.047	.963
	Openness to Experience	-.004	.012	-.032	-.358	.721
	Cognitive Reflection Test	**.059**	**.027**	**.211**	**2.182**	**.032**
	HAIS-Q Email	**.039**	**.016**	**.239**	**2.540**	**.013**
	Individualism	**.002**	**.001**	**.298**	**3.155**	**.002**
Spear-phishing	Age	.003	.035	.008	.093	.926
	Gender	.006	.062	.009	.095	.925
	Extraversion	-.006	.011	-.046	-.561	.577
	Agreeableness	.022	.014	.142	1.565	.122
	Conscientiousness	.001	.012	.009	.095	.924
	Emotional Stability	**-.022**	**.011**	**-.188**	**-2.002**	**.049**
	Openness to Experience	.008	.014	.047	.562	.576
	Cognitive Reflection Test	.042	.030	.127	1.367	.176
	HAIS-Q Email	**.053**	**.018**	**.268**	**2.974**	**.004**
	Individualism	**.005**	**.001**	**.521**	**5.881**	**<.001**

Table 1: Summary of multiple regression analyses for discrimination of phishing and spear-phishing emails (N=121)

4. Discussion and Conclusions

In terms of how well people can discriminate between a genuine and a malicious email, our results showed that the strongest predictors were variables based on national culture and ISA. For both phishing and spear-phishing, higher levels of ISA for emails (i.e., better knowledge, attitude and behaviour specific to email use) were associated with better detection of these deceitful emails. In addition, participants from countries associated with higher levels of Individualism, were better at discerning malicious emails, and this was found to be the strongest predictor. This may be attributable to low levels of Individualism being linked to a desire to maintain group harmony. This, in turn, results in an increased drive to respond to requests from others, including those requests in malicious emails.

Interestingly, there were differences between the factors that predicted phishing and spear-phishing detection. Lower levels of cognitive impulsivity and high levels of agreeableness were only linked to better discrimination of phishing emails. Higher levels of neuroticism were only associated with better discrimination of spear-phishing emails. This may be due to the link between neuroticism and compulsive thinking about possible threats (Nolan *et al.* 1978). In other words, heightened rumination may improve our ability to detect actual spear-phishing threats. Such rumination may be limited to spear-phishing emails due to the highly personalised nature of such cyber attacks where an individual may feel singled out. This could be investigated in further studies by the use of more detailed personality metrics than the Ten-Item Personality Inventory used in the present study.

There are also some limitations of our study that should be noted. We only used an approximation of cultural orientation derived from self-reported demographic data. Cialdini *et al.* (1999) found that the influence of cultural-based orientation on responding to requests was stronger when an individual's specific orientation was measured directly. Therefore, future studies should focus on direct measurement of an individual's tendencies, i.e., to investigate psychological attributes linked to the consideration of the self versus community. Another limitation of our study was the sample we used. The lab-based methodology meant we had a relatively small sample size which was limited to university students. Future research should seek to replicate these findings with a significantly larger on-line empirical study from a more diverse population. A more diverse sample may reveal findings not present in our study such as age and gender effects.

Despite these limitations, this study provides an insight into how individual differences and culture may affect the ability to discriminate between genuine and malicious emails. In particular, the prominence of a cultural factor over individual differences in predicting an individual's phishing susceptibility in our study suggests that future research should take a more holistic approach to examining the factors that influence our security-related behaviours.

5. References

Albaity, M., Rahman, M. and Shahidul. I. (2014), "Cognitive reflection test and behavioural biases in Malaysia", *Judgment and Decision Making,* Vol. 9, No. 2, pp149-151.

APWG Web Site (2017), "Global Phishing Survey: Trends and Domain Name Use in 2016", http://docs.apwg.org/reports/APWG_Global_Phishing_Report_2015-2016.pdf, (Accessed 7 July 2017)

Butavicius, M., Parsons, K., Pattinson, M. and McCormac, A. (2015), "Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails", In Burstein, F. et al (Eds.) *Proceedings of Australian Conference of Information Systems*, ISBN: 978-0-646-95337-3.

Cialdini, R.B. (2007*), Influence: The Psychology of Persuasion (Revised ed.),* HarperCollins, New York, ISBN: 978-0-0612-4189-5.

Cloudmark Web Site (2017), "Cloudmark survey conducted by Vanson Bourne", https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises, (Accessed 7 July 2017)

Costa, P.T., and McCrae, R.R. (1992). *NEO PI-R Professional Manual*. Odessa, Florida, ISBN: 978-9-9958-3346-6.

Flores, W.R., Holm, H., Nohlberg, M., and Ekstedt., M. (2014), "Investigating personal characteristics of phishing and the effect of national culture", *Information & Computer Security,* Vol. 23, No. 2, pp178-199.

Frederick, S. (2005), "Cognitive Reflection and Decision Making," *Journal of Economic Perspectives,* Vol. 16, No. 4, pp25-42.

Geert Hofstede Web Site (2017), "Dimension Data Matrix", http://geerthofstede.com/research-and-vsm/dimension-data-matrix, (Accessed 12 August 2017)

Gosling, S.D., Rentfrow, P.J., and Swann Jr., W.B. (2003), "A very brief measure of the Big-Five personality domains", *Journal of Research in Personality*, Vol 37, pp504-528.

Wombat Web Site (2017), "State of the Phish 2016", https://info.wombatsecurity.com/state-of-the-phish, (Accessed 7 July 2017)

Halevi, T., Lewis, J., and Memon, N. (2013), "A pilot study of cyber security and privacy related behaviour and personality traits", in Schwabe, D. et al. (Ed.) *WWW '13 Companion Proceedings of the 22nd International Conference on World Wide Web Companion*, ACM, NY, ISBN: 978-1-4503-2038-2.

Halevi, T., Memon, N., and Nov, O. (2015), "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks," https:/ssrn.com/abstract=2544742, (Accessed 2 July 2015)

Hofstede, G. (1980), *Culture's consequences: International differences in work-related values (Abridged),* Beverly Hills, CA, Sage, ISBN: 978-87-629-0377-7.

Jagatic, T., Johnson, N., Jakobssen, M., and Menczer, F. (2007), "Social Phishing," *Communications of the ACM,* Vol. 50, No. 10, ISSN: 0001-0782.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L.F., and Hong, J. (2007), "Getting users to pay attention to anti-phishing education: evaluation of retention and transfer", in Cronor, L.F. (Ed.) *eCrime '07: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit,* Pennsylvania, USA, ISBN: 978-1-59593-939-5.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017), "Individual differences and Information Security Awareness", *Computers in Human Behaviour,* Vol. 69, pp151-156.

McCrae, R.R., Terracciano, A., and 79 Members of the Personality Profiles of Culture Project (2005), "Personality profiles of culture: Aggregate personality traits", *Journal of Personality and Social Psychology,* Vol. 89, No. 3, pp407-425.

Nolan, S.A., Roberts, J.E., and Gotlib, I.H. (1978), "Neuroticism and ruminative response style as predictors of change in depressive symptomology" *Cognitive Therapy and Research*, Vol. 22, No. 5, pp445-455.

Parsons, K., Butavicius, M., Pattinson, M., McCormac, A., Calic, D. and Jerram, C., (2015), "Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?", In Burstein, F. et al (Eds.) *Proceedings of Australian Conference of Information Systems*, ISBN: 978-0-646-95337-3.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, (2017), The "Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies", *Computers & Security,* Vol. 66, pp40-51.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., and Jerram, C. (2013), "Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails," in Janczewski, L.J. et al. (Eds.) *Security and Privacy Protection in Information Processing Systems-IFIP Advances in Information and Communication Technology,* Springer, Berlin.

Pattinson, M., Butavicius, M, Parsons, K., McCormac, A., and Calic, D. (2015), "Factors that influence Information Security Behaviour: An Australian web-based study". In Tryfonas, T. & Askoxylakis, I. (Eds.). *Proceedings of Third International Conference on Human Aspects of Information Security, Privacy and Trust (HAS 2015),* Los Angeles, USA, ISBN: 978-3-319-20375-1.

Pattinson, M., Jerram, C., Parsons, K.M., McCormac, A., and Butavicius, M.A. (2012). Why do some people manage phishing emails better than others? *Information Management & Computer Security,* Vol. 20, No. 1, pp18-28.

Salgado, J.F. (2002), "The big five personality dimensions and counterproductive behaviors", *International Journal of Selection and Assessment*, Vol. 10, No. 1-2, pp117-125.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., and Downs, J. (2010), "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions", in Mynatt et al. (Eds.) *Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI '10),* Atlanta, GA, USA, ISBN: 978-1-60558-929-9.

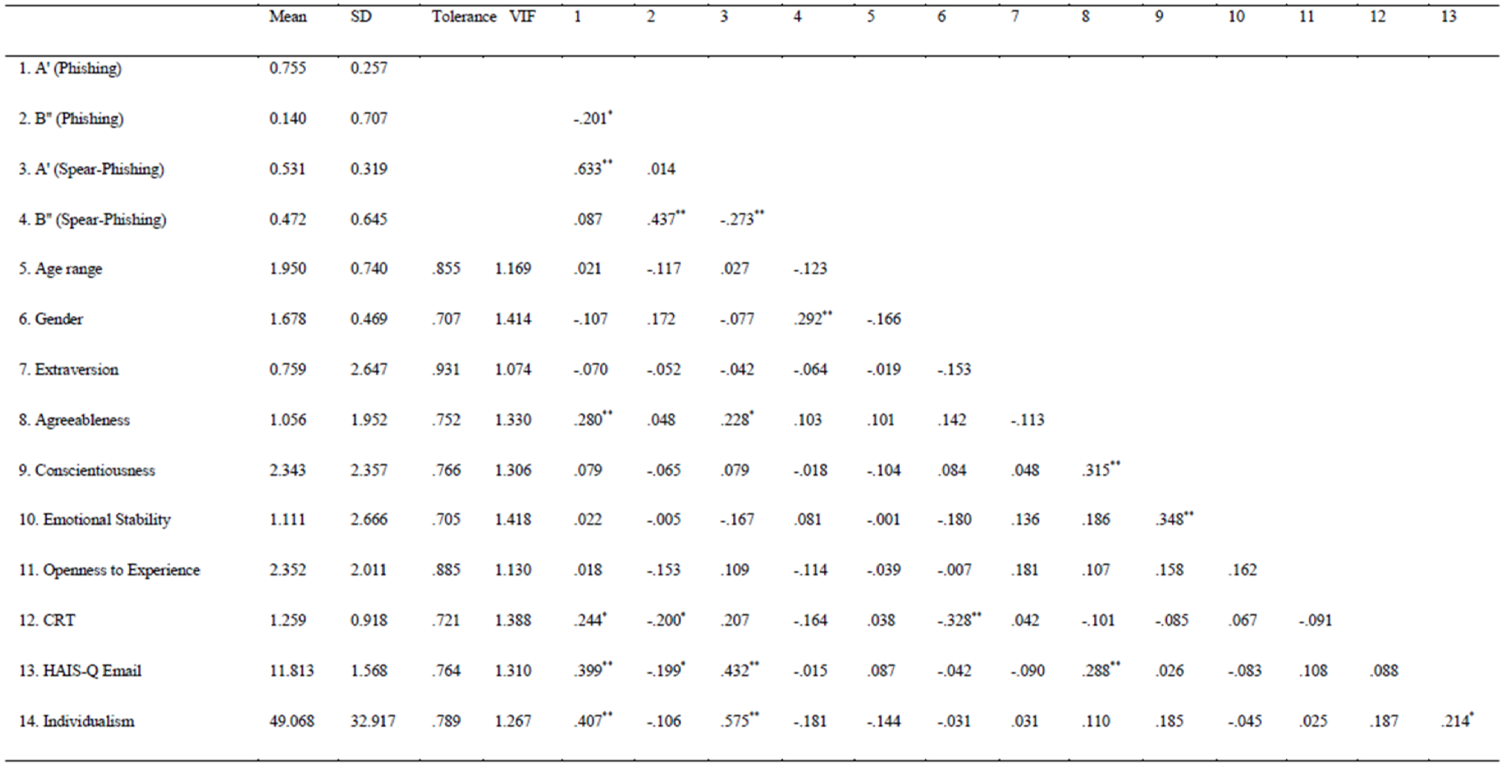
Stanislaw, H., and Todorov, N. (1999), "Calculation of Signal Detection Theory Measures," *Behavior Research Methods, Instruments & Computers*, Vol. 31, No. 1, pp137-149.

Swets, J.A. (ed.) (1964), *Signal detection and recognition by human observers*, New York, Wiley, no ISBN.

Tembe, R., Zielinska, O., Liu, Y., Wha Hong, K., Murphy-Hill, E., Mayhorn, C. and Ge, S. (2014), "Phishing in International Waters: Exploring Cross-National Differences in Phishing Conceptualizations between Chinese, Indian and American Samples", in Williams, L.A. et al. (Eds.) *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security (HotSoS '14)*, Raleigh, NC, USA, ISBN: 978-1-4503-4277-3.

Uebelacker, S., and Quiel, S. (2104), "The Social Engineering Personality Framework", in G. Bella and G. Lenzini (Eds.) Proceedings of the 4th International Worskhop on Socio-Technical Aspects in Security and Fraud, NJ, USA, IEEE, ISBN: 978-1-4799-7901-1.

Vishwanath, A. (2015), "Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack", *Journal of Computer-Mediated Communication,* Vol. 20, pp570-584.



	Mean	SD	Tolerance	VIF	1	2	3	4	5	6	7	8	9	10	11	12	13
1. A' (Phishing)	0.755	0.257															
2. B" (Phishing)	0.140	0.707			-.201*												
3. A' (Spear-Phishing)	0.531	0.319			.633**	.014											
4. B" (Spear-Phishing)	0.472	0.645			.087	.437**	-.273**										
5. Age range	1.950	0.740	.855	1.169	.021	-.117	.027	-.123									
6. Gender	1.678	0.469	.707	1.414	-.107	.172	-.077	.292**	-.166								
7. Extraversion	0.759	2.647	.931	1.074	-.070	-.052	-.042	-.064	-.019	-.153							
8. Agreeableness	1.056	1.952	.752	1.330	.280**	.048	.228*	.103	.101	.142	-.113						
9. Conscientiousness	2.343	2.357	.766	1.306	.079	-.065	.079	-.018	-.104	.084	.048	.315**					
10. Emotional Stability	1.111	2.666	.705	1.418	.022	-.005	-.167	.081	-.001	-.180	.136	.186	.348**				
11. Openness to Experience	2.352	2.011	.885	1.130	.018	-.153	.109	-.114	-.039	-.007	.181	.107	.158	.162			
12. CRT	1.259	0.918	.721	1.388	.244*	-.200*	.207	-.164	.038	-.328**	.042	-.101	-.085	.067	-.091		
13. HAIS-Q Email	11.813	1.568	.764	1.310	.399**	-.199*	.432**	-.015	.087	-.042	-.090	.288**	.026	-.083	.108	.088	
14. Individualism	49.068	32.917	.789	1.267	.407**	-.106	.575**	-.181	-.144	-.031	.031	.110	.185	-.045	.025	.187	.214*

Appendix A: Descriptive statistics and correlations (* = correlation significant at the .05 level, ** = correlation significant at the .01 level, two-tailed)