Which Individual, Cultural, Organisational and Interventional Factors explain Phishing Resilience?

K. Parsons[1], M. Butavicius[2], M. Lillie[1], D. Calic[2], A. McCormac[2] and M. Pattinson[3]

[1] School of Psychology, University of Adelaide, South Australia
[2] Defence Science and Technology Group, Edinburgh, South Australia
[3] Business School, University of Adelaide, South Australia
e-mail: {Kathryn.Parsons; Meredith.Lillie; Malcolm.Pattinson}@adelaide.edu.au;
{Marcus.Butavicius; Dragana.Calic; Agata.McCormac}@dst.defence.gov.au

Abstract

We report on the results of an online phishing study, and the factors that predict the ability to resist phishing attacks, which is termed *phishing resilience*. It is important to understand the factors that predict phishing resilience, because they can be used to develop effective strategies to protect organisational information security. We measured a larger number of individual, cultural, organisational and interventional factors than any previous study. Findings indicate that information security awareness (ISA) is most predictive of phishing resilience, which highlights the importance of security education. Results also suggest that older participants are less susceptible to phishing attacks and individuals who are very influenced by social pressure are more susceptible. When people trusted in the infallibility of technical safeguards, such as spam filters, they had lower phishing resilience, whereas people who preferred using a more rational decision making style had higher phishing resilience. These results suggest that teaching people not only how to behave, but also to stop and think before responding to emails, may ensure that they will have the best chance of resisting phishing attacks.

Keywords

Phishing; Social Influence; Cyber Security; Information Security Awareness; Individual Differences; Phishing Resilience

1 Introduction

Phishing is a form of social engineering, in which deception and social influence are used in an effort to convince an individual to divulge personal or sensitive information. In most phishing attacks, the victim is sent an email that is disguised as a known company or organisation, requesting that they click on a link or download an attachment (Butavicius *et al.*, 2015).

Although phishing has been studied for over a decade, it remains one of the greatest threats to organisational information security (Pricewaterhouse Coopers (PWC), 2015, Telstra Corporation, 2017). In a recent report, 76% of information security professionals indicated that their organisation had experienced phishing attacks in 2017 (Wombat Security Technologies, 2018). In an effort to reduce this threat, it is important to better understand why certain people are less prone to fall for phishing

attacks, which has been termed *phishing resilience*. Knowing which factors improve phishing resilience can be used to develop tailored training and education for those who are most at risk.

Previous studies have attempted to shed light on this problem, and have measured performance in phishing studies together with other individual, cultural, organisational or interventional factors (e.g., Sheng *et al.*, 2010, Welk *et al.*, 2015). However, as there are limits on the number of variables that can be measured in a single experiment, previous research has focused on a limited number of factors. For example, Sheng *et al.* (2010) limited their study to the effects of age, gender and aspects of security awareness, and Welk *et al.* (2015) focused on personality variables, including the role of trust and impulsivity and aspects of security behaviour and awareness. This means it is difficult to determine the factors that are most influential in predicting phishing resilience.

In this paper, we measure phishing resilience, and examine a larger number of individual, cultural, organisational and interventional factors than any previous study. It is only through assessing these factors together that we can understand which of the factors are most influential in predicting the ability to resist phishing attacks. This paper is organised as follows. In the next section, we provide a summary of related research, followed by an outline of our research aims. Section 3 presents our research method, and the results of our study are described in Section 4. In Section 5, we discuss the implications of our research findings and make concluding remarks.

2 Background

Previous research on people's susceptibility to phishing has revealed several potential predictors of phishing resilience. For example, previous phishing studies have consistently shown that age is important, with older participants regularly found to be less susceptible, and younger participants, particularly those between the ages of 18 and 25, found to be most susceptible to phishing attacks (Darwish *et al.*, 2012, Jagatic *et al.*, 2007, Sheng *et al.*, 2010). A number of studies have found that women are more susceptible to phishing attacks than men (e.g., Jagatic *et al.*, 2007, Sheng *et al.*, 2010), but Kumaraguru *et al.* (2007) did not find significant differences based on gender.

Previous research has demonstrated that people who are more resilient have higher information security awareness (ISA) (McCormac *et al.*, 2017). However, the relationship between resilience and phishing performance (i.e., phishing resilience) is yet to be examined. Findings have demonstrated that people who are better able to control their impulsivity are less susceptible to phishing, but these results have been inconsistent. For example, Welk *et al.* (2015) measured impulsivity using a self-report scale and found that people with lower impulsivity were less susceptible to phishing. Other studies have used the Cognitive Reflection Test (CRT) (Frederick, 2005) to measure impulsivity. While Butavicius *et al.* (2015) found that individuals who scored higher on the CRT were better at detecting phishing emails, Kumaraguru *et al.* (2007) found the opposite.

Phishing emails often include influence principles, which are tactics that can persuade people to comply with a given request. Cialdini (2009) outlined six influence principles, namely, authority, consistency, liking, reciprocity, scarcity and social proof, and all of these principles have been used within phishing emails (Akbar, 2014). For instance, in a demonstration of the liking principle, participants who were sent a phishing email that appeared to be from a friend were significantly more likely to comply with the request than those who received the email from an unknown address (Jagatic *et al.*, 2007). Evidence suggests that there are large individual differences in susceptibility to these influence principles, such that certain principles will have the opposite effect on some individuals (Kaptein *et al.*, 2012). However, these individual differences are yet to be examined in a phishing context.

Previous research has indicated that national culture is a strong predictor of phishing susceptibility, where those who are orientated towards the needs of the individual rather than the needs of society were less susceptible to phishing attacks (Butavicius *et al.*, 2017). From an organisational perspective, Calic *et al.* (2016) argued that individuals who feel particularly stressed with their job may not follow security rules, and therefore greater job stress and poorer organisational security culture might be associated with greater phishing susceptibility. Although findings have revealed that ISA is associated with both job stress (McCormac *et al.*, 2017) and organisational security culture (Parsons *et al.*, 2015), the relationship between phishing resilience and these variables is yet to be examined. In regards to interventional factors, previous findings have indicated that phishing resilience is associated with better ISA and better knowledge of phishing threats and risk (Butavicius *et al.*, 2017, Parsons *et al.*, 2017, Welk *et al.*, 2015).

In this paper, we measured phishing resilience and its relationship to a range of factors. In line with the recommendation by Karjalainen (2011), rather than using a theory-verification approach, we used an exploratory approach, and the factors of interest were chosen based on previous research findings. As such, we measured individual (e.g., demographics and impulsivity), cultural (e.g., individualism vs collectivism), organisational (e.g., job stress and organisational security culture) and interventional factors (e.g., information security awareness). The aim of this paper was to determine the factors that are most predictive of phishing resilience.

3 Method

3.1 Participants

A total of 607 participants (304 male and 303 female) completed an online experiment. All participants were recruited via Qualtrics panels and were all working Australian adults who spend at least 10% of their work time using a computer or portable electronic device. Approximately 8% of participants were between 18 and 29 years of age; 19% were between 30 to 39 years; 25% between 40 and 49 years; 27% between 50 to 59 years, and 20% were aged 60 years and older.

3.2 Study Design

An online experiment was conducted in two stages. The first stage was conducted in May 2017 and consisted of an online survey where participants were asked questions about ISA, and were also asked to complete questions relating to job stress, resilience and organisational security culture. The second stage was conducted between May and July 2017 and the same participants were invited to take part in this second online survey.

In the second stage, participants took part in a phishing study and were also asked to complete measures of national culture, cognitive ability and susceptibility to social influence. A unique ID was used to match the data of participants across the first and second stage. Ethics approval was obtained from the Human Research Ethics Subcommittee of the University of Adelaide, School of Psychology.

3.3 Measures

3.3.1 Individual factors

Participants were asked to provide their age and gender. For subsequent measures, responses were given on a five-point Likert Scale (1 = 'Strongly disagree' to 5 = 'Strongly agree') unless otherwise specified.

Participants' level of resilience was measured using the *Brief Resilience Scale*, which is a six-item measure by Smith *et al.* (2008). The Cronbach's alpha in this study was .89. Participants were also asked to complete the *Susceptibility to Persuasive Strategies* scale (Kaptein *et al.*, 2012). This scale consists of 20 items and measures how vulnerable an individual is to each of Cialdini's (2009) influence principles, namely, authority, consistency, liking, reciprocity, scarcity and social proof (Cronbach's alpha = .81).

Participants' tendency to use a systematic decision making style was measured using a sub-scale of the *Rational and Intuitive Decision Styles Scale* (Hamilton *et al.*, 2016). This *Rational Decision Making Scale* includes five items to measure rational or systematic decision making (Cronbach's alpha = .86). Participants were also asked to respond to the *Cognitive Reflection Test (CRT)*, which consists of three items, such that higher scores relate to a tendency to control impulsivity (Frederick, 2005).

3.3.2 Cultural factors

Participants' tendency to perceive themselves as independent from others or connected to others was measured using the short version of Singelis' (1994) *Self-Construal Scale* (Fernández *et al.*, 2005). The scale includes two factors to measure Independent tendencies (i.e., *Uniqueness* and *Low context*) and two factors to measure Interdependent tendencies (i.e., *Group loyalty* and *Relational interdependence*).

3.3.3 Organisational factors

Participants' level of job stress was measured using the *Job Stress Scale*, which is a five-item measure by Lambert *et al.* (2006). *Organisational Security Culture* was also measured using the six items from Parsons *et al.* (2015). The Cronbach's alpha values obtained in this study were .86 and .65, respectively.

3.3.4 Interventional factors

Participants' awareness of the information security threats associated with email use (i.e., *Email use ISA*) were measured using the *Email Use* focus area of the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons *et al.*, 2017). This consists of nine items and the Cronbach's alpha value was .78. Participants' knowledge of the fallibility of certain information technology safeguards was measured using the *Trust in Technical Controls Scale* (Butavicius *et al.*, 2018), which includes four items and the Cronbach's alpha value was .60.

3.4 Procedure

Participants were informed that the study was assessing how people manage their emails. They were presented with image of 14 emails, from the inbox of a fictitious individual, namely, 'Alex Jones'. These included 7 genuine emails and 7 phishing emails, and both types of emails either contained one of Cialdini's (2009) six influence principles, or no principle. For each email, participants were asked to respond to the statement *"It is okay to click on the link in this email"* on a five-point scale from 'strongly disagree' to 'strongly agree'.

4 Results

To measure phishing resilience, the hit rate was calculated, which is the portion of phishing emails that were correctly managed. Phishing emails were scored as correctly managed if participants responded with 'disagree' or 'strongly disagree' to the statement *"It is okay to click on the link in this email"*. A higher score represents better performance and the mean score was .61 (SD = .34). A series of Pearson's correlation analyses were conducted to determine which individual, cultural, organisational and interventional factors relate to phishing resilience. These results are displayed in Appendix A.

In regards to individual factors, results suggest that older participants had significantly higher phishing resilience (r = .21, p < .001), and were therefore less susceptible to phishing. However, there were no significant differences based on gender (r = -.07, p = .08) or the level of resilience of participants (r = .06, p = .12). Results also indicated that participants who were more susceptible to Cialdini's (2009) social influence principles generally had lower phishing resilience. However, there was no relationship between phishing resilience and susceptibility to the reciprocity principle (r = -.05, p = .23). Participants who scored higher on the CRT (r = .14, p < .001) and those who

preferred a rational decision making style (r = -.22, p < .001) were significantly less susceptible to phishing attacks.

In regards to cultural factors, only Group Loyalty was significant (r = -.15, p < .001), which means that people who were more orientated towards the needs of the group rather than the needs of the individual had lower phishing resilience. The organisational factor of organisational security culture was also significant, with findings indicating that individuals who reported better security culture tended to be more resilient against phishing attacks (r = .16, p < .001). There were no differences based on the level of job stress reported by participants (r = -.04, p = .37). There was a significant relationship between phishing resilience and both of the measured interventional factors, namely Email Use ISA (r = .29, p < .001) and Trust in Technical Controls Scale (r = -.27, p < .001). This means that people who had more knowledge of safe email practices or more awareness of the fallibility of technical safeguards such as spam filters had better phishing resilience.

A multiple regression analysis was conducted to evaluate which variables best predict phishing resilience (see Table 1). All Variance Inflation Factor (VIF) values were below 2, indicating that multicollinearity had not occurred. The regression model accounted for approximately 17% of the variation in phishing resilience (R^2_{adj} = .165, F = 10.97, p < .001). The most important predictors were, in order from highest to lowest, Email Use ISA, age, susceptibility to social proof, preference for rational decision making and trust in technical controls.

Variable	*B*	β standardised	*t*-value	*p*
Age	**.03**	**.11**	**2.84**	**.005***
Susceptibility Authority	-.03	-.06	-1.27	.204
Susceptibility Consistency	-.01	-.02	-.39	.696
Susceptibility Liking	.01	.01	.31	.758
Susceptibility Scarcity	.00	.00	.01	.994
Susceptibility Social Proof	**-.05**	**-.11**	**-2.22**	**.027***
Cognitive Reflection Test	.01	.04	1.00	.315
Rational Decision Making	**-.01**	**-.09**	**-2.19**	**.029***
Group Loyalty	-.03	-.06	-1.31	.192
Organisational Security Culture	.00	.03	.80	.427
Email Use ISA	**.01**	**.17**	**3.82**	**.000****
Trust in Technical Controls	**-.01**	**-.09**	**-2.10**	**.036***

* p < .005, ** p < .001

Table 1: Summary of multiple regression analysis for phishing resilience

5 Discussion

This study reports on the results of an online phishing study, and revealed that 61% of phishing emails were managed correctly. Although this result is higher than previous role-play phishing studies, in which 52% (Parsons *et al.*, 2013) and 48% (Sheng *et al.*, 2010) of phishing emails were managed correctly, from a real-world perspective, this is still a concerning finding. While a number of previous studies have investigated the factors associated with the ability to resist phishing attacks, findings have been inconsistent, and each study has focused on a limited number of factors (e.g., Kumaraguru *et al.*, 2007, Welk *et al.*, 2015). In this study, we measured a larger number of potential independent variables than any previous study.

In line with previous findings (e.g., Butavicius *et al.*, 2017, Welk *et al.*, 2015), individuals who had better awareness of what constitutes safe email behaviour and recognised the fallibility of technical safeguards had significantly higher phishing resilience. This highlights the importance of communicating information security risks and threats to employees. It is important to not only ensure they are aware of how they should behave, but also understand that protections such as spam filters are insufficient.

Our results also supported the previous finding (e.g., Jagatic *et al.*, 2007, Sheng *et al.*, 2010) that older people are less likely to fall for phishing attacks. This highlights the importance of communicating information security risks to young people. It remains to be seen if this difference is associated with more complacency and willingness to take risks in younger people, which may decrease with age, or if it represents a generational difference, which would then increase as these younger people become a larger portion of the workforce.

Our findings provide support for the influence of impulsivity in phishing performance. The preference for rational (as opposed to intuitive) decision making predicted phishing resilience. These results therefore highlight the importance of teaching people to stop and think before responding to emails. Finally, our results revealed that people who are more susceptible to the social proof principle are more susceptible to phishing. In other words, the social proof principle is based on the idea that people want to do what others are doing (Cialdini, 2009), and they may therefore have a greater need to want to follow the instructions in a phishing email.

Despite the importance of these findings, there are limitations. For example, our study did not directly measure phishing susceptibility, as participants were not required to click on links or enter personal information. Additionally, although this study measured the largest number of factors of any study and their effect on phishing resilience, the regression model accounted for 17% of variance. This means that other factors that were out of scope of the current study would account for the additional variance. This study did not examine the influence of risk-taking and did not examine the effectiveness of different types of training provided to employees. It is important to replicate this research with a larger number of participants to see if the same relationships are found. Although phishing attacks have threatened organisations for over a decade, we have yet to find a simple solution. With the growing sophistication

and diversity of these attacks, it is increasingly important to conduct this research to ensure that employees and organisations have the best chance of avoiding serious security breaches.

6 References

Akbar, N. (2014). Analysing persuasion principles in phishing emails. Masters degree, University of Twente.

Butavicius, M., McCormac, A., Parsons, K., Calic, D. and Pattinson, M. (2018), Predicting information security awareness of employees: The effect of individual, cultural, organisational and interventional factors. Manuscript in preparation.

Butavicius, M., Parsons, K., Pattinson, M. and McCormac, A. (2015), "Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails", 26th Australasian Conference of Information Systems (ACIS), Adelaide.

Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., Calic, D. and Lillie, M. (2017), Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. *Proceedings of the 11th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*. S. Furnell and Clarke, N. L. University of Plymouth pp 12-23.

Calic, D., Pattinson, M., Parsons, K., Butavicius, M. and McCormac, A. (2016), Naïve and accidental behaviours that compromise information security: What the experts think *Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2016)*. S. Furnell and Clarke, N. Frankfurt, Germany pp 12-21.

Cialdini, R. B. (2009), *Influence: Science and Practice*. New York, William Morrow.

Darwish, A., El Zarka, A. and Aloul, F. (2012), "Towards understanding phishing victims' profile", International Conference on Computer Systems and Industrial Informatics (ICCSII), Sharjah, UAE, IEEE.

Fernández, I., Paez, D. and González, J. L. (2005), "Independent and interdependent self-construals and socio-cultural factors in 29 nations", *Revue Internationale de Psychologie Sociale,* Vol. 18, No. 1, pp 35-63.

Frederick, S. (2005), "Cognitive reflection and decision making", *Journal of Economic Perspectives,* Vol. 16, No. 4, pp 25-42.

Hamilton, K., Shih, S.-I. and Mohammed, S. (2016), "The development and validation of the rational and intuitive decision styles scale", *Journal of Personality Assessment,* Vol. 98, No. 5, pp 523-535.

Jagatic, T. N., Johnson, N. A., Jakobsson, M. and Menczer, F. (2007), "Social phishing", *Communications of the ACM,* Vol. 50, No. 10, pp 94-100.

Kaptein, M., de Ruyter, B., Markopoulos, P. and Aarts, E. (2012), "Adaptive persuasive systems: a study of tailored persuasive text messages to reduce snacking", *ACM Transactions on Interactive Intelligent Systems (TiiS),* Vol. 2, No. 2, pp 10.

Kaptein, M. and Eckles, D. (2012), "Heterogeneity in the effects of online persuasion", *Journal of Interactive Marketing,* Vol. 26, No. 3, pp 176-188.

Karjalainen, M. (2011). Improving Employees' Information Systems (IS) Security Behaviour: Toward a Meta-Theory of IS Security Training and a New Frameword for Understanding Employees' IS Security Behaviour. PhD, University of Oulu.

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", Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, Pittsburgh, PA, ACM.

Lambert, E. G., Hogan, N. L., Camp, S. D. and Ventura, L. A. (2006), "The impact of work–family conflict on correctional staff: A preliminary study", *Criminology and Criminal Justice,* Vol. 6, pp 371-387.

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Pattinson, M. and Lillie, M. (2017), Understanding the relationships between resilience, work stress and information security awareness. *Proceedings of the 11th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*. S. Furnell and Clarke, N. Adelaide, Australia, University of Plymouth pp.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017), "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies", *Computers & Security,* Vol. 66, pp 40-51.

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. *Security and Privacy Protection in Information Processing Systems - IFIP Advances in Information and Communication Technology*. L. J. Janczewski, Wolf, H. and Shenoi, S., Springer.Vol. 405, pp 366-378.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M. and Jerram, C. (2015), "The Influence of Organisational Information Security Culture on Cybersecurity Decision Making", *Journal of Cognitive Engineering and Decision Making: Special Issue on Cybersecurity Decision Making,* Vol. 9, No. 2, pp 117-129.

Pricewaterhouse Coopers (PWC) (2015), Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. and Downs, J. (2010), "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions", Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM.

Singelis, T. M. (1994), "The measurement of independent and interdependent self-construals", *Personality and Social Psychology Bulletin,* Vol. 20, No. 5, pp 580-591.

Smith, B. W., Dalen, J., Wiggins, K., Tooley, E., Christopher, P. and Bernard, J. (2008), "The brief resilience scale: assessing the ability to bounce back", *International Journal of Behavioral Medicine,* Vol. 15, No. 3, pp 194-200.

Telstra Corporation (2017), Telstra Cyber Security Report 2017.

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E. and Mayhorn, C. B. (2015), "Will the "Phisher-Men" reel you in?: Assessing individual differences in a phishing detection task", *International Journal of Cyber Behavior, Psychology and Learning,* Vol. 5, No. 4, pp 1-17.

Wombat Security Technologies (2018), State of the Phish 2018. Pittsburgh, PA,.

	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Phishing susceptibility	-												
2. Age	.21**	-											
3. Susceptibility Authority	-.20**	-.16**	-										
4. Susceptibility Consistency	-.11**	-.12**	.34**	-									
5. Susceptibility Liking	-.10*	-.10*	.20**	.29**	-								
6. Susceptibility Scarcity	-.20**	-.22**	.41**	.37**	.35**	-							
7. Susceptibility Social Proof	-.30**	-.22**	.42**	.29**	.38**	.44**	-						
8. Cognitive Reflection Test	.14**	.08*	-.13**	-.08*	.02	-.11**	-.13**	-					
9. Rational Decision Making	-.22**	-.12**	.21**	.23**	.24**	.38**	.29**	-.27**	-				
10. Group Loyalty	-.15**	-.08*	.30**	.32**	.29**	.29**	.38**	-.06	.13**	-			
11. Organisational Security Culture	.16**	.11**	.00	.14**	-.11**	-.13**	-.23**	.01	-.13**	.01	-		
12. Email use ISA	.29**	.18**	-.09*	.10*	.02	-.12**	-.27**	.11	-.13**	-.01	.38**	-	
13. Trust in Technical Controls	-.27**	-.11**	.21**	.13**	.02	.22**	.35**	-.26**	.30**	.12**	-.17**	-.38**	-
Mean	.61	N/A	3.17	3.56	3.48	2.96	2.74	.80	15.91	3.34	22.01	38.60	8.69
SD	.34	N/A	.66	.54	.55	.72	.73	1.00	3.51	.61	3.21	4.88	2.54

* $p < .005$, ** $p < .001$

Table 1: Pearson's correlation matrix and descriptive statistics for variables of interest