Aligning Cyber-Security Training to Individual Cognitive Style

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

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

Abstract

This paper reports on the early stages of a project that investigates the concept of a framework of cyber-security controls (i.e. an Adaptive Control Framework (ACF)) that can be adapted or aligned to individual cognitive styles. The specific cyber-security control considered by this current research was employee cyber-security training, namely, email-use training to improve the detection of phishing-email attacks. Previous research suggests that an individual's cognitive processing style can be classified as either Field Independent (FI) or Field Dependent (FD) and that this personal characteristic may warrant a specific mode of training. Accordingly, the overall aim of this research project is to establish whether computer-based phishing training is more effective when it matches individual cognitive processing style. Two computer-based phishing training modules were developed using Articulate Storyline 360 software. These two modules, an FI version and an FD version, were designed in accordance with principles derived from the literature in order to maximise training effectiveness. Future research is planned to include empirical tests for improved cyber-security behaviour and other concepts of adaptive cyber-security training.

Keywords

Group Embedded Figures Test (GEFT), Field Independent (FI), Field Dependent (FD), Cognitive Styles.

1 Introduction

One of the most significant threats to the security of an organisation's information assets is the digital-device behaviour of its employees. Most insider security breaches are not caused by purposeful malicious actions, but rather by accidental, non-malicious behaviours, such as clicking on dubious links in emails or not changing passwords often enough.

Historically, the security of an organisation's digital information and systems was heavily reliant on various technical solutions (Denning 1999). However, it is increasingly acknowledged that a more effective means of mitigating cyber security risks within an organisation is to address the unintentional behaviour of digital-device users in parallel with, but not instead of, hardware and software solutions (Dhillon & Backhouse 2001; Furnell 2008; Pattinson & Anderson 2007; Schneier 2004; Stanton *et al*. 2005; Trček *et al*. 2007). Consistent with this recognition, recent studies have demonstrated that human behaviour is the major cause of information security incidents (Proofpoint 2016; Telstra_Corporation 2014).

Phishing emails are a major current threat for which there is no perfect technical solution to mitigate the risks associated with hacking, scams and invasion of privacy. Therefore, human behavioural controls are required to guarantee that most, if not all, phishing emails will be detected and dealt with appropriately. One approach is to train individuals how to distinguish a phishing email from a genuine email by exposing them to a series of common cues to look for. Parsons, McCormac*, et al.* (2015) identified a comprehensive list of cues that people should be aware of. Most of these have been incorporated in the computer-based phishing training modules of this research.

1.1 Aims

This paper reports on research that is part of a larger project to develop an Adaptive Control Framework (ACF) for cyber-security behaviour. Such an ACF would provide effective methods to communicate, educate and positively influence employees to improve their cyber-security behaviour. This comprehensive ACF will be customisable for a broad range of organisations according to specific cyber-security requirements and employee types.

This paper focuses on one of the attributes that training should be adapted to, namely, the Field Independent/Field Dependent cognitive style preference of the user. Previous literature is presented which relates to this cognitive style, both in its effects more generally and more specifically towards cyber-security behaviour and argue that adapting cyber-security training to this user preference will improve the effectiveness of the training. A number of principles of training design are identified, based on this review in order to tailor training to Field Independent/Field Dependent cognitive style preference and to embed these principles into a training package to improve people's ability to detect phishing emails. Finally, an experimental framework is proposed that tests the effectiveness of these training modules that is extendable to other components of the Adaptive Control Framework.

2 Background

This research project examines the effectiveness of behavioural controls in light of individual differences, i.e., how such controls may be more effective for different people. This will form the basis of an Adaptive Control Framework (ACF) and may involve tailoring communications about cyber security to suit specific individuals, departments or organisations.

Although there is a scarcity of research into human-centric controls within the cyber-security context, there is a wealth of psychological research and knowledge that can be applied to develop cyber-security behavioural controls. Two of these concepts are discussed below.

2.1 Cognitive Styles

As a personality dimension, an individual's cognitive style has a significant impact on the way that he or she collects and interprets information. Cognitive style is not considered to be a fixed trait, rather it is viewed as the preferred approach that an individual adopts when organising and presenting information (Pattinson & Anderson, 2005). For the current project, the focus is on the field dependence-independence (FDI) cognitive style, given that previous research has demonstrated that tailoring cyber security information in accordance with this preference will improve cyber security awareness (Pattinson & Anderson 2005).

2.2 Field Independence (FI) and Field Dependence (FD)

The concept of FI and FD cognitive styles was first developed by Witkin in 1960s and represents an established construct in the domain of psychology (Ausburn & Ausburn 1978; Sternberg & Grigorenko 1997). Based on this work, FI individuals tend to be analytical and prefer organisation and structure. In comparison, FD individuals prefer working with others and making decisions collaboratively. Characteristics of FI and FD individuals are summarised in Table 1, below.

Individuals classified as FI	Individuals classified as FD
Enjoys own company	Drawn to people
Not sensitive to others around them	Like to have people around them
Less non-verbal behaviour	More non-verbal behaviours
Prefer occupations with less interaction	Prefer occupations which require involvement with others
Solve problems rapidly	Take a longer time to solve problems
More aloof, theoretical	Alert to social cues
More abstract & analytical	Highly developed social skills
Initially thought to be males but inconclusive	Sensitive to social criticism
Less inclined to be influenced	Extremely influenced by others
Prefer maths & physical sciences	Teachers
Analytic way of perceiving	Global way of perceiving

Table 1: FI/FD Characteristics

The focus of this paper is on the cyber-security behaviour of employees and although this is a complex sociological and psychological phenomenon, the authors of this paper are proposing that one way of improving this type of behaviour is to provide training in a way that is aligned to each individual's FI/FD cognitive style.

3 Computer-based Phishing Training Modules

A review of previous research literature was conducted with the specific aim of developing computer-based phishing training modules. A number of design principles were then synthesized in adapting this training as shown in Table 2.

Pattinson and Anderson (2004) focused on the communication of risk, both verbal and written rather than the design of a training program. Consequently, they were concerned with how messages should be 'framed' for FI people versus FD people. As a result, their research contributed to the "Message Framing" module feature in Table 2 below.

Triantafillou *et al.* (2003) designed a computer-based module called an AES-CS (Adaptive Educational System based on Cognitive Styles) to support the notion that adaptive education improves students' learning. More specifically, this module looks at Field Dependence/Independence and tailors the software to suit. It details the various elements that have been designed for specific cognitive styles, i.e. global vs analytical approach, program control vs learner control, instructions and feedback. After testing it on students, the researchers then sought feedback and revised the system to make the instruction more effective. The authors of this research observed that FD learners appreciate explicit directions and lots of guidance. As a result, these findings contributed to the "Instructions/Guidance" and "Navigation" module features in Table 2 below. Consequently, animated arrows and a glossary were built into the FD module. Feedback was also an important module feature because FD learners prefer a lot of feedback and FI learners prefer a minimal amount.

Chen and Macredie (2002) developed a 'learning model' and discovered that FD learners prefer to navigate through the training in a linear manner, namely, guided, perhaps by a menu or a checklist. FI learners, on the other hand, prefer non-linear navigation, that is, in any order they decide. As a result, these findings contributed to the "Structure" module feature in Table 2 below. Consequently, these module features were included in the respective training modules developed as part of this current research.

Handal and Herrington (2004) focused on computer-based training (CBT) and the design features of such modules. For example, they observed that FD learners prefer more step-by-step instructions with more human direction as well. Consequently, the FD module developed in this current research contained voice-over instructions and advice as well as more text and graphics than for the FI module. They also found that FI learners appear to read more quickly, e.g. skim read, through the screens. Because of this observation, the developed FI module did not contain any audio so that they could progress at their own speed.

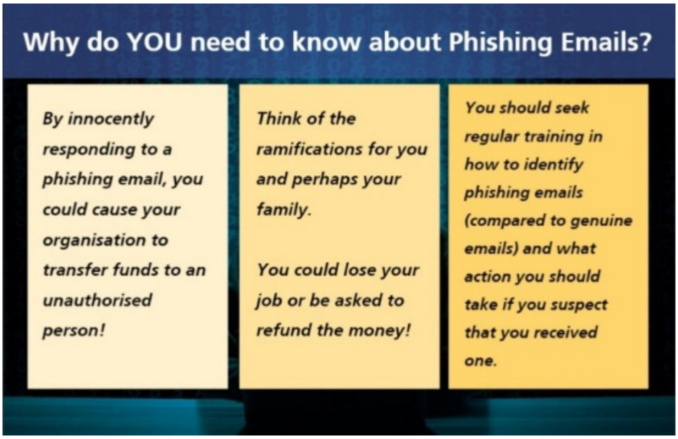
Table 2 below summarises the different module features between FI training and FD training in the design of each of the modules. The source of the module feature is also shown.

Module Feature	**FI**	**FD**	**Source**
Message Framing	Emphasise the direct effect on the participant.	Emphasise the effect on groups, the organisation or the participant's family.	(Pattinson *et al.* 2018)
Navigation	Enable the participant to navigate the module in any order, i.e. non-linear navigation with freedom.	Participant guided through each topic step-by-step. More linear navigation.	(Triantafillou *et al.* 2003)
Structure	Less structured. No menu provided.	More structured. Menu provided to track progress through the module.	(Chen & Macredie 2002)
Instructions/ Guidance	Minimal instructions and guidance provided.	Maximum amount of guidance by providing clear, explicit instructions, e.g. animated arrows.	(Triantafillou *et al.* 2003)
Feedback	Minimal feedback provided – e.g. the quiz answers only show the correct and incorrect, without explanations.	Maximum feedback. Quiz answers include specific explanations of incorrect answers.	(Triantafillou *et al.* 2003)
Human Element	Less human element e.g. Only text used. No audio provided so participant can skim-read.	More human element by providing voice-over in addition to text.	(Handal & Herrington 2004)
Graphics	Less text and graphics provided.	More text and graphics provided.	(Handal & Herrington 2004)

Table 2: Module Design Features

Although there is research suggesting that using these module features to match training to an individual's FI or FD preference improves learning, some research has reported contrary findings. For example, Witten (1989) investigated the relationship between FI/FD cognitive style and academic achievement and found that FI students performed better than FD students generally, regardless of whether their training was FI (i.e. matched) or FD (i.e. mismatched). As discussed below, this suggests the concepts presented in this paper need empirical testing.

Two examples of the FI and FD computer-based phishing training modules are shown below. In Figures 1a and 1b, the different message framing effects are shown. For the FI version (Figure 1a) the focus is more on the repercussions on the person's wider social group, organisation and family whereas for the FD-focused version (Figure 1b), the emphasis is on how falling for a phishing email may have deleterious effects on just the recipient. Figures 2a and 2b show how the human element design principle is included in the training. In the FI version (Figure 2a) text only is used to allow the user to skim through at their own pace whereas the FD version (Figure 2b) includes a voice-over that dictates the pace of the module and includes graphics in line with this design. In this case, the same text displayed in Figure 2a is the script of the voice-over in Figure 2b.



Why do YOU need to know about Phishing Emails?

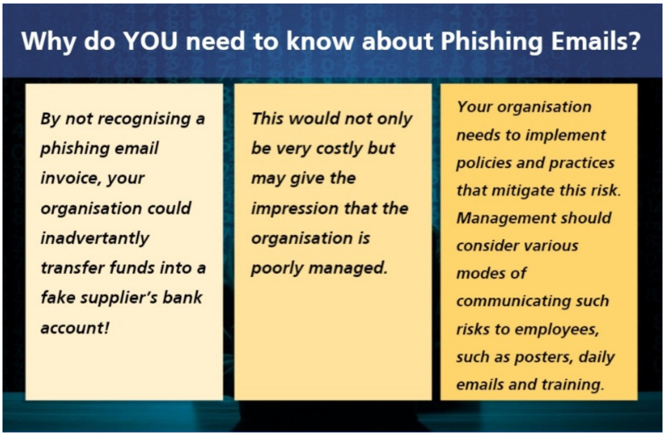
By innocently responding to a phishing email, you could cause your organisation to transfer funds to an unauthorised person!

Think of the ramifications for you and perhaps your family.

You could lose your job or be asked to refund the money!

You should seek regular training in how to identify phishing emails (compared to genuine emails) and what action you should take if you suspect that you received one.

Figure 1a: Message Framing - FI version



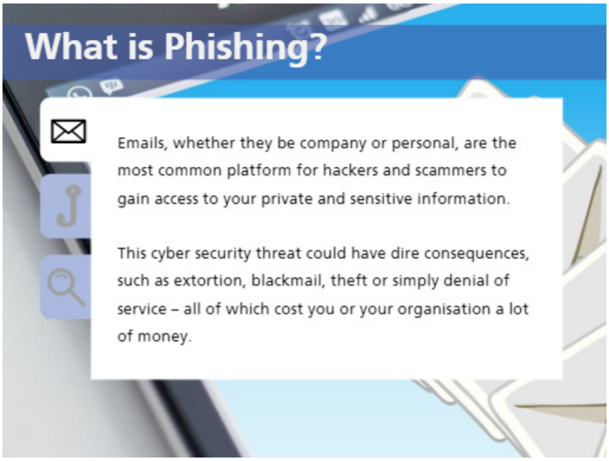
Why do YOU need to know about Phishing Emails?

By not recognising a phishing email invoice, your organisation could inadvertantly transfer funds into a fake supplier's bank account!

This would not only be very costly but may give the impression that the organisation is poorly managed.

Your organisation needs to implement policies and practices that mitigate this risk. Management should consider various modes of communicating such risks to employees, such as posters, daily emails and training.

Figure 1b: Message Framing - FD Version

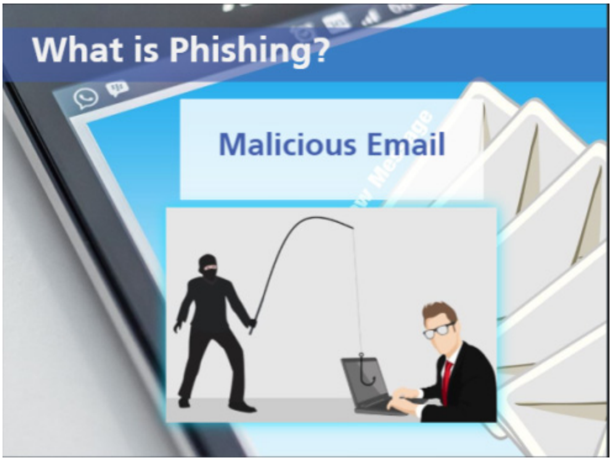


What is Phishing?

Emails, whether they be company or personal, are the most common platform for hackers and scammers to gain access to your private and sensitive information.

This cyber security threat could have dire consequences, such as extortion, blackmail, theft or simply denial of service – all of which cost you or your organisation a lot of money.

Figure 2a: Screen text only – FI version



What is Phishing?

Malicious Email

Figure 2b: Combination of screen text, voice-over and graphics – FD version

The design of both the phishing training modules focusses on the ability of participants to recognise common cues in emails. This research adopted the eight most common cues that are found in phishing emails and are shown in Table 3.

Inconsistent message	“The message within this email is inconsistent”
Dodgy links	“The links within this email do NOT appear legitimate”
Poor visual presentation	“The visual presentation/design of this email is poor”
Not personalised	“This email is NOT personalised to the recipient”
Spelling & grammatical errors	“This email has spelling and/or grammatical irregularities”
Unknown or dubious sender	“The email does NOT appear to be from the claimed sender”
Unfamiliar organisation	“I am NOT familiar with the named organisation or company”
Overly urgent or forceful	“This email is urgent or demanding”

(derived from Parsons, Butavicius, *et al.* (2015)

Table 3: Phishing-Email Cues

4 Future research

This project follows on from a similar research effort which investigated the concept of adapting cyber-security training to the preferred learning styles (using the VARK model) of employees who use digital devices to do their job (Pattinson *et al.* 2018). Both of these projects are based on the premise that better cyber-security behaviour by employees mitigates the risks associated with data breaches and other threats to the confidentiality, integrity and availability (CIA) of the digital information and systems within an organisation.

However, while the current project presents a model of training based on the ACF, it remains to be seen how well this individualised training will improve individual cyber security behaviour. To address this, future research is planned which will empirically test training effectiveness in a controlled experiment.

A random selection of students from a leading Australian University from various courses and levels of course will be invited by email to participate in a CBT exercise by using a digital device, such as a mobile phone, a laptop or a desktop computer to complete the following tasks.

4.1 Group Embedded Figures Test (GEFT)

Participants will be identified as an FI or FD learner in accordance with the Group Embedded Figures Test (GEFT) Manual (Demick 2014). A score of 5 or less (out of 18) classifies the participant as having an FD cognitive style. A score of 13 or more (out of 18) classifies the participant as having an FI cognitive style. This test is considered to be the most well established test of FDI preference (Witkin 1971). It consists of 18 items, depicting a complex figure for which the participants must identify a simple form therein. Each question will time out if not answered within 1 minute. This test will take 10 minutes.

4.2 Phishing-email Pre-test

A survey has already been developed by the authors, using Qualtrics survey software, to assess the ability of respondents to differentiate between phishing emails and genuine emails. This survey presents eight images of either genuine or phishing emails and asks the participant to respond to the following two questions:

a) Do you think that this is a phishing or genuine email?

b) What is your level of confidence in this decision? (1 No confidence) to 5 (Total confidence)

This test will take 10 minutes.

4.3 FI and FD Computer-based Phishing Training

Section 3 details the design of the FI and FD phishing training modules. A random sample of approximately 120 University of Adelaide students from various courses and levels will be invited by email to participate in a computer-based training (CBT) exercise by using a digital device, such as a mobile phone, a laptop or a desktop computer. Approximately half of the participants will be emailed the FI phishing training module and half will be emailed the FD phishing training module. This test will take 20 minutes.

4.4 Phishing-email Post-test

One week after the computer-based phishing training is undertaken, participants will be emailed an equivalent Qualtrics survey as per the phishing-email pre-test, except the eight emails to be assessed are unique. This survey assesses a participant's ability to distinguish phishing emails from genuine emails by applying the principles they learnt in the training module. This test will take 10 minutes.

5 Anticipated Outcomes

The results of the phishing-email pre-test survey will be compared to the post-test survey in order to address the following research question:

Do employees (who use digital devices as part of their job) manage their emails in a more risk-averse manner (i.e. less risky manner) when phishing training is aligned with their Field Independent/Field Dependent cognitive style?

In addition to testing the effectiveness of our concept of training modules adapted to an individual's FDI preference, further research is also needed into other components of the ACF. In particular, additional research will be necessary to investigate similar training concepts for other focus areas that form part of an Information Security Awareness package, namely, password management, internet use, social media use, mobile computing, information handling and incident reporting.

This research will contribute to the development of cyber security training programs that will improve cyber security behaviours in the workplace. In addition to adding to academic and theoretical understanding of human behaviour and cyber security, this project has the potential to contribute to the extension of current international standards, such as ISO's 27000 series, NIST's SP800 series or ISACA's COBIT5 by focussing on the previously neglected human element.

6 References

Ausburn, LJ & Ausburn, FB 1978, 'Cognitive styles: Some information and implications for instructional design', *Ectj*, vol. 26, no. 4, pp. 337-354.

Chen, SY & Macredie, RD 2002, 'Cognitive Styles and Hypermedia Navigation: Development of a Learning Model', *Journal of the American society for information science and technology*, vol. 53, no. 1, pp. 3-15.

Demick, J 2014, 'A revised manual for the Embedded Figures Test (including computerized GEFT)', Menlo Park, CA: Mind Garden.

Denning, D 1999, 'Information Warfare and Security, Addsion-Wesley Longman', Inc.

Dhillon, G & Backhouse, J 2001, 'Current directions in IS security research: towards socio-organizational perspectives', *Information Systems Journal*, vol. 11, no. 2, pp. 127-153.

Furnell, S 2008, 'Securing the Human Factor', in H Lacohée, P Cofta, A Phippen & S Furnell (eds), *Understanding Public Perceptions: Trust and Engagement in ICT Mediated Services*, International Engineering Consortium.

Handal, B & Herrington, A 2004, 'On Being Dependent or Independent in Computer Based Learning Environments', *E-Journal of Instructional Science and Technology*, vol. 7, no. 2.

Parsons, K, Butavicius, M, Pattinson, M, McCormac, A, Calic, D & Jerram, C 2015, 'Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?', paper presented at Australasian Conference on Information Systems, Adelaide, South Australia.

Parsons, K, McCormac, A, Pattinson, M, Butavicius, M & Jerram, C 2015, 'The design of phishing studies: Challenges for researchers', *Computers & Security*, vol. 52, pp. 194-206.

Pattinson, M & Anderson, G 2004, 'Risk communication, risk perception and information security', in *Working Conference on Integrity and Internal Control in Information Systems,* Springer, pp. 175-184.

Pattinson, M & Anderson, G 2005, 'Risk Communication, Risk Perception and Information Security', in *Proceedings of IFIP WG11.1 & WG11.5 Working Conference,* Fairfax, Virginia, USA.

Pattinson, M & Anderson, G 2007, 'How well are information risks being communicated to your computer end-users?', *Information Management & Computer Security*, vol. 15, no. 5, pp. 362-371.

Pattinson, M, Butavicius, M, Ciccarello, B, Lillie, M, Parsons, K, Calic, D & McCormac, A 2018, 'Adapting Cyber Security Training to Your Employees', in S Furnell & N Clarke (eds), *Proceedings of the 12th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018),* University of Plymouth, Dundee, Scotland, pp. 67-79.

Proofpoint 2016, 'The Human Factor 2016: Advanced Threat Report', viewed March 2015, <https://www.proofpoint.com/au/human-factor-report-2016>.

Schneier, B 2004, *The People Paradigm*, viewed June 23 2011, <http://www.csoonline.com/article/219787/bruce-schneier-the-people-paradigm>.

Stanton, J, Stam, K, Mastrangelo, P & Jolton, J 2005, 'Analysis of end user security behaviors', *Computers & Security*, vol. 24, no. 2, pp. 124-133.

Sternberg, RJ & Grigorenko, EL 1997, 'Are cognitive styles still in style?', *American psychologist*, vol. 52, no. 7, p. 700.

Telstra_Corporation 2014, 'Telstra Cyber Security Report 2014', viewed March 2015, <http://www.telstra.com.au/business-enterprise/download/document/telstra-cyber-security-report-2014.pdf>.

Trček, D, Trobec, R, Pavešsić, N & Tasič, J 2007, 'Information systems security and human behaviour', *Behaviour & Information Technology*, vol. 26, no. 2, pp. 113-118.

Triantafillou, E, Pomportsis, A & Demetriadis, S 2003, 'The design and the formative evaluation of an adaptive educational system based on cognitive styles', *Computers & Education*, vol. 41, no. 1, pp. 87-103.

Witkin, HA 1971, *A manual for the embedded figures tests*, Consulting Psychologists Press.

Witten, V 1989, 'Field Dependence-Field Independence: The relationship of cognitive style and academic achievement', Doctoral dissertation, North Carolina State University