The Development of Intervention E-Learning Materials and Implementation Techniques For Cyber-Security Behaviour Change

Tiffany Skinner, LiMETOOLS Ltd[1]

Prof. Jacqui Taylor, Bournemouth University[2]

John Dale, LiMETOOLS Ltd[3]

Dr John McAlaney, Bournemouth University[4]

LiMETOOLS Ltd. Bournemouth, UK[1]
Faculty of Science and Technology, Bournemouth University, UK[2]
LiMETOOLS Ltd. Bournemouth, UK[3]
Faculty of Science and Technology, Bournemouth University, UK[4]

Abstract

Many organisations show compliance in running security awareness programmes, but this does not necessarily mean end users will change their behavior. This highlights one of the main challenges in cyber security. Providing awareness in a tool is a useful first step but it doesn't necessarily lead to changing behaviour [3]. In contrast, completing compliance or achieving competence can actually lead people to being more averse to change than before or even partaking in risky behaviour. This paper describes the collaboration between a specialist computer business (LiMETOOLS) and psychology academics to draw on psychology theory (e.g. Social Cognitive Theory, [4]) and pedagogy (e.g. self-directed learning) to create innovative techniques using interactive learning tools resulting in behaviour change. The aim of this article is to show how we have moved beyond developing materials that change awareness, to those that effectively change digital behaviour. We examine methodologies that can be integrated within online learning tools to embed text, video clips, gamification, and quizzes to encourage measurable cyber security behaviour change. A challenge within behaviour change is the maintenance of these behaviours and we are exploring the potential impact of using 'drip-feed learning' in the form of a short video magazine with embedded quizzes and 'nudges' of behaviour changes that have previously learnt, delivered over a long period of time in very short stimulus packages.

CCS Concepts

Interactive learning environments

Learning management systems

Systems security

Network security

Human and societal aspects of security and privacy

Interaction paradigms

Interactive systems and tools

Keywords

e-learning, cyber security, behavior change, intermittent learning

ACM Reference format:

Tiffany Skinner

LiMETOOLS Ltd1

Prof. Jacqui Taylor

Bournemouth University2

John Dale

LiMETOOLS Ltd3

Dr. John McAlaney

Bournemouth University4.

The Development of Intervention E-Learning Materials and Implementation Techniques For Cyber-Security Behaviour Change. 9 pages.

1.0 Background to existing learning tools

LiMETOOLS creates cyber security interactive learning tools by using a blend of text, games, videos, and quizzes. Tools are developed within this scope to encourage and enable behaviour change. The business has started to draw on psychology research within the cyber security operational field to inform the product development. This process utilises techniques used by broadcast digital storytellers who make complex dramas and documentaries that recognise the human factor element of cyber security. LiMETOOLS has developed an integrated storytelling, scoring and authoring tool platform, for the creation of the e-learning content. The e-learning tool is uploaded onto a Learning Management System (LMS) allowing for learner data capture that can be aggregated to report on specific individuals and teams, to assess knowledge retention, and provide valuable feedback to businesses about their employees, across departments, site locations and countries. The tools aim to provide behavior change in cyber security through perceived susceptibility which could increase with relevant and consistent messages about behavioural cyber security changes that need to take place that are personal to

the individual [24]. This can lead to the necessary change in individuals' attitudes and intentions. The Elaboration Likelihood Model (Petty and Cacioppo 1986) [19] describes how attitudes are formed and persist and how this information can be used to persuade people to change behaviour. It is based on the notion that there is a central route and a peripheral route to attitude change. The central route is a conscious process with thoughtful, logical decisions, where the peripheral route is automatic and unconscious. Therefore, decision making when using the central route can only be processed through motivation with intention to change whilst paying attention to information, leading to a more permanent attitude change. Although attitudes are often different to enacted behaviour, providing a message that is personally relevant to the individual should motivate them to take the central route and a change in attitude and intention (Bada and Sasse 2014) [3]. Blythe (2013) [5] supports this notion in the workplace, to improve employee's virus prevention behaviour. Specific and personalised messages were designed as an intervention tailored from anti-virus software and other security systems that enforce cyber secure behaviour. By providing each employee with the consequences of visiting particular websites and attachment downloads lead to an increase in more secure behaviours. LiMETOOLS aim to deliver their tools in a personally relevant way using knowledge awareness, documentaries, dramas and quizzes.

2.0 Overview of innovative methods and techniques to achieve and measure behaviour change in cyber security within the workplace

There are three projects currently taking place within our collaborative research programme and in this article we will outline the work-in-progress for these and future plans.

2.1 Methods and Techniques for Motivating Learning and Improving Risk Perception and Risk-Related Behaviour

2.1.1 Knowledge based awareness via text.

Increasing an individuals' knowledge in cyber security, increases their awareness of the risks involved online. This further increases individual motivation which could lead to a change in their risky online behaviour. Heuristic decision making underpins this theory. Heuristics are a set of simplifying rules for processing information selectively in memory [11]. Kahneman (2011) [15] suggests there is System 1 processing which is automatic, fast, and unconscious decision making, whereas System 2 processing is deliberate, slow, and effortful. Typical online behaviours are likely to involve System 1 processing, using our existing knowledge, where individuals may not have time to deliberate their online behavior. For example, Guadagno and Cialdini (2005) [13] found that online users evoke cognitive heuristics to evaluate the sources information credibility decreasing cognitive effort and time pressures through confirmation bias to disregard information that is not consistent with ones' own beliefs. By increasing the knowledge in cyber security within the tools, individuals may

be more likely to consider cues to make better estimations, which could alert us to risky online behaviour. Davinson and Sillence (2010) [9] support this notion where participants were provided with phishing threat information, methods, and consequences. After reading and acknowledging this information, intention for users to behave more securely increased. However, a problem with many security awareness programmes based on solely knowledge, is that users are expected to identify the argument rationality from the information given, that cyber security is important and motivations to act accordingly will pursue that. The Cognitive Moral Development (CMD) theory (Kohlberg 1981) [16] demonstrates most rational people, in moral cases, would like an explanation for orders that they are given. Siponen (2000) [26] supports this theory where information security awareness achievement or failure correlates with behavioural readjustment in a positive way of acceptance, internalization and co-operation or alternatively, if the information is received without rationale, resistance or hate may be felt by some individuals. Further, internalizing security guidelines cannot be assumed to be achieved instantly, where if employees take a learning tool it cannot be presumed they will follow the guidelines at once. Therefore, it may be a long proves to get staff to comply with guidelines. This means it is important to understand individual differences in learning where some individuals may learn better with the use of video content, or gamification to understand the content and achieve the intended learning objectives. Therefore, implementation of other delivery methods into e-learning programmes may increase cyber security behavior change [2].

2.1.2 Video Drama.

Delivery methods and techniques are crucial in changing cyber security behaviour [17]. Interactive training though video drama that identifies with a recognisable peer could increase motivation to change online behaviour. The Social Cognitive Theory [4] underpins this notion and proposes that people learn by watching what others do in the social context of experiences, outside media influences and social interactions. Video-based delivery methods can be adapted to a particular audience to consider a recognisable peer. Recognisable peers could be shown through similar gender, age, ethnicity, or the person's situation. Pfleeger and Caputo (2012) [20] suggest that a recognisable peer could have the user gain a greater sense of self-efficacy and to further influence an imitation of their behaviour. The central route of heuristic decision making supports this notion whereby if the message is personally relevant and from a recognisable source, individuals will be motivated to make a more effortful decision and want to imitate the behaviour of their peer [3]. If people believe that they can act to solve a problem they become more inclined and committed to do so. This is linked to emotion, which is a fundamental part of rational decision making and individuals thought processes and linked to past experiences. The past experiences lead to emotional learning when people are confronted with a set of choices and this is what guides their decision by

highlighting potential decisions and eliminating others (Goleman, 1995) [12]. Consequently, security measures should aim at provoking emotions, therefore appealing to them in order to affect attitudes and motivation in a positive manner. This means that by providing video drama content that relates specifically to the user and the correct cyber secure behaviours can motivate the user to change their own behaviour.

2.1.3 Gamification.

Game-based delivery methods are used to challenge, engage, and motivate individuals to offer effective learning compared to more traditional modes of awareness. Interactive serious games combine graphics, play and training concepts to enhance behavioural change. Anti-Phishing Phil [25] was one of the initial interactive games which taught users how to identify phishing URLs. The authors found that the participants who played the serious game were better able to identify fraudulent web sites. However, serious games can be suggested to be over simplified and experiences in the game do not will not reflect long-term habit change. This means, although Anti-Phishing Phil resulted in learning, there is a need to have a shared meaning between the individual and the environment of why they are playing the game [17]. In light of this, Boopathi, Sreejith and Bithin (2015) [6] provide a game which not only provides a capture the flag gamification of cyber security attacks but also puts the attacks into context by embedding tutorials in the first learning round which is then tested in the next stage of the game. Now that users have developed an understanding of the context of the attacks, the interactive capture the flag gamification of cyber security attacks enhances real-world scenario application by using their new knowledge to cyber-attack other teams to capture their flag. Educational gamification therefore shows it can increase understanding of cyber security threats in a more engaging manner, to better help implement behavior change.

2.1.3 Blended Learning.

To maximise full cyber security awareness, motivation and ultimately change behaviour, implementing a blend of learning is important. Abawajy (2014) [1] evaluated the various channels of text-based, video-based and game-based security awareness delivery methods for phishing attacks. Within these delivery methods, the sessions consisted of informing participants of tactics and behaviours of exploitation attacks to encourage the learning to enable avoidance of phishing attacks. Furthermore, information of the over-arching aims of the attacks and the dangerous consequences involved if individuals submit to this type of attack is also given. The authors found the text-based training materials when read properly are helpful in identifying phishing websites but more importantly, game-based, and video-based delivery models are more suitable security delivery methods. Although this has been carried out solely on phishing scams, it is a promising implication for further research to examine the effects of delivery methods in alternate aspects of cyber security; for example, smart home working

vulnerabilities. This could mean that creating eLearning tools that deliver a blend of learning will be better able to appeal to a wider range of individuals to enable change in security behaviour.

2.2 Measuring Capacity Growth in Organisations

Virtual learning environments and e-learning systems are vast becoming an important part of the organizational education and learning process (Pituch & Lee, 2006) [21]. Some e-learning systems only provide a measure of compliance in an awareness programme; however this type of analytics does not necessarily provide evidence that the programme has created the learners to have the capabilities to act in the desired manner. This means, cyber security awareness programmes ideally have to deliver measurable benefits to influence behaviour changes [3]. The use of a Learning Management System (LMS) enables businesses to do this where reporting can show departmental or site-specific vulnerabilities and not just the ability to show a pass and fail compliance. By collecting regular metrics or 'business analytics' it can measure the effectiveness of the leaners and then allows adjustment to the learning tool for the visualization and investigation of company employee data sets allowing strategic advantages and improvement of education and learning of a workforce (Ferguson, 2012) [11]. A robust LMS can capture data about a course results and answers and data about the user activity. This data can be interpreted to assess questions and responses that a lot of people are struggling with through reporting features and therefore can adapt the course accordingly to work on delivering the material in a more understandable way (Dawson, McWilliam, & Tan, 2008). Schläfke, Silvi and Möller (2012) [22] support this notion where performance management analytics has been found to increase performance. This could be explained as business competition increases, slight advantages of data analytics can make all the difference to help best support management decision-making and employee performance. LiMETOOLS incorporates the LMS, Litmos, to capture appropriate metrics for example reporting on specific individuals and teams to access knowledge retention of eLearning module. The analytics provide valuable feedback to businesses about their employees to allow for the determination of which cyber security areas are better understood and where vulnerabilities lie. By determining what vulnerabilities there are in a business as a whole, a team or individual, enables future e-learning programmes to be tailored to improve these specific behaviours.

2.3 Long-Term Habit Change and Retention of Learning

In this section we consider the timing of persuasive messages/ when to interrupt the user and effective presentation of communications.

2.3.1 Proposal of a Habit Retention Product and Intermittent Learning.

We are looking to explore the most powerful way to increase eLearning retention in the workplace by using smaller, more incremental interventions. Ebbinghaus (1964) [10] proposes distributed practice or spacing effect increases memory compared to massed learning. This suggests, rather than providing information through an e-learning module on a one-time basis, delivering information using different formats could develop learning and increase habit retention. This may be through a video magazine with embedded learning information and quizzes, which could lead to the retention of a behaviour change. Schwarz and Clore (1983) [23] suggest messages are perceived more persuasive if it is consistent with user's mental representations. This may mean that by taking the full eLearning tool, the users are more likely to have built up representations of the material and therefore presenting 'bite-sized' reminders of the same tool, will aim to persuade them to maintain cyber secure behaviour and potentially cause long term habit change. The challenge that arises is for Bournemouth University and LiMETOOLS to ensure that these behavioural cyber security changes are retained permanently, as it could be suggested the longer retention, the greater return on investment for the business.

2.3.1 Intermittent Learning.

Research in academic settings has shown that in order for learning to occur, self-paced learning needs to arise outside of the formal teaching activities such as assessment, seminars and lectures. Effective spacing requires students to understand the benefits and also to possess a certain degree of self-regulated learning. Although numerous studies demonstrate the benefits of spacing learning activities, many students seem unaware of this strategy. Instead, Taraban, Maki, & Rynearson (1999) [27] found that students crammed revision before exams, thinking that this is effective learning. Similarly, across three studies, Kornell (2009) [12] showed that even when students experienced the benefits of spaced learning they still retained the false belief that learning a large quantity of material at one time was more effective than spacing. Therefore, when designing behaviour change materials it is important to enhance awareness of the need for spacing. Although there is a growing number of studies investigating spacing in educational environments demonstrating convincing evidence that spacing is an effective approach for enhancing learning, there is less research showing how this can be applied in non-educational contexts and in online settings. One such study by Pereira, Taylor and Jones (2009) [18] found that spacing was an effective technique in improving retention and test performance for adults working in project management teams within industry and using an online training system in both company and social time.

2.3.3 Timing and Presentation of the Habit Change Tool.

It is essential to develop a positive habit change programme to better protect individuals and organisations to help prevent cyber security incidents [1]. The timing of the habit change tool will directly affect whether individuals are willing to take on further learning and continue with

cyber secure behaviour change. The timing and presentation of persuasive technology of real-time reminders to maintain behaviour has been researched in the health sector. IJsselsteijn et al., (2006) [14] explored strategies that interrupt users to perform healthy behaviours and whether there is a long-term health change. Users were presented with interrupting commands at fixed intervals within their working day. The results found that when the command was polite, it positively correlated with compliance and predicted a long-term habit change. Moreover, when there was an annoying interruption, compliance dramatically decreased. This therefore expresses that timing of messages could interrupt the working day but providing the presentation of the command is articulated in a polite, respectful manner long-term habit change could occur. However, Cutrell et al., (2001) [7] expressed that any interruptions in the working day will affect performance negatively even if they are ignored. Alternatively, notification-based alerts to remind individuals that there is a new behaviour change command ready to be viewed may work better in changing behaviour. Czerwinski and Schumacher (1991) [8] found the pre- warning notification did not affect day to day performance because a user is put in control of when they view the full content of the notification. LiMETOOLS could implement a habit change tool whereby notifications are used to alert that a new intermittent learning tool is available, and individuals are more likely to participate and in turn could maintain cyber secure behaviours.

3.0 Discussion and Conclusion

We suggest in this article that the collaboration between technology companies and psychology researchers improves the quality of cybersecurity education and behavior change amongst end users. Also, we have highlighted that to enable behaviour change in cyber security practices in end users a blend of delivery methods is essential through knowledge-based awareness, video dramas and gamification methods. Applying analytics to a workforce's responses to eLearning can enable better understanding of where parts of the businesses are vulnerable in areas of cyber security. Tailored eLearning programmes can then be adapted to teams or individuals to help prevent cyber-attacks. To continue and maintain behaviour change, collaboration between academics and companies will conduct further research into the timing and delivery of intermittent learning strategies. By enabling better understanding of the underlying processes, better learning retention and long term cyber security habit changes can occur. Future research for this area would be using existing LiMETOOLS cyber learning tools and developing some smaller incremental learning product as oppose to massed learning. Comparative research can then be undertaken to see whether recall or habit change is better incrementally or in a massed fashion for both versions of the same tool. Moreover, future research could be the timing of the incremental tool within a corporate environment for when the best time to interrupt users in their working day is in order to watch the tool and how long the incremental learning tool should be.

References

<bib id="bib1" type="Other"><number>[1]</number>Abawajy, J., (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33* (3), pp.237-248.</bib>

<bib id="bib2" type="Other"><number>[2]</number>Ashenden, D. and Lawrence, D. (2013)Can we sell security like soap?: a new approach to behaviour change. *In Proceedings of the 2013 workshop on New security paradigms workshop* (pp. 87-94). ACM.</bib>

<bib id="bib3" type="Other"><number>[3]</number>Bada, M. and Sasse, A., (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?.</bib>

<bib id="bib4" type="Other"><number>[4]</number>Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Englewood Cliffs, NJ: Prentice-Hall</bib>

<bib id="bib5" type="Other"><number>[5]</number>Blythe, J., 2013. Cyber security in the workplace: Understanding and promoting behaviour change. Proceedings of CHI'2013 Doctoral Consortium, 1065, pp.92-101. Florence, Italy.</bib>

<bib id="bib6" type="Other"><number>[6]</number>Boopathi, K., Sreejith, S. and Bithin, A., (2015). Learning cyber security through gamification. *Indian Journal of Science and Technology*, *8* (7), pp.642-649.</bib>

<bib id="bib7" type="Other"><number>[7]</number>Cutrell, E., Czerwinski, M., Horvitz, E. (2001). Notification, Disruption, and Memory: Effects of Messaging Interruptions on Memory and Performance. In: INTERACT'01, pp. 263–269</bib>

<bib id="bib8" type="Other"><number>[8]</number>Czerwinski, M., S, C., and Schumacher, B. (1991). The effects of warnings and display similarities on interruption in multitasking environments. *SIGCHI Bulletin*.*23* (4) 38-39.</bib>

<bib id="bib9" type="Other"><number>[9]</number>Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*, 1739-1747. doi:10.1016/j.chb.2010.06.023</bib>

<bib id="bib10" type="Other"><number>[10]</number>Ebbinghaus, H. (1964). Memory: A contribution to experimental psychology. Ruger HA, Bussenius CE, Hilgard ER, translators. New York: Dover Publications.</bib>

<bib id="bib11" type="Other"><number>[11]</number>Ferguson, R. 2012. Learning analytics: drivers, developments and challenges. *International Journal of Technology Enhanced Learning*, *4* (5-6), 304-317.</bib>

<bib id="bib12" type="Other"><number>[12]</number>Goleman, D. (1995), **Emotional Intelligence** , Bantam Books, New York, NY</bib>

<bib id="bib13" type="Other"><number>[13]</number>Guadagno, R.E. and Cialdini, R.B., 2005. Online persuasion and compliance: Social influence on the Internet and beyond. The social net: The social psychology of the Internet, pp.91-113.</bib>

<bib id="bib14" type="Other"><number>[14]</number>IJsselsteijn, W., de Kort, Y., Midden, C., Eggen, B., & van den Hoven, E. (2006). Persuasive technology for human well-being: setting the scene. *Persuasive technology*, 1-5.</bib>

<bib id="bib15" type="Other"><number>[15]</number>Kahneman, D. (2011). Thinking, fast and slow. London: Allen Lane.</bib>

<bib id="bib16" type="Other"><number>[16]</number>Kohlberg, L. (1981), The Philosophy of Moral Development, San Francisco, CA.</bib>

<bib id="bib17" type="Other"><number>[17]</number>Light, G, Cox, R. and Calkins, S. (2010), *Learning and Teaching in Higher Education: The Reflective Professional*, 2nd ed., Sage, London.</bib>

<bib id="bib18" type="Other"><number>[18]</number>Pereira, C., Taylor, J. and Jones, M., 2009. Less learning, more often: the impact of the spacing effect in an adult e-learning environment. Journal of Adult and Continuing Education, 15(1).</bib>

<bib id="bib19" type="Other"><number>[19]</number>Petty, R.E. and Cacioppo, J.T., 1986. The elaboration likelihood model of persuasion. Advances in experimental social psychology, 19, pp.123-205.</bib>

<bib id="bib20" type="Other"><number>[20]</number>Pfleeger, S.L. and Caputo, D.D., (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31* (4), pp.597-611.</bib>

<bib id="bib21" type="Other"><number>[21]</number>Pituch, K. A., & Lee, Y.-K. (2006). The influence of system characteristics on e-learning use. Computers & Education, 47, 222–244.</bib>

<bib id="bib22" type="Other"><number>[22]</number>Schläfke, M., Silvi, R., & Möller, K. (2012). A framework for business analytics in performance management. *International Journal of Productivity and Performance Management*, *62* (1), 110-122.</bib>

<bib id="bib23" type="Other"><number>[23]</number>Schwarz, N., & Clore, G.L. (1983). Mood, misattribution, and judgments of well-being: Informative and directive functions of affective states. *Journal of Personality and Social Psychology*, 45, 513-523</bib>

<bib id="bib24" type="Other"><number>[24]</number>Shaw, R. S. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92–100. doi: 10.1016/j.compedu.2008.06.011</bib>

<bib id="bib25" type="Other"><number>[25]</number>Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E., (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. *In Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88- 99). ACM.</bib>
<bib id="bib26" type="Other"><number>[26]</number>Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8* (1), pp.31-41.</bib>
<bib id="bib27" type="Other"><number>[27]</number>Taraban,R., Maki, W.S., & Rynearson K. (1999) Measuring study time distributions: Implications for designing computer-based courses. Behavior Research Methods, Instruments, & Computers, 31, 263–269. doi:10.3758/BF03207718.</bib>
Received January 2018, revised March 2018, accepted April 2018