Using a Game to Explore Notions of Responsibility for Cyber Security in Organisations

Dorota Filipczuk
Charles Mason
Stephen Snow
University of Southampton
Southampton, UK
dorota@ecs.soton.ac.uk
cm21g15@soton.ac.uk
S.Snow@soton.ac.uk

ABSTRACT

Improving the cyber literacy of employees reduces a company's risk of cyber security breach. Game-based methods are found to be more effective in teaching users how to avoid fraudulent phishing links than traditional learning material such as videos and text. This paper reports on the development of a mobile app designed to improve cyber literacy and provoke users' perceptions of *who* is *responsible* for cyber security in organisations. Based on a preliminary trial with 17 participants, we investigated users perceptions of a tongue-in-cheek, provocative cyber security awareness game where users' jobs depend on their aptitude for protecting their organisations' cyber security. Findings suggest that users accepted the high responsibility levelled upon them in the game and that ludic elements hold promise for engagement and increasing users' cyber awareness.

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5971-9/19/05.
https://doi.org/10.1145/3290607.3312846

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; **Privacy protections**.

KEYWORDS

Cyber Security Awareness; Gamification; Mobile Learning

ACM Reference Format:
Dorota Filipczuk, Charles Mason, Stephen Snow. 2019. Using a Game to Explore Notions of Responsibility for Cyber Security in Organisations. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI'19 Extended Abstracts), May 4–9, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3290607.3312846

INTRODUCTION

In recent years, cyber attacks have become more prevalent and more costly. In 2015, 98% of organisations had received malware-related attacks, and 70% had been targeted by phishing or social engineering attacks [7]. On average, enterprises lost over half a million dollars from security breaches [7]. Users themselves are increasingly labelled as problematic, weaknesses, or liabilities for corporate cyber security: 52% of businesses suggested that employees are their "biggest weakness" in terms of cyber security protection, and the top three reported cyber security fears for businesses are all related to human factors and employee behavior [8].

Yet, formalised cyber security training is not common in organisations – in 2017, only 20% of UK companies had their staff receive or attend cyber security training [5]. Game-based learning approaches, particularly mobile learning (m-learning) [4], represent a relatively new approach to cyber security education. A study comparing the use of text, videos and games found that m-learning can be effective in raising awareness of cyber security issues, and that a game-based method was found to be more effective in teaching users how to avoid fraudulent phishing links than traditional text-based and video-based learning material [1].

The purpose of this paper is to explore effective and enjoyable mechanisms for the delivery of cyber security education for employees that will enable them to make more informed cyber security decisions. Aiming to transcend the monotony and time-intensive nature of existing PC-based workplace training platforms (e.g. health and safety training), we designed a simple m-learning game with the intention of fostering participation in cyber security awareness in offices. Beyond understanding how best to engage and inform users, we wanted to confront the ethical dimensions of the implicit, almost accusational positioning of users as "weaknesses" to their corporations' cyber security. Accordingly, we chose a purposefully playful yet provocative storyline, implicitly shouldering users with responsibility for their company's cyber security. We trialled the app with 17 participants with the aim to: (1)

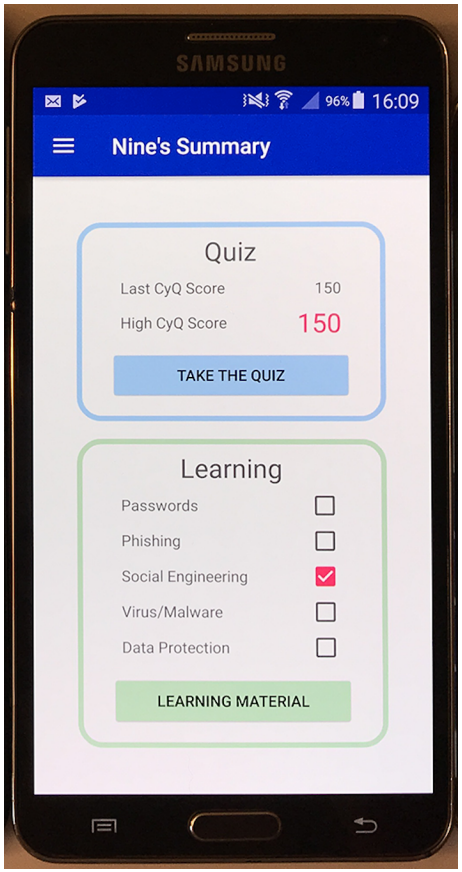

Figure 1: The main screen of the app. The learning material is grouped together under five categories: Passwords, Phishing, Social Engineering, Virus/Malware and Data Protection.

test which elements of the game hold potential for fostering engagement with cyber security and (2) understand how users interpret and react to a playful provocation of being made to feel solely responsible for their organisions cyber security, shining a light on the implicit positioning of users as the weakest link in cyber security literature [2, 3, 9, 11].

APPLICATION DESIGN

To produce an informative, fun, and quick experience that is palatable and enjoyable for time-constrained office workers, the game takes the form of a series of quizzes. Before taking a quiz, users can access a range of learning materials grouped under categories: Passwords, Phishing, Social Engineering, Virus/Malware and Data Protection, as presented in Fig. 1. These categories were deemed to be the most important areas of cyber security for non-expert professional knowledge workers to be made aware of from our review of existing products and literature. To be relevant for employers and managers, we designed the app to be capable of providing an assessment of all users' current knowledge with a short interaction time, using a multiple choice quiz format (see Fig. 2).

Our choice of the mobile platform for the game relates to the increased flexibility in delivery available with mobile content [10] and our wish for the app to be available to users anywhere, irrespective of Internet access (run locally once downloaded). In order to minimise business risk exposure, a design requirement identified was that the app must provide an assessment of each employee's current knowledge for the manager, as well as an enjoyable learning experience for the user.

Storyline: in the game, the user, employed at a fictional company, has to survive without being fired for making poor cyber security choices. Still [12] suggests that labeling users as the problem is an unfair displacement of responsibility. Yet, precisely how users feel about this implicit positioning has not yet been tested. Accordingly, we were interested in how users responded to this notion of responsibility and the palatability of a dark humour approach, in preference to the positive (and more common) storyline of the user becoming a hero, e.g. saving their company from malicious attack.

Game Play: each multiple choice quiz introduces a scenario before displaying the question and up to four answer choices. When a user selects an answer, they are presented with a dialog box displaying information relevant to the question. This repeats for the duration of the quiz. The goal is to answer all questions, getting fewer than three incorrect. Upon passing, the user is shown the number of questions they got correct in each category and their final score. They can navigate to the summary which displays a breakdown of their past scores and which educational material pages they have read. If the user fails the quiz, a button takes them to the learning material of the failed section - once they read the material, they can retake the quiz. A leaderboard allows users to benchmark themselves and compete with others. A number of parameters are logged, including the results of each individual

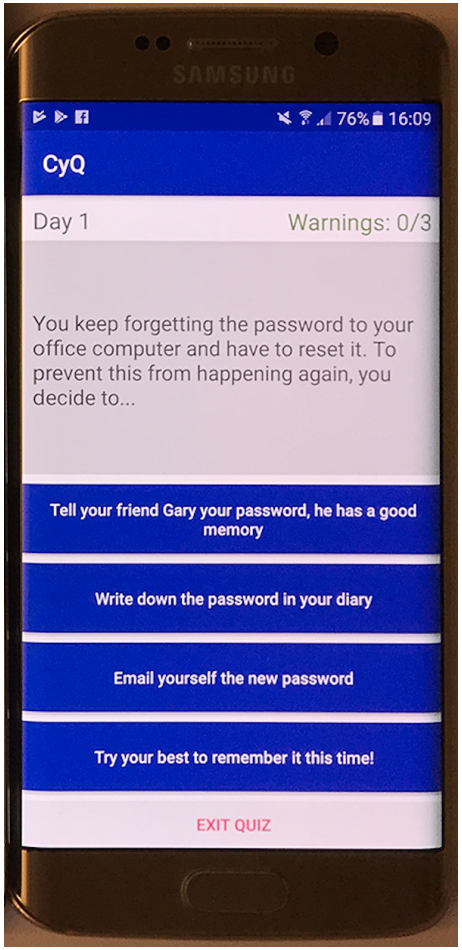

Figure 2: An example quiz screen. The multiple-choice question tests users' decision-making in vulnerable situations.

quiz attempt, which questions the participant answered correctly/incorrectly, the outcome of the quiz, the time taken to complete it and which learning material pages have been read.

PRELIMINARY USER STUDY

Following the approval of the study by our institution's ethics committee (IRB ref.: ERGO/FPSE/40173), 17 participants took part in the initial evaluation of the app (8 male, 9 female). Six of them were employers and managers from the healthcare, manufacturing and online publication industries; the remaining 11 were employees (not managers) from various sectors and students. The participants were sampled using convenience sampling where all represented contacts of the researcher. The participants were not experts in cyber security and had not previously been involved in the development of the app or iterations of the initial prototypes.

All participants received the same protocol. First, they filled out a questionnaire on demographics, self-reported existing cyber security literacy and any past cyber security training. Then, they were instructed to take the quiz to establish their baseline level of cyber security knowledge, the results from which could then be compared to subsequent quiz results to track their performance. If the participant failed the quiz, they were asked to revise the learning material, reading the information relevant to the incorrectly answered questions. This was repeated until they passed the quiz, after which they completed a closing questionnaire of Likert scale responses (1-Strongly disagree to 7-Strongly agree) and questions about the design and usability of the app, their learning experience, changes to their self-reported cyber security literacy and a question eliciting opinions on the scenario of the app. We did not elicit opinions on responsibility for cyber security in companies in the initial questionnaire, wishing to avoid the possibility of biasing responses. Instead, we chose to provide users with only functional instructions on how to use it and elicited general opinion on the scenario afterwards.

RESULTS

We present the results of the study, including the usability of the tool, self-reported cyber literacy, completion time, educational aspects, and participants' attitudes towards the scenario.

Usability. Participants were asked to rate the usability of the app, with all but one of the 17 participants agreeing with the statement "The app is easy to use and navigate" on a 7 point Likert Scale between 1-Strongly Disagree to 7-Strongly Agree (mode: 7, average 6.4). Suggestions for improvement were relatively minor, including the background colour and two users not noticing the "back" button in the top left hand corner of the app.

Game completion & content. All participants passed the quiz in fewer than five attempts. The majority of users took between 5 and 10 minutes to pass. Of the seven participants who passed on their first attempt, six indicated they had received at least some level of cyber security education prior to this study. Conversely, all but one of the 10 participants who did not manage to pass the quiz first

time indicated that they had never received cyber security education. 67% of the 'employers' group passed the quiz successfully first time, whereas only 27% of the 'general population' group were able to do so. The content of the app in its current state was deemed to be relevant and of sufficient detail for understanding, as confirmed by 15 participants.

Cyber awareness. 15 participants agreed that the app increased their awareness of cyber security issues. In particular, five participants mentioned that they learnt about the difference between HTTP and HTTPS, e.g. when asked "*What was a new thing that you learnt through use of the app?*, one of them answered: "*I didn't immediately know 'https' was more secure than 'http'*". Of the two participants who did not report the app increased their cyber security awareness, one participant noted they were already "*well informed*" and knew the material.

Perceptions on accountability scenario. On a 7-point Likert scale, 14 out of 17 agreed that the scenario (i.e. keeping the job by correctly answering questions) improved their engagement and enjoyment of the app (mode: 6, average: 5.6). Where user responses were further towards "disagree", the main justification was that some of the scenario-based questions in the quiz were not entirely relevant that participant's line of work, rather than due to reservations, the nature of the story-line, or the onus of responsibility for cyber security placed upon the user in the game.

DESIGN SUGGESTIONS

The game was found to be intuitive, usable and easy to navigate by the participants. All but two indicated their cyber literacy had been improved by using the app, however, future trials are necessary to enable us to better clarify its effectiveness as a learning tool. Nonetheless, the finding from this study supports [1] in that m-learning games for cyber security training seem to offer a high potential for engagement with cyber security. Our preliminary findings suggest that an increase in cyber literacy from using the game may be possible with a short interaction time (< 10 minutes). Moreover, participants' interaction times varied according to prior knowledge; users with a higher level of background knowledge completed the game faster than those without. These attributes suggest such a quiz-based platform may be suitable for the time-constrained context of office environments, offering time-saving advantages over traditional workplace e-learning platforms (e.g. Health and Safety) where all users must navigate through all scenarios. Additionally, the design benefits employers by ensuring a given level of competency among staff and providing a rough estimation of overall human security risks in an organisation. Labelling users as liabilities for corporate cyber security is commonplace [8], yet has been argued to represent an unfair displacement of responsibility for cyber security [12]. Future work might further explore how users themselves might feel about being burdened by this responsibility. We chose a tongue-in-cheek story-line in which the user gets fired if they incorrectly guess too many questions – surprisingly, despite this purposefully extreme scenario, our participants were not bothered by this high level of responsibility.

CONCLUSIONS AND FUTURE WORK

This paper has showcased our early-stage prototype for providing organisations with a fun, functional, low-interaction-time means of engaging users with cyber security training that transcends the monotony and time-drain of many obligatory workplace training platforms. Much future work is warranted in this area, for example, to: (1) gather more widespread, detailed and qualitative opinions from employees regarding perceived responsibility for their companies' cyber security; (2) understand "carrot" *vs.* "stick" incentives for cyber security learning materials – the prototype here applied an exaggerated and ludic "stick" method with the game revolving around not getting fired, yet this proved more palatable to office workers than we anticipated, and users may in fact respond well to a high expectation of responsibility for cyber security – alternative "carrot" incentive-based games might position the user as a hero who must save their company from cyber attack, or focus on what a user *can* safely safely do navigate a system, rather than what they *shouldn't* do (as emphasised in our prototype); (3) seek to more definitively measured higher order learning outcomes possible through cyber literacy games, using Blooms Taxonomy [6].

REFERENCES

[1] Jemal Abawajy. 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology* 33, 3 (2014), 237–248.

[2] Fadi A Aloul. 2012. The need for effective information security awareness. *Journal of Advances in Information Technology* 3, 3 (2012), 176–183.

[3] Ashley A Cain, Morgan E Edwards, and Jeremiah D Still. 2018. An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications* 42 (2018), 36–45.

[4] Tsvetozar Georgiev, Evgenia Georgieva, and Angel Smrikarov. 2004. M-learning-a New Stage of E-Learning. In *International conference on computer systems and technologies-CompSysTech*, Vol. 4. 1–4.

[5] Culture Media & Sport Gov.uk, Department for Digital. 2017. Cyber Security Breaches Survey 2017. https://www.statista.com/statistics/270291/

[6] David R Krathwohl. 2002. A revision of Bloom's taxonomy: An overview. *Theory into practice* 41, 4 (2002), 212–218.

[7] Kaspersky Lab. 2015. Global IT Security Risks Survey 2015. Retrieved September 20, 2018 from https://media.kaspersky.com/pdf/global-it-security-risks-survey-2015.pdf

[8] Kaspersky Lab. 2017. Report Human Factor in IT Security. Retrieved September 20, 2018 from https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2017/11/10083900/20170710_Report_Human-Factor-In-ITSec_eng_final.pdf

[9] Rebecca M Long. 2013. Using phishing to test social engineering awareness of financial employees. (2013).

[10] Brook Sattler, Irini Spyridakis, Ninad Dalal, and Judy Ramey. 2010. The learning experience: A literature review of the role of mobile technology. In *Professional Communication Conference (IPCC), 2010 IEEE International*. IEEE, 38–45.

[11] Scott Seidenberger. 2016. A new role for human resource managers: Social engineering defense. (2016).

[12] Jeremiah D Still. 2016. Cybersecurity needs you! *interactions* 23, 3 (2016), 54–58.