CSIR
our future through science

UNIVERSITEIT
iYUNIVESITHI
STELLENBOSCH
UNIVERSITY
100
1918 · 2018
forward together · saam vorentoe · masiye phambili

Proceedings of the
14th International Conference on Cyber Warfare and Security

Stellenbosch University
South Africa
28 February - 1 March 2019

Edited by

Noëlle van der Waag-Cowling

Stellenbosch University, South Africa

Dr. Louise Leenen

CSIR and the University of the Western Cape, South Africa

acpi

A conference managed by ACPI, UK

Proceedings of the

14th International Conference on Cyber Warfare and Security
ICCWS 2019

Hosted By
Stellenbosch University and the CSIR
South Africa

28 February - 1 March 2019

Edited by
Noëlle van der Waag-Cowling
and
Dr. Louise Leenen

Review Process

Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy

ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:
http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academic-conferences-and-publishing-international-limited/

Conference Proceedings

The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

The Electronic version of the Conference Proceedings is available to download from DROPBOX http://tinyurl.com/ICCWS19. Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.
The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-912764-12-9
E-Book ISSN: 2048-9889
Book version ISBN: 978-1-912764-11-2
Book Version ISSN: 2048-9870

Published by Academic Conferences and Publishing International Limited
Reading
UK
44-118-972-4148
www.academic-conferences.org

A Rollout Strategy for Cybersecurity Awareness Campaigns

Thulani Mashiane, Zama Dlamini and Thabo Mahlangu
Council for Scientific and Industrial Research, Pretoria, South Africa
tmashiane@csir.co.za
idlamini@csir.co.za
tmahlangu3@csir.co.za

Abstract: It is important that government, private sectors and the citizens are cybersecurity savvy. This is often a challenge as the size of the target group is large and the expertise is diverse. This is coupled with limited resources, in terms of time and funding, making is difficult to administer cybersecurity awareness campaigns to a large target group. With these challenges in mind, it is the aim of the current paper to propose a cybersecurity awareness campaign rollout strategy for large and diverse groups. The main components of the strategy include posters, face-to-face training, games and an eLearning experience. This rollout strategy can be considered as an innovative and sustainable solution of educating many Internet users. Not only will this strategy contribute to the safety and security of organisational system infrastructure, it will also elevate and develop individual self-defence skills of the users.

Keywords: cybersecurity, awareness, campaign, eLearning, cybersecurity education

1. Introduction

Any organisation that has an online presence cannot ignore the recent influx of cyber-attacks. The current situation requires that employees are aware and skilled in cybersecurity to avoid falling victim to these attacks. However, the reality is that most employees lack cybersecurity knowledge and skills. This creates a dangerous environment because employees, who are vulnerable to cybersecurity threats, could be used as entry points for cyber criminals.

Recent cyber threats such as Liberty email hack, the ‘ViewFines’ license scam, Facebook personal information scandal, Ster-Kinekor attack and Master Deed’s data leak have sparked a new fire on cybersecurity in South African organisations (Mohapi, 2018; Niselow, 2018; Shapshak, 2018). Many organisations continually take technological steps to ensure the safety of systems. It is equally important that users, as part of securing organisational systems, are also kept updated with cybersecurity knowledge and skills. This can be achieved through continuous cybersecurity awareness training. The aim of cybersecurity awareness training is to empower and equip users with knowledge and skills to enable them to defend themselves, in the event of a cyber-attack.

Unfortunately, in most cases not all employees are exposed to cybersecurity awareness training. This is due to:

- Lack of funding
- Employee availability
- Lack of Cybersecurity experts in the country
- A very large number and diversity of employees in the organisation

Solutions towards educating users in cybersecurity have been proposed in academia (Kritzinger Elmarie, 2016). These include short term solutions such as posters, competitions, workbooks and discussions (Kritzinger Elmarie, 2016). ELearning platforms such as the method proposed in (Stewart, Humphries, & Andel, 2009), which focuses on building skills for network configuration. Games that simulate the real world are discussed in (Thompson & Irvine, 2015). The games teach cybersecurity principals by allowing the user to encounter cybersecurity incidents in a sandbox environment. These solutions are innovative; however, they are not sufficient to be used for a large target audience. It is for this reason that the current paper seeks to address these challenges through a proposed rollout strategy.

The rest of the paper is presented as follows: the next section presents the background to the study on cybersecurity awareness, this is followed by the discussion on how one can plan the cybersecurity awareness campaign in Section 3. Section 4 proposes the cybersecurity awareness rollout strategy, and Section 5 concludes this paper.

2. Cybersecurity awareness

Cybersecurity is defined as the technologies, processes, controls and users that are set up to protect systems and system data. A large, and often neglected, part of cybersecurity are the users. Which is one of the reasons why, researchers and security practitioners agree that the human aspect of cybersecurity is very important. Cases of recent cybersecurity threats and vulnerabilities point at attackers exploiting the ignorance of users to successfully launch attacks. The cybersecurity discussion has grown to now include users as well infrastructure as a way to prevent successful cybersecurity attacks (Khan & Ayyob, 2017; Uchida, 2017). The discussion now includes the task of bringing users to an acceptable level of cybersecurity awareness.

Cybersecurity awareness campaigns are a form of security training that is used to inspire, stimulate, establish and build cybersecurity knowledge and skills amongst system users (Defence, 2008; Grobler, Dlamini, Ngobeni, & Labuschagne, 2011). A successful training program makes sure that the user is not only informed about these treats, but is also able to recognise and deal with threats and vulnerabilities in their own environment (Bada & Sasse, 2014). Furthermore, an awareness campaign must inspire a positive attitude towards upholding cybersecurity amongst the participants of the training (Grobler et al., 2011).

3. Planning cybersecurity awareness campaign

Cybersecurity awareness campaigns should have a plan, clearly defined goals and objectives, expected results, delivery methods, risks, and methods to evaluate the initiative. A users' level of cybersecurity awareness is measured by the users' cybersecurity knowledge about best practices, their consciousness of how important cybersecurity is as well as their ability to defend themselves when online.

The following components constitute the process of a typical cybersecurity awareness campaign:

- **Cybersecurity Awareness Goals and Objectives**: this must be defined in terms of the national legislation, laws, policies and standards as well as continental policies and agreements
- **Identify Intended Audience**: these are the target trainees, to whom the cybersecurity awareness campaign will be delivered (e.g. Community citizens, IT employees, non-IT employees, students, learner, etc.)
- **Define Topics to be Covered**: the list of topics must be evaluated in terms of relevance to each targeted audience
- **Define Delivery Methods to be Used**: this includes the way in which the cybersecurity awareness campaign will be presented to different audiences (e.g. For the primary learner, one can use cybersecurity posters and drawings; and for the employees, one can use e-mail system, company newsletter, seminars, etc.),
- **Develop a Strategy for Rollout**: this should be decided on all levels and the entire programme should be evaluated for possible loopholes. For instance, the programme's implementation should start from the grade zero, in schools; or the arrangement of the seminars in the workplace, that is, which group attends it first in order to avoid disturbing all the company processes
- **Develop Evaluation Methods:** these are the methods that will be used to test the effectiveness of the cybersecurity awareness campaign (e.g. The comparison of pre- and post-survey)

The cybersecurity awareness plan can be updated to suit various target audiences. The current paper's contribution is in addressing the development of the rollout strategy for cybersecurity awareness campaigns in large organisations.

3.1 Delivery methods

Cybersecurity awareness can be delivered in different ways. Researchers and practitioners of cybersecurity have presented different alternatives to drive the cybersecurity message to the users. Posters, Lectures, Games and eLearning are presented in the next session.

3.1.1 Posters

Posters are a visual art form used to relay information. In cybersecurity, posters are a traditional delivery method. Typical cybersecurity posters contain one cybersecurity message together with a catching slogan for employees to remember (Abawajy, 2014).

The power of posters is that employees are continuously exposed to the same message. Repeated exposure creates familiarity with the context as well a positive attitude towards the message on the poster (Zajonc, 1968). In other words, posters can be used as a form of conditioning employees to the principals of cybersecurity. There are concerns in the usage of posters, such as the misinterpretation or overlook of the message. Too much exposure to the same information may result in the importance of the message being diminished (Janiszewski & Meyvis, 2001).

3.1.2 Lectures

Lectures or Face-to-face interactions use an expert base approach were a facilitator or subject expert conducts a talk about cybersecurity. These talks have a lecture approach where the education is delivered in a top-down manner. The lectures have an opportunity to ask and answer questions during the lecture. However, this method has its disadvantages in the form of they are expensive, time consuming and may not be relevant to the entire audience (Abawajy, 2014; Dlamini & Modise, 2013). The success of face-to-face interactions is heavily reliant on the person presenting the lecture. If the presenter is not charismatic or interesting, the audience may not pay attention to what is being presented (Kritzinge Elmarie, 2017).

3.1.3 Games

Games are used as a supplement in Cybersecurity training. Games create excitement which motivates and engages employees. If the game has a competitive element, the game can create a challenge which drives employees to outdo each other (Grossklags, Christin, & Chuang, 2008; Jin, Tu, Kim, Heffron, & White, 2018). This is a good way to reinforce the Cybersecurity principals which were presented. A disadvantage of games is that the desire to win the game may overshadow the learning of Cybersecurity principals (Cone, Irvine, Thompson, & Nguyen, 2007; Cone, Thompson, Irvine, & Nguyen, 2006; Nagarajan, Allbeck, Sood, & Janssen, 2012).

3.1.4 eLearning

ELearning is a platform for conducting training where the geographical location of the lecturer and participant is different. Participants enrol into courses and can interact with the lecture as well as other students (Rjaibi, Rabai, & Mili, 2016; Skinner, Taylor, Dale, & McAlaney, 2018). Technology is the backbone of eLearning platforms and it allows for an interesting, different and diverse way to interact with learning material. The advantages of eLearning are that they are self-paced, and the participants may complete the course on their own time. A disadvantage however is that often participants are not motivated to complete the course (Oyelere, Sajoh, Malgwi, & Oyelere, 2015; Skinner et al., 2018; Tirumala, Sarrafzadeh, & Pang, 2016). For the Cybersecurity context eLearning has provided a platform where participants can gain some practical experience with dealing with Cybersecurity attacks such as phishing.

Table 1 presents a comparison of Cybersecurity delivery methods. Table 1 lists each method's strengths and weaknesses as a tool for Cybersecurity awareness.

Table 1: Comparison of delivery methods

Delivery Method	Description	Strength	Weakness	Authors
Lectures	A lecturer presents Cybersecurity content	Provide opportunity to clarify points Interactive	Can become overwhelming Success relies heavily on the person presenting the awareness Time consuming	(Dlamini & Modise, 2013; Kritzinge Elmarie, 2017; Locasto & Sinclair, 2009)
Games	An activity where a person engages in for entertainment or sport. Cybersecurity games have a cybersecurity element or theme attached to them.	Engages the user Entertaining while learning	The point may be lost by users focussing on the game instead of the awareness principals Limited players	(Cone et al., 2007; Cone et al., 2006; Jin et al., 2018)
Posters	An image which displays a message. In the context of Cybersecurity, the message	Conditions the user over time	Message portrayed in poster might be misunderstood	(Kritzinger Elmarie, 2016)

Delivery Method	Description	Strength	Weakness	Authors
	being portrait is to promote cybersecurity.	Can be presented to a large audience		
eLearning	Computer mediated learning. In the cybersecurity context the lessons being presented are cybersecurity focused.	Can be done at user's own pace Contains a level of anonymity through self-selected usernames Multi-directional communication (with course provider and other students)	The user must be motivated to start and finish the course No face-to-face communication	(Rjaibi et al., 2016; Skinner et al., 2018)
Video	A recording or broadcast of images with the cybersecurity message.	Entertaining Can stop, rewind and replay Can be presented to a large audience	Unidirectional communication	(Dlamini & Modise, 2013; Kritzinger Elmarie, 2016)

3.2 Motivation

Individually, the delivery methods mentioned in Table 1 have received some level of success however, their weaknesses have been pointed out by (Bada & Sasse, 2014). However, research has proven that a combined delivery method for Cybersecurity awareness training is more effective than using one delivery method (Abawajy, 2014). The combination of delivery methods can be used to form a strategy. The aim is to exploit the strengths of the delivery methods while attempting to minimise the effect of their weaknesses. The current paper proposes a strategy for Cybersecurity awareness training rollout that incorporates traditional face-to-face training, eLearning (eduCyber) and games to reach a large target audience. The paper addresses the following needs:

- Cybersecurity training scalability
- Cybersecurity training rollout method

4. Proposed cybersecurity awareness rollout strategy

The cybersecurity awareness program will be developed to balance traditional training methods with cybersecurity material and educational learning tools into a stimulating learning experience. The proposed cybersecurity strategy is a composed of four main delivery methods. Posters, face-to-face interaction, games as well as eLearning. See Figure 2.

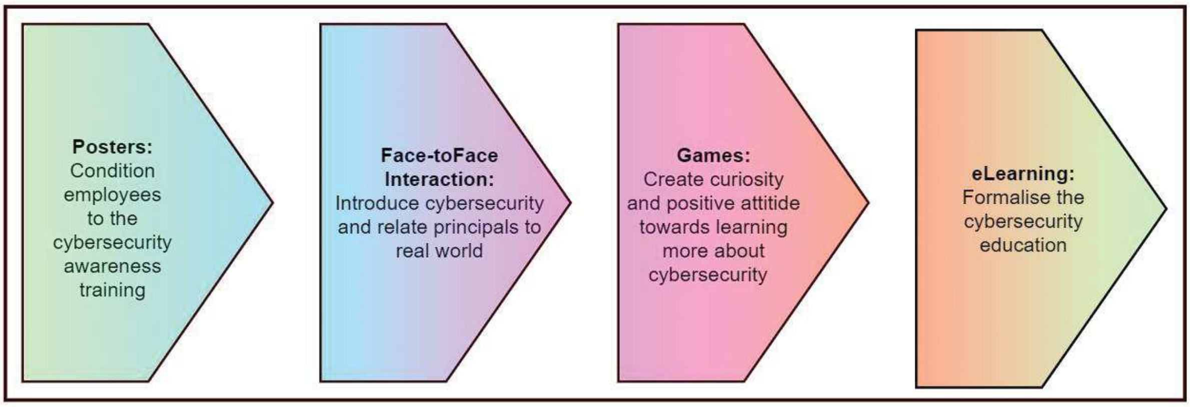

Posters: Condition employees to the cybersecurity awareness training
Face-toFace Interaction: Introduce cybersecurity and relate principals to real world
Games: Create curiosity and positive attitide towards learning more about cybersecurity
eLearning: Formalise the cybersecurity education

Figure 1: Cybersecurity rollout strategy

4.1 Posters

Design and print a set of posters with striking visuals and slogans are designed and put up around the common areas. The posters should be put up two weeks before the face-to-face interaction to create familiarity. The posters should then be removed after the last face-to-face interaction. An example poster is provided in the Figure 2.

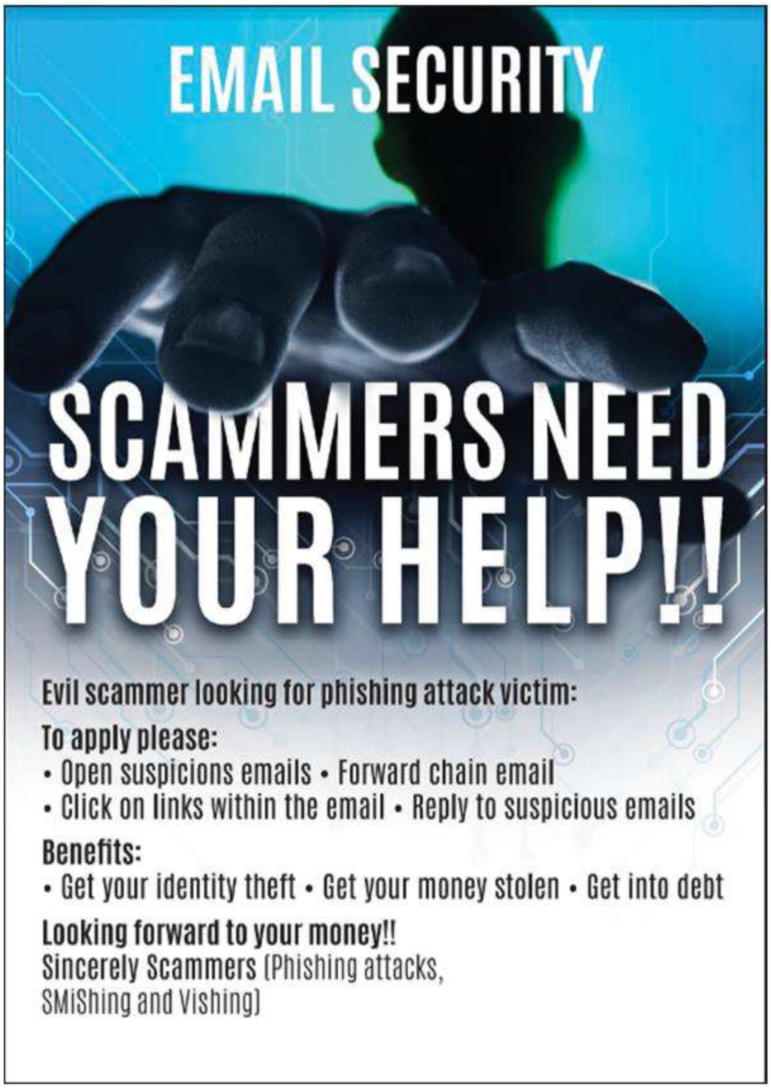

EMAIL SECURITY
SCAMMERS NEED YOUR HELP!!
Evil scammer looking for phishing attack victim:
To apply please:
• Open suspicions emails • Forward chain email
• Click on links within the email • Reply to suspicious emails
Benefits:
• Get your identity theft • Get your money stolen • Get into debt
Looking forward to your money!!
Sincerely Scammers (Phishing attacks,
SMiShing and Vishing)

Figure 2: Example of awareness poster

4.2 Face-to-Face interaction

The employees in a large organisation are divided into smaller groups, and a series of face-to-face interaction sessions are scheduled for each group. Group size should not exceed 100 people. The people in each group should be similar in job title. This is to enable the facilitators to present customised training for each group. Top management and a general working do not face the same cybersecurity challenges and therefore should be in different face-to-face sessions. These sessions should be kept under an hour to prevent cognitive overload of the employees.

The sessions are run by at least two facilitators. During the session, facilitators take turns in introducing the different topics in cybersecurity. The role of other facilitators is to encourage interaction of the employees. This is achieved by having the main facilitator as a presenter in front, while the other facilitators sit with the audience providing a few answers asked by the main facilitator. Once the audience is comfortable, the other facilitators may also pose questions to the audience to promote discussion.

The style of the presentations should be casual with elements of humour. The aim of the face-face interaction is for a facilitator to provide examples of how cybersecurity plays a role in the employees working and personal life. The customisation of examples for different groups plays an important role. For example, top managers should be aware of phishing emails that require the fraudulent signing of documents. While a general worker should be warned of phishing emails that might require the fraudulent executing of a purchase order. The aim of these sessions is to connect cybersecurity principals to the real world. At this stage it is not important for the facilitators to present formal definitions of terms.

At the end of the session the audience is divided into groups of four where each group is given a cybersecurity themed board game to play.

4.3 Board game

To end off the session, a cybersecurity game is played by the employees. The facilitators should explain the rules of the game and encourage participation. In this study, Securathon is used as an example game. Securathon is a cybersecurity themed board game, which has similar playing rules as the popular board game 30 Seconds. The game was designed for cybersecurity awareness training by, KFP Chan, a researcher at the Council for Scientific and Industrial Research (CSIR). Details of game play can be found in the Figure 3. The role of the game is to reinforce the lessons learnt during the face-to-face interaction. The game also introduces new principals not discussed during the session. The game session should not last more than 30 minutes. By the end of the face-to-face and game session the employees should be curious about cybersecurity and have a positive attitude towards learning more about the topics. This sets the stage for the final element of the cybersecurity strategy, the eLearning platform.

4.4 eLearning platform

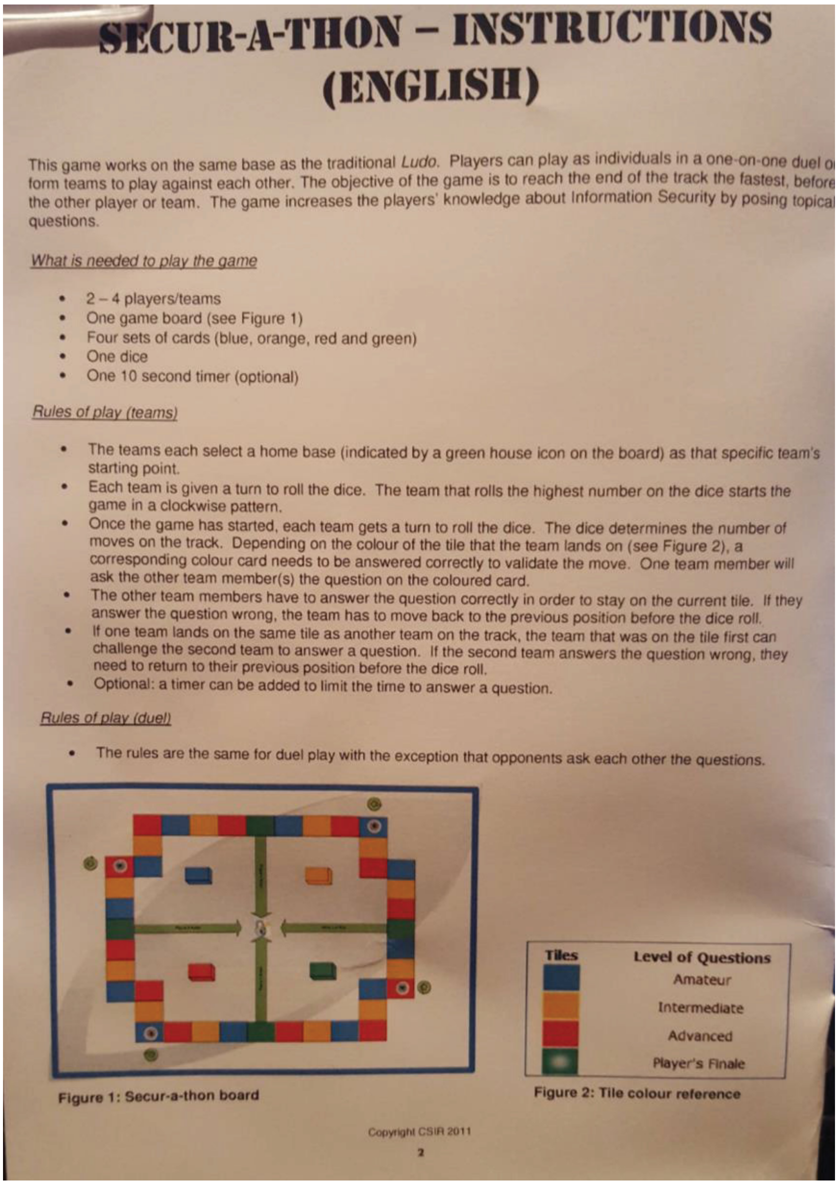
The final element of the rollout plan is providing the employees with the opportunity to formalise the training through the completion of an online course. At the end of the face-to-face session the users are given information on how to access the eLearning platform.

In this study, the online course is presented on eduCyber, a custom-built eLearning platform designed and implemented by the researchers. eduCyber is built on an open source platform and is easily customisable for different target groups. eduCyber allows a large number of users access to cybersecurity awareness training.

The main functionalities of eduCyber are:

- Online training based on the videos and slides
- Pre/post assessments
- Provide certificate of completion
- Provide analytics and reporting capability for the organization and training provider

Each employee is given the opportunity to complete the online course at their own pace and time. The employees should at this point be familiar with some of the cybersecurity principals. The role of the eLearning platform is to connect the practical examples given during the session to formal definitions.



SECUR-A-THON – INSTRUCTIONS (ENGLISH)

This game works on the same base as the traditional *Ludo*. Players can play as individuals in a one-on-one duel o form teams to play against each other. The objective of the game is to reach the end of the track the fastest, before the other player or team. The game increases the players' knowledge about Information Security by posing topical questions.

What is needed to play the game

- 2 – 4 players/teams
- One game board (see Figure 1)
- Four sets of cards (blue, orange, red and green)
- One dice
- One 10 second timer (optional)

Rules of play (teams)

- The teams each select a home base (indicated by a green house icon on the board) as that specific team's starting point.
- Each team is given a turn to roll the dice. The team that rolls the highest number on the dice starts the game in a clockwise pattern.
- Once the game has started, each team gets a turn to roll the dice. The dice determines the number of moves on the track. Depending on the colour of the tile that the team lands on (see Figure 2), a corresponding colour card needs to be answered correctly to validate the move. One team member will ask the other team member(s) the question on the coloured card.
- The other team members have to answer the question correctly in order to stay on the current tile. If they answer the question wrong, the team has to move back to the previous position before the dice roll.
- If one team lands on the same tile as another team on the track, the team that was on the tile first can challenge the second team to answer a question. If the second team answers the question wrong, they need to return to their previous position before the dice roll.
- Optional: a timer can be added to limit the time to answer a question.

Rules of play (duel)

- The rules are the same for duel play with the exception that opponents ask each other the questions.

Figure 1: Secur-a-thon board

Tiles	Level of Questions
🟦	Amateur
🟧	Intermediate
🟥	Advanced
🟩	Player's Finale

Figure 2: Tile colour reference

Copyright CSIR 2011

2

Figure 3: Securaton game play instructions

5. Conclusion

Even though most organisations have the tools and techniques to prevent organisation from cybersecurity threats, the recent trends are indicating that the human-aspects are the greatest contributors to organisations being vulnerable to cybersecurity threats. The paper presented a cybersecurity rollout strategy for a large organisation. The strategy consists of four elements, Posters, face-to-face presentation, games and eLearning. The advantage of the proposed strategy is that is scalable, and customisable for a large target audience. Future work in this research is the evaluation of the impact made by the strategy. As part of this goal, the current strategy has been rolled out to an organisation. With streamlined cybersecurity awareness programmes in organisations and communication, the national security posture could be improved.

References

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

Bada, Maria, & Sasse, Angela. (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

Cone, Benjamin D, Irvine, Cynthia E, Thompson, Michael F, & Nguyen, Thuy D. (2007). A video game for cyber security training and awareness. *computers & security, 26*(1), 63-72.

Cone, Benjamin D, Thompson, Michael F, Irvine, Cynthia E, & Nguyen, Thuy D. (2006). *Cyber security training and awareness through game play.* Paper presented at the IFIP International Information Security Conference.

Defence, Ministry of. (2008). Cyber Security Strategy Cyber Security Strategy Committee. http://www.sicurezzacibernetica.it/db/[Estonia]%20%20National%20Cyber%20Security%20Strategy%20-%20old%20-%202008%20-%20EN.pdf

Dlamini, Zama, & Modise, Mapule. (2013). Cyber security awareness initiatives in South Africa: A synergy approach. *Case Stud. Inf. Warf. Secur. Res. Teach. Stud*, 1.

Elmarie, Kritzinge. (2017). *A Curriculum Approach to Improving Cyber Safety in South African Schools.* Paper presented at the International Symposium on Emerging Technologies for Education.

Elmarie, Kritzinger. (2016). Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal, 28*(1), 1-17.

Grobler, Marthie, Dlamini, Zama, Ngobeni, Sipho, & Labuschagne, Aubrey. (2011). Towards a cyber security aware rural community.

Grossklags, Jens, Christin, Nicolas, & Chuang, John. (2008). *Secure or insure?: a game-theoretic analysis of information security games.* Paper presented at the Proceedings of the 17th international conference on World Wide Web.

Janiszewski, Chris, & Meyvis, Tom. (2001). Effects of brand logo complexity, repetition, and spacing on processing fluency and judgment. *Journal of consumer research, 28*(1), 18-32.

Jin, Ge, Tu, Manghui, Kim, Tae-Hoon, Heffron, Justin, & White, Jonathan. (2018). *Game based Cybersecurity Training for High School Students.* Paper presented at the Proceedings of the 49th ACM Technical Symposium on Computer Science Education.

Khan, Mudassir, & Ayyob, Mohammed. (2017). Computer Security in the Human Life. *Computer Security in the Human Life, 6*(1), 35-42.

Mohapi, Tefo. (2018). 4 things about the ViewFines website that shocked us. https://www.iafrikan.com/2018/05/30/viewfines-security-popular-passwords/

Nagarajan, Ajay, Allbeck, Jan M, Sood, Arun, & Janssen, Terry L. (2012). *Exploring game design for cybersecurity training.* Paper presented at the Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on.

Niselow, Tehillah. (2018). Five massive data breaches affecting South Africans. https://www.fin24.com/Companies/ICT/five-massive-data-breaches-affecting-south-africans-20180619-2

Oyelere, SS, Sajoh, DI, Malgwi, YM, & Oyelere, LS. (2015). *Cybersecurity issues on web-based systems in Nigeria: M-learning case study.* Paper presented at the Cyberspace (CYBER-Abuja), 2015 International Conference on.

Rjaibi, Neila, Rabai, Latifa Ben Arfa, & Mili, Ali. (2016). The Mean Failure Cost Cybersecurity Model to Quantify Security in E-Learning Environments *Developing Successful Strategies for Global Policies and Cyber Transparency in E-Learning* (pp. 95-120): IGI Global.

Shapshak, Toby. (2018). Liberty hack the 'biggest breach yet'. https://www.businesslive.co.za/fm/fm-fox/2018-06-21-liberty-hack-the-biggest-breach-yet/

Skinner, Tiffany, Taylor, Jacqui, Dale, J, & McAlaney, John. (2018). *The Development of Intervention E-Learning Materials and Implementation Techniques For Cyber-Security Behaviour Change*.

Stewart, Kyle E, Humphries, Jeffrey W, & Andel, Todd R. (2009). *Developing a virtualization platform for courses in networking, systems administration and cyber security education.* Paper presented at the Proceedings of the 2009 Spring Simulation Multiconference.

Thompson, Michael F, & Irvine, Cynthia E. (2015). CyberCIEGE: a video game for constructive cyber security education.

Tirumala, Sreenivas Sremath, Sarrafzadeh, Abdolhossein, & Pang, Paul. (2016). *A survey on Internet usage and cybersecurity awareness in students.* Paper presented at the Privacy, Security and Trust (PST), 2016 14th Annual Conference on.

Uchida, Katsuya. (2017). *Establish Security Psychology–How to Educate and Training for End Users.* Paper presented at the International Conference on Human-Computer Interaction.

Zajonc, Robert B. (1968). Attitudinal effects of mere exposure. *Journal of personality and social psychology, 9*(2p2), 1.