



salvos: A Game to Enhance Cyber Security Awareness in Sri Lankan Universities

J.A.P. Madushani
(Reg. No.: MS20908706)
M.Sc. in IT
Specialized in Cyber Security

Supervisor: Mr. Amila Senarathna

December 2021

**Faculty of Graduate Studies & Research
Sri Lanka Institute of Information Technology**

Table of Contents

Table of Contents.....	2
List of Figures	4
List of Tables	5
Acknowledgements.....	6
Abstract.....	7
Chapter 1 Introduction	9
1.1 Universities in Sri Lanka and their ICT adoption	11
1.2 Motivation.....	12
1.3 Aims and Objectives.....	16
1.4 Research Questions	17
1.5 Thesis Structure	18
Chapter 2 Review of the Literature.....	19
2.1 Introduction to Cybersecurity Awareness	19
2.2 Importance of Cybersecurity Awareness.....	19
2.3 Cyber Security Awareness Training Methods.....	22
2.4 Drawbacks of the current training methods.....	24
Chapter 3 Methodology.....	26
3.1 Introduction	26
3.1.1 Theoretical Framework.....	27
3.1.2 Hypothesis.....	28
3.1.3 Type of Study	28
3.1.4 Data Collection Method and Research instruments.....	29
3.1.5 Sampling Technique.....	30
3.1.6 Intended Data Analysis Techniques	32
3.2 Game Design	33
3.2.1 Goals.....	33
3.2.2 Need of a Game	33
3.2.3 Target Audience	34
3.3 Game Components	34
Chapter 4 Implementation of Salvos	42
4.1 Topics Considered for the Salvos	42
4.2 Gamification Concept	44
4.3 Learning Principles.....	44
4.4 Game Mechanism and Play.....	48
	2

Chapter 5 Results	53
5.1 Survey Results	53
5.2 Evaluation of Salvos	69
5.2.1 Normality Test.....	72
5.2.2 Paired sample t-test.....	74
5.2.3 Usability content.....	76
5.2.4 Learning Content.....	77
Chapter 6 Discussion.....	79
Chapter 7 Conclusions and Future Work	82
Bibliography	83
Appendix A: A Survey on Current Security Maturity in Universities.....	86
Appendix B: Instructions for the Game - Salvos	92
Appendix C: Pre-Test Survey	93
Appendix D: Post-Test Survey	98

List of Figures

Fig. 1.1 Top 10 targeted industries in 1st quarter of 2020 [10].....	14
Fig. 1.2 Total number of reported incidents [11].....	15
Fig. 1.3 Security incident categories – 2020	15
Fig. 3.1 Theoretical Framework	27
Fig. 3.2 Stratified sampling.....	31
Fig. 3.3 Unity Engine - IDE.....	35
Fig. 3.4 Salvos UI Components.....	41
Fig. 4.1 characteristics of an effective security awareness [5]	46
Fig. 4.2 Start Screen	49
Fig. 4.3 Play Mode.....	49
Fig. 4.4 Game Statistics	50
Fig. 4.5 Question and answer interface	51
Fig. 5.1 Have you experienced a security breach in the last 12 months?.....	53
Fig. 5.2 How many people work in your IT department?	54
Fig. 5.3 Does your university adhere to IT process or security frameworks and/or standards, and if so, which ones?	55
Fig. 5.4 How secure do you think your university's network is?.....	56
Fig. 5.5 Does your university have staff responsible for network security?	57
Fig. 5.6 What has raised your awareness of information security attacks?	58
Fig. 5.7 How do you keep informed of new forms of information security attacks and threats?.....	59
Fig. 5.8 What maturity level is your university currently at?.....	60
Fig. 5.9 What do you think will help to improve your university's security levels?.....	61
Fig. 5.10 What do you consider to be your greatest security risk?	62
Fig. 5.11 Which security measures have your university implemented?	63
Fig. 5.12 What tools does your university use to detect attacks?	64
Fig. 5.13 Does your university provide staff training to raise security awareness?	65
Fig. 5.14 What are the training methods your university is using to raise staff security awareness?	66
Fig. 5.15 Do you think that security awareness training for academic and non-academic members are essential?	67
Fig. 5.16 What areas do you think are the most important areas to address from a security awareness training?	68
Fig. 5.17 Gender.....	71
Fig. 5.18 Age groups.....	71
Fig. 5.19 Skill level related to IT	72
Fig. 5.20 Quantile-quantile plot for data set.....	73
Fig. 5.21 Box plot for pre and post marks.....	74
Fig. 5.22 Paired box plot for pre and post marks.....	75
Fig. 5.23 Rating of the usability content	77
Fig. 5.24 Rating of the learning content	78

List of Tables

Table 1.1 2020 Crime Types by Victim Count [9]	13
Table 1.2 2020 Crime Types by Victim Loss [9]	14
Table 3.1 Sampling groups	31
Table 3.2 Marks allocation	38
Table 5.1 Pre-test and post-test marks for each player	69

Acknowledgements

Praise to Almighty God who gives me the strength and blessings throughout my Master's degree and keeps me motivated each time I failed.

First and foremost, I would like to express my thanks and gratitude to my parents and my dearest husband for the love, motivation and constant support they have given, the commitments they made struggling with me and for sharing my hardship. Special thanks to Thiwanka Umagiliya and my friends who supported me by sharing the surveys and collecting data in a short period of time and Dinindu Sandaruwan for supporting me in developing Salvos.

I wish to express my honest gratitude to my supervisor Mr Amila Senarathne, who guide me throughout this study and gave his fullest support until I met the end. I would have never been completed this work without his guidance. I also wish to thank Coodinator, Dr Lakmal Rupasinghe and all my lecturers who taught me throughout this Master's degree and the things I learned from them always helped me complete this study.

I am grateful to all the participants who spend their time and supported me to evaluate Salvos by playing and giving their feedback.

Abstract

With the Covid-19 pandemic, the universities have completely changed their whole procedure of delivering lectures and doing other administrative and academic works. Various kinds of restrictions and lock-downs took this general education system to an e-education system. Adapting to electronic resources and internet-based teaching made it easy for distance learning. However, increasing network access and usage of other e-resources caused a significant increment in the risks for cyberattacks as well. Even though there are many controls and policies implemented in universities to mitigate these risks, the results from the survey carried among universities show they are not 100% secure. Not like other IT organizations, most of the system and e-resource users in universities are non-technical staff. Therefore, it is important to reduce user mistakes that expose vulnerabilities within the universities.

To increase the awareness level of the staff, this study has introduced Salvos. Salvos is a mobile game that covers basic cyber security concepts in an educational environment. The Salvos addresses the main areas, Internet security, Malware protection, Email security, Password security and Physical security. This can be used to deliver security training to university staff in an entertaining way without being another boring instructor-led theory session.

To achieve the proposed solution, 25 persons were selected from different universities and measured their awareness level using a pre-test survey. After training with the Salvos, it was evaluated using a post-test survey given to them. Further, security backgrounds in the universities were studied using a questionnaire shared among universities. In the game evaluation, analytical tests were done using R. However, a normality test was done for the pre-test and post-test results since the data set is smaller than 30. Then a paired t-test was carried out to find whether there is a significant increment in user awareness level after training with the Salvos.

Among the 17 universities who responded to the survey, 100% have agreed that it is essential to provide security awareness training to academic and non-academic staff. Further, important areas identified to address in the Salvos were malware (100%), password management (88%), email threats (82%), internet security (59%) and physical security (47%). In the evaluation, paired t-test shows -68.6087 mean difference of the marks from the

pre and post questionnaire. Moreover, the p-value of the test was $5.008e-15$ which rejects the null hypothesis and conclude that the security awareness level of the participants has increased after the training through Salvos.

This study presents the current user awareness level among different categories of the university staff and security backgrounds of the Sri Lankan universities. Study results provide evidence for the need for security training and final analysis proved that the training through Salvos can actually increase security awareness among university staff. Further, Salvos can use by staff with any background and it can easily customize for the user needs.

The methods used, results collected and analysis made are further discussed in the rest of the chapters.