

INVESTIGATING SECURITY AWARENESS AMONG
SECONDARY SCHOOL STUDENTS

SAIDA ISSA MASOUD AL-JERBIE

(Matric No: 3130212)

Thesis Submitted in fulfillment of the requirements for the degree of
MASTER IN COMPUTER SCIENCE VIA MIXED MODE
INFORMATION SECURITY AND ASSURANCE

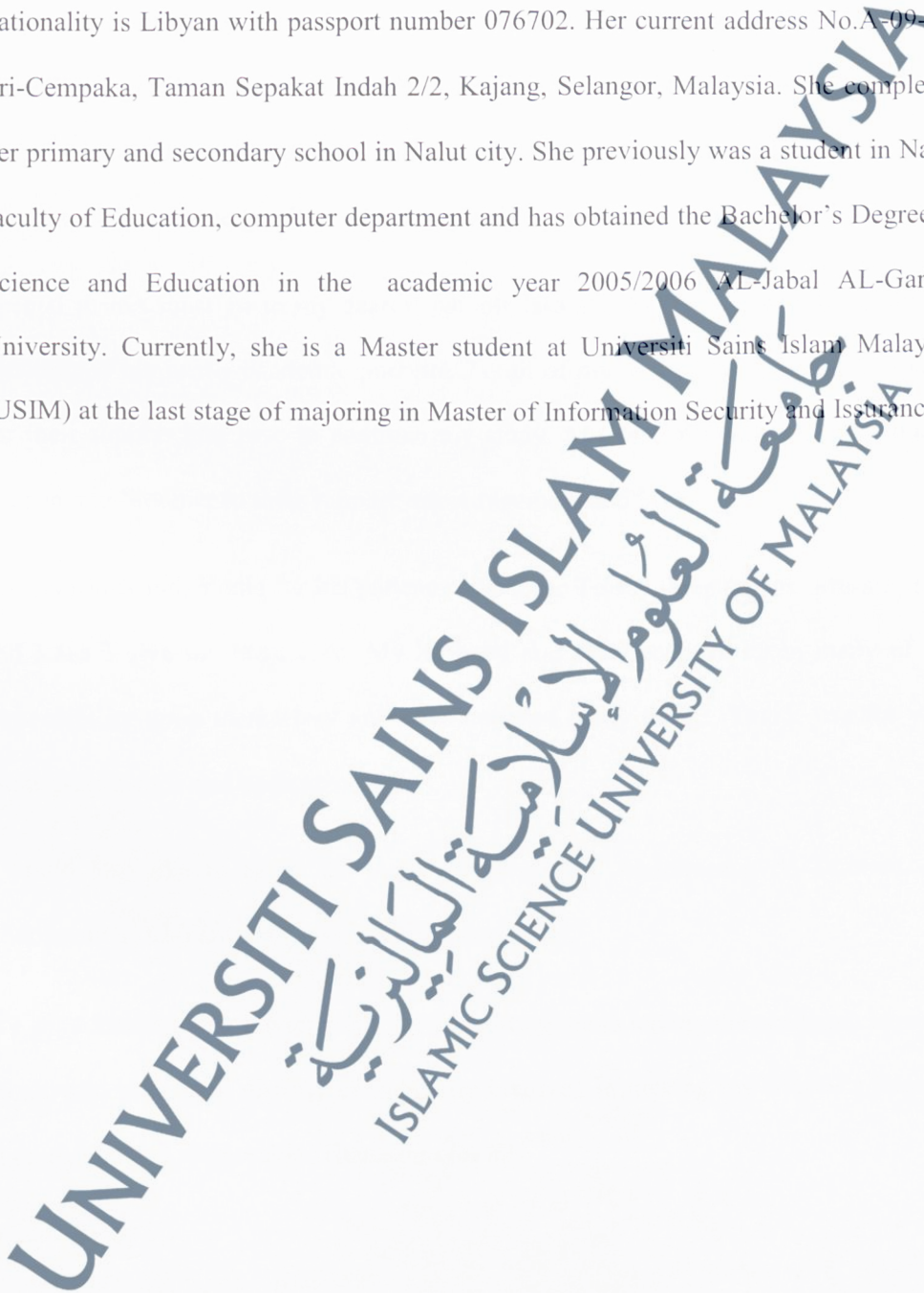
Faculty of Science and Technology
UNIVERSITI SAINS ISLAM MALAYSIA

NILAI

Feb 2015

BIODATA OF AUTHOR

Saida Issa Masoud Aljerie (3130212) was born on the 10th of February 1985. Her nationality is Libyan with passport number 076702. Her current address No.A-09-03, Sri-Cempaka, Taman Sepakat Indah 2/2, Kajang, Selangor, Malaysia. She completed her primary and secondary school in Nalut city. She previously was a student in Nalut faculty of Education, computer department and has obtained the Bachelor's Degree in Science and Education in the academic year 2005/2006 AL-Jabal AL-Garbie University. Currently, she is a Master student at Universiti Saint Islam Malaysia (USIM) at the last stage of majoring in Master of Information Security and Insurance.



AKNOWLEDGEMENT

I would like to express my deepest gratitude to many people for their continuous support and encouragement, without which this achievement would not have been possible. In particular, I am extremely grateful to my supervisors: Dr Mohd Zaliham Jali, for his patience, attention to detail, sound advice, and determination to help me get things done correctly, all of which is greatly appreciated.

Special thanks must go to my dearest parents Issa and Mabrouka, who have always encouraged me in my academic pursuits. To all of my sisters, my niece and nephew for their support and love to continue my study. My special thanks to my brothers Ahmad and Mounier to their support, encouragement and love.

My dear husband, Yonis for his patience and love. To my three angels, Masara, Isra, and Rana I give my huge love. My husband and children have taken many of my responsibility upon themselves and have suffered many things. Thank you for your immense patience and understanding.

I would also like to thank Dr. Adel Alsokeni, Dr. Abdolrazzag Al-Tamtam, Dr. Abdolmonem Al-Tamtam for their help and support.

My great thanks to my government, for supporting me in having the academic pursuit. To all who have been directly or indirectly involved in making my Master's journey an enjoyable and memorable. Thank you for all.

ABSTRACT

Children face many challenges with respect to the usage of ICT. There are difficulties to seek for suitable security awareness training tools for secondary school students. The age of the targeted group of this research concerned 13-18 years students, as they exposed with different Internet usages and vulnerable to security risks, as the result, it is very important for us to safeguard them to enable good and quality of life. This research aims to identify potential tools that can be used by children to educate them related to the security risks. Then, the research assesses the students' awareness level related to social networks, passwords, and cyber bullying. In order to obtain these objectives, a survey was conducted to assess children awareness level as well as measuring the effectiveness of training tool. Specifically, the process of identifying security awareness training tools was based on the wide search on security cyber portal of South East Asia. To assess security practices related to social network, passwords and cyber-bullying, Libyan secondary school students in Malaysia were chosen as the target participants due to the fact that they are the future generation and more exposed to danger according to literatures. The process of data collection done with 50 Libyan secondary school students participated, and it can be reported that even they have shown a slight level of awareness; however they still did not practice information security correctly. With respect to the training tools, it shows that majority of participants' preferred game type of tools. Future work must consider a wider range of security risks that students may encounter.

ABSTRAK

Kanak-kanak menghadapi banyak cabaran berkenaan dengan penggunaan ICT. Terdapat kesukaran untuk mencari alat yang sesuai latihan kesedaran keselamatan untuk pelajar sekolah menengah. Umur kumpulan sasaran kajian ini berkenaan 13-18 tahun pelajar, kerana mereka terdedah dengan kelaziman Internet yang berbeza dan lebih terdedah kepada risiko keselamatan, sebagai hasilnya, ia adalah sangat penting bagi kita untuk melindungi mereka bagi membolehkan baik dan kualiti hidup. Kajian ini bertujuan untuk mengenal pasti alatan yang disediakan yang boleh digunakan oleh kanak-kanak untuk mendidik mereka berkaitan kepada risiko keselamatan. Kemudian, kajian ini akan menilai tahap kesedaran pelajar berkaitan dengan rangkaian sosial, kata laluan, dan buli siber. Dalam usaha untuk mendapatkan maklumat-maklumat ini, satu kaji selidik telah dijalankan untuk menilai tahap kesedaran kanak-kanak dan juga mengukur keberkesanan alat latihan. Secara khusus, proses mengenal pasti alat latihan kesedaran keselamatan berdasarkan carian lebar di portal keselamatan siber di Asia Tenggara. Untuk menilai amalan keselamatan yang berkaitan dengan rangkaian sosial, kata laluan dan siber-buli, Libya pelajar sekolah menengah di Malaysia telah dipilih sebagai peserta sasaran disebabkan oleh hakikat bahawa mereka adalah generasi masa depan dan lebih terdedah kepada bahaya menurut kesusasteraan. Proses pengumpulan data dilakukan dengan 50 pelajar sekolah menengah mengambil bahagian Libya, dan ia boleh melaporkan bahawa walaupun mereka telah menunjukkan tahap yang sedikit kesedaran; namun mereka masih tidak mengamalkan keselamatan maklumat dengan betul. Sebagai contoh, mereka menunjukkan tingkah laku berisiko dalam cara mereka menggunakan tarikh kelahiran mereka sebagai kata laluan mereka. Berkenaan dengan alat latihan, ia menunjukkan bahawa kebanyakan pilihan jenis permainan. Program latihan menunjukkan keberkesanan sebagai menyebabkan tahap kesedaran pelajar dalam pasca soal selidik. Kerja masa hadapan perlu mengambil kira pelbagai risiko keselamatan yang mungkin dihadapi oleh pelajar.

ملخص البحث

يواجه الأطفال العديد من التحديات فيما يتعلق استخدام تكنولوجيا المعلومات والاتصالات. هناك بعض الصعوبات في الحصول على أدوات تدريبية للتوعية الأمنية المناسبة لطلاب المدارس الثانوية. عمر الفئة المستهدفة في البحث 13-18 عاما، كما أنهم أكثر عرضة مع أستهالات الإنترنت المختلفة، وأكثر عرضة للمخاطر الأمنية، ونتيجة لذلك، من المهم للغاية بالنسبة لنا للحفاظ عليها لتمكين جيدة ونوعية الحياة. يهدف هذا البحث إلى التعرف على الأدوات المتاحة التي يمكن استخدامها من قبل الأطفال لتتقنهم بالمخاطر الأمنية ذات الصلة. ثم، يستند البحث إلى تقييم مستوى وعي الطلاب المتعلق بشبكات التواصل الاجتماعي، كلمات السر، والتسلط عبر الإنترنت. من أجل الحصول على هذه الأهداف، أجري مسح لتقييم مستوى وعي الأطفال وكذلك قياس فعالية أداة التدريب. على وجه التحديد، استندت عملية تحديد أدوات تدريبية للتوعية الأمنية على البحث واسع للبوابة أمن الإنترنت لدول جنوب شرق آسيا. لتقييم الممارسات الأمنية المتعلقة الشبكة الاجتماعية، وكلمات السر والتسلط عبر الإنترنت، قد تم اختيار عينة من طلاب المدارس الثانوية الليبية في ماليزيا و الهدف من ذلك يرجع إلى حقيقة أنهم جيل المستقبل وأكثر عرضة للخطر وفقا للدراسات السابقة. ثم جمع البيانات فعليا من 50 طالب من المدارس الثانوية الليبية، وحسب التقارير أظهر الطلاب مستوى طفيف من الوعي. إلا أنهم لا يمارسون أمن المعلومات بشكل صحيح. على هذا المثال، أظهر الطلاب سلوك محفوف بالمخاطر في الطريقة التي يستخدمون فيها تاريخ ميلادهم ككلمة المرور الخاصة بهم. وفيما يتعلق بأدوات التدريب، أظهرت الغالبية أن الألعاب هي النوع المفضل من أدوات التدريب. وأظهر البرنامج التدريبي فعاليته في مستوى وعي الطلاب في مرحلة الاستبيان الثاني. الدراسات المستقبلية يجب أن تركز في مجموعة واسعة من المخاطر الأمنية التي قد تواجه الطلاب.

TABLE OF CONTENTS

CONTENTS	PAGE
DECLARATION OF THESIS AND COPYRIGHT	i
AUTHOR BIODATA	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	iiii
ABSTRAK	ivi
MULAKHAS AL-BAHTH	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	ixi
LIST OF FIGURES	xi
LIST OF APPENDICES	xiii
CHAPTER I: INTRODUCTION	1
1.1 Background	1
1.2 Problem Statement	6
1.3 Research Questions	9
1.4 Research Objectives	9
1.5 Scope of the Research	9
1.6 Research Outcome	10
1.7 Thesis Structure	10
CHAPTER II: INFORMATION SECURITY AWARENESS	12
2.1 Introduction	12
2.2 Information Security Awareness Definitions	13
2.3 Related Studies	14
2.3.1 Information Security Risks	14
2.3.2 Security Awareness Training Tools	22
2.3.3 Evaluation of Information Security Awareness	26
2.3.4 Information Security Awareness Challenges	31
2.3.5 Success of Information Security Awareness	33
2.4 Summary	35

CHAPTER III: RESEARCH METHODOLOGY	37
3.1 Introduction	37
3.2 Literature Review	38
3.3 Data Collection	38
3.3.1 Training Tools	39
3.3.2 Questionnaire Design	40
3.3.3 Population and Sample	41
3.3.4 Steps Studets Need to Follow	42
3.4 Data Analysis	42
3.5 Pilot Study	43
3.6 Consolidation	43
3.7 Summary	45
CHAPTER IV: FINDING AND RESULTS	46
4.1 Introduction	46
4.2 Information Security Awareness ISA “Training Tools”	47
4.2.1 Method	47
4.2.2 Review and Results	50
4.2.3 Discussion	51
4.3 Pre-Questionnaire Results	51
4.3.1 Demographic and General Security Information	51
4.3.2 Security Awareness for the Pre-Questionnaire	60
4.3.3 Security Practices for the Pre-Questionnaire	64
4.3.4 Personal Opinion for the Pre-Questionnaire	72
4.4 Post-Questionnaire Results	78
4.4.1 Demographic and General Security Information for the Post-Questionnaire	78
4.4.2 Security Awareness for the Post-Questionnaire	81
4.4.3 Security Practices for the Post-Questionnaire	83
4.4.4 Personal Opinion for the Post-Questionnaire	87
4.5 Training Program Evaluation “Post-Questionnaire”	89
4.5.1 Evaluation of Cyber Safe Training Materials	89
4.5.2 Evaluation of Cyber Wellness Materials	92

4.6	Finding and Results of the Pre and Post-Questionnaire	93
4.7	Summary	98
CHAPTER V: CONCLUSION AND FUTURE WORKS		99
5.1	Introduction	99
5.2	Study Achievement	100
5.3	Study Limitation and Difficulties	102
5.4	Future Works	103
5.5	Summary	103
REFERENCES		104
APPENDICES		111

LIST OF TABLES

	PAGE
Table 1: Cyberbullying Potential Risks	16
Table 2: Method Used to Evaluate Information Security Awareness	30
Table 3: Description of Research Activities	37
Table 4: Tasks and Outcome of the Study	44
Table 5: Available-Non Available Cyber Security Portals	48
Table 6: Available CERTs and Security Program	49
Table 7: Security Awareness Tools	50
Table 8: Frequency by Source of Knowledge about Social Networks	54
Table 9: Number of Social Networks Used by Students	55
Table 10: General Security Information	57
Table 11: Cyberbullying Forms between Students	58
Table 12: Cyberbullying Related Issues	60
Table 13: General Information Security Questions “Post-Questionnaire”	81
Table 14: Training Materials Evaluation	94
Table 15: Crosstab Values for Security Awareness in the “Pre-Questionnaire”	95
Table 16: Crosstab Values for “Post-Questionnaire”	96
Table 17: The Significant Value for Security Awareness and Security Practices	97
Table 18: Anova Test for Significance	98

LIST OF FIGURES

	PAGE
Figure 1: The Internet Use by Age Group	3
Figure 2: Classification of Information Security	13
Figure 3: Research Planned Strategy	46
Figure 4: Gender Frequency of the Respondents	51
Figure 5: Respondents Age Categories	52
Figure 6: Students' Educational Level	52
Figure 7: Nationality Frequency of the Respondents	53
Figure 8: Social Networks Usages	53
Figure 9: Source of Knowledge about Social Networks Indicated by Students	54
Figure 10: The Number of Social Networks used by Students	55
Figure 11: Passwords Habits of Students	56
Figure 12: Changing Passwords by Students	56
Figure 13: Technology used to Bully Students	57
Figure 14: Effects Caused by Cyberbullying Utilities	59
Figure 15: Action Taken by Students when Victimized in Cyberbullying	59
Figure 16: Posting Personal Information via Social Networks Sites	61
Figure 17: Dealing with the Privacy Setting in Social Network Sites	61
Figure 18: Knowledge about Passwords Length	62
Figure 19: Changing Passwords based on Students' Indication	63
Figure 20: Cyberbullying Awareness among Students	63
Figure 21: Sharing Daily Activities with Friends via Social Networks	65
Figure 22: Posting Personal Information via Social Networks	65
Figure 23: Accepting Friend Request from other People	66
Figure 24: Students Interact with Posting their Location via Social Networks	67
Figure 25: Students Attitude about the Contents of their Passwords	67
Figure 26: Sharing Passwords with Friends	68
Figure 27: Writing down the Passwords to Remember it	69
Figure 28: Passwords Contain Personal Information	69
Figure 29: Telling others about being bullied	70
Figure 30: Receiving a Hate Message for Someone	71

Figure 31: Majority of Students Bullying Others	71
Figure 32: Cyberbullying Impact on Students Ability on Going to School	72
Figure 33: Is “123” is a Good Password	73
Figure 34: Changing Passwords after Sharing them	73
Figure 35: Using the Same Password for all Accounts	74
Figure 36: Posting Personal Photos via Social Networks	75
Figure 37: Good to Make New Friends via Social Networks	75
Figure 38: Accept Friends’ Request from Unknown People	76
Figure 39: Cyberbullying is more Dangerous than Traditional Bullying	77
Figure 40: It is a Crime when Bullying Someone	77
Figure 41: Repeating the Action of Bullying to the Bullier	78
Figure 42: Action will be Taken by Students when Bullied	79
Figure 43: Number of Passwords will be Used by Students	80
Figure 44: Times Students will Change their Passwords	81
Figure 45: Post-Questionnaire Results about Posting Personal Information	82
Figure 46: Dealing with Privacy on social network sites	82
Figure 47: Changing Passwords based on the Post-Questionnaire	83
Figure 48: How Students will Share their Daily Activities	84
Figure 49: Future Dealing with Friends Request on Social Networks by Students	84
Figure 50: How Students will Share their Passwords	85
Figure 51: Students’ Interaction in Writing their Passwords Down	86
Figure 52: Bullying Someone by Internet	86
Figure 53: Reduce the Negative Effect Caused by the Bullier	87
Figure 54: Considering “123” as a Good Password	88
Figure 55: How Students will Share their Daily Activities via Social Networks	88
Figure 56: Students Indication on Posters	90
Figure 57: Students Evaluation of the Value of Posters	90
Figure 58: The Video Explains the Risk very Well	90
Figure 59: How Video Provides the Knowledge about Information Security	91
Figure 60: Students Understanding of the issue Presented in the Game	91
Figure 61: Game Makes Students Learn How to Solve Security Problem	92

Figure 62: Students Evaluation on Game of Cyberwellness	92
Figure 63: The Percentage of Game Benefits	93



LIST OF APPENDECES

	PAGE
Appendix A: Pre-Questionnaire	111
Appendix B: Post-Questionnaire	116
Appendix C: Pre-Questionnaire Related Tables	122
Appendix D: Posters: source “cyber safe.my”	124
Appendix E: Brief Statements about Security Risks	127
Appendix F: Research Paper and Certificate	129

