AN INTEGRATED PERSUASIVE TECHNOLOGY MODEL FOR INFORMATION SECURITY AWARENESS

BY

MOHAMMED ABDULLAH SAEED BAWAZIR

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy in Information Technology

Kulliyyah of Information and Communication Technology
International Islamic University Malaysia

DECEMBER 2021

ABSTRACT

In this digital era, information assets are becoming increasingly important, thereby necessitating measures to ensure information security. Globally, end-users are also struggling to ensure the security of their information. In the domain of information security, it is the human factor that constitutes the greatest vulnerability. While security education, training, and awareness programmes are evolving as valuable approaches to increasing awareness and behaviour intention to information security, changing security awareness and behaviour by end-users remains the most complex and challenging aspect of information security. Furthermore, the conventional methods for influencing information security awareness are still very expensive, time-consuming, and require regular repeating. Given such challenges, this research introduces persuasive technology to improve users' awareness and behaviour intention. Persuasive technology has proved to be successful in improving the end-users' attitudes and behaviour. In this context, this research establishes an integrated model of improving end-users' security awareness by incorporating relevant literature and multiple empirically verified theories, including the Fogg behaviour model (FBM), Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), and Technology Acceptance Model (TAM). A multidimensional research model has been proposed based on the main categories of FBM (motivation, ability, and trigger) to identify the effects of key factors in the persuasive technology context for influencing end-users' security awareness and behaviour intention. The prototype has been developed in order to implement the factors of the proposed model and measure the effectiveness of persuasive technology to enhance information security awareness. This research adopts a mixed-methods approach to evaluate the proposed model and prototype. The proposed research model was validated through paired sample T-test and partial least squares (PLS), which were administered to 100 participants to measure security awareness in the light of persuasive technology. Furthermore, content analysis was performed using NVivo software for 45 semi-structured interviews to collect qualitative data on the end-users' perception of the prototype. The collection of data is based on secondary and primary data. In order to improve primary information, secondary data references were collected from publications, journals, and books. The data for this study was acquired through the use of a quasi-experiment. The experiment began with a pre-prototype questionnaire, followed by the use of the prototype, followed by a post-prototype questionnaire, and finally, a short interview. The results validate the effectiveness of the prototype utilising the factors of the research model, specifically FBM attributes. Moreover, the results indicate that the research model significantly predicts the key factors affecting security awareness and behaviour intention in respect of persuasive technology. This study contributes to the body of knowledge by providing empirical results for the key factors that affect security awareness and intention of security behaviour in a persuasive technology context. The findings provide organisations and security practitioners with a model for the creation and development of a proactive and customised security awareness system. This research has contributed significantly to Human-Computer Interaction (HCI), specifically in the design and content of persuasive technology to influence security awareness and intention of security behaviour in the safe and secure use of information technology.

خلاصة البحث

في هذا العصر الرقمي اليوم ، أصبحت أصول المعلومات ذات أهمية متزايدة حيث أصبحت التدابير ضرورية بنفس القدر لحماية أمن المعلومات. في الوقت نفسه ، يكافح المستخدمون النهائيون عالميًا للحفاظ على أمان موارد المعلومات الخاصة بهم. في الواقع ، يشكل العامل البشري ضعفًا خطيرًا باعتباره الحلقة الأضعف في مجال الأمن. بينما تتطور برامج التعليم والتدريب والتوعية الأمنية كطريقة قيمة لزيادة الوعي ونية السلوك لأمن المعلومات ، يظل تغيير الوعي الأمني والسلوك من قبل المستخدمين النهائيين هو الجانب الأكثر تعقيدًا وتحديًا لأمن الكمبيوتر. علاوة على ذلك ، لا تزال الأساليب التقليدية للتأثير على الوعي بأمن المعلومات باهظة الثمن وتستغرق وقتًا طويلاً وتتطلب تكرارًا منتظمًا. لذلك ، فإن الغرض من هذا البحث هو إدخال التكنولوجيا المقنعة، والتي تستخدم لتحسين وعي المستخدم ونية السلوك. و قد وجدت التكنولوجيا المقنعة فعالة في تغيير مواقف وسلوكيات المستخدمين النهائيين بشكل كبير. في هذا السياق، يطور هذا البحث نموذجًا متكاملًا لتحسين الوعي الأمني للمستخدمين النهائيين من خلال دمج الأدبيات ذات الصلة والنظريات المتعددة التي تم التحقق منها تجريبياً ، بما في ذلك نموذج سلوك Fogg (FBM) ، ونظرية تحفيز الحماية (PMT) ، ونظرية السلوك المخطط (TPB) ، ونموذج قبول التكنولوجيا (TAM). تم اقتراح نموذج بحث متعدد الأبعاد استنادًا إلى الفئات الرئيسية لـ FBM (الدافع ، والقدرة ، والتحفيز) ، لتحديد تأثيرات هذه العوامل الرئيسية في سياق التكنولوجيا المقنعة لتحسين وعي المستخدمين النهائيين بالأمن ونية السلوك. تم تطوير النموذج الأولي من أجل تنفيذ عوامل النموذج المقترح وقياس فعالية تكنولوجيا الإقناع لتعزيز الوعي بأمن المعلومات . يتبنى هذا البحث أساليب مختلطة ، نوعية وكمية لتقييم النموذج المقترح والنموذج الأولي. تم التحقق من صحة نموذج البحث المقترح من خلال paired sample T-test وpartial least squares (PLS) ، والتي تم إجراؤها على 100 مشارك لقياس الوعي الأمني في ضوء تكنولوجيا الإقناع. علاوة على ذلك ، تم إجراء تحليل المحتوى باستخدام برنامج NVivo لـ 45 مقابلة شبه منظمة لجمع البيانات النوعية حول تصور المستخدمين النهائيين للنموذج الأولي. يعتمد جمع البيانات على البيانات الثانوية والأولية. من أجل تحسين المعلومات الأولية ، تم جمع مراجع البيانات الثانوية من المنشورات والمجلات والكتب. تم الحصول على بيانات هذه الدراسة من خلال استخدام شبه تجربة. بدأت التجربة باستبيان ما قبل النموذج الأولي ، متبوعًا باستخدام النموذج الأولي ، متبوعًا باستبيان ما بعد النموذج الأولي ، وأخيراً مقابلة قصيرة. تحققت هذه النتائج من فعالية النموذج الأولي باستخدام عوامل نموذج البحث وخاصة سمات FBM. علاوة على ذلك ، تشير النتائج إلى أن نموذج البحث يتنبأ بشكل كبير بالعوامل الرئيسية التي تؤثر على الوعي الأمني ونية السلوك فيما يتعلق بالتكنولوجيا المقنعة. تساهم هذه الدراسة في المعرفة من خلال تقديم النتائج التجريبية للعوامل الرئيسية التي تؤثر على الوعي الأمني و نية السلوك الأمني في سياق التكنولوجيا المقنعة. لذلك ، توفر نتائج البحث للمنظمات والممارسين الأمنيين نموذجًا لإنشاء وتطوير نظام وعي أمني مخصص و استباقي. قدم هذا البحث مساهمة كبيرة في التفاعل بين الإنسان والحاسوب (HCI) ، وتحديداً في تصميم ومحتوى تكنولوجيا الإقناع للتأثير على الوعي الأمني ونية السلوك الأمني في الاستخدام الآمن لتكنولوجيا المعلومات.

APPROVAL PAGE

The thesis of Mohammed Abdullah Saeed Bawazir has been approved by the following:

Murni Mahmud
Supervisor

Nurul Nuha Abdul Molok
Co-Supervisor

Akram M Zeki
Co-Supervisor

Abd Rahman Ahlan
Internal Examiner

Wan Fatimah Wan Ahmad
External Examiner

Ismaiel Hassanien Ahmed
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Mohammed Abdullah Saeed Bawazir

Signature .... Date ....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

AN INTEGRATED PERSUASIVE TECHNOLOGY MODEL FOR INFORMATION SECURITY AWARENESS

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.

3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Mohammed Abdullah Saeed Bawazir

……..…………………….. ………………………..
Signature Date

DEDICATION

This thesis is dedicated to:

My late father, Abdullah Saeed Bawazir

My mother, Khadijah Saeed Bahaj.

My wife, Amani Saeed Bawazir and my children, Alaa, Abdullah, and Ammar

ACKNOWLEDGEMENTS

All praise due to the Lord, Allah alone, I praise him, seek his help and forgiveness. First of all, I thank Almighty Allah, who always blessed me and gave me the strength to accomplish objectives in my life. I am pleased to dedicate this work to my dear parents and family who granted me the gift of their unwavering belief in my ability to achieve this goal, thank you for your support, patience, encouragement, uplifting spirit, and unconditional love. My appreciation and thanks to my wife Amani, who has provided love, patience and encouragement throughout the years. My love and gratitude go to my daughter Alaa, and my sons Abdullah, and Ammar, who never fail to cheer me up during my study.

Heartfelt and special thanks to my supervisor Assoc Prof Dr Murni Mahmud, for her superb supervision. Her constructive criticisms, guidance, strong encouragement and support throughout the research have enabled me to complete this thesis. I am very grateful for her kindness, patience and tolerance towards my weaknesses and the difficult times I had. Thanks for showing many alternative thoughts and ways to do and publish research work. I thank her for treating me as a student and a friend at the same time, I will be forever grateful.

I wish to express my appreciation and thanks to those who provided their time, effort and support for this project. To the members of my dissertation committee, Asst Prof Dr Nurul Nuha Abdul Molok and Prof Dr Akram M Zeki, thank you for sticking with me. I will also thank my friends and classmates, colleagues for their support, while my sincere gratitude goes to Dr Sharyar Wani and Dr Nahel Abdallah.

I would like to thank Kulliyyah of Information and Communication Technology, International Islamic University Malaysia for giving me the opportunity to develop my skills in Information Technology. Lastly, I would like to thank everyone who has contributed directly and indirectly to the completion of this research.

TABLE OF CONTENTS

Abstract ii
Abstract in Arabic iii
Approval Page iv
Declaration v
Copyright Page vi
Dedication vii
Acknowledgements viii
Table of Contents ix
List of Tables xv
List of Figures xix
List of Abbreviations xxi

CHAPTER ONE: INTRODUCTION 1
1.1 Introduction 1
1.2 Background of The Study 4
1.3 Statement of The Problem 7
1.4 Purpose of The Study 9
1.5 Research Objectives 11
1.6 Research Questions 12
1.7 Proposed Research Model 12
1.8 Scope of Study 13
1.9 Significance of The Study 14
1.10 Definitions of Terms 16
1.11 Overview of Thesis Structure 20
1.12 Chapter Summary 21

CHAPTER TWO: LITERATURE REVIEW 23
2.1 Introduction 23
2.2 Information Security 25
2.2.1 Information System Security (ISS) 27
2.2.2 Information Security Goals (CIA Triad) 27
2.2.3 Information Security Threats 28
2.2.4 Cost of Information Security 31
2.2.5 Information Security Countermeasures 32
2.3 Information Security Awareness (ISA) 33
2.3.1 Cognitive Perspective 36
2.3.2 Behavioural Perspective 37
2.3.3 Process Perspective 37
2.4 Information Security Behaviour 38
2.5 Information Security Awareness’ Influence on Behaviour 39
2.5.1 Theory of Planned Behaviour (TPB) 41
2.5.2 General Deterrence Theory (GDT) 42
2.5.3 Protection Motivation Theory (PMT) 42
2.5.4 Technology Acceptance Model (TAM) 42
2.6 Persuasive Technology (PT) 43

2.6.1 Fogg Behaviour Model (FBM) 47
2.6.2 Design Elements of (FBM) 49
2.6.3 Behaviour Change Support Systems 52
2.6.3.1 A-Change 52
2.6.3.2 B-Change 52
2.6.3.3 C-Change 53
2.6.4 Behaviour Reduction 53
2.6.5 Persuasive Strategies 55
2.6.6 Creating Persuasive Technology Design Process 58
2.7 Persuasive Technology to Enhance Information Security Awareness and Behaviour 61
2.7.1 The Role of Persuasive Technology to Improve ISA And Behaviour 69
2.7.2 Using Persuasive Technology to Improve ISA and Behaviour 71
2.7.3 Research Gap 73
2.8 Chapter Summary 74

CHAPTER THREE: THEORETICAL FRAMEWORK AND HYPOTHESES 75
3.1 Introduction 75
3.2 The Basic Research Proposal 75
3.3 Variables Identification And Hypotheses Formulation 77
3.3.1 Motivation Factors 78
3.3.1.1 Perceived Usefulness (PU) 79
3.3.1.2 Subjective Norm (SN) 80
3.3.1.3 Perceived Severity of Threats(PSOT) 81
3.3.1.4 Rewards (RW) 83
3.3.2 Ability Factors 85
3.3.2.1 Perceived Ease of Use (PEOU) 86
3.3.2.2 Self-Efficacy (SE) 88
3.3.3 Trigger Factord 89
3.3.3.1 Spark Trigger (ST) 91
3.3.3.2 Facilitator Trigger (FT) 92
3.3.4 Information Security Awareness’ Influence on Behaviour Intention 92
3.4 Enhanced Proposed Research Model 94
3.5 Chapter Summary 96

CHAPTER FOUR: RESEARCH METHODOLOGY 98
4.1 Introduction 98
4.2 Research Design 99
4.2.1 Mixed-Method Research 100
4.2.2 Quasi-Experimental 101
4.2.3 Research Design Stages 102
4.3 Participants and Sampling Design 105
4.3.1 Participants 105
4.3.2 Sampling Technique 106
4.3.3 Sample Size and Recruitment 107
4.4 Instrumentation Development 109

4.4.1 Questionnaire Construction 109
4.4.1.1 Measurement of Motivation 112
4.4.1.2 Measurement of Ability 114
4.4.1.3 Measurement of Trigger 116
4.4.1.4 Measurement of Information Security Awareness 117
4.4.1.5 Measurement of Behaviour Intention 118
4.4.1.6 Measurement of Prototype 118
4.4.2 Prototype 120
4.4.3 Interview 120
4.4.4 Pre-Testing The Instruments 121
4.5 Pilot Study 124
4.5.1 Procedures 125
4.5.2 Findings of The Pilot Study 126
4.5.2.1 Participants' Profile 126
4.5.2.2 Reliability Test 128
4.5.2.3 Paired Sample T-Test 129
4.6 Data Analysis Strategy 131
4.7 Chapter Summary 133

CHAPTER FIVE: THE PROTOTYPE DEVELOPMENT 135
5.1 Introduction 135
5.2 Background 135
5.3 The Fogg Behaviour Model and Persuasive Security Prototype 137
5.4 Eight Steps In Early-Stage Persuasive Design 138
5.5 System Architecture 141
5.6 Design of Prototype 143
5.6.1 Mapping Security Factors, PT Strategies, and Prototype Features 143
5.6.2 Prototype Content and Design 146
5.6.3 Prototype Interfaces 149
5.6.3.1 Short Security Test 149
5.6.3.2 Security Expression 150
5.6.3.3 Security Customisation 150
5.6.3.4 Simple Security Steps. 151
5.6.3.5 Security Statistical 152
5.6.3.6 Adverse Security Story 152
5.6.3.7 Security Recommendation 153
5.6.3.8 Virtual Security Points 153
5.7 Chapter Summary 154

CHAPTER SIX: ANALYSIS AND FINDINGS-EFFECTS OF PROTOTYPE INTERVENTION 155
6.1 Introduction 155
6.2 Experimental Procedure 155
6.3 Demographic Profile 157
6.3.1 Participants' Demographic Profile 157
6.3.2 Participants' Computer and Internet Experience 159
6.3.3 Information Security Practices Background 160
6.4 Data Screening 163

6.4.1 Missing Data and Treatment 163
6.4.2 Normality Test 166
6.5 Reliability Analysis 168
6.6 Experimental Data Analysis (Pre and Post Data) 169
6.6.1 Data Analysis and Interpretation of Items and Factors (Pre And Post Data) 171
6.6.1.1 Perceived Usefulness (PU) 172
6.6.1.2 Subjective Norms (SN) 174
6.6.1.3 Perceived Severity of Threat (PSOT) 177
6.6.1.4 Reward (RW) 180
6.6.1.5 Perceived Ease of Use (PEOU) 183
6.6.1.6 Self-Efficacy (SE) 185
6.6.1.7 Spark Trigger (ST) 188
6.6.1.8 Facilitator Trigger (FT) 190
6.6.1.9 Security Awareness (SA) 193
6.6.1.10 Behaviour Intention (BI) 196
6.6.2 Summary For A Paired Sample Test Result of Factors 198
6.6.3 Data Analysis and Interpretation of Dimensions (Pre And Post Data) 201
6.6.3.1 Motivation Dimension 202
6.6.3.2 Ability Dimension 203
6.6.3.3 Trigger Dimension 204
6.6.4 Summary For Paired Sample Test Of Dimensions 205
6.7 Hypothesis Result 207
6.8 Quantitative Analysis of The Prototype 208
6.8.1 Descriptive Statistics of Prototype Content 208
6.8.2 Descriptive Statistics of Prototype Design 210
6.8.3 Pearson’s Correlations Between PTC, PTD, SA, and BI 212
6.9 Qualitative Analysis (Users’ Opinion) 214
6.9.1 Content Analysis 215
6.9.2 Stage 1: Reading and Interpretation of Text 216
6.9.3 Stage 2: Coding of Text 216
6.9.4 Stage 3: Result Presentation 216
6.9.4.1 Users Experience 217
6.9.4.2 Persuasion 226
6.10 Chapter Summary 234

CHAPTER SEVEN: MODELLING USER SECURITY AWARENESS IN PERSUASIVE TECHNOLOGY 237
7.1 Introduction 237
7.2 Data Screening and Preparation 237
7.2.1 Assessment of Outliers 238
7.2.2 Normality Test 239
7.2.3 Linearity and Homoscedasticity 240
7.2.4 Multicollinearity Assumption 242
7.3 Assessment of The Measurement Model 243
7.3.1 Convergent Validity 245
7.3.1.1 Indicator Reliability: Loadings (Outer Loading) 247

7.3.1.2 Construct Reliability: Composite Reliability (CR) and Cronbach's Alpha 249
7.3.1.3 Convergent Validity: Average Variance Extracted (AVE) 250
7.3.2 Discriminant Validity 251
7.3.2.1 Cross-Loadings 252
7.3.2.2 Fornell-Larcker Criterion-Square Root of Ave 254
7.3.2.3 The Heterotrait-Monotrait Ratio of Correlation (Htmt) ... 255
7.4 Bivariate Correlations 256
7.4.1 Bivariate Correlations Between Factors 256
7.4.2 Bivariate Correlations Between Dimensions 258
7.5 Structural Model Assessment 258
7.5.1 Direct Hypotheses Testing - Path Coefficients (Β) 261
7.5.2 Coefficient of Determination (R^2 Value) 266
7.5.3 Effect Size F^2 267
7.5.4 Predictive Relevance (Blindfolding) Q^2 268
7.5.5 Goodness-of-Fit Of The Model (Gof) 269
7.6 Chapter Summary 270

CHAPTER EIGHT: DISCUSSION AND CONCLUSION 272
8.1 Introduction 272
8.2 Discussion of The Findings 272
8.2.1 Motivation Factors 278
8.2.1.1 Perceived Usefulness (PU) 280
8.2.1.2 Subjective Norm (NS) 281
8.2.1.3 Perceived Severity of Threats (PSOT) 282
8.2.1.4 Rewards (RW) 283
8.2.2 Ability Factors 284
8.2.2.1 Perceived Ease of Use (PEOU) 286
8.2.2.2 Self-Efficacy (SE) 288
8.2.3 Trigger Factors 289
8.2.3.1 Spark Trigger (ST) 291
8.2.3.2 Facilitator Trigger (FT) 292
8.2.4 Information Security Awareness' Influence on Behaviour Intention 294
8.2.5 The Prototype 295
8.3 Summary of Discussion 298
8.4 Research Contribution 299
8.4.1 Theoretical Contribution 301
8.4.2 Empirical Contribution 303
8.4.3 Practical Contribution 306
8.5 Research Implications 308
8.6 Research Limitations 312
8.7 Recommendations 313
8.8 Future Research 315

REFERENCES 318

APPENDIX ONE: QUESTIONNAIRE 339

APPENDIX TWO: FACTORS OF SECURITY AWARENESS IN PREVIOUS STUDIES..353
APPENDIX THREE: CONSENT FORM..355
APPENDIX FOUR: INTERVIEW QUESTIONS..356
APPENDIX FIVE : RECRUITMENT FLYER..357
APPENDIX SIX : APPROVAL LETTER TO COLLECT DATA...................358

LIST OF TABLES

Table No.		Page No.
2.1	Most Frequently Used Theories to Explain ISS Behaviour	41
2.2	Persuasive Strategies	56
2.3	Summary of Studies in Information Security Using Persuasive Technology	64
3.1	Summary of Research Hypotheses	96
4.1	G*Power result of sample size calculation	108
4.2	Structure of the questionnaire	111
4.3	Perceived Usefulness Scale	112
4.4	Subjective norm scale	113
4.5	Perceived severity of threat scale	113
4.6	Reward scale	114
4.7	Perceived ease of use scale	115
4.8	Self.efficacy scale	115
4.9	Spark trigger scale	116
4.10	Facilitator trigger scale	117
4.11	Information security awareness scale	117
4.12	Behaviour intention scale	118
4.13	Prototype scale	119
4.14	Participants' demographic profile based on the pilot	127
4.15	Reliability of instrument measures based on the pilot study	129
4.16	Paired sample T-test results based on the pilot study	130
5.1	Mapping between security factors, PTstrategies and prototype	145
6.1	Demographic profile of participants	158
6.2	Computer experience of participants	159

6.3 Security Practices Background of Participants 161
6.4 Item-Level missing data examination 164
6.5 Normality Test 167
6.6 Reliability Test Result 169
6.7 Descriptive statistics of perceived usefulness (PU) 172
6.8 Paired Sample T-test of PRE-PU and POST-PU items 173
6.9 Paired Sample T-test of PRE-PU and POST-PU factor 174
6.10 Descriptive statistics of subjective norms 175
6.11 Paired Sample T-test of PRE-SN and POST-SN items 176
6.12 Paired Sample Test of PRE-SN and POST-SN factor 176
6.13 Descriptive statistics of perceived severity of threats 177
6.14 Paired Sample T-test of PRE-PSOT and POST-PSOT items 179
6.15 Paired Sample T-test of PRE-PSOT and POST-PSOT factor 179
6.16 Descriptive statistics of reward 180
6.17 Paired Sample T-test of PRE-RW and POST-RW items 181
6.18 Paired Sample T-test of PRE-RW and POST-RW factor 182
6.19 Descriptive statistics of perceived ease of use 183
6.20 Paired Sample T-test of PRE-PEOU and POST-PEOU items 184
6.21 Paired Sample Test of PRE-PEOU and POST-PEOU factor 185
6.22 Descriptive statistics of self-efficacy 186
6.23 Paired Sample T-test of PRE-SE and POST-SE items 187
6.24 Paired Sample Test of PRE-SE and POST-SE factor 187
6.25 Descriptive statistics of spark trigger 188
6.26 Paired Sample T-test of PRE-ST and POST-ST items 189
6.27 Paired Sample T-test of PRE-ST and POST-ST factor 190
6.28 Descriptive statistics of facilitator trigger 191
6.29 Paired Sample T-test of PRE-FT and POST-FT items 192

6.30 Paired Sample Test of PRE-FT and POST-FT factor 193

6.31 Descriptive statistics of security awareness 194

6.32 Paired Sample T-test of PRE-SA and POST-SA items 195

6.33 Paired Sample T-test of PRE-SA and POST-SA factor 196

6.34 Descriptive statistics of behaviour intention 196

6.35 Paired Sample T-test of PRE-BI and POST-BI items 197

6.36 Paired Sample T-test of PRE-BI and POST-BI factor 198

6.37 Summaries for paired sample T-test of factors 200

6.38 Descriptive statistics of Motivation dimension 202

6.39 Paired Sample T-test of pre-motivation and post-motivation 202

6.40 Descriptive statistics of Ability dimension 203

6.41 Paired Sample T-test of PRE-ABILITY and POST- ABILITY 203

6.42 Descriptive statistics of Trigger dimension 204

6.43 Paired Sample Test of pre-trigger and post-trigger dimension 204

6.44 Summaries for paired sample T-test of dimensions 205

6.45 Summary of Hypothesis Results 207

6.46 Descriptive Statistics of prototype content 209

6.47 Descriptive Statistics of Prototype Design 211

6.48 Correlations between PTC, PTD, SA, BI 213

6.49 Frequency of the attitude towards user experiences of the prototype 219

6.50 Example of positive, neutral, and negative for the prototype design 221

6.51 Example of positive, neutral and negative for satisfaction theme 222

6.52 Examples of positive, neutral and negative justification foreffectiveness theme. 223

6.53 Example of positive, neutral and negative justification for Ease of Use Theme 224

6.54 Example of positive, neutral and negative justification for efficiencyTheme 225

6.55 List of most persuasive features themes with frequency 227

6.56 List of emphasis features themes with frequency 229

6.57 List of prototype preferences themes with frequency 231

7.1 Outliers 239

7.2 Results of Skewness and Kurtosis for Normality Test 240

7.3 Tolerance and VIF Values 243

7.4 Factor Loading 247

7.5 Cronbach's Alpha and Composite Reliability 250

7.6 Average variance extracted (AVE) results 251

7.7 Cross-loading 252

7.8 Results of discriminant validity by Fornell-Larcker criterion 254

7.9 Results of discriminant validity by HTMT 255

7.10 Pearson correlations between Factors 257

7.11 Pearson correlations between Dimensions 258

7.12 Summary of the Direct Effect 265

7.13 R^2 of Endogenous Latent Variables 266

7.14 Effect size f^2 267

7.15 Predictive relevance (Blindfolding) Q^2 269

8.1 Results of Proposed Hypotheses 277

LIST OF FIGURES

Figure No.		Page No.
1.1	Basics of the Proposed Research Model	13
1.2	Significant of the study	14
2.1	Layers of Information Security	26
2.2	CIA Triad of Information Security	28
2.3	Categorisation of Information Security Threats	29
2.4	Frequent Information Security Threats	30
2.5	Sources of Information Security Incidents	30
2.6	Sources of Financial Loss	32
2.7	Information security countermeasures	33
2.8	Describes the Area Where Computing Technology and Persuasion Overlap	46
2.9	The Fogg Behaviour Model Has Three Factors: Motivation, Ability and Triggers.	47
2.10	Three-dimensional Mapping of Persuasive Technologies	55
2.11	Eight Steps In Persuasive Design	59
3.1	Basic Research Model	76
3.2	Enhanced proposed research model	95
4.1	Overview of Research Design of the Study	103
4.2	X-Y plot of sample size range	108
5.1	Early-Stage Persuasive Design Principles Adapted to the Prototype	140
5.2	System Architecture of Persuasive Security Prototype	142
5.3	Yellow Background of the Prototype	148
5.4	The Interface of Short Security Test.	149
5.5	The Interface of Security Expression	150

5.6 The Interface of Security Customisation. 151

5.7 The Interface of Simple Security Steps 151

5.8 The Interface of Security Statistical 152

5.9 The Interface of Real Security Story 152

5.10 The Interface of Security Recommendation 153

5.11 The Interface of Virtual Security Points 153

6.1 Distribution of Participants’ Demography Profile 158

6.2 Distribution of Participants’ Computer Experience 160

6.3 Distribution of Participants’ Security Practices Background 163

6.4 Normality Histogram 166

6.5 Research Model (left side) 171

6.6 Score differences between pre and post prototype of factors 200

6.7 Value of the differences in factors (t-value) 201

6.8 Score differences between pre and post prototype of dimensions 206

6.9 Value of the differences in dimensions 206

6.10 Histogram of Prototype Content 210

6.11 Histogram of Prototype Design 212

6.12 Qualitative analysis stages 215

6.13 The Prototype Themes 218

7.1 Normal Regression Plot 241

7.2 Homoscedasticity Scatterplot 242

7.3 Research Model (right side) 244

7.4 Measurement Model 246

7.5 PLS Bootstrapping (T Statistics) 260

8.1 Final Structural Model 295

8.2 Persuasive Security Model (PSM) 299

LIST OF ABBREVIATIONS

BI	Behaviour Intention
CR	Composite Reliability
FBM	Fogg Behaviour Model
FT	Facilitator Trigger
GOF	Goodness of Fit
HCI	Human-computer interaction
ICT	Information and Communication Technology
ISA	Information Security Awareness
ISP	Information Security Policy
ISS	Information Security System
IT	Information Technology
PEOU	Perceived Ease of Use
PLS	Partial Least Squares
PMT	Protection Motivation Theory
PSOT	Perceived Severity of Threats
PT	Persuasive Technology
PTC	Prototype Content
PTD	Prototype Design
PU	Perceived Usefulness
RW	Reward
SE	Self-efficacy
SN	Subjective Norm
SPSS	Statistical Package for Social Science
ST	Spark Trigger
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour

CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION

Currently, the internet is visibly becoming an essential product for any business, similar to electricity and other utilities; without them, many businesses are unable to get the job done. Nevertheless, information security for both business and home users is significant. Electronic networks and computer technologies are growing at a rapid pace, leading to growth in information systems and extending their capabilities in most business sectors. Information and communication technology (ICT) constantly change to capitalise on advancing technology. However, the resulting ongoing changes can present numerous concerns regarding the protection of information assets.

Moreover, information assets are mostly in electronic form and processed by information systems. Information assets are communicated extensively on the internet and over a private network. Therefore, high levels of connectivity, the enormous growth of electronic commerce, the availability of sophisticated hacking tools, and other factors create challenges to information security (Hu, Hart, & Cooke, 2007; Humayun, Niazi, Jhanjhi, Alshayeb, & Mahmood, 2020). Viruses, spyware, and security breaches occur almost daily, requiring constant monitoring and protection. Turner and Broucek (2003) revealed that "*In the age of hacktivism, malware, and cyber-warfare, an increasing number of publications are being produced by computer security specialists and systems administrators on technical issues arising from illegal or inappropriate online behaviours.*"

People use computing devices for a variety of reasons, which require information security. The weakest link in information security is human beings

(Abraham, 2013; Han, Dai, Han, & Dai, 2015). Implementing information security best practices increases in complexity due to the many options available to access networks from home computers and mobile devices. This has led to increased developments in cybercrime and related risks to the home user (end-users).

In addition, these home users are becoming more vulnerable to security threats due to the use of information communication technologies, 95% of attacks by targeting home computer users (Furnell, Bryant, & Phippen, 2007; Sophos, 2009; Symantec, 2007). Eighty per cent of the zero-day attacks used home computer users' applications in 2014-2015(McAfee, 2015). Compliance with security policies is important in an organisational setting. However, there are no rules for home users, and they are not expected to engage in safe and secure behaviour. While home users are highly likely to provide intruders with useful information (for example, email, internet banking, online shopping, instant messaging, and online trading), home user security information should also be a concern to organisations (Li & Siponen, 2011). Therefore, security for home digital devices and services is becoming increasingly important as many home users (end-users) face online threats and attacks (Nthala & Flechais, 2019).

A variety of security measures exist to protect end-users. Such methods continue to evolve and grow in complexity to combat the increasing nature of the information security risks. To function effectively, they depend fundamentally on the end-user to install, configure and run them (Talib, Clarke, & Furnell, 2010). Information security relies primarily on technical solutions, including encryption, anti-spyware, malware prevention, and firewalls (Spears & Barki, 2010; Stanton, Stam, Mastrangelo, & Jolton, 2005). It is not enough, however, to invest in technical information security system countermeasures, because 50-70% of overall information security system (ISS) incidents are expected to result directly or indirectly from the misuse of end-users from innocent to deliberate damage (Siponen & Vance, 2010). In order to improve information security, both technological and social resources require investments (Bulgurcu, Cavusoglu, & Benbasat, 2010). Against this context, scholars and practitioners have recently turned their attention to the human aspect of information security through the application of behaviour and social psychology concepts. In fact, Experts believe that technology cannot entirely assure a safe environment for information (Bada, Sasse, & Nurse, 2019; Dhillon & Backhouse, 2000; Hwang et al., 2019; Safa et al., 2015)

Therefore, end-users' behaviour should be thought of as an essential aspect within this domain; people are the critical elements of information security policies and are accountable for their use of computing resources. There is no guarantee that people will strictly comply with security policies. Addressing the threat posed by end-users, the emphasis has been put on awareness of information security and the need to educate and inform end-users (Ikhalia, Serrano, Bell, & Louvieris, 2019).

Information security awareness (ISA) was described as one of the most critical information security behaviour prerequisites and a key factor for policy compliance. If people have high levels of ISA, they understand not only information security risks better but make more significant efforts to keep information secure (Al-Omari, El-Gayar, & Deokar, 2012a; Alotaibi, Clarke, & Furnell, 2020; Dinev & Hu, 2007; Siponen, 2000c, 2000a). Extreme losses of information can be caused by any end-user who compromises security. Some security incidents have been captured by the media and caused financial and reputational losses for the organisations. For example, due to the carelessness of one end-user in a hospital in Massachusetts resulting in the loss of files containing personally identifiable information, the hospital had to pay one million dollars (USD) in settlements (Abraham, 2013).