

ANTECEDENTS AND OUTCOMES OF
INTERNET ABUSE IN THE WORKPLACE: THE
MODERATING EFFECTS OF GENDER, AGE AND
INTERNET EXPERIENCE.

YULIHASRI

UNIVERSITI SAINS MALAYSIA
2012

ANTECEDENTS AND OUTCOMES OF
INTERNET ABUSE IN THE WORKPLACE: THE
MODERATING EFFECTS OF GENDER, AGE AND
INTERNET EXPERIENCE

by

YULIHASRI

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

February 2012

DEDICATION

To my wife “Dian Messalina”

To my children

Alan Lasena and Hikmatul Shalihah

ACKNOWLEDGMENT

Firstly, I would like to express my deepest gratitude to Allah S.W.T for giving me the will, ambition and perseverance to complete this research. This research project would not have been completed without assistance of people, whom I would like to thank.

Apart from that, my greatest gratitude goes to my supervisor, Professor T. Ramayah for his valuable advice, suggestion and dedication in supervising me throughout this research project. I would also wish to extend special thanks to the examiners of this thesis: Associate Prof. Abdul Razak Ibrahim, Associate Prof. Dr. Nornina Dahlan and Associate Prof. Dr. Suhaiza Hanim. Furthermore, I would like to extend special thanks and appreciation to YBhg. Prof. Dato' Dr. Ishak Ismail (the Dean), Associate Prof. Dr. Zamri Ahmad (Deputy Dean), Dr. Siti Rohaida, Dr. Noor Hazlina Ahmad, Prof. Dr. Zainal Arifin Ahmad, other lecturers and staffs of School of Management for their selfless kindness, warmth, and helps during my study in Universiti Sains Malaysia.

In addition, it is impossible for this thesis to be done with the help of my friends and Dr. Syaiful, Dr. Jasmine, Dr. Aminul Islam, Dr. Yudi Fernando, Jason Lee, Syafrizal, Ardi Muluk, Ronald, and top management of Andalas University, Prof. Dr. Musliar Kasim, Prof. Dr. Novisar Jamarun, Prof. Dr. Werry Dart MA, Prof. Dr. Syafruddin Karimi, Prof. Dr. Tafdil Husni, Prof. Dr. Herri , Dr. Harif Rivai, Dr. Vera Pujani, and so on for their efforts and time.

In addition, I would like to express my gratitude to Universiti Sains Malaysia (USM) in providing the Postgraduate Fellowship and the learning environments and facilities. Finally to all the respondents and college friends who have directly and indirectly assisted me to collect valuable data for this thesis.

TABLE OF CONTENTS

	Pages
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
TABLE OF CONTENTS	v
LIST OF TABLES	xiv
LIST OF FIGURES	xvii
LIST OF APPENDICES	xviii
LIST OF PUBLICATION AND SEMINARS	xxi
ABSTRAK	xxii
ABSTRACT	xxiv
CHAPTER 1: INTRODUCTION	
1.1 Introduction	1
1.2 Background of Study	2
1.2.1 Worldwide Internet Usage	2
1.2.2 Internet Usage in Malaysia	3
1.2.3 Internet Abuse in the Workplace	7
1.3 Research Problem	12
1.4 Research Objectives	17
1.5 Research Questions	18
1.6 Significant of the Study	19
1.7 Definition of Key Variables	21
1.8 Organization of the Chapters	26

CHAPTER 2: LITERATURE REVIEWS

2.1	Introduction	27
2.2	Internet Abuse at the Workplace	28
2.3	Workplace	31
2.4	The Theory of Planned Behaviour (TPB) and Decomposed Theory of Planned Behaviour (DTPB) model	32
2.4.1	The Theory of Planned Behaviour (TPB)	32
2.4.2	The Decomposed Theory of Planned Behaviour Model	34
2.5	Application of Decomposed Theory of Planned Behaviour to Internet abuse	36
2.5.1	Attitudes	38
2.5.1.1	Perceived Usefulness	40
2.5.1.2	Perceived Ease of Use	41
2.5.1.3	Compatibility	42
2.5.1.4	Playfulness	44
2.5.2	Subjective Norm	46
2.5.2.1	Peer Culture	48
2.5.2.2	Supervisor Culture	49
2.5.2.3	Family Culture	51
2.5.2.4	Mass Media	53
2.5.3	Perceived Behavioural Control	54
2.5.3.1	Facilitating Conditions	56
2.5.3.2	Self-Efficacy	57
2.5.3.3	Workplace Privacy	59
2.5.3.4	Internet Policy	61

2.5.3.5	Electronic monitoring	63
2.5.4	Moderating Variables (Gender, Age, and Internet Experience)	66
2.5.4.1	Gender	66
2.5.4.2	Age	69
2.5.4.3	Internet Experience	72
2.6	Outcomes of Deviant Use of Internet Technology	74
2.7	Internet Abuse and Outcomes	76
2.7.1	Internet Abuse and Work Inefficiency	76
2.7.2	Internet Abuse and Security Threats	78
2.7.3	Internet Abuse and Depression	80
2.7.4	Internet Abuse and Loneliness	81
2.8	Research Framework	85
2.9	Research Hypotheses	90
2.9.1	Belief Dimensions of Attitude towards Internet Abuse	90
2.9.2	Belief dimensions of Subjective Norm and Internet Abuse	96
2.9.3	Belief dimensions of Perceived Behavioural Control and Internet Abuse	105
2.9.4	Independent Variables (attitude, subjective norm, perceived behaviour control) and Internet Abuse	114
2.9.5	Demographic Variables	118
2.9.5.1	Genders	119
2.9.5.2	Ages	124
2.9.5.3	Internet Experience	128
2.9.6	Internet Abuse and Workplace-related outcomes	131
2.9.6.1	Work Inefficacy	131

2.9.6.2	Security Threats	133
2.9.7	Internet Abuse and Psychological Outcomes	135
2.9.7.1	Loneliness	135
2.9.7.2	Depression	138
2.10	Summary	139
CHAPTER 3: RESEARCH METHODOLOGY		
3.1	Introduction	141
3.2	Research Design	141
3.3	Population and Sampling	141
3.4	Data Collection Procedure	147
3.5	Extra Data Collection Procedure	148
3.6	Variables and Measures	149
3.7	Questionnaire Design	157
3.8	Pilot Study	159
3.9	Data Analysis Techniques	161
3.10	Summary	161
CHAPTER 4: RESULTS		
4.1	Introduction	163
4.2	T test of the main data and extra data	163
4.3	Response Rate	167
4.4	Profile of Respondents	169
4.5	Goodness of Measures	172
4.5.1	Factor Analysis	172
4.5.1.1	Factor Analysis on Belief Dimensions of Attitude towards Internet Abuse	173

4.5.1.2	Factor Analysis on Belief Dimensions of Subjective Norm	174
4.5.1.3	Factor Analysis on Belief Dimensions of Perceived Behavioural Control	175
4.5.1.4	Factor Analysis on Determinants of Internet Abuse	177
4.5.1.5	Factor Analysis on Internet Abuse	178
4.5.1.6	Factor Analysis on Outcomes of Internet Abuse	179
4.5.2	Reliability Analysis	181
4.6	Modification of Research Framework and Restatement of Hypotheses	182
4.7	Descriptive Analysis	185
4.8	Correlation Analysis	188
4.9	Hypothesis Testing	192
4.9.1	Multiple Regression Analysis	192
4.9.1.1	The Relationship between Belief Dimensions and Attitude towards Internet Abuse	192
4.9.1.2	The Relationship between Belief dimensions and Subjective Norm	193
4.9.1.3	The Relationship between Belief Dimensions and Perceived Behavioural Control	194
4.9.1.4	The Relationship between Independent Variables (Attitude, Subjective Norm, Perceived Behavioural Control) and Internet Abuse	195
4.9.1.5	The Relationship between Internet Abuse and Project Work Inefficiency	195
4.9.1.6	The Relationship between Internet Abuse and Time	

	Material Inefficiency	196
4.9.1.7	The Relationship between Internet Abuse and Security Threats	196
4.9.1.8	The Relationship between Internet Abuse and Depression	197
4.9.1.9	The Relationship between Internet Abuse and Loneliness	197
4.9.2	The Moderating Effect of Gender, Age and Internet Experience on the Relationship between the Independent Variables (Attitude towards Internet Abuse, Subjective Norm and Perceived Behavioural Control) and Internet abuse	
4.9.2.1	The Moderating Effect of Gender	198
4.9.2.2	The Moderating Effect of Age	198
4.9.2.3	The Moderating Effect of Internet Experience	200
4.9.3	Level of Internet Abuse in Malaysia	203
4.9.3.1	Overall Level of Internet abuse among Employees in Malaysia	205
4.9.3.2	Level of Internet Abuse among Different Gender Groups	205
4.9.3.3	Level of Internet Abuse among Different Age Groups	205
4.9.3.4	Level of Internet Abuse among Different Internet Experience Groups	207
4.9.3.5	Level of Internet Abuse among Different Position Group	208

4.10	Summary of Major Findings and Results of Hypotheses	210
CHAPTER 5: DISCUSSION AND IMPLICATIONS		
5.1	Introduction	213
5.2	Discussion of Finding	213
5.2.1	Belief Dimensions of Attitude towards Internet Abuse	214
5.2.1.1	Perceived Usefulness	214
5.2.1.2	Perceived Ease-of-Use	216
5.2.1.3	Compatibility	217
5.2.1.4	Playfulness	219
5.2.2	Belief Dimensions of Subjective Norm	220
5.2.2.1	Peer Culture	220
5.2.2.2	Supervisor Culture	221
5.2.2.3	Family Culture	223
5.2.2.4	Mass Media Influence	224
5.2.3	Belief Dimensions of Perceived Behavioural Control	226
5.2.3.1	Self-Efficacy	227
5.2.3.2	Facilitating Conditions	228
5.2.3.3	Internet Policy	230
5.2.3.4	Workplace Privacy	232
5.2.3.5	Electronic Monitoring	234
5.2.4	Attitude and Internet Abuse	236
5.2.5	Subjective Norm and Internet Abuse	238
5.2.6	Perceived Behavioural Control and Internet Abuse	240
5.2.7	Internet Abuse and Workplace-related Outcomes (Project Work Inefficiency and Time Material Inefficiency)	242

5.2.8	Internet Abuse and Workplace-Related Outcomes (Security Threats)	244
5.2.9	Internet Abuse and Psychological Outcomes (Depression and Loneliness)	246
5.2.10	Moderating Effect of Gender on the Relationship between Attitude, Subjective Norm, Perceived Behavioural Control and Internet Abuse	248
5.2.11	Moderating Effect of Age on Relationship between Attitude, Subjective Norm, Perceived Behavioural Control and Internet Abuse	251
5.2.12	Moderating Effect of Internet Experience on Relationship between Attitude, Subjective Norm, Perceived Behavioural Control and Internet Abuse	256
5.2.13	Level of Internet Abuse among the Employees in Malaysia	259
5.3	Implications of Research	260
5.3.1	Theoretical Contributions	260
5.3.2	Practical Contributions	268
5.3.2.1	Addressing Employee Attitude	269
5.3.2.2	Implementing Controls	269
5.3.2.3	Addressing Playfulness and Attitude	272
5.3.2.4	Internet Policy Awareness	273
5.3.2.5	Addressing Work Inefficiency	274
5.3.2.6	Addressing Security Threats	275
5.3.2.7	Addressing Psychological Issues	275
5.4	Limitations of the Study	276

5.5	Future Research	277
5.6	Conclusion	279
	REFERENCES	282

LIST OF TABLES

	Page	
Table 1.1	World Internet Usage and Population Statistics 2009	3
Table 1.2	Internet Usage and Population Growth in Malaysia	4
Table 1.3	Top 10 Time-Wasting Activities in the Workplace	7
Table 3.1	Questionnaire Design	158
Table 3.2	Reliability Analysis for the Pilot Study	160
Table 4.1	T test of comparing main data and extra data	164
Table 4.2	Response Rate	168
Table 4.3	Profile of the Respondents	170
Table 4.4	Factor Analysis on Belief dimensions of Attitude towards Internet Abuse	173
Table 4.5	Factor Analysis on Belief dimensions of Subjective Norm	175
Table 4.6	Factor Analysis on Belief dimensions of Perceived Behavioural Control	176
Table 4.7	Factor Analysis on Determinants of Internet Abuse	177
Table 4.8	Factor Analysis on Internet Abuse	178
Table 4.9	Factor Analysis on Outcomes of Internet Abuse	180
Table 4.10	Reliability Test	181
Table 4.11	Restatement of Hypotheses	184
Table 4.12	Mean Values and Standard Deviation Variables of the Study (N=501)	187
Table 4.13	Inter-correlation of this study's variables	191
Table 4.14	Multiple Regression between Belief dimensions of Attitude and Attitude towards Internet Abuse	193
Table 4.15	Multiple Regression between Belief dimensions and Subjective Norm	193

Table 4.16	Multiple Regressions between Belief dimensions and Perceived Behavioural Control	194
Table 4.17	Multiple Regression between Independent Variables and Internet Abuse	195
Table 4.18	Multiple Regression between Internet Abuse and Project Work Inefficiency	196
Table 4.19	Multiple Regressions between Internet Abuse and Time Material	196
Table 4.20	Multiple Regressions between Internet Abuse and Security Threat	197
Table 4.21	Multiple Regressions between Internet Abuse and Depression	197
Table 4.22	Multiple Regressions between Internet Abuse and Loneliness	198
Table 4.23	The Moderating Effect of Gender on the Relationship between the Independent Variables (Attitude, Subjective Norm and Perceived Behavioural Control) and Internet Abuse	199
Table 4.24	The Moderating Effect of Age on the Relationship between the Independent Variables (Attitude, Subjective Norm and Perceived Behavioural Control) and Internet Abuse	201
Table 4.25	The Moderating Effect of Internet Experience on the Relationship between the Independent Variables (Attitude, Subjective Norm and Perceived Behavioural Control) and Internet Abuse	203
Table 4.26	Comparison of Male and Female on Internet Abuse	205
Table 4.27	Mean and Standard Deviations Comparing Age on Internet Abuse	206
Table 4.28	One-Way Analysis of Variance Table Comparing Internet Abuse on Age	206
Table 4.29	Post Hoc Test: Multiple Comparison	206
Table 4.30	Means and Standard Deviations Comparing Internet Experience on Internet Abuse	207
Table 4.31	One-Way Analysis of Variance Table Comparing Internet Abuse on Internet Experience	208
Table 4.32	Post Hoc Test: Multiple Comparison	208

Table 4.33	Means and Standard Deviations Comparing Current Position on Internet Abuse	209
Table 4.34	One-Way Analysis of Variance Table Comparing Internet Abuse on Current Position	209
Table 4.35	Post Host Test: Multiple Comparisons	209
Table 4.36	Summary of Hypothesis Analysis Results	211

LIST OF FIGURES

		Page
Figure 1.1	Internet User in Malaysia	4
Figure 2.1	Theory of Planned Behaviour (TPB)	33
Figure 2.2	Decomposed of Theory of Planned Behaviour	38
Figure 2.3	Outcomes of Deviant use of Internet Technology Model	75
Figure 2.4	Research Framework	89
Figure 4.1	The modified research framework	183
Figure 4.2	The Impact of Gender on the Relationship between Perceived Behavioural Control and Internet abuse	200
Figure 4.3	The Impact of Age on the Relationship between Attitude and Internet abuse	202
Figure 4.4	The Impact of Internet Experience on the Relationship between Perceived Behavioural Control and Internet abuse	204

LIST OF APPENDICES

		Page
Appendix A	Research Questionnaire	307
Appendix A1	A Copy of Questionnaire Cover Letter from Deputy Dean	308
Appendix A2	A Copy of Questionnaire Cover Letter from Researcher and Supervisors	310
Appendix A3	Survey Questionnaire	311
Appendix B	Frequency Table for Respondent Profile	322
Appendix C	T-Tests on All the Variables of Main Data and Extra Data	325
Appendix D	Factor Analysis	327
Appendix D1	Factor Analysis on Belief Dimensions of Attitude Variables towards Internet Abuse	327
Appendix D2	Factor Analysis on Belief Dimensions of Subjective Norm towards Internet Abuse	329
Appendix D3	Factor Analysis on Belief Dimensions of Perceived Behavioural Control towards Internet Abuse	330
Appendix D4	Factor Analysis on Antecedents of Internet Abuse	332
Appendix D5	Factor Analysis on Internet Abuse	333
Appendix D6	Factor Analysis on Outcomes of Internet Abuse	334
Appendix E	Reliability Analysis	335
Appendix E1	Usefulness	335
Appendix E2	Ease of Use	335
Appendix E3	Compatibility	336
Appendix E4	Playfulness	336
Appendix E5	Attitude	337
Appendix E6	Peer Culture	337
Appendix E7	Supervisor Culture	338

Appendix E8	Mass Media	338
Appendix E9	Family Norm	339
Appendix E10	Subjective Norm	339
Appendix E11	Self-Efficacy	340
Appendix E12	Facilitating Condition	340
Appendix E13	Workplace Privacy	341
Appendix E14	Electronic Monitoring	341
Appendix E15	Internet Policy	342
Appendix E16	Perceived Behavioural Control	342
Appendix E17	Internet Abuse	343
Appendix E18	Time Material Inefficiency	344
Appendix E19	Work Project Inefficiency	344
Appendix E20	Security Threats	345
Appendix E21	Depression	345
Appendix E22	Loneliness	346
Appendix F	Correlation Analysis	347
Appendix G	Descriptive of Variables	348
Appendix H	Multiple Regression Analysis	349
Appendix H1	Regression Analysis between Dimensions and Attitude towards Internet Abuse	350
Appendix H2	Regression Analysis between Dimensions and Subjective norm	351
Appendix H3	Regression Analysis between Dimensions and Perceived Behavioural Control towards Internet Abuse	352
Appendix H4	Regression Analysis between Independence Variables and Internet Abuse Activities	352
Appendix H5	Regression Analysis between Internet Abuse and Project Work Inefficiency	354

Appendix H6	Regression Analysis between Internet Abuse and Time Material Inefficiency	355
Appendix H7	Regression Analysis between Internet Abuse and Security Threats	356
Appendix H8	Regression Analysis between Internet Abuse and Depression	357
Appendix H9	Regression Analysis between Internet Abuse and Loneliness	358
Appendix H10	Regression Analysis of the Moderating Effect of Gender	359
Appendix H11	Regression Analysis of the Moderating Effect of Age	361
Appendix H12	Regression Analysis of the Moderating Effect of Internet Experience	362
Appendix I	Level of Internet Abuse	364
Appendix I1	Level of Internet Abuse among Different Gender	364
Appendix I2	Level of Internet Abuse among Different Age	364
Appendix I3	Level of Internet Abuse among Different Internet Experience	365
Appendix I4	Level of Internet Abuse among Different Position	367

LIST OF PUBLICATION AND SEMINARS

Use and Misuse of the Internet in the Malaysian Workplace: Preliminary Findings from an Exploratory Study

Yulihhasri, T. Ramayah, Amlus Ibrahim and Norzalila Jamaludin,

The proceeding of The 15th International Conference on Management of Technology (IAMOT), “East Meets West: Challenges and Opportunities in the Era of Globalization” 22 –26 May, 2006 Beijing: China.

The Impact of Internet Abuse on Psychological Well-being of Employees in Malaysia

Yulihhasri, T. Ramayah

The proceeding of The 21th International Conference on Management of Technology (IAMOT), “Managing Technology-Service Convergences in the Post-Industrialized Society”, 18-22 march, 2012 Hsinchu: Taiwan.

Internet Abuse and Productivity among the Employees in Malaysia

Yulihhasri, T. Ramayah

The proceeding of The 21th International Conference on Management of Technology (IAMOT), “Managing Technology-Service Convergences in the Post-Industrialized Society”, 18-22 march 2012 Hsinchu: Taiwan.

**ANTESEDEN DAN KESAN PENYALAHGUNAAN INTERNET DI TEMPAT
KERJA: KESAN PENYERDERHANAAN DARIPADA JANTINA, UMUR,
DAN PENGALAMAN INTERNET**

ABSTRAK

Internet menjadi satu kemudahan asas yang penting di dalam organisasi hari ini. Penyalahgunaan internet adalah suatu masalah yang dihadapi oleh hampir semua organisasi. Kesan-kesan penyalahgunaan Internet oleh para pekerja di dalam organisasi menjadi sangat serius jika masalah tersebut tidak ditangani dengan sempurna. Maka, kajian ini sangat diperlukan di negara timur yang sedang membangun seperti Malaysia. Satu kerangka teoretis diperlukan untuk membolehkan penyelidikan tentang penyalahgunaan Internet yang lebih komprehensif and menyeluruh dapat dijalankan. Maka, tujuan kajian ini adalah untuk mengenalpasti penyebab dan kesan penyalahgunaan Internet di tempat kerja secara empirikal. Kerangka penyelidikan dalam kajian ini ialah satu hasil persepaduan antara Teori Tingkah Laku Terancang Dikomposisi (DTPB) dan Akibat daripada Penggunaan Teknologi Internet secara Devian (DUIT). Berdasarkan Teori Tingkah Laku Terancang Dikomposisi, terdapat tiga pembolehubah tidak bersandar tentang penyalahgunaan Internet di tempat kerja, iaitu sikap, norma subjektif, kawalan tingkah laku yang tanggap. DUIT model mengkonsepsikan kesan penyalahgunaan Internet sebagai ketidakcekapan kerja, ancaman keselamatan Internet, dan kesejahteraan psikologi. Tambahan pula, rangka kerja tersebut akan menyelidik peranan faktor-faktor demografi jantina, umur, dan pengalaman Internet sebagai pembolehubah penyederhanaan antara tiga pembolehubah tidak bersandar-dalam isu penyalahgunaan Internet. 501 set borang soal selidik telah dikutip daripada para pekerja penuh masa untuk tujuan kajian ini. Penemuan kajian ini menunjukkan bahawa tahap penyalahgunaan Internet di Malaysia adalah sederhana tinggi, dan memerlukan perhatian and tindakan yang

sewajarnya perlu diambil sebelum masalah ini semakin serius. Tambahan pula, hasil kajian juga menunjukkan bahawa penyalahgunaan Internet adalah suatu kelakuan yang bermotivasi secara dalaman. Hasil kajian ini mendapati bahawa sikap adalah anteseden yang paling berpengaruh terhadap penyalahgunaan Internet, diikuti oleh kawalan tingkah laku yang tanggap dan norma subjektif. Jantina dan pengalaman Internet didapati mempunyai kesan penyerhanaan antara kawalan tingkah laku yang tanggap dan penyalahgunaan Internet. Selain itu, hasil analisis menunjukkan bahawa umur menyederhanakan hubungan antara sikap dan penyalahgunaan Internet. Tambahan pula, penyalahgunaan Internet didapati menyebabkan ketidakcekapan kerja, ancaman keselamatan Internet, kesunyian, dan kemurungan. Kajian ini telah menyumbang melalui penyesuaian DTPB model yang biasanya digunakan dalam kajian kelakuan normal ataupun positif, dan sebagai satu kerangka kerja yang sesuai untuk meramalkan kelakuan negatif, khususnya dalam penyalahgunaan Internet. Lazimnya, kesejahteraan psikologi, iaitu kesunyian dan kemurungan ditemui dalam kajian sebelum ini sebagai kesan penggunaan Internet berlebihan. Kajian ini telah mencapai penemuan baru dengan membuktikan bahawa penyalahgunaan Internet juga akan menyebabkan kemerosotan kesejahteraan psikologi para pekerja. Berdasarkan hasil penemuan dalam kajian ini, kelemahan dan implikasi praktikal kajian turut dibincangkan.

ANTECEDENTS AND OUTCOMES OF INTERNET ABUSE IN THE WORKPLACE: THE MODERATING EFFECTS OF GENDER, AGE AND INTERNET EXPERIENCE

ABSTRACT

Internet abuse is a problem that encountered by almost all of the organizations nowadays as Internet becomes one of the fundamental facilities in the organizations. The impacts of Internet abuse on employees and organizations can be tremendous if the problem were left to be unsolved. Hence, a study in the Eastern and developing countries like Malaysia is needed. Furthermore, there is a need for a theoretical framework that can provide more sophisticated and holistic investigation on the Internet abuse problem. Therefore, the purpose of this study is to empirically investigate the antecedents and outcomes of Internet abuse behaviour at the workplace. The research framework in this study is an integration of Decomposed Theory of Planned Behaviour (DTPB) and Outcomes of Deviant Use of Internet Technology (DUIT). By drawing theoretical support from DTPB, there are three antecedents of Internet abuse behaviour, namely attitude, subjective norm, and perceived behaviour control. The DUIT model conceptualized the outcomes of Internet abuse as work inefficiency, Internet security threats, loneliness, and depression. Moreover, the framework examined the roles of demographics particularly gender, age and Internet experience as moderators between the three antecedent variables and Internet abuse behaviour. A total of 501 usable responses collected from fulltime employees based on purposive sampling were used for the purpose of this study. The findings of this study indicated that Internet abuse level in Malaysia was slightly higher than moderate, which deserved proper attention before it goes rampant. Furthermore, the result demonstrated that Internet abuse is more of an inwardly-motivated behaviour, as attitude was found as the most influential

antecedent of Internet abuse, followed by perceived behavioural control and subjective norm. With regard to the moderating variables, Gender and Internet experience were found to have significant moderating the relationship between perceived behavioural control and Internet abuse behaviour. Moreover, age was found to significantly moderating the relationship between Attitude and Internet abuse. In terms of the outcomes, Internet abuse was found to be significantly led to work inefficiency, Internet security threats, loneliness, and depression. This study has contributed through the adaptation of DTPB model which commonly used for the investigation of positive and normal behaviour to be a framework that suitable for the prediction of a negative behaviour, specifically Internet abuse. Psychological wellbeing variables, namely loneliness and depression were commonly found to be the outcomes of excessive use of Internet. However, this study taken an advance step to proven that Internet abuse could also lead to the deterioration of employees' psychological wellbeing. Based on the findings, discussions of the limitations, practical implications of the study were provided as well.

CHAPTER 1

INTRODUCTION

1.1 Introduction

The Internet is currently the world's largest interconnected computer environment, a worldwide system of interconnected computer networks that link billion of users together. Apart from being an information and communication technology (ICT) for the general public, it has also become an important tool for businesses around the globe. Internet usage is a routine activity in the workplace, which is rapidly growing and gradually becoming an indispensable part of business operations. Greengard (2000) mentioned that in this era of an emerging digital economy, the Internet has come to establish itself alongside the telephone and computer, as another basic technology in the workplace for operating daily activities.

Moreover, the Internet has gradually changed its role in that for business entities to compete and survive in today's business arena it is no longer a competitive advantage but a necessity (Acosta & Cerdan, 2009). Sharma and Gupta (2003) added that the Internet functions as a 'backbone' of the communication network for companies to disseminate information within and outside of the organisation. For instance, email is an Internet application that has contributed tremendous benefits to business organisations. Without the Internet, most of today's organisations could not operate effectively or even survive.

Based on the anecdotal evidence, it is widely recognised that Internet in the workplace is a double-edged sword (Niemann, 2002; Lim, Teo & Loo, 2002), in which the availability of Internet facilities in the workplace has also given a way to the potential for Internet abuse and subsequently the rise of undesired consequences.

With regard to this, Sharma and Gupta (2003) found employees have exploited the Internet for personal purposes, which do not add value to their work. Furthermore, personal use of the workplace Internet is believed to be linked to outcomes such as, reduced worker productivity, legal issues and security threats (Anandarajan & Simmers, 2004; Young & Rodger, 1998; Ting & Grant, 2005).

With personal use of the workplace Internet gaining prominence in today's business environment, this research aims to closely examine the issues of Internet abuse and gain deeper insights into the antecedents and outcomes of Internet abuse, specifically among Malaysian employees. This chapter begins with a discussion on the background of study, followed by the research problem, research questions, research objectives, significance of the study and definitions of terminologies.

1.2 Background of Study

1.2.1 Worldwide Internet Usage

The discussion on Internet abuse would be incomplete without a preview of Internet usage. According to www.Internetworldstats.com (2010), the number of Internet users for the year 2010 reached 1.966 billion, equivalent to 28.7% of the world's population. The future for Internet usage looks promising, as ever increasing numbers of individuals and organisations will have access to the Internet. Table 1.1 shows worldwide Internet usage statistics in year 2010 according to world continents.

As indicated in Table 1.1, North America (comprising the USA and Canada) is currently the region with the highest Internet penetration rate, around 77.4% of the population in that region. In terms of world usage, North America attributes for 13.5% of the world's Internet usage, whereas Asia has the highest percentage of

Internet usage in the world (42.0%), although the Internet penetration stands at a mere 21.5% of the population, as compared to North America. Although much wider spread of Internet penetration is recorded among the population in North America, Asia remains as the region that contains almost half of the world's Internet users. According to the statistics, the number of Internet users worldwide has increased steadily over the years. Between the years 2000 and 2010, the number of global Internet users recorded growth of 444.8%.

Table 1.1 World Internet Usage and Population Statistics 2010

World Region	Population (2010 Est.)	Internet Users Dec.31, 2000	Internet usage (Jun.30, 2010)	Penetration (% Population)	Users Growth % 2000-2010	Usage % of World
Africa	1,013,779,050	4,514,400	110,931,700	10.9	2,357.3	5.6
Asia	3,834,792,852	114,304,000	825,094,396	21.5	621.8	42.0
Europe	813,319,511	105,096,093	475,096,448	58.4	352.0	24.2
Middle East	212,336,924	3,284,800	63,240,946	29.8	1,825.3	3.2
North America	344,124,450	108,096,800	266,244,500	77.4	146.3	13.5
Latin America/ Caribbean	592,556,972	18,068,919	204,689,836	34.5	1,032.8	10.4
Oceania/ Australia	34,700,201	7,620,480	21,263,990	61.3	179.0	1.1
WORLD TOTAL	6,845,609,960	360,985,492	1,966,514,816	28.7	444.8	100.0

(Source: www.Internetworldstats.com)

1.2.2 Internet Usage in Malaysia

In 2010, with an Internet penetration rate of 64.6%, Malaysia was ranked seventh out of 35 Asian countries, after South Korea, Brunei, Japan, Singapore, Taiwan, and Hong Kong (<http://www.internetworldstats.com/stats3.htm>). According to Malaysian government statistics (www.statistics.gov.my) and the Euro Monitor Institution (www.euromonitor.com) in 2010, Internet usage in Malaysia increased

drastically between the years 2000 – 2010, as shown in Table 1.2. In 2000, the percentage of Internet users over the country population was 15.7%. Since then the percentage of Internet users has grown to 58.5% of the country population, so over ten years the growth rate is 446%. Following this trend, it is rational to expect that the percentage of Internet users in Malaysia will continue to grow in the coming years. In addition to Table 1.2, the trend of Internet users in Malaysia is presented in Figure 1.1.

Table 1.2 Internet Usage and Population Growth in Malaysia

YEAR	Users	Population	Percentage Usage
2000	3,700,000	23,494,900	15.7%
2005	10,040,000	26,476,900	37.9%
2006	11,016,000	26,831,500	41.1%
2007	14,791,500	27,186,000	54.4%
2008	15,074,000	27,540,500	54.7%
2009	15,354,500	27,895,300	55.0%
2010	16,518,040	28,250,500	58.5%

(Source: www.statistics.gov.my & www.euromonitor.com)

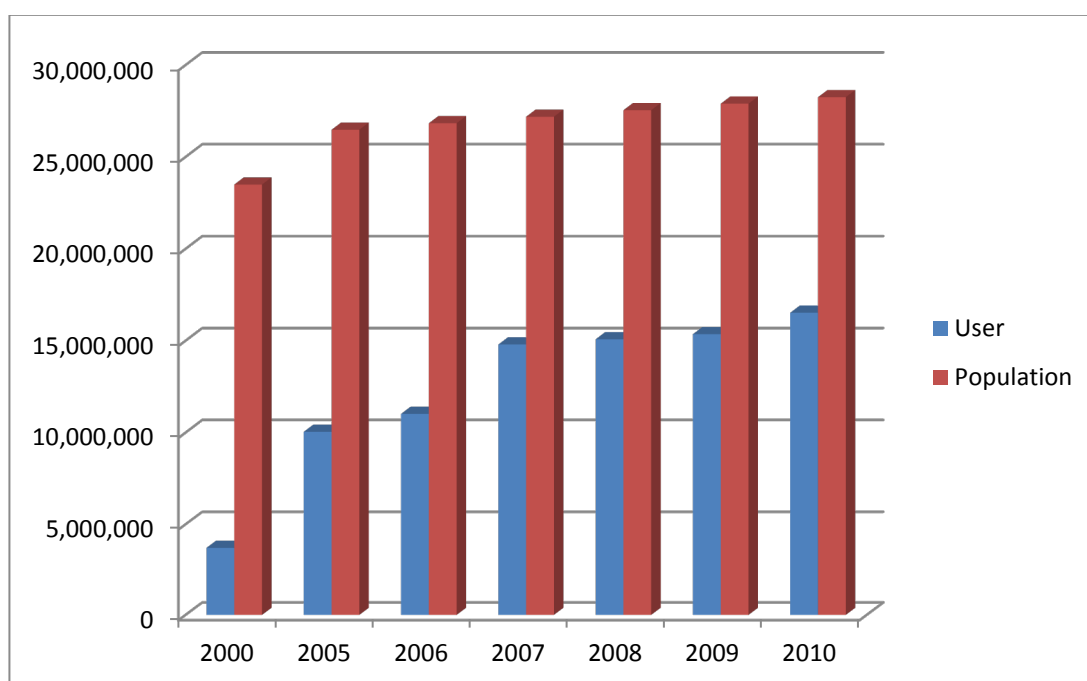


Figure 1.1 Internet Users in Malaysia

The rise in the number of Internet users in Malaysia may be attributed to the efforts of local government and related agencies, who have put considerable effort into making the necessary infrastructure readily available, and constantly encouraging Malaysians to be Internet savvy through various programs. The government has cooperated with Internet service providers to open the Internet services market to a greater number of providers. For instance, the emergence of P1 WiMAX, Yes 4G networks and other broadband Internet services have developed and increased the competitiveness in the Internet services market. The healthy competition in the industry has benefited the consumers in Malaysia, with Internet services that are reliable, affordable and accessible.

Despite all the emerging Internet providers and increasing numbers of Internet users, it should be recognised that Malaysia is falling behind in most aspects of the Internet, particularly when compared to developed countries such as USA, UK, Germany, Canada, etc. Malaysia is still facing various challenges, from unsophisticated telecommunications infrastructure, difficulties in utilising the full potential of Internet, and managing its information flow (Xue, 2005). For these reasons, Malaysia, like other Asian countries, is driven to develop and sustain world-class infrastructure to support the growth of information communication technologies like the Internet. In order to achieve the country's aspiration, the Multimedia Development Corporation (MDec) has developed a National Electronic Commerce Master Plan, which is designed to facilitate a supportive environment for the development of Internet facilities in Malaysia.

Even though Malaysia has one of the world's strictest forms of media censorship, with nearly a hundred movies banned in this decade on the pretext of upholding morality, the Internet in Malaysia remains unfettered in line with

upholding civil liberties and maintaining democratic choices. In other words, there is no censorship imposed by the government (Australian Net Censorship Bill, 1999) on Internet usage in Malaysia. Recently, the Prime Minister of Malaysia, Datuk Seri Najib Razak further announced that the government has no plans to filter Internet access, as filtering Internet access only leads to public discontent. In addition, the Prime Minister also took into consideration China's unpleasant experience in Internet filtering, where the implementation of a filtering programme across the country caused delays due to problems such as breaches in user security (New Straits Times, 2009, August, 8). In other words, Internet users in Malaysia have the freedom to fully access any resources on the internet, without restriction. Nevertheless, the Malaysian government is studying proposals to introduce new laws controlling the transmission of electronic information, possibly in response to an incident where a few Malaysian students in foreign countries posted articles on the Internet that "challenged" the status of the Malaysian government (Ang & Nadarajan, 1996).

With the ever-increasing reach of Internet access and prominence of social networking websites, Internet users in Malaysia can easily connect with other users around the world, to the point where Malaysia has been recognised as a country with users spending a lot of time on Facebook (Choong, 2011). According to the Global Market Monitor Report by eMarketer.com, Malaysia sits among the top ten countries with the highest growth of Facebook usage in the world, together with the US, Indonesia, Philippines, Turkey, Italy, India, and others (comScore Malaysia, 2011). One of the most common online activities of Malaysian Internet users is to access social networking website such as Facebook, Twitter, and LinkedIn.

1.2.3 Internet Abuse in the Workplace

Despite all the benefits surrounding the use of the Internet, such as greater liberating effects than other media because of its decentralized nature, reduced structural barriers to entry, and potential for diversity of voices (Royal, 2007), there are also negative impacts of the technology. In particular, personal use of Internet by employees in the workplace has become a serious issue that warrants much attention. Internet abuse, which generally refers to the use of the Internet for personal-related reasons during working hours, has become a growing concern of management in organisations (Taillon, 2004; Young & Case, 2003). Lavoie and Pychyl (2001) described the use of Internet for personal purposes as a modern, technologically mediated manifestation of procrastination. With regard to this, Internet abuse has been found to be the number one time-wasting activity in the workplace. Table 1.3 demonstrates the top 10 time-wasting activities in the workplace.

Table 1.3 Top 10 Time-Wasting Activities in the Workplace

No.	Top time-wasting activities	Percentage (%)
1.	Surfing the Internet (personal use)	44.7
2.	Socialising with co-worker	23.0
3.	Conducting personal business	6.8
4.	Spacing out	3.9
5.	Running errands off-premises	3.1
6.	Making personal phone calls	2.3
7.	Applying for other jobs	1.3
8.	Planning personal events	1.0
9.	Arriving late/Leaving early	1.0
10.	Other	12.5

(Source: www.sadastem.com (2007))

Table 1.3 indicates the ranking of top 10 time-wasting activities in the workplace according to descending order. The source pointed out that the most

prevalent time-wasting activity is internet surfing for personal purpose, which constitutes approximately 45% of all the time-wasting activities. This number reflects the severity of Internet abuse issue in the workplace. Activities such as socialising with co-workers and conducting personal business ranked after Internet surfing with respective percentages of 23% and 6.8%.

Other empirical evidence has indicated that personal use of the Internet in the workplace is proliferating in the business organisations. An online survey has revealed that 84% of employees sent non work-related email, while another 90% surf the Internet for recreational purposes during work hours (Lim, 2002; Lim et al., 2002). Furthermore, Sharma and Gupta (2003) found that 25% of employees spent more than an hour using the Internet during office hours for reasons not related to their work, 22% spent 30 minutes to an hour, and 25% spent 10 to 30 minutes while nearly 10% said they never surfed for personal use. The statistics indicate the prevalence of the misuse of the Internet in the workplace and signal that personal use of the Internet in the workplace is an issue that deserves the attention from the organisations' management.

In a study of 500 U.S. companies that included government agencies, financial institutions, medical institutions and universities, Fertell (2002) found that 78% of the respondents confessed to the abusing Internet use during office hours. Furthermore, other data collected from United States estimated that employees spend between 3.7 and 10 hours-a-week on Internet for personal usage (Galleta & Polak, 2003). In other words, U.S. workers generally spend 25% of a 40-hour work-week surfing the Internet for personal-related purposes (Young & Case, 2004a). The few most popular non-work related websites accessed were news (84%), travel (64

percent), personal e-mail (56%), shopping (55%), online banking (53%), pornography (42%), and online chatting (13%) (Greenspan, 2004).

In the context of Malaysia, Ramayah (2010) reported that 70% of the respondents agreed that it is acceptable to use the internet in the workplace for personal searches. Moreover, the study demonstrated that about 90% of the respondents indicated that they access internet for personal use a few times a week with about 60% accessing internet for personal use at least once a day. In addition, his findings revealed that approximately 84% of its respondents believe that it is acceptable for people to use the internet for personal purposes during non-working hours, like the lunch break. Similarly, another study carried out in Malaysia has revealed that respondents perceived personal email and online chatting during working hours as a common practice and did not perceive it to have much impact on the organisation (Zauwiyah & Hasmida, 2010). The results of these studies indicate that the Internet abuse problem is issue in the workplace and it is worthy of further investigation in the context of Malaysia.

There are varieties of activities involved in the misuse of workplace Internet. Young and Case (2003) and Taillon (2004) noted that the common Internet abuse activities are online chatting, personal e-mailing, online shopping, and bill paying, while extreme cases involve surfing pornography websites or online gambling during work hours. A specific study on Internet gambling has pointed out that Internet gamblers are found to be at risk of developing gambling problems and a substantial proportion of them can be properly classified as problem gamblers (Wood & Williams, 2007). Such Internet abuse in the workplace potentially causes problems to other workers due to the behaviour disorders and mediocre productivity of the gamblers. Internet abuse also includes the unauthenticated transfer of sensitive data

and business secrets, such as marketing plans, sales contracts, product development and pricing data, negotiations between companies, and other data that could be valuable for the competitors or outsiders (Hasim & Salman, 2010).

Another impact of Internet abuse is in the form of monetary loss. Mahatanankoon, Anandarajan and Igbaria (2004) showed that Internet abuse in the workplace can cost organisations up to US \$1 billion annually in terms of lost productivity, excluding other potential legal issues, such as libel, defamation, and harassment lawsuits. Moreover, it reported that employee access to Internet pornography during work hours have cost America's businesses billions of dollars in lost productivity, exposing them to sexual harassment lawsuits (Internet Channel Initiative, 2005). Internet abuse is also well known to place a significant drain on network capacity and decrease system responsiveness for job-related functions (Young, 2010a). This increases IT costs to organisations in terms of additional fees to administer servers, more expensive Internet services and hardware to accommodate the increased network traffic and data storage.

Internet abuse in the workplace could even affect Malaysia's economy because public and private business organisations constitute the backbone of the economy. As a consequence of Internet abuse, organisations need to increase ICT expenditure to control and prevent Internet abuse. The National ICT Security and Emergency Response Centre ICT Security Survey for Malaysia, 2000/2001, reported that the 205 participating Malaysian organisations suffered costs from employee Internet abuse: RM43.8 million due to from downloading pornography; RM1.04 million inappropriate usage of e-mail; RM 4.2 million due to employees' installing pirated software; and RM 820,000 due to the sabotage of data or networks (National ICT Security And Emergency Response Centre, 2003). These numbers show that

Internet abuse results in the waste of resources (both financial and non-financial) from activities that add no value to the country's economy, and the resources could be better spent increasing productivity of the private sector and indirectly the quality of living in the country.

Companies have taken various actions to reduce the amount of Internet abuse. These actions include verbal warnings, written warnings, payment deductions, and eventually, termination in serious cases (Bellm, 1998; Greengard, 2000). In addition, Greengard (2000) mentioned that nearly 70% of U.S firms have disciplined employees for Internet abuse and less than 30% of the firms have terminated workers due to Internet abuse. According to Greenfield and Davis (2002), several organisations such as the New York Times, Roll Royce and Xerox have terminated employees for Internet abuse based on two reasons. First, the employees downloaded pornographic materials during working hours or secondly, they sent emails to their friends during working hours.

As the Internet is an evolving technology, the emergence of new Internet applications will post new challenges or dilemmas to organisations in managing Internet abuse. Social networking websites have become pervasive in recent years, and when websites such as Facebook, MySpace and Twitter first emerged, some organisations viewed them as a distraction from work and banned them. Furthermore, Cyber Security Malaysia reported the most commonly used techniques to harass victims was via social networking websites, such as Twitter and Facebook (Haron & Yusof, 2010), in Malaysia. As a popular Internet application, social networking websites could be misused as a tool to harass other people, and eventually lead to legal liability for the organisation if such behaviours are carried out from business premises during working hours. Despite these drawbacks, social

networking has now evolved into a medium for mass communication and many companies view websites such as Facebook, Twitter, and LinkedIn as a valuable marketing channel (New Zealand Management, 2010).

Furthermore, data and information can be transmitted rapidly and inexpensively, reducing the need to go through layers of hierarchical structures (Asunda, 2010). Considering these new legitimate business uses of the social networking websites, an Internet policy that bans social networking sites seems counterproductive. However, the benefits of these Internet applications do not guarantee total safety nor keep the organisation out of trouble. In other words, completely unrestricted use of social networking websites is impractical, considering the potential increase in costs and legal liabilities organisations face as more and more new Internet applications are made available. Thus, the study of Internet abuse should also evolve to keep pace with the rapidly changing Internet.

1.3 Research Problem

Internet abuse in the workplace has become a major issue in many parts of the world, and Malaysia is no exception. A recent Malaysian study has reported that 90% of the respondents admitted that they have used the Internet in the workplace for non-work purposes (Ramayah, 2010). Furthermore, employees in Malaysia are more likely to visit websites related to arts and entertainment, sport and news, personal business and financial, travel and leisure, and information searching during working hours (Anandarajan & Simmers, 2003). The evidence here signals that Internet abuse is a pervasive issue in the workplace in Malaysia, which deserves immediate and thorough investigation.

A previous study has indicated that productivity losses of 30 – 40% may result from inappropriate Internet usage (Lim, Teo & Loo, 2002), with an estimated \$7 million per annum wasted in a company of 1,000 employees, or about 12.5% of the wages bill, due to Internet abuse (Mahatanankoon, 2002). Moreover, Internet abuse could lead to vulnerabilities for viruses and other threats. As optimal performance of an organisation's Internet infrastructure is an integral part of any modern organisation's productivity, the illegitimate behaviour of sending personal emails, streaming audio or video files could slow down or even halt the Internet infrastructure for legitimate business use (Valli, 2001). Such Internet abuse activities threaten the security of confidential business information, which could be compromised due to the security threats. Thus, the outcomes from Internet abuse are tremendous, and capable of creating an organisational disaster. In a serious case, Internet abuse could even jeopardise the survival of the organisation.

In addition, this study believes that Internet abuse not only affects the earlier mentioned work-related factors, but it is also speculated to have adverse impacts on the psychological aspects of the Internet abusers themselves. Previous studies (Caplan, 2003; Engelberg & Sjöberg, 2004; Kraut et al., 1998; Niemz, Griffiths & Banyard, 2005) have indicated that excessive use of the Internet leads to depression and loneliness problems among users. As Internet abuse, such as excessive Internet usage, is a negative Internet usage, it is important to investigate the effects of Internet abuse on the psychological aspects of Internet abuser, such as depression and loneliness. Furthermore, the existing literature on Internet abuse has overlooked the outcomes of Internet abuse from the perspective of an employee's psychological well-being. Thus, this study is set to take a step ahead in understanding the outcomes of Internet abuse on two psychological variables, depression and loneliness.

While the existing studies commonly investigate the gender, age and other demographic variables as the antecedents of the behaviour under study, or as the grouping variables in t-tests, the effect of these demographic variables on the development of the behaviour is unknown. Hence, this study attempts to close the gap by including the gender, age and Internet experience as moderating variables between the antecedent of Internet abuse and Internet abuse. Using this approach, analysis can achieve a greater granularity by examining the moderating impacts on each pairing of internet abuse and its antecedents. Furthermore, there is no empirical measurement of the level of Internet abuse in Malaysia, so by measuring the level of Internet abuse this study will provide a clearer picture of the status of Internet abuse in Malaysia.

In order to truly understand Internet abuse, the contributing factors or antecedents of Internet abuse must be investigated as well. Understanding the contributing factors to Internet abuse enables actions to be developed and taken to solve the problems at the root cause. Research conducted in this area by Zauwiyah and Hasmda (2009) has reported that 28% of the Malaysian respondents viewed Internet abuse as “could be right”, while about 32% perceived that using Internet resources in the workplace for personal purposes was not wrong. These figures imply that the majority (60%) of the employees in Malaysia have the perception that using the organisation’s Internet for non-work purposes is acceptable. Due to this perception by employees in Malaysia, they are more likely to be involved in Internet abuse. The point here is to stress that the attitude of employees towards Internet abuse could be the cause of the Internet abuse problems in Malaysia.

Furthermore, another study in Malaysia has reported that the respondents perceived that online chatting and sending personal emails during working hours

were normal and harmless to the organisations (Zauwiyah & Hasmida, 2010). This suggests the norms and practices in Malaysia could lead employees to accept that Internet abuse behaviours in the workplace are an acceptable practice. Combined with Malaysia's well-known collectivist community traditions (Ahmed, Mouratidis & Preston, 2008), where influences from senior individuals and surrounding factors are given important consideration, the norms of Internet abuse could spread pervasively. Taking these issues into account, it is important to examine the subjective norm as an antecedent of Internet abuse behaviour of employees in Malaysia.

Also connected to these issues, research by Anandarajan and Simmers (2003) on Internet abuse across Malaysia, Nigeria and the United States, reported that employees in Malaysia contend that companies should not block the access to certain websites. In other words, this reflects that employees in Malaysia might have different perceptions toward the control mechanisms, such as the Internet filtering, monitoring and Internet policy. Moreover, Lim et al. (2002) found that about half of the employees in Singapore found the Internet policy there unacceptable. Hence, one of the areas of interest of this study is to understand the problem of Internet abuse from the perspective of perceived behavioural control that is how employees perceive the control mechanisms.

From the conceptual aspect, more sophisticated research models need to be developed to comprehend the mechanics behind the Internet abuse phenomenon. In other words, room exists for more research frameworks in order to fully understand the nature of Internet abuse. Although Internet abuse is an important area to be studied, but a comprehensive, holistic framework that captures the workings of Internet abuse from its factor to consequences is yet to be developed. In addition, the

outcomes of Internet abuse are often overlooked by the existing studies. Hence, there is a need for a theoretical framework that can provide a more sophisticated investigation into the Internet abuse problem, from the causes to the outcomes.

As Malaysia is a developing nation that champions the use of information communication technologies in Asia, it was expected that a considerable amount of research had been undertaken on the Internet abuse problem in Malaysia, however, there remains a lack of empirical research on workplace Internet abuse. In fact, most of the previous research has been carried out in Western developed countries, such as USA. Based on the lack of research and different employee perceptions, it is worthy to investigate the Internet abuse issue within the context of an Asian developing country, given the management approaches and culture of Western countries are significantly different from those in Asian countries. For instance, a study by Laturkar (2010) identified Western organisations as output-oriented and prioritises profit maximisation. On the other hand, Eastern organisations tend to realise material gains through achievement of social or human welfare. Furthermore, it was claimed that Eastern organisations provide more room for individual development in the workplace. In addition, Anandarajan and Simmers (2003) have reported that cultural differences between Malaysia and the U.S. have a significant impact on a wide array of business practices, such as compensation, leadership, global research and development activities, and software piracy. With significant differences between these two distinctive cultures, it is therefore probable that findings based on a Western context may not generalise to Asian countries. Accordingly, it is important to advance research into the workplace Internet abuse problem in a typical Eastern developing country Malaysia that has been neglected in the mainstream of Internet abuse literature.

In conclusion, this study is to empirically investigate the phenomena of employee Internet abuse in the Malaysian workplace. In order to provide a holistic view of the issue, this study addresses both antecedents and outcomes of Internet abuse. In addition, the differences within genders, age and Internet experience are studied as the moderating variables between the antecedents and Internet abuses, and the outcomes of Internet abuse, namely work inefficiency, Internet security threats, depression and loneliness are examined.

1.4 Research Objectives

The goal of this research is to study Internet abuse in the workplace by adopting the DTPB theory (Taylor & Tood, 1995a) with the antecedents of Internet abuse (attitudes towards internet abuse, subjective norm, and perceived behavioural control), and the Model of Deviant Usage of Internet Technology (Mahatanokoon, 2002) to investigate the outcomes of Internet abuse. In addition, this research examines the level of Internet abuse among the employees in Malaysia. More specifically the detailed research objectives are stated as follows:

1. To investigate usefulness, ease of use, compatibility and playfulness as belief dimensions of attitude towards Internet abuse.
2. To investigate peer culture, supervisor culture, family culture and mass media influence as belief dimensions of subjective norm.
3. To investigate self-efficacy, facilitating conditions, workplace privacy, electronic monitoring, and Internet policy as belief dimensions of perceived behavioural control.

4. To investigate the antecedents for Internet abuse at the workplace, namely attitude towards internet abuse, subjective norms and perceived behavioural control.
5. To examine the consequences/outcomes of Internet abuse in terms of workplace-related outcomes (work inefficiency, security threats) and psychological outcomes (depression, loneliness).
6. To determine whether the demographic variables (i.e. age, gender and Internet experience) moderate the relationship between attitudes towards internet abuse, subjective norms, perceived behavioural control and Internet abuse itself.
7. To assess the overall level of employee Internet abuse in Malaysia, including the differences of Internet abuse levels among different demographic groups, such as gender, age, position, internet experience and current position.

1.5 Research Questions

Based on the above research objectives, the following research questions are proposed:

1. What are the belief dimensions of attitude towards Internet abuse? Do usefulness, ease of use, compatibility and playfulness encourage attitudes towards Internet abuse?
2. What are the belief dimensions of subjective norm? Do peer culture, supervisor culture, family culture, and mass media influence lead to subjective norm?
3. What are the belief dimensions of perceived behavioural control? Do self-efficacy, facilitating conditions, workplace privacy, electronic monitoring, and Internet policy lead to perceived behavioural control?

4. What are the antecedents of Internet abuse? Do attitudes towards Internet abuse, subjective norms, and perceived behavioural control lead to Internet abuse?
5. What are the outcomes of Internet abuse? Does Internet abuse result in workplace-related outcomes such as work inefficiency, security threats and psychological outcomes such as depression and loneliness?
6. Do demographic variables such as age, gender and Internet experience moderate the relationship between attitudes towards Internet abuse, subjective norm, perceived behavioural control and Internet abuse?
7. What is the level of employee Internet abuse in Malaysia, and are there any differences in the level of Internet abuse among different genders, age, Internet experience and current position?

1.6 Significance of the Study

Firstly, this study is significant because it reveals the transitions through a systematic process to develop, test, and validate a framework to understand the phenomenon of Internet abuse. Both antecedents and outcomes of Internet abuse are addressed by the proposed framework, which differs from frameworks in previous studies that focus solely on the antecedents. Specifically, this study adapts the Decomposed Theory of Planned Behaviour (DTPB) to conceptualise the relationships between antecedents and Internet abuse, and the Outcome of Deviant Use of Internet Technology (DUIIT) to conceptualise the outcome variables of Internet abuse behaviours. This study attempt to adapt the DTPB model to examine a deviant behaviour at the workplace–Internet abuse. In addition, the study adapts and appends dimensions of each antecedent under study, specifically tailored to the domain of Internet abuse. Hence, the model proposed in this study provides a holistic

framework that can be used specifically to understand Internet abuse behaviour, from its antecedents to outcomes, providing a more complete picture about Internet abuse in the workplace. In addition, the model provides a fundamental framework that can be adapted to suit the study of other deviant behaviours in the workplace.

Furthermore, this study indicates the severity of Internet abuse in the workplace in Malaysia, by measuring the level of Internet abuse, and consequently the findings could signal related authorities in Malaysia to undertake initiatives to reduce the Internet abuse problem. Besides identifying the outcomes of Internet abuse, policy makers or the Internet abusers themselves would be aware of the severity of Internet abuse.

The results of this study provide a better understanding of the root causes of Internet abuse behaviours among employees in Malaysia. This information is valuable to assist business organisations in formulating countermeasures of Internet abuse based on the studied variables, such as attitude towards Internet abuse, influences of subjective norm, and perceived behavioural control, Internet policy, and workplace privacy. It is hoped that this study will help policy makers and practitioners reduce occurrences of Internet abuse, and subsequently reduce the resulting impact.

Finally, the findings of this study are important because it tests various respondent profiles (i.e. gender, age and Internet experience) as the moderators between the three antecedents and Internet abuse behaviour. Moreover, the means of Internet abuse among different genders, age, Internet experience and job position are compared, which offer better explanation capability on the Internet abuse behaviours. With a clear picture of the differences among groups, this study provides richer

insights to the policy maker enabling more effective strategies for various types of employees.

1.7 Definition of Key Variables

Some of the terms that are used in this study have been defined briefly as follows:

1. **Internet Abuse**—Galleta and Polak (2003) defined Internet abuse among employees as Internet usage for non-work-related purposes during working hours. The commonly reported purposes for which the Internet is used for during working hours include writing and forwarding personal e-mails, instant messaging, selling and purchasing products, entertainment, surfing for news and information, online gambling, making bookings/reservations for airlines, trading stocks and other personal finance, non-essential software update, etc.
2. **Attitude**—Ajzen (1991), Taylor and Todd (1995a) defined attitude as the degree to which a person has a favourable or unfavourable evaluation of the behaviour in question. In the context of this study, attitude refers to the employees' attitude towards using the Internet at the workplace as to whether they have a favourable or unfavourable perception towards using the Internet for personal purposes at work.
3. **Usefulness**—Davis (1989) defined usefulness as the degree to which a person believes that using a particular system would be beneficial for the user. In the context of Internet abuse, usefulness refers to the extent to which the employees believe that the use of Internet in the workplace for personal purposes would be advantageous or beneficial to them.

4. **Ease of use**—Davis (1989) defined ease-of-use as the degree to which a person believes that using a particular system would be free of effort. In this study, ease-of-use refers to the extent to which the employees perceive that using Internet in the workplace for personal purposes would be free of effort.
5. **Compatibility**—Moore and Benbasat (1991), and Rogers (1995) defined compatibility as the degree to which the technology fits with the potential adopter's existing values, previous experience and current needs. In the context of Internet abuse, compatibility is the degree to which the employees perceive that the use of workplace Internet for personal usage would fit with their existing values, previous experience and current needs.
6. **Playfulness**—According to Davis et al. (1992) and Hsu and Chiu (2004b) playfulness is the extent to which the activity of using a computer system is perceived to be personally enjoyable in its own right aside from the instrumental value of the technology. In the case of Internet abuse, playfulness is described as the degree to which the use of workplace Internet for personal purposes is perceived to be personally enjoyable, besides the extrinsic value of personal use of the Internet in the workplace.
7. **Subjective Norm**—Taylor and Todd (1995a) and Crespo and Bosque (2008) defined subjective norm as an individual's beliefs about whether significant others would approve or disapprove of his/her engaging in a given behaviour. In this study, subjective norm refers to the employees' beliefs regarding whether their important others would approve or disapprove on their use of the workplace Internet for personal purposes.
8. **Peer Culture**—Peer culture is defined as the influence or pressure from known sources to perform a given behaviour (Galleta & Polak, 2003). In the context of

this research, peer culture is the influences or pressures by known sources to use the Internet in the workplace for personal purposes, which more specifically refers to the peers of the employees. The peers are generally people with a similar position status and around the same age group as the employees.

9. **Supervisor Culture**—Galleta and Polak (2003) defined the supervisor culture as the influence or pressure from a person who is in a higher position than the employees. In this study of Internet abuse, the influence or pressure to use the Internet in the workplace for personal purposes is from known sources in higher positions.
10. **Family culture**—Ajzen (2006) defined family culture as the influence or pressure from known sources, one's family members, to adopt or accept certain technologies. Specifically in the case of this Internet abuse study, family culture refers to the influence or supportive norm from the employee's family members that encourage the employee to engage in Internet abuse activities.
11. **Mass Media Influence**—Yuen and Azree (2005) defined mass media influence as the influence from significant but unknown others through the mass media. The mediums of communication include newspapers, radio, television, Internet, broadcast e-mails, official announcements, etc. Within the context of Internet abuse, mass media influences refer to the influences from various mediums mentioned that induce the employees to participate in Internet abuse.
12. **Perceived Behavioural Control**—Ajzen (1991) and Crespo & Bosque (2008) defined perceived behavioural control as the beliefs regarding access to the resources and opportunities needed to affect behaviour. Specifically in the study of Internet abuse, perceived behavioural control refers to the beliefs regarding

access to the sources and opportunities required to carry out Internet abuse behaviour.

13. **Facilitating Conditions**—Shih and Fang (2004) defined facilitating conditions as the availability of resources needed to perform a particular behaviour. This might include access to time, money and other specialised resources (Compeau & Higgins 1995). In this study, facilitating conditions refer to the availability of resources that needed to use workplace Internet for personal purposes, such as Internet access rights, time, and Internet facilities.
14. **Self-efficacy**—Anandarajan et al. (2000) defined self-efficacy as a person's confidence in his/her ability to behave successfully in a particular situation or to perform a particular task. By extending the definition to this study, self-efficacy refers to the employee's confidence in his/her ability to use the workplace Internet for personal purpose successfully.
15. **Workplace Privacy**—Galleta and Polak (2003) defined workplace privacy as the degree to which one's social interaction is regulated in the workplace, due to the setting of the workplace layout. When applying this definition into the context of Internet abuse, privacy refers to the extent to which the employee's behaviour on using the workplace Internet for personal purposes is regulated in the workplace, due to the arrangement of workplace layout.
16. **Electronic Monitoring**—Galleta and Polak (2003) defined electronic monitoring as the limiting or filtering mechanisms applied on a particular technology to curb undesired behaviour. Specifically in the context of Internet abuse, electronic monitoring refers to the existence of monitoring software to monitor the Internet usage in the workplace, and to report the cases of deviant usage of the Internet.

17. **Internet Policy**—Galleta and Polak (2003) defined Internet policy as organisations' rules to guide employees' behaviour in using Internet in the workplace. In this study, Internet policy refers to the degree to which the employee perceives the Internet policy exists is strict and enforced.
18. **Work Inefficiency**—Work inefficiency refers to the time taken to complete work, the amount of wasted time, and the amount of re-work and extra work materials caused by some behaviour that is performed (Anandarajan et al., 2000). In this instance, the specific behaviour is Internet usage for personal reasons during working hours. Hence, the work inefficiency refers to time taken to complete work, the amount of wasted time, the amount of re-work and extra materials caused by the employee's behaviour in using the workplace Internet for personal purposes.
19. **Security Threats**—Security threats can be identified as any unwelcome entity in the form of system viruses, unsecured websites, competitive intelligence, etc., that hamper or disrupt the performance of a technology (Anandarajan et al., 2000). Specifically in this study of Internet abuse, security threats refer to the risks of inducing online security threats due to the personal usage of the workplace Internet.
20. **Depression**—Depression is diagnosed as a feeling of sadness and lost hope or mental illness (<http://www.psychiatry-malaysia.org>). In the context of this study, depression refers to the feeling of sadness and lost hope resulted from the personal use of the workplace Internet.
21. **Loneliness**—Davis, Gordon and Besser (2002) described loneliness as a feeling of emptiness and restlessness due to the lack of intimate relationships and the feeling of boredom and marginality due to the lack of meaningful friendships or